



# THE DIRECTORS' TOOLKIT

May 2022

[KPMG.com.au](https://www.kpmg.com.au)

## • FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# Foreword

It seems that every time we launch a new version of our *Directors' Toolkit* we comment on how the governance landscape has exploded since the last version. However, the last two years were unprecedented in delivery of an avalanche of events such as COVID-19, catastrophic weather events, war in eastern Europe, outcomes from the Royal Commission into Aged Care Quality and Safety, significant cyber attacks and inquiries into multiple casino operators.

Whenever such events happen the question that is asked of impacted organisations is "did the board of directors do the right thing?".

With the availability of information and the prominence of social media, this question is asked (and answered) by a far broader group of stakeholders than was the case a decade ago. Further, what the "right thing" is has evolved too and environmental, social and governance (ESG) considerations are now front of mind for all directors. After all, directors are the G in ESG. It is the board who will set policy and the "tone from the top" that will ultimately determine whether the company that they have oversight over is judged to be successful, or not, when compared against increasing ESG expectations.

It is an exciting time to be an officer charged with responsibility for governance as the transformation that will be required to meet the ESG agenda resides with us. This update of the toolkit is intended to provide the necessary resources to arm directors to successfully navigate the risks and opportunities that will be before them in this super charged governance environment.

The information contained herein is of a general nature only, and is not intended to be comprehensive. It is not legal advice, and should not be relied upon as such. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. Accordingly, KPMG makes no warranties or representations regarding any of the content. No one should act on such information without appropriate professional advice after a thorough examination of their particular situation and circumstances. KPMG excludes, to the maximum extent permitted by law, any liability which may arise in relation to the content.

With all eyes on directors, we are frequently asked what the critical success factors of highly effective boards are. Typically, such boards,

- are structured in such a way to support diversity of thought
- understand their role in governance
- discharge their legal duties
- ensure accountability to shareholders
- understand stakeholder expectations and consider these in decision making
- effectively use board committees to enhance governance
- build a talented management team
- champion a productive and ethical culture
- make informed decisions efficiently
- actively contribute to strategy, and closely monitor strategic effectiveness
- ensure a disciplined approach to risk governance
- receive independent assurance
- undertake professional development and actively seek to understand current and emerging issues relevant to their organisation and the political, social and economic environment in which it operates.

## • • FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

This toolkit does not attempt to establish a model or pattern for the optimum composition and conduct of a company board. KPMG appreciates that the way in which a board and its management pursue organisational objectives is influenced by many factors, including:

- the industry or industries in which the company operates
- its stage in the typical corporate life cycle
- the personalities of those who comprise the board and executive
- business strategy
- risk appetite
- ownership structure
- the places in which it does business
- the legal and regulatory environment(s)
- economic conditions
- stakeholder expectations
- approach to technology.

The board should be alert to the risk indicators (red flags) that may affect the organisation. As in previous versions of the toolkit, we have provided a number of red flags plus a list of pertinent questions that directors may ask on the first page of each chapter.

This Directors' Toolkit is intended to provide the information that boards need in a form that is easily digestible. It is designed primarily for directors of listed public companies and major private entities. Nevertheless, much of its content is relevant to those vested with governance responsibilities for a range of organisations, including small private companies, not-for-profits, incorporated associations, statutory bodies, and sporting and community-based organisations.

KPMG can see that more regular updates of the toolkit will be required as the pace of change in the world of governance continues to increase. As significant changes are identified the toolkit will be updated for these and new versions released, all registered users will receive notification of these updates. This is a change from the previous bi-annual updates.

A further change is that where specialists within KPMG have supported the Governance team by contributing to the material within a specific chapter, their details are included at the end of the relevant chapter so that further enquiries on specialist topics may be directed to them.

We hope you find this practical guide helpful to improve board performance, and we are looking forward to hearing your feedback.



**Caron Sugars**

**National Lead**

**Board Advisory Services**

**Governance, Risk and Controls Advisory**

# The role of boards and directors

---

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 1. Directors' Legal Duties

Company directors have significant legal responsibilities. It is critical to understand these duties, maintain compliance and keep up to date on any relevant changes to legislation.

## In this chapter

- Constitution
- ASX listing requirements
- Key duties and responsibilities
- Acting in good faith
- Use of position and information
- Care and diligence
- Business judgment rule
- Other legal obligations
- Directors' indemnities and insurance
- Conflict and disclosure of interests
- Related party transactions
- Insolvent trading and safe harbour
- Continuous disclosure
- Insider trading
- Record keeping
- Share trading by directors
- Resignation
- Enforcement, penalties and remedies

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Do I have a good working knowledge of the constitution, laws, regulations and the Australian Securities Exchange (ASX) Listing Rules relevant to the company?
2. Do the directors have access to company records, reports from management and updates about material changes to the relevant laws and regulations? Are they provided quality information in a timely manner sufficient to discharge their duties?
3. Has the board adequately considered its responsibilities under relevant WHS legislation and other legislation relevant to the company and its industry?
4. Does the company secretary monitor compliance with the company's constitution or the 'replaceable rules' (whichever applies)?
5. Do I understand the scope and limitations of the directors' and officers' liability insurance policy?
6. Is the board immediately advised of queries received from the ASX, The Australian Securities and Investments Commission (ASIC) or other regulators?
7. Is there a system in place for regulatory breaches to be reported to the directors?
8. Am I fully aware of my duties and responsibilities regarding conflicts of interest? Are directors' interests properly disclosed in the financial statements and directors' report?
9. Is there an effective procedure for identifying and disclosing related party transactions?
10. Does the company have effective monitoring mechanisms in place to ensure that market sensitive information is not leaked to the public before it is provided to the ASX?
11. Am I fully aware of my duties and responsibilities regarding solvency and the safe harbour provisions?
12. Am I fully aware of my responsibilities under continuous disclosure requirements?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The company's constitution is never, or rarely, referred to in board discussions/documentation.
- Certain directors are perceived to have conflicts of interest (for example, they have close personal ties with a major supplier or contractor).
- The directors fail to act in the best interests of the company as a whole (e.g. by having undue regard to the interests of a special interest group or major shareholder).
- A director lets price sensitive information slip at a social gathering or on social media.
- The board ignores a solvency problem or do not act accordingly to seek further information (accounting or otherwise) or implement a plan.
- There are concerns about certain directors or officers trading in company securities immediately before public announcements and/or there is a lack of awareness in relation to the company's securities trading policy.
- Insufficient time is paid to major decisions/proposals or the annual financial statements.
- Directors have difficulty accessing company information in a timely manner.
- The board does not receive updates on changes to relevant WHS legislation and other legislation relevant to the company and its industry.
- No reporting on regulatory compliance and breaches are provided to the directors.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Company directors' responsibilities are derived from the *Corporations Act 2001* (Cth) (the Corporations Act), the company's constitution, relevant common law principles and a range of other legislative and regulatory regimes. This includes trade practices law, workplace health and safety (WHS) obligations, environmental obligations, privacy and equal opportunity requirements. Company directors should be familiar with the material laws, regulations and rules relevant to the entities that they govern.

Whilst this chapter contains an overview of some of the key duties, it is not intended as a comprehensive summation of all company officer and director duties. Board of directors should always seek legal advice if they are uncertain about their legal position.

Circumstances can arise where directors of a company can be held personally responsible for breaching certain laws, even when they did not specifically authorise such a breach.

Directors have the power to control the management of a company's property and affairs and, as such, are subject to special duties and responsibilities, including among others:

- a duty to act with due care, skill and diligence
- a duty to act in good faith in the best interests of the company and for a proper purpose
- a duty to avoid conflicts of interest
- a duty not to misuse position or information obtained in their capacity as a director
- a duty to prevent the company from trading while insolvent
- a duty of skill, competence and diligence in the understanding of the financial report.<sup>1</sup>

<sup>1</sup> ASIC Information Sheet 183 <https://www.asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

Directors need to be vigilant to ensure that they do not expose themselves to civil or criminal liabilities by failing to properly discharge their legal duties. In practice, directors should take particular care when:

- considering whether or not the company should enter into a related party transaction
- considering if they have sufficient information (including independent expert advice) and reviewing that information when making decisions
- a company is at risk of trading whilst insolvent
- a company is involved in a takeover, either as an offeror or offeree
- a company raises money from shareholders or the general public by issuing shares or other securities.

As evidenced in the APRA CBA report,<sup>2</sup> individual directors should request further information from the company's management and/or seek their own independent legal advice if they have misgivings about a decision contemplated or taken by their board, or actions of the company's management.

In addition to their individual legal duties, the key responsibilities of the board include:

- monitoring the performance and risk management of the company
- setting, testing and improving company strategy
- setting the company's risk appetite/profile
- appointing, assessing and, where necessary, removing the CEO
- approving major capital decisions (above CEO delegation limits) including acquisitions, investments and divestments
- approving annual budgets and funding decisions.

<sup>2</sup> APRA Prudential Inquiry into The Commonwealth Bank Of Australia report (April 2018) [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

More recently, the role of the board as conduct and cultural leaders of the company has come under the spotlight. As stated in the APRA CBA report,<sup>3</sup> “conduct risk management goes beyond what is strictly allowed under law and regulation (“can we do it?”) to consider whether an action is appropriate or ethical (“should we do it?”).<sup>4</sup> The principle of “Should I do this? What is the right thing to do?” is also echoed in the Hayne Royal Commission interim and final reports<sup>5</sup> and “Principle 3: Instil a culture of acting lawfully, ethically and responsibly” of the ASX Corporate Governance Principles and Recommendations.

Encouragingly, notwithstanding the decrease in trust in Australian public institutions and the COVID-19 pandemic, the 2021 Edelman Trust Barometer shows that community trust in Australian directors and CEOs remains steady (trust in directors rose from 35 to 36 percent and trust in CEOs decreased from 39 to 37 percent).<sup>6</sup>

Refer to [Chapter 21 Culture and Conduct](#) for more information.

**Restrictions on being a director**

An individual cannot be a director without court consent if he/she:

- is an undischarged bankrupt
- is subject to a personal insolvency agreement or an arrangement under Part X of the *Bankruptcy Act 1966* (Bankruptcy Act) that has not been fully complied with
- has been convicted of certain offences, including under the Corporations Act, such as a breach of duties as a director or

<sup>3</sup> APRA Prudential Inquiry into The Commonwealth Bank Of Australia report (April 2018) [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)

<sup>4</sup> *ibid*

<sup>5</sup> Refer to Section 3.1 of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry's Interim Report <https://financialservices.royalcommission.gov.au/Documents/interim-report/interim-report-volume-1.pdf> and Section 1.2 of Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 1 <https://www.royalcommission.gov.au/system/files/2020-09/fsr-vol-1-final-report.pdf>

<sup>6</sup> Refer to Edelman Trust Barometer 2021 [https://www.edelman.com.au/sites/g/files/aatuss381/files/2021-02/2021%20Edelman%20Trust%20Barometer%20-%20Australia%20Country%20Report%20FINAL\\_0.pdf](https://www.edelman.com.au/sites/g/files/aatuss381/files/2021-02/2021%20Edelman%20Trust%20Barometer%20-%20Australia%20Country%20Report%20FINAL_0.pdf)

insolvent trading. If an individual has been convicted of one of these offences, he/she must not manage a company within five years of the conviction. If imprisoned for one of these offences, the individual must not manage a company within five years after release from prison.<sup>7</sup>

**CONSTITUTION**

The power to control the affairs of the company is typically vested in the directors by the company's constitution or, where the company does not have a constitution or the constitution does not so provide, by the “replaceable rules” of the Corporations Act.<sup>8</sup>

The provisions of the constitution are a key component of a company's governance framework. Directors should be familiar with the constitution and take the necessary steps to ensure it is understood, complied with and that it provides the appropriate framework for the operation of the company.

**ASX LISTING REQUIREMENTS**

Companies and directors of companies listed on the ASX must comply with the Listing Rules. The **Listing Rules** are additional obligations imposed only on listed companies, and govern the admission of companies to the ASX's “Official List”, the quotation of companies' securities, continuous disclosure obligations, directors' disclosures, suspension of securities from quotation and the removal of companies from the Official list. The Listing Rules are contractually binding between each listed company and the ASX and are enforceable against listed companies and their associates under the Corporations Act.<sup>9</sup>

<sup>7</sup> Refer to Sections 201B and 206B of The Corporations Act 2001 and ASIC Bankruptcy and personal insolvency agreements <https://www.asic.gov.au/regulatory-resources/insolvency/insolvency-for-directors/bankruptcy-and-personal-insolvency-agreements> ASIC Information Sheet 79 <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>

<sup>8</sup> Corporations Act 2001, Sections 135, 136 and 198A.

<sup>9</sup> Corporations Act 2001, Sections 793C and 1101B.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Most notably, the continuous disclosure requirements under the Listing Rules are also enforceable under the Corporations Act.<sup>10</sup> Refer to the *Introduction to the Listing Rules*<sup>11</sup> to see the principles upon which they are based.

The ASX Corporate Governance Principles and Recommendations (Corporate Governance Principles) include a range of expected processes, disclosures and practices that listed companies apply to their organisations. Recommendations 3.1, 3.3 and 3.4, in particular, are “directed to setting ‘the tone from the top’ and ensure that the board is provided with the information it needs to monitor the culture of the organisation”.<sup>12</sup> Whilst not mandatory, these principles adopt an ‘if not, why not’ approach to reporting against the Recommendations, whereby organisations are required to report on the process in place regarding governance frameworks, assurance and risk management (as may be applicable) with respect to each Recommendation. Where processes or frameworks are not in place with respect to a particular Recommendation, then organisations are required to explain the reason for the omission, placing an onus on directors to be more transparent to shareholders across a range of governance matters.

### Non-listed entities

Many non-listed entities choose to adopt the corporate governance guidance developed by the ASX as a means of ensuring that they align with better practice.

Registered charities (not-for-profit) organisations are not required to meet all of the reporting obligations of the Corporations Act. Registered charities are subject to the requirements of the Australian Charities and Not-for-profits Commission (ACNC). Refer to [Chapter 4 Not-for-Profit organisations](#) for more information.

<sup>10</sup> Corporations Act, Section 674.

<sup>11</sup> ASX, The Listing Rules, <https://www.asx.com.au/documents/rules/introduction.pdf>

<sup>12</sup> Refer to ASX Corporate Governance Principles and Recommendations, February 2019 <https://www.asx.com.au/documents/regulation/cgc-principles-and-recommendations-fourth-edn.pdf>

Government entities are not required to meet the requirements of the Corporations Act, being instead subject to the requirements of the entity’s Enabling Act. Refer to [Chapter 3 Government](#) for more information regarding Government entities.

## KEY DUTIES AND RESPONSIBILITIES

Whether a director of a listed, private, not-for-profit or government entity, a director’s key duties are his/her fiduciary duties, whereby directors are expected:

- to act with due care and skill and in good faith
- to exercise power for a proper purpose and
- avoid conflicts of interest.

In addition, the key statutory duties under the Corporations Act are that directors must:

- act with care and diligence
- act in good faith, in the best interests of the corporation, and for a proper purpose and
- not use position or information obtained through their position to gain an advantage for themselves or others, or cause detriment to the company.<sup>13</sup>

The law provides that a director’s duty is owed to “the company”, and the courts have typically characterised the company as being the sum of the shareholders. Whilst directors’ legal duties are narrowly defined in this sense, there is a growing public expectation that directors should play an active role in “instilling a culture of acting lawfully, ethically and responsibly”<sup>14</sup> by taking account of the interests of broader stakeholder groups.

<sup>13</sup> Corporations Act 2001, Sections 180-183.

<sup>14</sup> Refer to Principle 3 of ASX Corporate Governance Principles and Recommendations (4th edition) <https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf>

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The introduction of the Modern Slavery Acts and enhanced Whistleblower Protections<sup>15</sup> also echo this shift towards boards' broader responsibilities and accountability.

However, any decisions must ultimately be in the best interests of the company's shareholders collectively for directors to discharge their duties under the Corporations Act (as set out below).

The Corporations Act outlines the duties and liabilities of directors and other "officers"<sup>16</sup> of a company. The duties apply not only to validly appointed directors (including alternate directors), but also to "de facto directors" and "shadow directors".

## ACTING IN GOOD FAITH

Directors and other officers of a company are under a statutory and common law duty to act in good faith and in the best interests of the company as a whole and for a proper purpose.<sup>17</sup> This duty recognises that a director's primary responsibility is to the company and that this responsibility must ordinarily take precedence over the personal interests of the director or the interests of a third party. The duty to act in good faith is a broad duty that requires directors to:

- exercise their powers only for proper corporate purposes
- avoid actual, potential and perceived conflicts of interest
- account to the company for business opportunities that arise.

<sup>15</sup> Refer to The Modern Slavery Act 2018 (and NSW Modern Slavery Act 2018), Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017 and the recommendation to "have and disclose a whistle-blower policy" in Principle 3.3 of ASX Corporate Governance Principles and Recommendations (4th edition). Please also refer to The Corporations Act 2001 at Pt 9.4AAA which provides a consolidated whistleblower protection regime, as well as ASIC Regulatory Guide 270: *Whistleblower policies*.

<sup>16</sup> Corporations Act, Section 9: an "officer" includes, most relevantly, a "director or secretary of the corporation or a person who makes or participates in making decisions that affect the whole or substantial portion of the company, or who has the capacity to affect significantly the corporation's financial standing..."

<sup>17</sup> Corporations Act 2001, Section 181(1).

## USE OF POSITION AND INFORMATION

Directors and other officers and employees of a company must not improperly use their position or information they receive to gain an advantage for themselves or someone else, or to cause a detriment to the company.<sup>18</sup>

This duty would, for example, prohibit a director from obtaining a personal benefit through the misuse of the company's client or supplier list.

An offence is committed under both statute and common law if it can be shown that the conduct was undertaken with the intention of gaining an advantage. It is not necessary to establish that the advantage was actually obtained.

## CARE AND DILIGENCE

Directors and other officers must exercise their duties with the degree of care and diligence that a reasonable person would exercise if they were a director or officer in the circumstances of the company and occupied the same responsibilities within the company as the director.<sup>19</sup> Matters to consider include the director's position and responsibilities within the company, the company's circumstances and any special expertise of the director.<sup>20</sup>

<sup>18</sup> Sections 182 and 183 Corporations Act 2001.

<sup>19</sup> Section 180 Corporations Act 2001.

<sup>20</sup> For case law guidance on the standard required of directors to effectively discharge the duty of care and diligence, see *Daniels v Anderson* (1995) 37 NSWLR 438; 118 FLR 248; 16 ACSR 607; 13 ACLC 614 (the AWA case), *ASIC v Adler* (2002) 168 FLR 253; 41 ACSR 72; 20 ACLC 576; [2002] NSWSC 171 at [372].

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## BUSINESS JUDGMENT RULE

A director who makes a business judgment is taken to satisfy their duty of care and diligence in respect of the judgment if they:

- make the business judgment in good faith and for a proper purpose (a 'business judgment' being any decision to take or not take action in respect of a matter relevant to the operations of the corporation)<sup>21</sup>
- do not have a material personal interest in the subject matter of the judgment
- inform themselves about the subject matter of the judgment to the extent they reasonably believe to be appropriate
- rationally believe that the judgment is in the best interests of the company.<sup>22</sup>

The business judgment rule does not protect a cavalier attitude to business risk. Directors are expected to make informed business judgments and they must have a rational belief that their decisions are in the best interests of the company. The director's belief that the judgment is in the best interests of the company is a rational one, unless the belief is one that no reasonable person in their position would hold. This means that directors should exercise their powers and discharge their duties with the degree of care and diligence expected of any reasonable person in their position.

Directors making a business judgment are regarded as having discharged their duty of care and diligence under the Corporations Act and their equivalent duties at common law or in equity (including the duty of care that arises under the common law principles governing the liability for negligence). The business judgment rule only applies as a defence to section 180(1) of the Corporations Act.

<sup>21</sup> Corporations Act 2001, Section 180(3).

<sup>22</sup> Corporations Act 2001, Section 180(2).

Courts do not, in general, second guess the business judgment of directors based on the outcome of the decision. This statutory codification emphasises that directors are supposed to make business judgments and that the legal test is for these judgements to be made rationally and on an informed basis.

## OTHER LEGAL OBLIGATIONS

Company directors are also subject to a range of legal obligations, including those under various federal and state/territory tax and revenue laws, workers' compensation laws, consumer protection laws, consumer credit laws, equal opportunity laws, sexual harassment laws, environmental laws, WHS laws and industrial agreements. Directors can be held personally liable under many of these laws and should seek legal advice if unsure of their obligations.

## DIRECTORS' INDEMNITIES AND INSURANCE

Directors must understand the extent of their potential personal liabilities, and the extent to which they can be indemnified for these liabilities through indemnities granted by the company and the provision of directors' and officers' liability insurance (D&O insurance).

The Corporations Act precludes indemnification of officers (including directors) by a company against:

- liabilities owed to the company or a related body corporate
- liabilities owed to other parties that do not arise out of conduct in good faith
- certain liabilities for pecuniary penalties and compensation orders
- certain legal costs.<sup>23</sup>

<sup>23</sup> Corporations Act 2001, Section 199A.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A company is prohibited from obtaining insurance to cover officers (including directors) against liabilities arising out of conduct involving:

- a wilful breach of duty in relation to the company
- a contravention of the duties of officers (and others) to not improperly use their position or information they obtain due to their position.<sup>24</sup>

Given these limitations in company indemnities, public companies, in particular, nearly always take out D&O insurance on behalf of their directors. Various forms of D&O insurance are available, providing different levels of protection for the individual director. The director should ensure that the level of insurance cover is appropriate. The level of cover should be reviewed on an annual basis.

Details of any indemnification or insurance must be set out in the directors' report.<sup>25</sup>

Directors should ask for a copy of the policy and any deed of indemnity and insurance the company has in place for the benefit of the directors. Directors should ensure that the level of cover is appropriate to their particular circumstances.

## CONFLICT AND DISCLOSURE OF INTERESTS

### Conflicts of interest

A director should avoid being in a position where other interests or duties conflict with their duty to the company. Conflicts of interest can arise in several ways including:

- director contracts with the company (e.g. for the supply of services)
- related-party loans, guarantees and other securities
- profiting from a business opportunity that belongs to the company.

Sometimes a conflict is unavoidable. In such a case, the directors are obliged to disclose their conflict of interest or duty and take appropriate action to avoid any adverse consequences.

Directors should tread cautiously when considering an actual, potential or perceived conflict of interest. Any actual or potential conflicts of interest are best dealt with by way of full disclosure to the board.

Moreover, company stakeholders and the media can be highly critical of director conduct that can be perceived as self-serving. The reputations of both individual directors and their companies can suffer dramatically.

### Material personal interests

The Corporations Act requires a director with a material personal interest in a matter relating to the affairs of a company to notify the other directors of that interest.<sup>26</sup> The constitution may also contain additional disclosure obligations. Whilst the Corporations Act does not define "material personal interest", case law requires that materiality be considered in the context of the director (not the company) and must be personal to the director. That is, courts will look at the substance of the interest, its nature and capacity to influence the director's discharge of their fiduciary duties.<sup>27</sup>

The company's notification requirements are typically set out in the director's letter of appointment, and often certain disclosures are required for the office being accepted. The notification must detail the nature and extent of the interest and how the interest relates to the affairs of the company, and must be provided as soon as practicable after the director becomes aware of the relevant interest.<sup>28</sup> A director may give other directors standing notice about an interest.

<sup>24</sup> Corporations Act 2001, Section 199B.

<sup>25</sup> Corporations Act 2001, Section 300(1) (g).

<sup>26</sup> Corporations Act 2001, Sections 191(1) and 191(2).

<sup>27</sup> See, for example, *Grand Enterprises Pty Ltd v Aurium Resources Ltd* (2009) 256 ALR 1 and *McGellin v Mount King Mining* (1998) 144 FLR 288.

<sup>28</sup> Corporations Act 2001, Section 191(3).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Subject to certain exceptions, directors of a public company cannot vote on any matters in which they have a personal material interest, or be present while such matters are being considered at a meeting.<sup>29</sup> However, the other directors may pass a resolution which identifies the nature and extent of that director's interest and its relation to the affairs of the company, and permit the director to vote notwithstanding the interest.<sup>30</sup> This approval must be recorded in the minutes of the meeting.

Depending on the extent of the conflict of interest, disclosure and abstaining from voting may not fully discharge a director's duty. There could be circumstances where a director needs to take further actions to protect the company's interests. For example, a director who has not yet made a formal notification in respect of a conflict could instruct the company secretary to withhold relevant information, such as board papers pertaining to the conflict.

In extreme cases, a director's resignation may be the only effective means of avoiding a serious conflict of interest.

## RELATED PARTY TRANSACTIONS

Restrictions on related party transactions apply to a wide range of entities including, public companies, or entities controlled by a public company, and there are significant procedural steps involved in managing such transactions, which are designed to protect shareholders' interests. For the purposes of the Corporations Act, a 'related party transaction' is any transaction through which a public company or controlled entity provides a financial benefit to a 'related party' (which includes directors, their spouses, parents and children), and which by their nature raise a risk of a conflict of interest.<sup>31</sup>

In general, a public company or its controlled entities must not undertake a transaction with a 'related party' unless it is approved by the company's members or the transaction otherwise falls within one of the relevant exemptions in the Corporations Act.<sup>32</sup>

<sup>29</sup> Corporations Act 2001, Section 195.

<sup>30</sup> Corporations Act 2001, Section 195(2).

<sup>31</sup> Refer to Section 228 of The Corporations Act 2001 for definition of 'related party'.

<sup>32</sup> Sections 208 and 210-216 of the Corporations Act 2001.

Where a company seeks and obtains the approval of its members to give a financial benefit to a related party, the benefit must be provided within 15 months of the approval being given.<sup>33</sup>

Related party status endures for 6 months after the entity concerned ceases to be a related party.<sup>34</sup> Related party status also applies if the entity believes, or has reasonable grounds to believe, that it is likely to become a related party at any time in the future.<sup>35</sup> Further, an entity will be a related party if it acts in concert with a related party of a public company on the understanding that, if the company gives the entity a 'financial benefit', the related party will also receive a 'financial benefit'.<sup>36</sup>

The term 'financial benefit' has a wide application, encompassing a multitude of potential transactions – including "indirect" transactions through interposed entities, informal or oral agreements, agreements that have no binding force, and transactions that do not involve paying money.<sup>37</sup>

Although failure to obtain member approval for conferring the financial benefit will not invalidate the contract or transaction, a director may be held to have committed an offence if they are involved in this failure and the involvement is dishonest.<sup>38</sup>

The ASIC Regulatory Guide 76 Related Party Transactions<sup>39</sup> provides useful guidance on the application of the Corporations Act and ASIC's expectations with regards to various aspects of related party transactions.

Accounting standards have a broader definition of 'related party' and require disclosure of related party transactions. Some of these related party disclosures are now required to be disclosed in the remuneration report for listed companies under the Corporations Regulations.<sup>40</sup>

<sup>33</sup> Corporations Act 2001, Section 208(2).

<sup>34</sup> Corporations Act 2001, Section 228(5).

<sup>35</sup> Corporations Act 2001, Section 228(6).

<sup>36</sup> Corporations Act 2001, Section 228(7).

<sup>37</sup> Corporations Act 2001, Section 229(2).

<sup>38</sup> Corporations Act 2001, Section 209(3).

<sup>39</sup> ASIC, 2011, Regulatory Guide 76, Related party transactions, <https://download.asic.gov.au/media/1239851/rg76-published-11-may-2011.pdf>

<sup>40</sup> AASB 124 and Corporation Regulation 2M.3.03.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## INSOLVENT TRADING AND SAFE HARBOUR

Directors also have a positive duty to ensure that the company does not trade whilst it is insolvent.<sup>41</sup> Directors who permit a company to incur a debt, where there are reasonable grounds for suspecting that the company is *already* insolvent or that incurring the debt will cause insolvency, may contravene section 588G of the Corporations Act. In certain circumstances, directors may be held personally liable for the debts incurred if the company trades whilst being insolvent. A company will be deemed to be insolvent if it is not able to pay its debts as and when they become due and payable.<sup>42</sup>

However, if after suspecting insolvency, or that the company may become insolvent, a director starts developing or takes a course of action that is reasonably likely to lead to a better outcome for the company than the immediate appointment of an administrator or a liquidator,<sup>43</sup> the director will not be liable for debts incurred directly or indirectly in connection with the course of action,<sup>44</sup> provided certain conditions are met (as set out in further detail below).

It should be noted that directors wishing to rely on this exception will bear the evidentiary burden of establishing that they took the necessary action.<sup>45</sup>

### Some practical implications for directors

Developing and undertaking a course of action to achieve a better outcome is no mean feat. In examining a selected course of action directors should have regard as to whether:

- appropriate steps are being taken to ensure a company is keeping appropriate financial records consistent with the size and nature of the company, and to prevent the officers or employees of the company from engaging in misconduct that could limit the entity's ability to pay its debts

<sup>41</sup> Corporations Act 2001, Section 588G.

<sup>42</sup> Corporations Act 2001, Section 95A.

<sup>43</sup> Corporations Act 2001, Section 588GA(1)(a).

<sup>44</sup> Corporations Act 2001, Section 588GA(1)(b).

<sup>45</sup> Corporations Act 2001, Section 588GA(3).

- they are always keeping themselves properly informed of the company's financial position
- they are developing or implementing a plan to restructure the company to improve its financial position
- an appropriate level and extent of advice is being sought from an appropriately qualified professional and whether sufficient information has been provided to the professional to facilitate the giving of sound advice.

It should be noted that regard may be had to the above factors in formal proceedings as part of the assessment of whether a course of action was 'reasonably likely' to result in a better outcome for the company.<sup>46</sup>

Ultimately recognising the early signs of distress and taking early action remains the best way for directors to improve their chances of achieving a better outcome for the company and its stakeholders.

### Where safe harbour is not available

If a company is not able to take advantage of the safe exception, there is a defence that the director had reasonable grounds to expect, and did expect, that the company was solvent.<sup>47</sup> This defence usually requires a careful assessment of the company's circumstances to determine whether they provide a director with the requisite 'reasonable grounds' to expect solvency.

### Insolvent trading 'red flags'

Directors should constantly be on the lookout for signals that may suggest their company's financial reporting is misleading or disguising a serious deterioration in its financial stability. An understanding of the company's financial position at the time of sign-off of the yearly financial reports is insufficient. Insolvent trading 'red flags' that raise concerns for directors include:

- irregular financial reporting
- lack of management focus on key ratios

<sup>46</sup> Corporations Act 2001, Section 588GA(2).

<sup>47</sup> Corporations Act 2001, Section 588H(2).

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- insufficient and immature liquidity analysis of the company's debt profile
- lack of budgets or in-depth analysis of failure to meet budgets.

**Directors' responsibilities during insolvency**

Insolvency, or the threat of insolvency, requires directors to act in the interest of creditors. It is a situation in which directors must subordinate the interests of shareholders to those of the company's creditors. In this context, directors should note that the company must not pay a dividend unless:

- the company's assets exceed its liabilities immediately before the dividend is declared and the excess is sufficient for the payment of the dividend
- the payment of the dividend is fair and reasonable to the company's shareholders as a whole
- does not materially prejudice the company's ability to pay its creditors.<sup>48</sup>

The issue of insolvent trading is accentuated as corporate structures become more complex and parent companies become responsible for the affairs of numerous 'controlled entities'. From a Corporations Act perspective, the concept of a controlled entity is not confined to a wholly-owned subsidiary. A company can be said to control another if it has the capacity to dominate the decision-making of the other entity, or to impose its interests on the other entity. Boards should seek professional advice if there is any doubt as to whether an entity is a 'controlled entity'.<sup>49</sup>

ASIC Regulatory Guide 217 Duty to prevent insolvent trading: guide for directors provides useful guidance around the key principles that directors need to take into account in order to comply with their duty to prevent insolvent trading.<sup>50</sup>

<sup>48</sup> Corporations Act 2001, Section 254T(1).

<sup>49</sup> Directors should be aware that the Corporations Act 2001 definition of 'control' of another entity differs from the definition of 'control' as contained in AASB 10 Consolidated Financial Statements.

<sup>50</sup> ASIC, 2010, Regulatory Guide 217, Duty to prevent insolvent trading: Guide for directors, <https://download.asic.gov.au/media/1241384/rg217-29july2010.pdf>

**CONTINUOUS DISCLOSURE**

The Corporations Act and the ASX Listing Rules impose duties on the officers and employees of listed and unlisted disclosing entities to make immediate disclosures to markets about certain materially price sensitive information.<sup>51</sup>

The board has general oversight of an entity's disclosure obligations. The board will often delegate its powers to a disclosure committee or other senior executives within the organisation for the day-to-day management of disclosure issues. However, the board cannot delegate its responsibility for disclosure in a number of circumstances, for example, financial reporting. The GIA suggest that it may be useful to include a continuous disclosure confirmation as the final item of business on listed entity board agendas and to appoint a disclosure officer who can report to the board on continuous disclosure. Consideration of disclosure issues should form part of the board and executive considerations, and should be part of team discussions and culture within an organisation.<sup>52</sup>

Under Listing Rule 3.1 "once an entity is or becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities the entity must immediately tell the ASX that information".<sup>53</sup> There are, however, limited exceptions to this obligation prescribed under the ASX Listing Rules.<sup>54</sup>

The continuous disclosure framework is designed to ensure that the market is fully informed at all times and that all investors have access to material information. Sustainable investment indices rely either wholly or in part on the public disclosure of relevant information by listed entities. It is widely recognised that there are significant financial and reputational benefits to companies whose practices are recognised through favourable ratings from such indices.

<sup>51</sup> Sections 674–675 of the Corporations Act 2001 and ASX Listing Rule 3.1.

<sup>52</sup> Refer to GIAs "Continuous disclosure: listed and other disclosing entities" guidelines.

<sup>53</sup> Refer to ASX, Chapter 3, Continuous disclosure, <https://www.asx.com.au/documents/rules/Chapter03.pdf>

<sup>54</sup> ASX Listing Rule 3.1A.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Those ratings can be significantly enhanced by good governance practices in connection with continuous and periodic disclosure or, conversely, damaged by poor practices.<sup>55</sup>

With the introduction of the *Treasury Laws Amendment (2021 Measures No 1) Act 2021*, the continuous disclosure obligations have been modified such that now,<sup>56</sup> companies and officers will only incur liability in breach of their continuous disclosure obligations if they had acted with the requisite “knowledge, recklessness or negligence”.<sup>57</sup> The implications of introducing such fault elements allows “companies to more confidently make forecasts of future earnings or provide guidance updates without facing the undue risk of class actions” especially in the aftermath of COVID-19.<sup>58</sup> These changes have been further discussed in [Chapter 7 Accountability to Shareholders](#).

**Share price and media monitoring**

The ASX strongly encourages an entity that is relying on the exemptions to disclosure about a market sensitive transaction it is negotiating, or that otherwise chooses not to request a trading halt or voluntary suspension in advance of its market sensitive announcement, to monitor “blogs, chat-sites and other social media that regularly post comments about the entity” for any signs the information has been leaked.<sup>59</sup>

Monitoring the share price of an entity is necessary to ensure that any suspected leaks of confidential information can be quickly identified and dealt with. Monitoring media, including social media, is also useful in identifying whether the market may be operating on the basis of false information. Reporting services are available to assist with collating media reports.

<sup>55</sup> Refer to GIAs “Continuous disclosure: listed and other disclosing entities” guidelines.

<sup>56</sup> Corporations Act 2001, Sections 674 and 675.

<sup>57</sup> Corporations Act 2001, Sections 674A and 675A.

<sup>58</sup> The Hon Josh Frydenberg MP, Media Release <https://joshfrydenberg.com.au/latest-news/permanent-changes-to-australias-continuous-disclosure-laws/>

<sup>59</sup> Refer to ASX, Chapter 3, Continuous disclosure, <https://www.asx.com.au/documents/rules/Chapter03.pdf>

**INSIDER TRADING**

Under the Corporations Act it is an offence if a person with ‘inside information’ applies for, acquires or disposes of securities, or enters into an agreement to do any of those things. A person with inside information is also prohibited from procuring another party to do any of those things.

The purpose of the insider trading regime is to ensure that the securities market operates freely and fairly with all participants having equal access to relevant information so that no party has an unfair advantage over another. Refer to the ‘share trading by directors’ section of this chapter for further information.

By virtue of their roles, directors and officers of companies will be privy to inside information and should, therefore, take particular care to ensure they observe the prohibition against insider trading in the Corporations Act. Insider trading involves the misuse of price-sensitive company information that is not generally available.

Importantly, an ‘insider’ can be a natural person or a corporation, and need not be directly associated with the company. The Corporations Act prohibits any person in possession of inside information from:

- dealing – applying for, acquiring or disposing of the relevant financial products or entering into an agreement to do any of these things (trade)
- procuring – enabling another person to trade in those financial products
- tipping – communicating the information, or causing the information to be communicated, to another person who is likely to trade in those financial products, or procure someone else to so trade.<sup>60</sup>

For the purposes of the insider trading provisions of the Corporations Act, the definition of ‘financial products’ is contained in section 1042A of the Corporations Act and includes, for example, shares, debentures, options and any other product that is able to be traded on a financial market.

<sup>60</sup> Corporations Act 2001, Section 1043A.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Under the continuous disclosure provisions of the Corporations Act and ASX Listing Rules, listed companies will, in general, have disclosed all price-sensitive information to the market as it becomes available. Accordingly, in practice, the insider trading restrictions will generally apply to price-sensitive information that has been withheld from disclosure pursuant to one of the exceptions (e.g. an incomplete proposal for a takeover).

Generally, around the time of the results announcement/annual general meeting is the most 'pure' or 'clean' time when a company is least likely to have insider information.

Further, a company should have a securities trading policy in place to prevent the misuse of insider information.

In relation to unlisted companies, directors should take particular care in relation to a capital or debt raising, or share transfers in relation to the company, where there may not be equal knowledge of the company's activities by parties to the proposed raising or share transfer.

Insider trading is a serious offence attracting substantial fines and potential imprisonment. Civil liability may also attach to the offence.

## RECORD KEEPING

The Corporations Act also requires that directors are personally responsible for preparing and maintaining key documents and reports. Directors are required to keep, either in hard or soft copy:

- up-to-date financial records that accurately reflect the company's financial position, including transaction level details (i.e. general ledger, cash balances, wage and salary details, debtor and creditor listings, property/asset register, tax returns and details of investments)
- registers of members (shareholders), including option holders (if applicable)

- minutes of general meetings
- minutes of meetings of directors
- registers of charges created by the company over company property.<sup>61</sup>

Financial records must be kept by all entities covered by the Corporations Act, however a 'small proprietary company' or a small company limited by guarantee (as defined in the Corporations Act), is not generally required to prepare and submit an annual report to ASIC. Larger companies (including not-for-profits) are required to lodge audited financial statements to ASIC each year, with exceptions for some public companies limited by guarantee.<sup>62</sup> Further, charities who are registered with the Australian Charities and Not-for-profits Commission (ACNC) are required to lodge either an annual information statement or a financial report (depending on their size) with the ACNC as opposed to ASIC.<sup>63</sup>

## SHARE TRADING BY DIRECTORS

Subject to the general prohibition against insider trading, the ASX Listing Rules, and the restrictions applying to directors under the share trading policy of a listed company, directors can, in certain circumstances, buy and sell shares and other securities in their companies.

ASX listed companies are required to have a share trading policy restricting dealing in the company's securities by its directors and other key management personnel.<sup>64</sup>

<sup>61</sup> ASIC, Information Sheet 79, Your company and the law, <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>

<sup>62</sup> For more details on record keeping obligations, see ASIC Information Sheet 131 <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/companies-limited-by-guarantee/obligations-of-companies-limited-by-guarantee/> and ASIC Information Sheet 76 <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>

<sup>63</sup> Section 111L of the Corporations Act 2001 and Australian Charities and Not-For-Profits Commission Act 2012(Cth), division 60.

<sup>64</sup> See ASX Listing Rule 12.9 and ASX Listing Rules Guidance Note 27 – 'Trading Policies' and Recommendation 1.3 of ASX Corporate Governance Principles and Recommendations (4th edition).

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Under such policies, the directors and other key management personnel are restricted from trading in the company's securities during specified 'prohibited periods' (often referred to as 'black-out' or 'closed' periods – typically for a period before the release of financial results), and/or only permitted to trade during certain defined 'trading windows' (e.g. after the public release of financial results).

The Corporations Act requires directors of listed companies to notify the ASX of any interests they have in the securities of their listed company (or a related body corporate), and of any contracts to which they are a party, or from which they are entitled to a benefit.<sup>65</sup> The ASX Listing Rules also contain similar notification requirements, although the notification obligation rests with the listed entity, rather than the director.<sup>66</sup>

## RESIGNATION

With the enactment of the *Treasury Laws Amendment (Combating Illegal Phoenixing) Act 2020*, the *Corporations Act* has been amended such that directors now have additional obligations regarding their resignation. Specifically, a director's resignation will only be effective on the date that the person ceases to be a director if notice of this resignation is lodged with ASIC within 28 days of its occurrence.<sup>67</sup>

<sup>65</sup> Corporations Act 2001, Section 205G. See also ASIC Regulatory Guide 193 <https://download.asic.gov.au/media/1241069/rg193.pdf>

<sup>66</sup> ASX Listing Rules 3.19A and 3.19B. See also ASX Guidance Note 22 – 'Director disclosure of Interests and Transactions in Securities – Obligations of Listed Entities'.

<sup>67</sup> Corporations Act 2001, Section 203AA.

If lodged later than 28 days but within 56 days, an application can be made to ASIC providing reasons, with ASIC having the liberty to accept the application and fix the resignation date as the claimed resignation date.<sup>68</sup> Should this notice not be received within 28 days and an application is not made to ASIC within 56 days or less, the date of the director's resignation will only take effect the date the notice is received by ASIC.<sup>69</sup> In contrast with the previous provisions which imposed a fine for late registration of notices, this amendment means that the tenure of a director will be artificially extended until such time notice of their resignation is lodged.

In instances where the resignation of the director or the passing of a resolution to remove a director will leave the company without any directors, the resignation will be deemed void, though note that exceptions exist for companies being wound up.

## ENFORCEMENT, PENALTIES AND REMEDIES

Directors who breach their legal responsibilities face a range of criminal and civil penalties, and can also expect to suffer damage to their reputations and their professional or commercial careers. Moreover, it can also affect the company's reputation.

As summarised by Rod Sims, the ACCC Chair, "as a company director you have a responsibility to ensure that your company is meeting its legal obligations. Beyond the good corporate citizen aspects of compliance, now more than ever the costs of non-compliance are significant. The impact of regulatory action, with increasing penalties and costly litigation, is one thing; lost reputation, reduced customer trust, distracted management and remedial actions also take their toll on companies".<sup>70</sup>

<sup>68</sup> Refer to ASIC, Resigning or removing a company director, <https://asic.gov.au/for-business/small-business/starting-a-company/small-business-company-directors/resigning-or-removing-a-company-director/>

<sup>69</sup> Corporations Act 2001, Section 203AA.

<sup>70</sup> Refer to Section 3.3.1 of the 'AICD's Essential Director Update:18' <https://aicd.companydirectors.com.au/membership/membership-update/essential-director-update-18-highlights>

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Criminal penalties**

In certain circumstances, directors can be charged with criminal offences. Criminal penalties can be imposed for a number of actions including:

- if a director is reckless or dishonest, and fails to act in good faith, in the best interests of the company or for a proper purpose
- breach of other statutory duties, such as the duty not to make improper use of a director's position or of information received as a director
- contravention of the prohibition against insider trading.

Directors found guilty of these criminal breaches can be fined and/or imprisoned.

**Industrial Manslaughter Laws**

Following a Senate Inquiry, the Education and Employment References Committee published its report in October 2018 titled *"They never came home – the framework surrounding the prevention, investigation and prosecution of industrial deaths in Australia"*. One of the key recommendations was "the formal harmonisation of WHS laws process" in each State and Territory.<sup>71</sup>

Industrial manslaughter was first introduced in Australia when it was passed by the Australian Capital Territory's Legislative Assembly on 27 November 2003 under the *Crimes (Industrial Manslaughter) Amendment Act 2002* (ACT), which took effect on 1 March 2004.

In December 2018, Maria Carla Jackson, 72, was the first individual in Victoria to be sentenced to prison under the breach of duty provisions of occupational health and safety legislation. Ms Jackson was convicted and sentenced to six months' jail under the Victorian Occupational Health and Safety Act 2004, after the death of a man at her scrap metal yard in Foster, Victoria.

<sup>71</sup> Refer to Recommendation 5 of the report, available at [https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024170/toc\\_pdf/Theynevercamehome%e2%80%94theframeworksurroundingthe%20prevention%20investigationandprosecutionofindustrialdeathsinaustralia.pdf;fileType=application%2Fpdf](https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024170/toc_pdf/Theynevercamehome%e2%80%94theframeworksurroundingthe%20prevention%20investigationandprosecutionofindustrialdeathsinaustralia.pdf;fileType=application%2Fpdf)

Robbie Blake was killed when he fell three metres from a raised forklift (being operated by Ms Jackson, who does not hold a fork-lift licence) and was hit by a falling bin in February 2017. Ms Jackson pleaded guilty to breaching the Occupational Health and Safety Act by failing to comply with her duty as a self-employed person not to expose other people to risk.<sup>72</sup>

Accordingly, it is important that directors understand their responsibilities regarding workplace health and safety and are receiving the necessary information to be able to understand whether the control environment is aligned to their risk appetite. [Chapter 20 Health, Safety and Wellbeing](#) discusses how industrial manslaughter laws are being approached in each state.

**Civil penalties**

Civil penalties can apply to a range of breaches of statutory duty, including:

- the duty to exercise reasonable care and diligence
- the duty to act in good faith in the best interests of the company and for a proper purpose
- related party rules
- market manipulation
- the duty to prevent insolvent trading.

Directors who have benefited from a breach of duty may also be ordered to account for any profits received. Penalties can include fines, a disqualification order or a compensation order. In civil proceedings, the burden of proof is on the balance of probabilities, rather than beyond the reasonable doubt demanded in criminal proceedings.<sup>73</sup>

<sup>72</sup> Hook, M, 2019, <https://www.abc.net.au/news/2019-01-25/victorian-junkyard-woman-sentenced-to-jail-over-death/10746110> and WorkSafe Victoria, Prosecution Result Summaries and Enforceable Undertakings, <https://www.worksafe.vic.gov.au/prosecution-result-summaries-enforceable-undertakings>

<sup>73</sup> See ASX Listing Rules Guidance Note 27 and Recommendation 1.3 of ASX Corporate Governance Principles and Recommendations (4th edition)

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## CASE STUDY



## Case Study – Storm Financial

In March 2020, the Federal Court rejected Cassimatis' appeal and upheld their 2018 penalties judgement in the Storm Financial matter. It brought to an end the long-running ASIC litigation arising out of the collapse of the Queensland financial planning business a decade ago.

The court held that Mr and Mrs Cassimatis, both executive directors of Storm Financial, had contravened their duty of care and diligence under section 180(1) of the Corporations Act 2001. Their conduct facilitated Storm to provide the "Storm model" of financial advice to a group of financially vulnerable investors. In doing so, they caused or permitted Storm to contravene the financial services laws and exposed it to the risk of losing its AFS licence. Mr and Mrs Cassimatis were each ordered to pay civil penalties of \$70,000 and disqualified from managing corporations for seven years.

***Cassimatis v Australian Securities and Investments Commission (ASIC) [2020] FCAFC 52***  
***HIH Insurance Limited***



## Case Study – The collapse of HIH Insurance

The demise of HIH Insurance Limited (HIH) is considered to be the largest corporate collapse in Australia's history. HIH was Australia's second largest general insurer. In 2001, HIH and a number of its subsidiaries were placed into liquidation with losses of \$800 million. The main reasons cited for the HIH collapse were poor management and greed, characterised by a lack of accountability for performance, lack of integrity in internal processes, and lack of attention to detail and skills. [FN55]

*"The governance of a public company should be about stewardship. Those in control have a duty to act in the best interests of the company. They must use the company's resources productively. They must understand that those resources are not personal property."* – **Report of the HIH Royal Commission (Justice Owen), April 2003**

***ASIC v Adler & Ors (2002) NSWSC 171***

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US



## Case Study - James Hardie Industries Limited

In May 2012, the High Court found that seven former non-executive directors of James Hardie Industries Limited (James Hardie) had breached their duties as directors when they approved the release of a misleading ASX announcement regarding the foundation which was established to cover the asbestos claims made against the James Hardie group. The ASX announcement stated that the foundation was “fully funded” for the purposes of meeting all future compensation claims, when in actual fact there was a funding shortfall of more than \$1.5 billion.

The High Court also separately determined that the former James Hardie company secretary and general counsel, Mr Shafron, had contravened section 180(1) of the Corporations Act (the duty of care and diligence) by failing to properly advise the board and CEO in relation to the establishment of the asbestos foundation.

The High Court remitted the case to the NSW Court of Appeal to hear the directors' appeals on penalties and relief from contravention. In November 2012, the NSW Court of Appeal imposed fines on the non-executive directors and banned each of them from being involved in the management of a corporation for varying periods of time (which was a reduction of the original penalties and disqualification periods that had been imposed by the NSW Supreme Court). In respect of Mr Shafron, the court reinstated the fine and disqualification period imposed by the trial judge (namely a \$75,000 fine and disqualification period of 7 years).

***ASIC v Hellicar [2012] HCA 17***

***ASIC Media Releases: 12-275MR (Decision in James Hardie penalty proceedings) and 12-85MR (Decision in ASIC's appeals in James Hardie Matter)***

**Remedies**

A cause of action may also arise under general law against directors for breach of:

- the duty of care and diligence arising from common law negligence
- contractual obligations
- the equitable duty to exercise reasonable care and skill.

In addition, if a director breaches the fiduciary duties owed to the company and it suffers a consequential loss, the company may pursue compensation by way of equitable remedy. This is similar to the common law remedy of damages.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- ASIC Information Sheet 183, Directors and Financial Reporting, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>
- ASIC Regulatory Guide 76 – Related party transactions, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-76-related-party-transactions/>
- ASIC Regulatory Guide 217 – Duty to prevent insolvent trading: Guide for directors, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-217-duty-to-prevent-insolvent-trading-guide-for-directors/>
- ASX Guidance Note 8 – Continuous Disclosure: Listing Rules 3.1 – 3.1B, [https://www.asx.com.au/documents/rules/gn08\\_continuous\\_disclosure.pdf](https://www.asx.com.au/documents/rules/gn08_continuous_disclosure.pdf)
- Australian Accounting Standards Board, AASB 124 – Related Party Disclosures, [https://www.aasb.gov.au/admin/file/content105/c9/AASB124\\_07-15.pdf](https://www.aasb.gov.au/admin/file/content105/c9/AASB124_07-15.pdf)
- Australian Institute of Company Directors, <http://aicd.companydirectors.com.au/>
- Baxt, B., Duties and Responsibilities of Directors and Officers, 20th edition, Australian Institute of Company Directors, 2012. Corporations Act 2001 (Cth).
- Lipton, P., Hertzberg, A. and Welsh M., Understanding Company Law, 16th edition, Thomson Reuters Australia Limited, 2012.
- APRA Prudential Inquiry into The Commonwealth Bank Of Australia report (April 2018) [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry's Interim Report <https://financialservices.royalcommission.gov.au/Documents/interim-report/interim-report-volume-1.pdf>
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 1 <https://www.royalcommission.gov.au/system/files/2020-09/fsrc-volume-1-final-report.pdf>
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 2 case studies <https://www.royalcommission.gov.au/system/files/2020-09/fsrc-volume-2-final-report.pdf>
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 3 Appendices <https://www.royalcommission.gov.au/system/files/2020-09/fsrc-volume-3-final-report.pdf>

## For further information please contact:

**Hoda Nahlous**

**Partner, Corporate, M&A & Securities Law – KPMG Law  
NSW State Lead – Deals, Tax & Legal  
hnahlous@kpmg.com.au**

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## 2. Governance Roles

There are many instruments, roles and responsibilities required for a board to deliver its governance function effectively. Key factors such as independence, board composition and skills play a critical role in board performance.

### In this chapter

- Governance scope
- Board charter
- Annual board agenda
- Retained authorities
- Delegated authorities
- Accountabilities framework
- Types of directors
- Chair's role
- Deputy chair or senior independent director
- Company secretary's role
- Induction and professional development



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is the composition of the board appropriately diverse for it to perform effectively?
2. Is the board sufficiently independent of management to enable it to make tough decisions?
3. Is a regular assessment of each director's independence made by the board?
4. Does the board periodically review the board and chair's performance, and if so, is the review done by an external body?
5. Does the board tailor its charter to the organisation's circumstances and is the charter periodically reviewed?
6. Is there an annual agenda, approved by the board that is linked to the board's key responsibilities, as detailed in the board charter?
7. Are matters that must be referred to the board for approval clearly articulated to management?
8. Does the board clearly set out the roles and authority of the CEO and directors in writing?
9. Are delegations to management, including the delegations policy, set out in a single document?
10. Is the board monitoring that directors allocate sufficient time to discharge their responsibilities?

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board spends too much time on operational matters with limited time for strategic discussions.
- Policies and procedures are not updated regularly.
- The board is heavily weighted towards a certain skill set, background, or gender.
- Some directors have family ties or cross-directorships that have not been discussed or are overlooked.
- Assessments of director independence are informal and infrequent.
- The board's charter is outdated with the last date of review unknown.
- A statement of 'matters reserved to the board' does not exist, or is not explicit and clear.
- There are no board approved instruments, such as a code of conduct and delegations of authority.
- Assessments of the board's performance are only done internally (or not at all) and are routinely positive with little to no action taken to address any opportunities for improvement identified.
- The director induction process is procedure-based only.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## GOVERNANCE SCOPE

At its very centre, the role of the board is governance of the organisation. Governance is a unique concept and very different to management, which is the role and function of the executive team. Governance requires a balance between a 'hands-off' approach to implementation, and a greater focus on **oversight, insight** and **foresight** in the context of stewardship, direction setting and monitoring performance of the management team against the approved strategic objectives.

The board's governance scope refers to the key roles and responsibilities of the board and includes the following key functions:

- developing, along with senior management, the company's vision, purpose, core values, strategic direction and objectives
- evaluating and challenging management's recommendations on important strategic and operational matters
- holding management to account for its performance and decisions
- scrutinising key financial and non-financial risks to which the enterprise is exposed and ensuring the implementation of an effective risk management, compliance and internal control framework
- ensuring the adequacy of internal regulatory and policy compliance systems
- setting and demonstrating the corporate culture of the organisation
- adopting appropriate ethical standards, code of conduct and appropriate behaviours, and ensuring that these are adhered to at all times
- communicating and reporting to shareholders and other stakeholders in a transparent and insightful manner
- overseeing management succession plans
- evaluating the board's own practice and performance and the contribution of individual directors.

The board's governance scope should be clearly documented in the board charter.

## BOARD CHARTER

The ASX Principles state in Recommendation 1.1 that a listed entity should have and disclose a board charter setting out:

- the respective roles and responsibilities of its board and management and
- those matters expressly reserved to the board and those delegated to management.

The purpose of a board charter is to document the board's terms of reference, and to articulate the board's approach to important governance practices. The charter should contain a statement clarifying the division of responsibilities between the board and management. Many boards define the roles, powers and responsibilities that it specifically reserves for itself, and those which it delegates to management.

All entities, whether private, public, listed, non-listed, not-for-profit or Government, should have a document that clearly outlines the board's purpose, functions and key operating mechanisms. The document could be called a Charter, By-laws (in the case of Government entities) or Terms of Reference. For the purposes of this discussion, we will use the term 'Charter'.

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

While the content of the board Charter will vary, the board Charter of an ASX listed company (which can be used as better practice guidance for non-listed entities) will typically cover the following matters:

- overview of board roles, functions and responsibilities
- board structure and composition
- the chair's role
- the role of the company secretary
- the board's policy for assessing independence
- retained authorities
- board delegations
- board meeting procedures
- oversight of strategy, financial and risk management, and remuneration frameworks.

The board should periodically review its Charter to ensure it remains relevant to the circumstances of the company. The Charter should be available to directors, management, staff, auditors and shareholders. The ASX Principles recommend that the roles and responsibilities be set out in a Charter or some other document published on the company's website.<sup>74</sup>

See *Appendix 1 Board Charter for an example.*

## ANNUAL BOARD AGENDA

Boards commonly formulate an annual board agenda as an effective planning tool. The chair should refer to the annual agenda before approving the agendas for individual board meetings.

An effective annual agenda will:

- provide coverage of all the board's key activities
- provide adequate time for discussion
- ensure all the obligations included in the charter will be addressed

<sup>74</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 6.1.

- provide opportunities for the continuous development of directors.

The annual agenda can also be used as an evaluation tool to assess whether the board has achieved the activities planned in the agenda.

See *Appendix 2 Annual Agenda for an example.*

## RETAINED AUTHORITIES

The ASX Principles encourage all companies (both listed and non-listed) to disclose the respective roles of its board and management and adopt a formal statement of matters reserved for the board's decision or a formal board charter that specifies its functions and responsibilities.<sup>75</sup> The ASX Corporate Governance Council has compiled a list of responsibilities<sup>76</sup> that boards normally reserve for themselves.

Some of these responsibilities include:

- demonstrating leadership, defining the entity's purpose and setting its strategic objectives
- appointing the chair and appointing and replacing the CEO
- approving the appointment and replacement of other senior executives
- overseeing the integrity of the entity's accounting and corporate reporting systems
- ensuring that the entity has in place an appropriate risk management framework (for both financial and non-financial risk)
- ensuring that the entity's remuneration framework is aligned with the entity's purpose, values, strategic objectives and risk appetite
- monitoring the effectiveness of the company's governance practices.

Some boards adopt a formal delegation of authority policy, delineating respective board and management authorities, while setting financial limits on decisions that can be made without specific board approval. Ensuring that the CEO and the board itself understand their respective roles and responsibilities is a priority of every board.

<sup>75</sup> Ibid, Recommendation 1.1.

<sup>76</sup> Ibid See commentary to Recommendation 1.1.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DELEGATED AUTHORITIES

Given the complexity and size of the typical large business enterprise, it is not possible, nor is it desirable, for a board to exercise all of its possible powers and functions directly. The Corporations Act provides that, unless a company's constitution provides otherwise, directors may delegate any of their powers to a board committee, a director, an employee of the company, or any other person.<sup>77</sup>

Directors are entitled to rely on others, where they believe, on reasonable grounds at all times the delegate would exercise the power in conformity with the duties imposed on directors of the company under the Corporations Act and the company's constitution<sup>78</sup>, and the director believed on reasonable grounds, in good faith and after making proper enquiries that the delegate was reliable and competent in relation to the power delegated.<sup>79</sup> If these conditions are not met, the directors will be responsible for the exercise of power by the delegate as if the directors themselves had exercised the power.<sup>80</sup>

This provision implies that boards must take responsibility not only for the appointment of a reliable and competent CEO, but must also make a judgement about the competence of the entire senior management team, as well as being satisfied that the company has established proper processes for the hiring of competent employees.

In delegating their powers to committees or management, boards must:

- ensure the delegation is consistent with and in accordance with the entity's risk appetite
- demonstrate and maintain rigorous oversight over the exercise of those powers
- ensure that management and committee reporting back to the board strikes the right balance between summary and detailed information
- ensure seamless communication between board committees.

<sup>77</sup> Corporations Act 2001, 198D.

<sup>78</sup> Corporations Act 2001, 190(2)(a).

<sup>79</sup> Corporations Act 2001, 190 (2)(b).

<sup>80</sup> Corporations Act 2001, 190 (1).

It is important that directors review materials and financial reports presented by management and auditors with a critical eye, and not accept or approve materials without question, to ensure that reasonable grounds exist to rely on the work of management (as was famously highlighted in the James Hardie and Centro cases).<sup>81</sup> Case law makes it clear that directors cannot substitute reliance upon the advice of management for their own attention and examination of an important matter that falls within the board's responsibilities (such as, for example reporting obligations).<sup>82</sup>

The delegations policy, which is approved by the board, should specify the limits of authority to take action and/or make financial and non-financial decisions for all individuals, including the delegations from the CEO to senior management and from senior management to staff. This will assist the board in fulfilling its duty of care and be a useful reference to all company personnel as to who has responsibility for decision-making.

<sup>81</sup> ASIC Information Sheet 183

<sup>82</sup> ASIC v Healey & Ors [2011] FCA 717 at 175.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

## ACCOUNTABILITIES FRAMEWORK

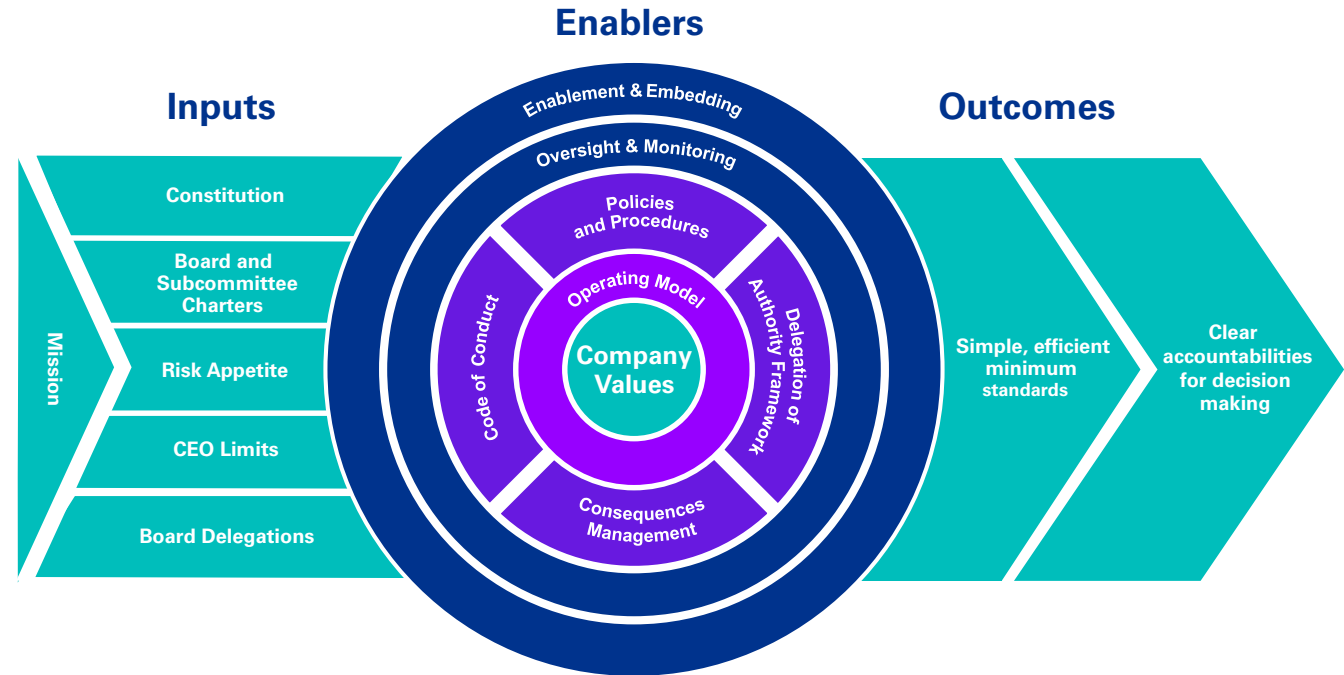
The KPMG accountabilities framework outlines below the inputs and enablers to deliver simple, efficient minimum standards and clear accountabilities for decision-making across the organisation.

To achieve an effective accountabilities framework requires the board to endorse these instruments, oversee their implementation and regularly consider their compliance and currency.

## TYPES OF DIRECTORS

There are two principal types of directors: executive directors and non-executive directors. However, the Corporations Act also defines a range of other types of directors, that share the same overall fiduciary responsibilities, but with some slight differences. It is important to understand what type of director you are and how this impacts on your ability to effectively and lawfully fulfil the requirements of the role.

KPMG Accountabilities Framework



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Non-executive directors**

A non-executive director is someone who is not employed by the company in a management position but is involved in policy and planning exercises.

Being independent of the management of the organisation, non-executive directors play a vital role. Although written in 2003, the Higgs Report<sup>83</sup>, looking at the role and effectiveness of non-executive directors, is still relevant as it pertains to the main responsibilities of a non-executive director, being to:

- constructively challenge and contribute to the development of strategy
- scrutinise the performance of management in meeting agreed goals and objectives, and monitor the reporting of performance
- satisfy themselves that financial information is accurate and that risk management systems are robust and defensible
- appoint, evaluate and remove senior management personnel in line with succession plans
- determine appropriate levels of remuneration for executive directors.

This report also suggests that, in order to discharge their responsibilities, effective non-executive directors should possess key personal attributes:

- integrity and high ethical standards
- sound judgement
- ability and willingness to challenge and probe
- strong interpersonal skills.<sup>84</sup>

An important characteristic of a non-executive director is the willingness to confront management and raise difficult issues. Non-executive directors must have *“sufficient strength of character to seek and obtain full and satisfactory answers within the collegiate environment of the board”*.<sup>85</sup>

83 Higgs, D., Review of the Role and Effectiveness of Non-Executive Directors, Department of Trade and Industry (UK) Jan 2003, P80 at para A1.4, <http://www.ecgi.org/codes/documents/higgsreport.pdf>

84 Ibid p29 at para 6.12

85 Ibid p 29 at para 6.15.

**Independent directors**

Independent directors play an important role in the separation of power between the management of the company, including executive directors, and can offer new perspectives and challenge old paradigms.

The ASX Principles recommend that a majority of the board should be independent directors.<sup>86</sup> An independent director can be defined as *“a director who is free of any interest, position, or relationship that might influence, or reasonably be perceived to influence, in a material respect their capacity to bring an independent judgement to bear on issues before the board and to act in the best interests of the entity as a whole rather than those of an individual security holder or other party.”*<sup>87</sup>

The ASX Principles go on to provide examples of interests, positions, affiliations and relationships that might raise issues about the independence of a director.<sup>88</sup> These include if the director:

- is, or has been, employed in an executive capacity by the entity or any of its child entities and there has not been a period of at least three years between ceasing such employment and serving on the board
- receives performance-based remuneration (including options or performance rights) from, or participates in an employee incentive scheme of, the entity
- is, or has been within the last three years, in a material business relationship (eg as a supplier, professional adviser, consultant or customer) with the entity or any of its child entities, or is an officer of, or otherwise associated with, someone with such a relationship
- is, represents, or is or has been within the last three years an officer or employee of, or professional adviser to, a substantial security holder
- has close personal ties with any person who falls within any of the categories described above

86 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.4

87 Ibid, Glossary definition

88 Ibid, Box 2.3

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- has been a director of the entity for such a period that their independence from management and substantial holders may have been compromised.

In each case, the materiality of the interest, position or relationship needs to be assessed by the board to determine whether it might interfere, or might reasonably be seen to interfere, with the director's capacity to bring an independent judgement to bear on issues before the board, and to act in the best interests of the entity as a whole, rather than in the interests of an individual security holder or other party.

Directors considered by the board to be independent should be identified as such in the corporate governance statement of the annual report. The board should state its reasons if it considers a director to be independent and the corporate governance statement should disclose the existence of any relationships that might suggest otherwise. In this context, it is important for the board to consider materiality thresholds from the perspective of the company and the director, and to disclose these.

For some entities, having a majority of board members as independent directors may not be possible or appropriate. The size of the board, the nature of the business and the skills required, may limit the number of independent appointments. In this situation, it is important to ensure that the organisation has at least one independent director to provide challenge and perspective that only someone from outside the organisation can bring.

**Executive directors**

Executive directors are paid employees of the company. They are often members of the company's senior management team. The CEO may also be an executive director and in some cases other senior executives may also be appointed to the board.

In rare instances, a CEO may also be the chair of the Board. Whilst there is no empirical evidence to suggest which model is better, combining these roles can see the lines between the board and management being blurred, requiring the individual to have a strong understanding of where and when they take on the relevant role.

Whilst in certain countries, like Germany, the practice of having a CEO appointed as chair is not allowed, this has historically been more common in the United States. It is notable however that this practice is reducing and the Wall Street Journal reported that as at June 2021 nearly 60 percent of S&P 500 companies have separate CEO and Chair roles according to ISS ESG data.<sup>89</sup>

In Australia, where the CEO is appointed chair, an explanation of why this is considered appropriate must be provided in the annual corporate governance statement. Recommendation 2.5 of the ASX Principles states that the chair of the board of a listed entity should not be the same person as the CEO of that entity.

The argument in favour of executive directors is that they add value to a board's decision-making process through their technical expertise and knowledge of the business and its industry.

The presence of executives on the board can be beneficial to the extent that they can inform non-executive directors by providing their relevant expertise and current working knowledge. Executives might also offer a valuable second opinion to the statements and recommendations of the CEO. A risk exists that their loyalty to the CEO could conflict with their statutory duty as directors to act in the best interests of the company.

**Nominee directors**

A nominee director is a director appointed by a shareholder, creditor or interest group. Nominee directors have the same overriding duty as other directors. However, they are often thought to have an ongoing allegiance to the nominator responsible for their appointment.

Whilst a nominee cannot favour the nominator's interests over that of the company, they can have regard to the interests of the nominator, provided that the nominee director ultimately acts for a proper purpose and in the best interests of the company. Where the interests of the nominator and the company diverge, the nominee should not participate in the decision.

<sup>89</sup> Wall Street Journal, "Microsoft's Combination of CEO and Chairman Roles Goes Against Trend", 17 June 2021



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A nominee director must not divulge to the nominator information obtained from the company in the nominee's capacity as a director if there is a conflict between the interests of the company and the nominator. In the event of a conflict, the nominee must either discharge their duty to the company and not to the nominator, or resign from the company's board.

The Corporations Act provides that directors appointed to the board of a wholly-owned subsidiary may act in the best interests of the holding company if certain conditions are satisfied and the constitution of the wholly-owned subsidiary expressly allows it.<sup>90</sup>

**Alternate directors**

Where directors find themselves unable to attend all board meetings or otherwise fulfil their board commitments, if the company constitution allows, then an 'alternate' director may be appointed. Depending on the scope of the appointment, the alternate director may exercise some or all of the appointing director's powers for a specified period. However, the appointment of alternate directors is becoming less common now that technology allows for participation in board meetings from a distance.

When an alternate director exercises the appointing director's powers, the exercise of powers is just as effective as if the power were exercised by the appointing director.<sup>91</sup> The appointment process for alternate directors is typically governed by a company's constitution and is usually conditional upon board approval.<sup>92</sup>

In the event that the appointing director has a conflict, the alternate (if exercising the appointing director's powers at that time) may still vote on the matter before the board. However, if the alternate also has a conflict then they must declare the conflict and refrain from voting.

The board should ensure that the terms of the appointment of an alternate director clearly set out:

- the scope of appointment (including any right to vote) and duration of the appointment
- the conditions under which the directorship may be revoked
- if the alternate director is permitted to attend all board meetings
- if there is an entitlement to receive all board papers and other communications.

**De facto directors**

A de facto director is a person not validly appointed as a director, but who by their actions is considered to in effect act in the position of a director. An example is where a person holds himself/herself out as a director by signing deeds as a director, despite not having a confirmation of appointment as a director, or not having been appointed in accordance with applicable procedures.

In practice, whether or not someone is deemed a de facto director will depend on the circumstances of each case, having regard to such factors as the size of the company, its internal structures and practices, and how the alleged director's position is perceived by outsiders who deal with the company.

Anyone deemed to be a de facto director is subject to the same duties and obligations as those applying to formally appointed directors, including the duty to prevent insolvent trading.

**Shadow directors**

A shadow director is a person who is not formally appointed as a director, but on whose instructions or wishes a company's directors are 'accustomed to act' as a matter of regular practice rather than as a one-off or isolated event.

A shadow director is subject to the same duties and obligations as those applying to formally appointed directors, including the duty to avoid insolvent trading.

<sup>90</sup> Corporations Act, 187.

<sup>91</sup> Corporations Act, replaceable rule 201K.

<sup>92</sup> Corporations Act, 201K.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A person will not be construed as a shadow director merely because the directors act on advice given by that person, due to their professional capacity or their business relationship with the directors. This is designed to protect lawyers, accountants, merchant bankers and others providing high-level advisory services to companies.

## CHAIR'S ROLE

Just as the board sets the tone for the entire company, the chair sets the tone for the board. The chair is first among equals, leading by example, displaying the utmost professionalism and engaging in conduct that is beyond reproach. In this sense, it is difficult to imagine a well-performing board without an effective chair.

At its core, the chair's leadership role involves facilitating the effective contribution of all directors and promoting constructive and respectful relations between all directors and management.

An effective chair:

- demonstrates personal integrity through ethical behaviour and exercises power in the appropriate manner
- provides leadership by empowering and motivating board colleagues
- develops a positive relationship with the CEO and senior management
- commands respect by winning the confidence of fellow directors
- demonstrates strong communication skills, both verbal and written
- understands and demonstrates a commitment to corporate governance principles and practices
- operates as a team player, respecting, acknowledging and building on the views and perspectives of others
- promotes a suitable vision and strategy, offering strategic insight and direction
- oversees the development of a sound risk management framework.

The duties of the role and the personal characteristics and competencies required should be embodied in a chair's position description that is reviewed by the board on a regular basis.

To ensure a clear division of responsibilities at the head of the company, the ASX Principles recommend that the chair should be an independent director and that the respective roles of chair and CEO should not be exercised by the same individual.<sup>93</sup>

Similarly, the ASX Principles acknowledge the demanding and time-consuming nature of the chair's role.<sup>94</sup> This means that other commitments must not be allowed to detract from the chair's role.

The chair may be exposed to 'additional liability' where circumstances may arise that they are a recipient and 'gatekeeper' of information that may not be available to other directors. It is paramount to ensure that any significant performance shortcomings attributed to the CEO are brought to the board's attention and that the chair resists any complicity with the CEO to hold back information.

In addition, the chair must not prevent the CEO from raising issues with the board, nor should the chair fail to raise any matter that would reasonably be judged worthy of the board's consideration.

Given the significance of the chair's role, boards should give careful attention to the election of a chair. The common practice of electing a chair according to a notion of seniority should not be the default position. The role should be filled by the candidate best able to fulfil the duties referred to above.

<sup>93</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.5.

<sup>94</sup> Ibid, Commentary to Recommendation 2.5.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DEPUTY CHAIR OR SENIOR INDEPENDENT DIRECTOR

Where the chair is not independent, it may be beneficial to consider the appointment of an independent director as deputy chair or as a 'senior independent director'.<sup>95</sup>

The specific responsibilities of a senior independent director will vary among companies, but may include:

- acting as an intermediary between independent directors and the CEO, but not impeding opportunities for other directors to build constructive relationships with the CEO
- setting the agenda and briefing the CEO on issues arising from those sessions
- collaborating with the chair/CEO in the preparation of the board agenda and supporting papers
- acting as a sounding board for the CEO on issues where the CEO wants to 'test the waters' prior to raising an issue with the full board
- leading the appraisal of the chair/CEO
- providing a separate communication channel to the security holders (especially where those communications involve the chair).

The senior independent director is usually appointed by only independent directors and a company's former CEO should not be appointed to this role.

## COMPANY SECRETARY'S ROLE

The company secretary plays an important role in supporting the effectiveness of the board and its committees, including advising on governance matters.<sup>96</sup> As directors require more information, both in terms of quantity and quality, the company secretary fulfils an increasingly valued role, becoming a senior governance adviser to the board.

<sup>95</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.5.

<sup>96</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Commentary to Recommendation 1.4

Both the Act and the ASX Principles state that the power to appoint and remove a company secretary should lie with the board.<sup>97</sup> The Act does not contain any general description of the role of the company secretary. It is a matter of the board's expectations of the person performing this role that will determine their ultimate responsibilities.

Company secretaries may have dual reporting lines if they hold multiple roles within the company.

The following general principles should apply to the company secretary's role:

- the company secretary is responsible to the board and should be accountable to the board through the chair on all governance matters
- the company secretary should report to the chair on all relevant matters relating to the board
- the company secretary's remuneration is usually approved by the board on the recommendation of the board remuneration committee
- a detailed position description for the company secretary should be prepared and approved by the board.

Company secretaries fall within the definition of a 'company officer' and essentially have the same legal duties and obligations as directors. It is increasingly common for company secretaries to perform a dual role (e.g. company secretary and general counsel), which has raised interesting issues regarding the extent of the application of the duty of care and diligence in section 180 of the Corporations Act, as was evidenced in the High Court's decision in the James Hardie case. The High Court in the decision against James Hardie's company secretary and general counsel, Mr Shafron, found that he was clearly an 'officer' and that his duties and responsibilities as general counsel and company secretary could not be divided or distinguished in the context of this matter.

<sup>97</sup> Section 204D and 204F of the Corporations Act 2001 and Recommendation 1.4 of ASX Corporate Governance Principles and Recommendations (4th edition 2019).

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The role of the company secretary may include:

- advising the board on corporate governance issues
- preparing the board agenda in consultation with the chair and CEO
- co-ordinating the timely completion and despatch of board papers
- ensuring that appropriate company records are maintained
- monitoring that board and committee policy and procedures are followed
- ensuring that the business at board and committee meetings are accurately captured in the minutes and
- helping to organise and facilitate the induction and professional development of directors.

## INDUCTION AND PROFESSIONAL DEVELOPMENT

Induction training and ongoing professional development for directors is critical to enable directors to effectively discharge their obligations.

ASX Principles Recommendation 2.6 indicates that a listed entity should have a program for inducting new directors and for periodically reviewing whether there is a need for existing directors to undertake professional development to maintain the skills and knowledge needed to perform their role as directors effectively.

It is important, that induction training be comprehensive and commence immediately upon (if not prior to) the director's appointment, as director's liability and remuneration commences immediately.

Induction training should provide directors with an understanding of the entity's structure, operations, history and culture and involve appropriate site visits to key operations. Where gaps in directors' knowledge exist, induction training should be provided on key matters such as directors' legal duties and responsibilities under the relevant legislation governing the entity, and on key accounting matters and the responsibilities of directors in relation to the entity's financial statements.

Further, the ASX Principles recommend that companies should have and disclose a 'board skills matrix' setting out the mix of skills the board currently has or is looking to achieve.<sup>98</sup> A structured professional development program should be implemented that addresses gaps in directors' knowledge and skills as well as providing training in relation to emerging issues.

## Useful references

- Appendix 2 Annual Agenda.
- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.
- Australian Institute of Company Directors, Role of chief executive officer or managing director, <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/pdf/05446312memdirectorgrrroleofchiefexecutiveofficerceoormana.ashx>
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, February 2019, <https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf>
- IE University, CEO Duality: For Better and for Worse, <https://www.ie.edu/insights/articles/ceo-duality/>

<sup>98</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.2

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 3. Government

The roles, responsibilities and expectations of Government directors may differ in some respects from those of their corporate counterparts. Accountabilities may also differ – the public interest, engagement with the community and the relationship with Ministers, Departments and Government are critical.

## In this chapter

- Types of Government boards
- Roles
- Government is different
- Enabling Act for agencies
- Other legislation and policies
- Parent (or Lead) Department
- Appointment process
- Guidelines on elections and the caretaker conventions
- Acting in the public interest
- Community engagement
- Government engagement
- Strategic priorities
- Receiving assurance

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that directors of Government entities should ask

1. Are the board well versed with the enabling legislation which creates the entity for which they are a board member?
2. Are each of the board members displaying strong working knowledge of the strategic priorities?
3. Do all the directors understand their responsibilities under the legislation governing public entities (e.g. financial management and public administration legislation) and in relation to compliance with that legislation?
4. Is there an effective framework for community engagement and are the board taking steps to ensure that the entity engages with the community and understands their expectations?
5. Is the board aware of its duty to act in the public interest?
6. Are directors fully aware of what is involved in ethical conduct in the public sector and their duties regarding conflicts of interest, privacy and confidentiality?
7. Are there strong working relationships across the organisation with government departments?
8. Does the board understand its role with the Government, Minister and Parliament?
9. Are directors aware of the requirement to avoid the use of government resources in a manner that advantages a particular party?
10. Is the board adequately informed about the policy context and broader issues that impact the entity's ability to meet its strategic objectives?

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The enabling legislation for the entity is never, or rarely, referred to in board discussions/documentation.
- Certain directors are perceived to have conflicts of interest that are not appropriately managed.
- The chair of the board does not have regular meetings with the responsible Minister and senior executives of the entity's parent Department.
- The entity or the board receives a written direction from the Minister or Government in respect of a particular issue (not a written direction setting general expectations, which is becoming increasingly common).
- The board chair is not consulted about the appointment of new board members.
- There are no frameworks for the entity to engage with the community.
- The directors fail to act in the public interest in decision making.
- A director is demonstrating actual or perceived bias regarding a lobby or stakeholder group.
- Board members accept gifts and entertainment from stakeholders where that acceptance is not consistent with Government policies.
- The board ignores the strategic priorities in its decision-making framework.
- Members display a lack of understanding of Government funding and budget processes.
- The entity and/or parent Department does not provide a thorough induction program for new board members.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

## TYPES OF GOVERNMENT BOARDS

The terminology for government organisations differs. The organisation may be named an agency, corporation, authority, commission or committee. This Chapter will refer to government organisations as 'the agency' and the governance representation as the 'agency board'. You may be called a director, commissioner, member or committee member and we will refer to you a 'director' throughout this chapter. The focus of this chapter is on boards that serve in a governance role. It is not intended to cover those boards or committees that serve in purely advisory roles.

Whilst this chapter contains an overview of key principles of government agencies, it is important to note that every locality, State and Federal jurisdiction has different requirements, guidelines and legislation. Each director must invest time in understanding the relevant government laws and policies that bind their specific agency and impact on their obligations.

## ROLES

A government director usually has formal duties and responsibilities to Parliament, the Minister and the public. It is important to understand and clarify how the chair, board and CEO roles relate to the roles of Parliament, the relevant Ministers, relevant government departments and other stakeholders.

Government boards that have governance and oversight roles in some cases also provide policy advice to their relevant Department or Minister.

## GOVERNMENT IS DIFFERENT

Participating in governance in government is different. The diagram below highlights five key factors that sets government agencies apart:

	<b>Organisational Leadership</b>	Often they don't have the authority to determine <b>leadership</b> of the organisation and appoint the CEO
	<b>Community Expectations</b>	Stakeholders are wide and varied, with <b>expectations</b> from the community heightened for government agencies
	<b>Not-For-Profit Motives</b>	Agencies are <b>not-for-profit</b> motivated and are guided by the strategic direction set by government
	<b>Political Influence</b>	Challenges that present governance in a <b>political</b> environment with influence in decision-making
	<b>Funding Constraints</b>	Government agencies don't have continuous disclosure requirements, but must work within the <b>funding</b> constraints and timelines of government budget processes



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## ENABLING ACT FOR AGENCIES

The foundation of an agency's governance framework is generally its enabling legislation. This legislation usually defines the agency's purpose, objectives, general powers, functions and duties and the responsibilities of its directors.

The director should be well versed with the agency's enabling legislation and review all agency instruments, processes and functions against it, and any other legislation that the agency is required to administer.

## OTHER LEGISLATION AND POLICIES

In addition to an agency's enabling legislation, there is a wide range of other legislation applicable to agencies in every jurisdiction, whether State or Federal. A director should be fully aware of relevant laws including:

- overarching government legislation and policy
- other legislation, government policy and obligations relevant to the agency's activities
- guidelines and directions issued by the Minister, government departments or other regulators.

Common examples of overarching government legislation in place in most states and federally relating to government activities includes whistleblowing, privacy, financial management, general public administration, equal opportunity, freedom of information and public records. Policies can include those related to approval of business plans, industrial relations, public sector employment principles, procurement, advertising, risk management, litigation, and investments.

The agency should advise the board on which overarching government policy frameworks and any specific departmental policies, apply to their agency. Directors should thoroughly review the key agency specific policies and assure themselves that they are fully aligned with government requirements before endorsing them. Formal Ministerial directions can override some policies, if the government's overarching policy or the agency's legislation permits this.

Agencies are also normally subject to all the other laws that apply to the private sector including environmental protection, occupational health and safety, fair trading and taxation. Government agencies are normally expected by the community and other regulators to be exemplars in compliance with these requirements.

## PARENT (OR LEAD) DEPARTMENT

A director should understand the engagement framework in place with the relevant lead government department and the role the director can play in driving this engagement.

A director should use his/her oversight role to challenge the agency to ensure it engages with the relevant government departments, as and when it needs, in order to clarify policy, guidance and strategic priorities.

## APPOINTMENT PROCESS

Ministers generally make appointments (and re-appointments) to government boards for a fixed term. The appointments are often advertised and outline the core skills and competencies required. The board chair, board members, and the CEO may in some cases have input into the decision-making process and can position themselves to inform the appointment process. Existing directors and the chair can sometimes help to create a pool of potential candidates.

Further agency appointments can sometimes occur via elections, and ex-officio 'requirements'.

*Criteria for selection*

The selection criteria for the appointment of board members and a chairperson may include, but are not limited to:

- the status and integrity of the individual within the community that they work
- any other legislative requirements applicable to that board (e.g. mandatory governance requirements of other commissions)
- working knowledge and understanding of accountability relationships

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- relevant experience within the sector and their field(s) of expertise
- ability to think and act strategically
- understanding of government sector operations
- understanding of the objectives and role requirements of their position
- existing intergovernmental relationships and connectivity
- understanding of the key risks and challenges present in the sector
- understanding governance standards
- the need to ensure diversity of board membership, particularly regarding gender
- capacity to contribute and attend board and sub-committee meetings.

## GUIDELINES ON ELECTIONS AND THE CARETAKER CONVENTIONS

Caretaker conventions dictate that once an election date is determined, the government assumes a 'caretaker role' in the period between calling and holding an election. Prior to the election period, the board members should familiarise themselves with the caretaker conventions in their jurisdiction. Specific published conventions are employed during this period which aim to protect the apolitical character of the public service and limit the commitments, made in advance, of a (potential) incoming Government including:

- not making any major decisions, such as entering into major contracts or undertakings, that are likely to inappropriately commit an incoming Government
- running advertising or information campaigns that highlight the role of a Minister or address an issue of contention between political parties
- engaging in any other activity, such as public presentations, speeches or comment that compromises the agency's actual or perceived apolitical status.

The agency board should be aware that some government or departmental decisions that might affect an agency (such as appointments or re-appointments of board members) are not normally made during the caretaker period, and should be delayed until after an election, particularly if a new Minister is appointed. The board should factor such potential delays into its planning.

## ACTING IN THE PUBLIC INTEREST

Directors of government agencies have an additional duty to act in the public interest. Government agencies oversee the spending of taxpayers' funds, public assets and community needs. Therefore, the support of the agency in the maintenance of public trust is key.

As such, in the duty of public interest, consideration should be given to the following:

- compliance with the ethical frameworks for the public sector
- compliance with the defined values and standards generally outlined in the agency's code of conduct
- ensure a full understanding of legal and public responsibilities
- act with integrity and ensure ethical decision-making occurs across delegated powers and in favour of public interest
- compliance with government, financial, asset management and procurement requirements in addition to conscientious expenditure of public funds
- awareness and declarations of all conflicts of interest
- escalation of identified or suspected corruption
- attentiveness to the requirements associated with the acceptance or offering of gifts, hospitality, or rewards.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## COMMUNITY ENGAGEMENT

In the discharge of his/her duties, an agency director should recognise the diversity of the community, be aware of the community's needs and balance the varying demands. Engagement across the community by the agency often facilitates enhancing the director's understanding of the different needs and challenges facing the community and informs his/her oversight role.

Community engagement can take many forms, both informal and formal. It can include representation on community participation forums, attendance at community related agency events, community visitation plans and liaising with community interest groups.

Directors should also ensure that the agency has in place proper processes and policies which ensure community engagement, where relevant and required.

## GOVERNMENT ENGAGEMENT

Directors should also be aware of the importance of government engagement and the approach taken to engage the government on agency decisions and strategy. Agencies should have a policy in place for communicating and engaging with the government in order to ensure a consistent approach is taken across the agency, and that discussions with the relevant Minister and Departments are not approached on an 'ad hoc' individual basis.



## Case Study – Queensland Health

The report titled *"Fraud, financial management and accountability in the Queensland public sector"* provides a detailed account of the fraudulent activity that took place at Queensland Health (QHealth) by an individual employee which resulted in a series of 65 fraudulent transactions, totalling \$16.69 million, committed over a four year period from 2004 – 2011. The report includes key learnings for the general application across the public sector, focusing on high risk employees and internal control weaknesses that place an agency at risk.

Recommendations resulting from the example:

**Management should increase vigilance in the following five main areas:**

1. Financial management
2. Managerial standards and accountability
3. Acceptance of gifts and benefits
4. Managing risk in a context of organisational change
5. Fraud awareness and prevention

Additionally, it is recommended that agencies consider and address these issues in all levels of their organisation including, but not limited to, executive management, with particular consideration by members of risk and audit committees. All managers and supervisors are encouraged to regularly review their internal processes and practices in order to identify any emerging issues.

The full report can be found at [Fraud, financial management and accountability in the Queensland public sector: An examination of how a \\$16.69 million fraud was committed on Queensland Health | CCC – Crime and Corruption Commission Queensland](#)

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US



## Case Study – Department of Communities (Western Australia)

In November 2021, Paul Whyte was jailed for 12 years after defrauding the government of \$27 million between 2008 and 2019. It was reported in court that Mr Whyte approved fictitious invoices and credit card transactions which resulted in payments to three companies owned by a co-accused who was a personal friend of Mr Whyte's. Police were able to uncover how some of these funds ultimately were used to pay Mr Whyte's mortgage.

In addition, payments were made to a company, Ausmodular, owned by another co-accused for construction of a camp where no work was performed. This money was extracted by Mr Whyte's brother through invoices submitted to Ausmodular with the funds being used to buy a house in a luxury suburb in Mr Whyte's wife's name.

The judge, Justice Joe McGrath, made the point that there was a failure of the public service to have the appropriate controls in place to prevent and detect the fraudulent activity that Mr Whyte engaged in and as he held a senior role, he was aware of these weaknesses and exploited them for his own benefit.

The Corruption and Crime Commission stated that *"In short, Mr Whyte was the ideal public servant. Except it was all a lie".*<sup>99</sup> He was uncovered after they received information that suggested *"conduct associated with questionable behavioural and lifestyle habits".*<sup>100</sup>

Auditor-general Caroline Spencer described that whilst fraud involving collusion can be difficult to detect, she *"wanted good management controls, robust internal audit functions and audit committees which followed up on recommendations."* and that *"segregation of duties and rotation of duties within public agencies was also important".*<sup>101</sup>

99 Ramsey, M. (2021), The Western Australian, <https://www.perthnow.com.au/news/court-justice/wa-bureaucrat-epitome-of-corruption-c-4581797>

100 ibid

101 Weber, D. (2019), ABC News, <https://www.abc.net.au/news/2019-11-21/paul-whyte-department-communities-fraud-not-detected-auditing/11726292>

## STRATEGIC PRIORITIES

The overall strategic direction and framework for government agencies is often set by the elected Federal or State Government. Agencies should align their strategic oversight and delivery within this framework and be consistent with the direction set by the relevant Minister.

All directors should be familiar with the strategic priorities and intention of the agency. The agency should oversee the alignment of the strategic and operational activities with these priorities.

Priorities generally adopted by agencies include the following:

- long term strategic initiatives with a focus on continuous agency functionality and the ability to respond to varying external factors
- responsiveness and attentiveness to community and stakeholder requests and attitudes
- efficient and effective ability to monitor progress via planning, reporting and sound controls.

## RECEIVING ASSURANCE

Directors should recognise and understand the different assurance and investigative bodies within government.

An Auditor-General exists for each State and Federal jurisdiction, and generally provides external financial auditing and performance auditing functions. They are appointed under legislation to examine, on behalf of Parliament, the management of resources within the public sector.

The Ombudsman is usually appointed by Parliament and has a significant degree of independence to perform investigative roles with respect to compliance issues within its defined jurisdiction. The Ombudsman is generally industry or service based and can also be referred to as a Commissioner. They also exist to receive and investigate complaints relating to government departments and agencies.

Several jurisdictions also have specialist anti-corruption bodies which can investigate activities of departments and agencies.

Government agencies generally establish a sub-committee for audit and risk to oversee and monitor risks and receive assurances on behalf of the agency.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- Australian National Audit Office, Audit Insights: Board Governance, 2019, <https://www.anao.gov.au/work/audit-insights/board-governance>
- Australian National Audit Office, Effectiveness of Board Governance at Old Parliament House, April 2019, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-old-parliament-house>
- Australian National Audit Office, Governance of the Special Broadcasting Service Corporation, April 2019, <https://www.anao.gov.au/work/performance-audit/governance-special-broadcasting-service-corporation>
- Australian National Audit Office, April 2019, Effectiveness of Board Governance at the Australian Institute of Marine Science, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-the-australian-institute-marine-science>
- Australian National Audit Office, May 2019, Effectiveness of Board Governance at the Sydney Harbour Federation Trust, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-the-sydney-harbour-federation-trust>
- Victorian Government, Victorian Public Service Commission, <https://vpvc.vic.gov.au/#board-members>
- Government of Western Australian, Governance of WA government boards and committees [Governance of WA government boards and committees \(https://www.wa.gov.au/organisation/public-sector-commission/governance-of-wa-government-boards-and-committees\)](https://www.wa.gov.au/organisation/public-sector-commission/governance-of-wa-government-boards-and-committees)
- The Department of the Prime Minister and Cabinet, Guidance on Caretaker Conventions, December 2021, <https://www.pmc.gov.au/resource-centre/government/guidance-caretaker-conventions>
- The Department of Finance (Cth) has published the following guidance relevant to GBEs: *Resource Management Guide No. 126 – Commonwealth Government Business Enterprises – Governance and Oversight Guidelines*. Refer to: [Government Business Enterprises \(GBEs\) \(RMG 126\) | Department of Finance](#)

For further information please contact:



**Brandon Brown**

**Partner, Audit, Risk and Assurance**  
[brandonbrown@kpmg.com.au](mailto:brandonbrown@kpmg.com.au)

# 4. Not-For-Profit Organisations

The roles, responsibilities and expectations of directors of Not-For-Profit (NFP) organisations are inherently the same as those of their corporate and government counterparts. Key differences exist however, with respect to aspects of legal compliance, tax obligations, strategic and operational areas of focus and accountability to members.

## In this chapter

- Directors' legal responsibilities
- Structuring an effective NFP board
- NFP leadership
- Strategic priorities
- Stakeholder engagement
- Identification, management and mitigation of risk
- Receiving assurance

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that a NFP director should ask

1. Are all directors well versed with the Constitution and rules of the board?
2. Do all directors understand their responsibilities relating to the Constitution, related government legislation and tax compliance?
3. Does each board member display strong working knowledge of the strategic priorities?
4. Are directors taking steps to engage with members and understand expectations?
5. Is the board aware of its duty to meet the objectives and vision of the organisation?
6. Are all directors fully aware of their duties and responsibilities regarding conflicts of interest?
7. Is there an effective framework for membership/ constituent engagement?
8. Are there strong working relationships across the organisation with members and stakeholders (including government departments for government boards)?
9. Is the board's role with members and the services provided to members well understood?
10. Do directors recognise the importance of ethical conduct in the NFP sector?

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The mission or purpose of the organisation is ambiguous, and never, or rarely, referred to in board discussions/documentation.
- There is no discussion of risk.
- There is no regular and/or accurate presentation of results or forecast cashflows.
- Certain directors are perceived to have conflicts of interest.
- There is concern that participation and engagement with members is poor.
- The directors fail to act in accordance with the objectives/purpose of the organisation.
- The Board, or certain directors, do not invest sufficient time on governance of the organisation.
- A director is demonstrating strong bias towards lobby groups (or similar) within its membership.
- The board ignores its strategic priorities in its decision making framework.
- Directors display lack of understanding of NFP organisation's funding and compliance obligations.
- Some directors are on the board for many years.



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

NFP entities are organisations that exist for 'public benefit', whereby their key objective is to provide a range of community services or advocacy activities (such as health, education, counselling or spiritual guidance, lobbying or improving the environment) for the communities they serve. Ensuring the ability to deliver these services to their communities over time, means that being financially viable is important. The key difference between a corporation and an NFP entity is that any profits are applied by the NFP entity to fulfil its overall purpose, rather than generating gains or benefits for distribution to members.

Setting and understanding the overall objective, vision, mission and values of a NFP entity is critical to establishing the context of its operations and the strategic focus of the board.

This section focuses on key differences that directors of NFP entities need to be cognisant of and be able to manage effectively. For clarity, this section does not specifically cover Government entity boards as this is covered in [Chapter 3 Government](#).

## DIRECTORS' LEGAL RESPONSIBILITIES

### *NFP legal structures*

It is important to recognise that there are many different types of NFP organisations, each one with a unique set of legal obligations, tax obligations, regulators and reporting requirements. In developing this chapter, we have focused on general observations applicable to NFP entities more broadly, however there may be specific considerations that are applicable to your NFP entity. As a director of an NFP entity, you must pay careful attention to the legal structures under which the NFP entity operates and ensure that independent professional advice is sought with respect to your duties and responsibilities within your organisation.

NFPs may be referred to as an 'association', 'college', 'club', 'company', 'foundation', 'fund', 'institute', 'league', or 'society'. The classification is determined largely by the legal structure under which the organisation is established and whether the organisation is a registered charity, which in turn, will impact on its tax status.

Throughout this chapter, we will refer to the NFP organisation as 'the NFP entity' and the governance representation as the 'NFP entity board'. You may be called a director, member, councillor or committee member and we will refer to you as a 'director' through this chapter.

The legal structure used to establish the NFP entity will determine the various financial, operational and compliance functions of the board. In addition to the legal duties outlined in [Chapter 1 Directors' Legal Duties](#), the different legal structures applicable to NFP entities, means that directors must invest time in understanding the relevant laws and the associated legal, operational, financial (e.g. tax-exemptions) and reporting requirements in order to effectively fulfil their duties.

Some of the more common legal structures include:

- Companies limited by guarantee
- Incorporated Associations
- Unincorporated Associations
- Co-operatives
- Indigenous Corporations
- Gift Funds
- Trusts
- Trade Unions
- Entities created by Acts of Parliament ("creature of statute")
- Federated models

A significant number of NFP entities are established as either an incorporated association or a company limited by guarantee.

Incorporated associations are legal entities separate from its individual members and are subject to the relevant state or territory legislation in which they operate. This means that the majority of their operations tend to be restricted to that jurisdiction. The liabilities and financial protections of the entity are limited.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Companies limited by guarantee are governed by the *Corporations Act 2001* (regulated by ASIC). NFP entities established under this legal structure are public companies, and the liabilities of the company members are also limited to the extent of the guarantee.

Some key considerations for NFP entities in determining the most appropriate legal structure are:

- Where will the non-profit operate?
- Will there be changing membership?
- What is the nature of the activities?
- How will the organisation raise money?

As noted above, NFP entities and individual directors should seek specific advice from a professional advisor with respect to legal, tax or accounting matters, prior to implementing or affecting changes to the NFP entity's legal structure.

**Charitable NFPs**

Not all NFPs are charities, however under Australian law, all charities must be an NFP. The *Charities Act 2013 (Cth)*<sup>102</sup> defines an entity as an NFP entity that serves 'for the public benefit'. Being a registered charity allows NFPs to receive certain tax concessions from the ATO and, therefore, is regulated by a national regulator, the Australian Charities and Not-for-profits Commission (ACNC).

With respect to discharging their legal duties, directors of charitable NFPs have an additional duty to ensure that they dutifully oversee how members' funds, assets, and products and services are managed to meet their community's needs. Therefore, the support of the charitable NFP entity in the maintenance of 'public benefit', or its mission, is key.

As such, in the duty of public benefit, directors should give consideration to the following:

- compliance with the relevant NFP ethical frameworks
- compliance with the defined values and standards generally outlined in the NFP's code of conduct
- ensuring a full understanding of the organisation's legal obligations and director's individual responsibilities
- acting with integrity and ensuring ethical decision making occurs across delegated powers in favour of public benefit
- compliance with NFP, financial, asset management and procurement requirements, in addition to conscientious expenditure of membership funds
- awareness and declarations of all conflicts of interest
- escalation of identified or suspected corruption
- attentiveness to the illegality of acceptance or offering of gifts or rewards.

<sup>102</sup> Charities Act 2013, <https://www.legislation.gov.au/Details/C2013A00100>

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Tax concessions for NFPs**

The ATO can provide tax concessions (including income tax, FBT concessions/exemptions and deductible gift recipient status) to certain types of NFPs (including registered charities, health organisations, community service organisations etc), but only where its constituent or governing documents explicitly state that profits or assets are prevented from being distributed for the benefit of particular individuals (i.e. owners, shareholders) – both while it is operating and when it winds up.

NFPs that are registered charities with the ACNC must go through an endorsement process with the ATO. The tax concession application process forms part of the application to become a registered charity with the ACNC and is submitted by the latter to the ATO to assess eligibility. Other NFPs do not require this endorsement and can become income tax exempt through a self-assessment process outlined by the ATO. Additional tests and rules, including annual reviews to determine ongoing eligibility apply.

**Regulation of charitable NFPs**

For entities that are registered charities (under the *Charities Act 2013*), there are also additional obligations that are regulated by the ACNC.

Established in 2012, the ACNC actively monitors and engages with charitable NFPs to ensure ongoing compliance with the conditions for maintaining charitable status through ensuring that the charity is:

- working towards its charitable purpose
- using its profits and assets only for its charitable purpose
- meeting its reporting obligations
- meeting its records keeping obligations
- meeting the ACNC Governance Standards.<sup>103</sup>

**ACNC Governance Standards**

Charities are required to meet a minimum set of governance standards that are set out by the ACNC. Failure to meet these standards puts the charitable NFP at risk of losing its charitable status, which can have significant financial, tax and reputation impacts. Standard 6 was added in February 2021 with the purpose of maintaining and enhancing public trust and confidence in the Australian charity sector by ensuring that a registered charity's governance enables it to be accountable for its past conduct relating to institutional child sexual abuse.

<sup>103</sup> Refer to ACNC Governance Standards, <https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-standards>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## ACNC Governance Standards:

**Standard 1 – Purpose and not-for-profit nature**

Charities must be not-for-profit and work towards their charitable purpose. They must be able to demonstrate this and provide information about their purposes to the public.

**Standard 2 – Accountability to members**

Charities that have members must take reasonable steps to be accountable to their members and provide them with adequate opportunity to raise concerns about how the charity is governed.

**Standard 3 – Compliance with Australian Laws**

Charities must not commit a serious offence (such as fraud) under any Australian law or breach a law that may result in a penalty of 60 penalty units (equivalent to \$12,600 as at December 2018) or more.

**Standard 4 – Suitability of Responsible Person**

Charities must take reasonable steps to:

- be satisfied that its Responsible Persons (such as board or committee members or trustees) are not disqualified from managing a corporation under the Corporations Act 2001 (Cth) or disqualified from being a Responsible Person of a registered charity by the ACNC Commissioner, and
- remove any Responsible Person who does not meet these requirements
- Ensure that the charity's financial affairs are managed responsibly
- Not allow a charity to operate while insolvent.

## ACNC Governance Standards:

**Standard 5 – Duties of Responsible Person**

Charities must take reasonable steps to make sure that Responsible Persons are subject to, understand and carry out the duties set out in this Standard:

- Act with reasonable care and diligence
- Act honestly and in the best interests of the charity and its purpose
- Not misuse the position of responsible person
- Not misuse information obtained in performing duties
- Disclose any actual or perceived conflict of interest
- Ensure that the charity's financial affairs are managed responsibly
- Not allow a charity to operate while insolvent.

**Standard 6: Maintaining and enhancing public trust and confidence in the Australian not-for-profit sector**

Charities must take reasonable steps to become a participating non-government institution if the charity is, or is likely to be, identified as being involved in the abuse of a person either:

- in an application for redress made under section 19 of the National Redress Scheme for Institutional Child Sexual Abuse Act 2018 (Cth) (Redress Act), or
- in information given in response to a request from the National Redress Scheme Operator (Secretary of the Department of Social Services) under section 24 or 25 of the Redress Act.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The AICD have also published the *Not-for-Profit Governance Principles* (January 2019).<sup>104</sup> The guide contains ten key principles that cover similar concepts as those outlined in the Corporations Act, with specific tailoring for the NFP sector. The principles are:

1. Purpose and Strategy
2. Roles and responsibilities
3. Board composition
4. Board effectiveness
5. Risk management
6. Performance
7. Accountability and transparency
8. Stakeholder engagement
9. Conduct and compliance
10. Culture

Directors must ensure that they are aware of all of the requirements of legislation governing charitable NFPs, remembering that in essence the obligations are the same as a 'for profit' entity, with the addition of ensuring (and demonstrating) that the "public benefit" continues to be met.

**Applicability of the Corporations Act 2001**

To reduce any misalignment between the governance requirements of the Corporations Act and the ACNC Governance Standards, the following Corporations Act requirements are not applicable for NFP entities registered under the ACNC Act. Instead, registered charities are required to take reasonable steps to ensure that any responsible persons comply with governance standard 5.<sup>105</sup>

Provisions that no longer apply	Summary of provisions
<b>Directors duties</b>	
sections 180 to 183; and section 185, to the extent that it relates to sections 180 to 183	Civil obligations of directors and other officers to: – exercise due care and diligence – act in good faith – not improperly use their position, and – not improperly use company information
section 188, to the extent that it relates to another provision mentioned in this table	Responsibilities of secretaries and directors for certain contraventions
section 191 – 194	Interests of directors
Additionally the following provisions of the Corporations Act are not applicable, as they are replaced by provisions from the ACNC Act:	
<b>Corporate reporting</b>	
subsection 136(5)	Public company must lodge with ASIC a copy of a special resolution adopting, modifying or repealing its constitution
section 138	ASIC may direct company to lodge a consolidated constitution

<sup>104</sup> Refer to AICD Not-for-Profit Resource Centre, <http://aicd.companydirectors.com.au/resources/not-for-profit-resources>

<sup>105</sup> ASIC, Corporations Act provisions that no longer apply to charities registered with the ACNC, refer to <https://asic.gov.au/for-business/running-a-company/charities-registered-with-the-acnc/corporations-act-provisions-that-no-longer-apply-to-charities-registered-with-the-acnc/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Provisions that no longer apply	Summary of provisions
section 139	Company must send copy of constitution to members
subsection 142(2), section 146 and subsection 146A(2)	Company must notify ASIC of changes of address
section 201L and 205A to 205C; section 205D, to the extent it relates to section 205B and section 205E	Public information about directors
Chapter 2N	Updating ASIC information about companies and registered schemes
Part 2G.2 (other than sections 250PAA and 250PAB); and Part 2G.3, to the extent that it relates to meetings of the body corporate's members	Meetings of members
Parts 2M.1 to 2M.3	Financial reports and audit
sections 601CDA, 601CK and 601CTA	Foreign companies
subsection 601CT(3), section 601CV and subsection 601DH(1) to (1A)	Registered body must notify ASIC of certain changes

**Other legislation**

Whilst this chapter contains an overview of key principles relevant to directors of NFP entities and charitable NFPs, it is important to note that every jurisdiction has different requirements, guidelines and legislation.

Other regulators include the Office of the Registrar of Indigenous Corporations (ORIC) and the Australian Taxation Office (ATO).

A list of regulators that may affect NFP entities can be found on the Australian Charities and Not-for-Profit (ACNC) website (<https://www.acnc.gov.au/list-regulators-may-affect-charities>)

Similarly, overarching legislation and regulations such as privacy, equal opportunity, freedom of information, environmental protection, occupational health and safety and fair trading laws apply equally to NFPs as they do to 'for profit' entities. These are discussed in more detail in [Chapter 1 Directors' Legal Duties](#).

Each director must invest time in understanding the relevant laws that bind their specific association and the impact on their obligations.

**Reporting obligations for charities to change in 2022**

The ACNC have reduced the reporting thresholds for charities<sup>106</sup> so that less charities will need to produce financial reports and can rather complete an Annual Information Statement instead. In addition, the changes enable smaller charities to elect for a review rather than an audit of their financial reports.

When charities complete their 2022 Annual Information Statements (which, for many, will cover a reporting period between 1 July 2021 and 30 June 2022), the thresholds for determining whether a charity is small, medium or large for financial reporting purposes will change to those shown below.

<sup>106</sup> ACNC, January 2022, Upcoming changes to charity size thresholds are good news for charities, refer to [www.acnc.gov.au/media/news/upcoming-changes-charity-size-thresholds-are-good-news-for-charities](https://www.acnc.gov.au/media/news/upcoming-changes-charity-size-thresholds-are-good-news-for-charities)

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Size of charity	Current revenue thresholds for 2021 Annual Information Statements	Revenue thresholds from 1 July 2022 for 2022 Annual Information Statements	Audit/review requirement
Small	Less than \$250,000	Less than \$500,000	Only have to complete their Annual Information Statement online.
Medium	\$250,000 – \$999,999	\$500,000 – \$2,999,999	Financial report can be either reviewed or audited.
Large	\$1 million or more	\$3 million or more	Financial report must be audited

## STRUCTURING AN EFFECTIVE NFP BOARD

Depending on the constitution of the entity, boards may be elected by members, or appointed through a competitive selection process. Depending on the constitution, some boards may be comprised solely of members whilst others may allow for some independent directors so as to expand the skills of the board.

Where the NFP has adopted a federated structure, coordinating any number of component bodies (often state-based with a national body at the top), a board of the top (potentially national) entity will be responsible for oversight of the individual component bodies as well as the stewardship of one single federated body. To ensure appropriate representation, boards of the overall federated body typically comprise representatives (also called nominees) from each of its component bodies.

Though this model presents some clear strengths, it is becoming more common to include one or more independent directors (and especially an independent chair) on the federation board, where the constitution allows. This helps to protect and promote the necessary balance in focus between maintaining oversight of the individual component bodies and guiding the overall strategic direction of the federated organisation.

*Appointment process*

Members generally vote to make appointments to NFP boards for a fixed term. Whilst not always the case, the appointments are generally advertised to members via public media, which outline the core skills and competencies required. The board chair, CEO and NFP entity members may in some cases select 'public members' to the board, or there may be a Nominations Committee as part of the board governance structure, that has been established specifically to address board appointments. Public members are selected to address board skills deficits or to balance elected board member composition (gender, experience and qualifications, geographical) through an expression of interest. Existing directors and the chair can help to create a pool of potential candidates through continuous networking as a form of succession planning. In some cases, there may be a combination of member elected board members and board appointed directors, to achieve a balance between member representation and ensuring the appropriate skills are in place. Further entity appointments can occur via elections, ex-officio 'requirements', expressions of interest, nominations for improved NFP entity composition, and reappointments.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Criteria for selection**

The selection criteria used by NFP entities to elect and/ or appoint board members and a chair may include, but is not limited to:

- the status and integrity of the individual within the community (membership) in which they work
- adherence to the duties of a non-executive director with reference to the Corporations Act, if applicable
- any other legislative requirements applicable to that board (e.g. mandatory governance requirements of other commissions)
- working knowledge and understanding of accountability relationships
- relevant experience within the sector and their elected field(s) of excellence
- ability to think and act strategically
- understanding of the NFP organisation and sector operations
- understanding of the objectives and role requirements of their position
- existing relationships and connectivity
- understanding of the key risks and challenges present in the NFP sector
- governance standards understanding
- capacity to contribute (in time and often financially) and attend board and sub-committee meetings.

To achieve a 'balance of expertise' on an NFP board, there may be a greater need to consider, and give heavier weight to, the candidate's corporate business and financial expertise, advocacy or stakeholder engagement.

**Sourcing**

Strategic workforce planning at a board level should be informed by board evaluation and completion of skills matrices to highlight gaps and drive selection based on 'public member' candidate expertise. Embedded in this is the management of talent identification and due diligence.

Probity considerations that should be taken into account when sourcing and selecting candidates may include, but are not limited to:

- proof of identity checks
- verification of qualifications
- ASIC registration/disqualification check
- working with children check
- police/criminal record check
- declaration of private interests/conflict of interests
- personal reference checks.

Depending on the jurisdiction in which the NFP entity operates, these requirements may differ.

**Director resignation, retirement and removal**

Director involvement on NFP boards can often be driven by personal values or connections to the organisation. Sometimes, however, despite this passion and commitment, the director does not have the skills or experience required to operate effectively on the board. Other issues associated with board renewal in the NFP sector include board members who – due to constitutional limitations or other reasons, like a sense of obligation – have remained on the board for many years, thereby limiting options for new members to join and bring a fresh perspective. This can create significant issues with respect to the ability of the board to fulfil its legal and governance duties. This is where a clearly defined board governance framework, including clearly documented appointment processes, tenure, skills requirements and performance measures of directors is critical.



## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Removing a director in these types of sensitive situations can be challenging. The options available will depend on the legal structure of the NFP entity. For example, an NFP entity may be able to move the director to a sub-committee (e.g. fundraising) to focus their effort on a specific function to which they feel strongly connected and to which they can make a more significant contribution, but they cannot do this if they are a company limited by guarantee. Directors of NFP entities operating as companies limited by guarantee can often only be removed by a member vote.

### Challenges of finding and retaining NFP directors

Directors of NFP entities are often unpaid. The AICD's *2021, NFP Governance and Performance Study*<sup>107</sup> found that only 20 percent of respondents were remunerated, however this varies by sector. The report notes that "the days of a volunteer board, especially in a sector like aged care, are probably coming to an end. The risk and the required level of knowledge and skill have changed dramatically over the last couple of years".<sup>108</sup>

In addition, the survey also found that 45 percent of respondents report their time spent on their director role is somewhat more or twice as much (33 percent and 12 percent respectively) compared to last year.<sup>109</sup>

Finding candidates who are willing to invest the time and effort in a 'volunteer' role with such high levels of responsibility and accountability can often be challenging. Conversely, some NFPs find that directors join with great passion and intent for the purpose, but do not have strong governance skills, especially when NFP boards are often the first governance role for individuals looking to gain governance experience in an unlisted and "less high profile" environment. The reality is that the expectations, accountabilities and obligations are inherently the same for NFPs as for 'For Profit' entities.

<sup>107</sup> AICD, November 2021, Not-for-Profit Governance and Performance Study 2021, refer to <https://aicd.companydirectors.com.au/advocacy/research/2021-nfp-governance-and-performance-study>

<sup>108</sup> ibid

<sup>109</sup> ibid

## NFP LEADERSHIP

The relationship between CEO and the board is a critical one for NFPs. Unlike other organisations where the CEO reports to the board, often in NFPs, the CEO is a key resource for directors – providing assistance in:

- assisting directors (who are often volunteers) to understand their duties
- making recommendations for board recruitment that align with the NFP entity's culture and skill needs
- increasing the awareness of directors about the organisation's objectives and programs
- participating in strategy development and board committees.

It is critical that CEOs and NFP directors have an effective working relationship that is based on shared objectives, open communication and a strong understanding and respect for each other's role and skills.

Within NFPs, the line between board and management can be less clear than in private organisations (especially listed companies). Resource constraints can often mean that directors are required to get more involved in operational issues, thereby stepping out of their oversight role and into implementation – i.e. less 'steering' of the boat and more 'rowing'.

Again, in these instances, it is critical for the board to recognise and clearly define when it is required to move into operational matters. Whilst the Board Charter is an important document to define the role of the board (and all NFPs should have a clearly documented Board Charter), the Delegations of Authority (DoA) is critical to explicitly define how board and management interact, and the levels of responsibility for decision-making with respect to implementation of the NFP's mission and strategy.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## STRATEGIC PRIORITIES

Like corporate boards, the overall strategic framework, direction and priorities for an NFP entity are set by the board. NFP entities should set their strategic priorities within this framework and be consistent with the board's direction. It is the duty of a director to ensure that they are familiar with the mission and strategic priorities of the entity. The NFP's CEO should oversee the alignment of the mission with its strategic direction and operational activities.

Part of the development of strategic priorities requires a clear understanding and agreement on the mission or objectives of the NFP entity. Membership based associations may be motivated by public benefit, prestige and advocacy within the industry, and the relationships between members and stakeholders. In contrast, other NFPs (health and education services) may be motivated by achieving the best possible health, education and/ or wellbeing outcomes for the communities that they support.

Types of issues specific to NFPs and the development of strategic priorities are detailed below.



### Case Study – The Returned and Services League of Australia (NSW Branch)

In February 2018, the NSW Government released the findings of an inquiry into the financial and fundraising activities of RSL NSW. The inquiry was commissioned as a result of concerns regarding *RSLs compliance with the NSW Charitable Fundraising Act 1991 (NSW)*, specifically with respect to how funds raised were used by the organisation, with concerns that funds were not being used for a charitable purpose.

The NSW state branch was rocked in late 2016 by revelations that the State President (and director) had spent \$475,000 on a corporate credit card over a six-year period, including \$213,000 in cash withdrawals.

There were further allegations of \$150,000 of spending by the director that was not accounted for with receipts; the use of an RSL NSW credit card to fund his son's use of a presidential suite at a Sydney hotel over a period of 7 years; and the use of the RSL NSW credit card to cover mortgage repayments, flights for family and meals over an 11 year period. In addition, some board members, including the State President and former National RSL President, received tens of thousands of dollars a year in 'consulting fees' from the league's aged care arm, RSL LifeCare.

The inquiry undertaken by Supreme Court Judge Patricia Bergin, identified a number of areas of director financial misconduct, and recommended that the former RSL NSW President be referred to police over misuse of credit cards.

The high-level inquiry also recommended:

- 13 directors be referred to charity watchdogs in connection with the to cover-up of expenses
- Eight board members and executives of the aged care arm be referred to the watchdogs in connection with payments made to some voluntary board members that appeared to breach charities regulations.

### The importance of purpose

The foundation of the NFP entity's governance framework is its constitution. This legal instrument defines the organisation's mission, purpose, objectives, general powers, functions and duties, and the responsibilities of its directors. The constitution should clearly outline the entity's legal structure, charitable / non-for-profit status and governing laws.

The directors should be well versed with the constitution and review all NFP entity instruments, processes and functions against it.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A key component of the constitution is to define the organisation's mission and purpose. Critically, for NFP entities, the alignment of activities with its mission can be challenging. In some instances, social drivers (such as increasing demand for diversified services), resource/skills constraints and funding pressures can move organisations away from their mission, thereby creating unique risk and strategy issues for directors.

For example, NFPs often generate 'revenue' through donations or grants. In the case of grant funding, money is often provided to meet specific government policy objectives. In some cases, these objectives will broadly align with the organisation's mission, however, may require the NFP to direct some of the resources into other related – but non-core – services. Over time, these 'new' services can move the organisation into areas that do not fully align with the NFP's mission.

In this instance, risk and strategy issues can arise that might put the organisation into conflict with itself. For example, an NFP established to provide assistance to low income households may receive funding to retrofit households with energy efficient light bulbs (reducing energy bills for low income earners). Whilst in alignment with the NFP's mission, it may require specialist skills with respect to installation of equipment or electrical modifications within a home. Whilst the funding would no doubt assist the NFP achieve its mission, it comes with a range of legal, operational and reputational risks that need to be considered. Pursuing this service offering could distract the organisation from its core purpose and further constrain the use of scarce resources.

Directors, therefore, need to understand the range of risks that these opportunities can present (particularly in a competitive funding environment). This requires a thorough understanding and oversight of risk management practices within the organisation.

Governance roles are also characterised by the size and nature of the organisation and its scope of operations. For example, larger NFP entities operating multi-million dollar budgets and operating at a national scale will have vastly different governance requirements than a community sporting club.

### Managing funding constraints

NFPs reinvest any profit generated back into the entity in order to fulfil its purpose. All NFPs have a responsibility to remain solvent, generate sufficient profit for the long-term sustainability of the organisation through diverse funding streams (i.e. apart from membership contributions alone), and the judicious management of funds to benefit the ongoing viability of the organisation.

As noted above, there are important considerations for directors when seeking and obtaining funding from grants and donors that have specific objectives. Competition for funding can lead NFPs to move into the provision of services that are related to, but misaligned with, the NFP's overall mission and strategy. This is where a strong governance framework for managing risk and opportunity is critical – and it is the duty of the board to ensure that these frameworks are in place, and that member interests are being met through the achievement of the organisation's purpose.

## STAKEHOLDER ENGAGEMENT

As highlighted in [Chapter 8 Stakeholder Engagement](#), all boards have an accountability to their stakeholders. An NFP director's individual role is to represent its members and communities. Part of this responsibility includes providing stakeholders with adequate channels for raising concerns and reporting back to stakeholders on a transparent and regular basis. In the discharge of their duties, an NFP director should recognise the diversity of the membership, be aware of the members' needs and balance the varying demands and incorporate these into the strategic priorities of the NFP entity.

As a collective, an NFP entity's board must also engage across the membership. This often facilitates the individual director and overall board's understanding of the different needs and challenges facing the members and informs their oversight role. Member engagement can take many forms; both informal and formal. It can include representation or participation in member forums, attendance at related events, visitation plans and liaising with membership groups.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Members have wide and varied expectations that the NFP entity will fulfil most/all relevant needs. Obtaining value for money and the cost of membership are often critical issues for members.

Outputs of the engagement process should inform strategy development and priority setting. This will keep the NFP's thinking fresh and ensure that member needs and the NFP's overall mission are being met.

Directors should also be aware of the importance of stakeholder engagement and the approach taken to engage stakeholders on decisions and strategy. Stakeholders can, in this instance, include relevant government departments, funders and sponsors, industrial bodies, education providers, research institutes and collaborators and community interest groups.

NFP entities should have a policy in place for communicating and engaging with stakeholders to ensure a consistent approach is taken across the NFP entity and that discussions with the relevant key and critical stakeholders (government departments) are not approached on an "ad hoc" individual basis.



### Case Study – The Royal Commission into Aged Care Quality and Safety

The evidence heard by the Royal Commission illustrated disturbing evidence of failures in the aged care sector concerning the care and dignity of the elderly population. Arising from the Royal Commission were a series of board-level recommendations.

#### Board structure and composition – Recommendation 88

The Royal Commission proposed legislative amendments to improve provider governance modifications to board structure, arrangement and governance:

- Majority of the board being independent, non-executive directors

- Mandatory care governance committee, chaired by a non-executive member with appropriate experience in care provision
- Fit and proper person test for key personnel
- Requirement in governance standards that boards have a mix of governance skills, expertise and knowledge
- Nominated member of the board attesting annually on behalf of the board to deliver safe and high-quality care

#### Governance Standards – Recommendation 90

Additionally, new standards were proposed with respect to corporate governance. These include:

- Governance standards requiring boards to establish systems for feedback and receiving complaints as well as proper risk management practice
- Obligation to notify the regulator of changes to key personnel, including directors
- Mandatory annual reporting to governments by providers

In response, the Aged Care and Other Legislation Amendment (Royal Commission Response No. 2) Bill 2021 was tabled which includes a number of governance requirements for aged care providers including that a majority of members of the governing body must be independent non-executive directors; and at least one member of the governing body to have experience in the provision of clinical care ('Independence Requirement'). The Independence Requirement is set to begin on 1 March 2022 but existing providers have until 1 March 2023 to fulfil this requirement. At the time of writing this, there are delays with the Bill, which may result in the Independence Requirement taking effect after 1 March 2022.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## IDENTIFICATION, MANAGEMENT AND MITIGATION OF RISK

Risk management is a critical function for any organisation, particularly the board. NFP boards have some unique risks that require additional consideration, including ensuring the health and safety of staff and volunteers – who can often be placed in dangerous situations. For example, NFPs that provide health and support services to mental health patients, may have volunteers who assist in delivering these services. The volatile nature of members may place these volunteers at risk of injury or stress. To adequately fulfil their duties, directors need to ensure that they are cognisant of the unique circumstances and potential legal, reputational and physical risks that exist within their operations.

*Resilience to long term and emerging risks*

Long term strategic initiatives with a focus on sustainable functionality, and the NFP entity's ability/agility to respond to varying external impacts/challenges, are critical for both corporate and NFP boards. However, the ability of an NFP entity to continue to deliver community services in the face of long term social and environmental challenges needs to be understood and scenario tested within the NFP entity's risk tolerance and risk appetite frameworks. For example, the World Economic Forum (WEF) lists issues such as ageing population, growing income disparity, natural resources shortages, increasing urbanisation, climate change and cyber disruption as key long-term global risks. NFP entities providing community services to support – for example – 'at risk' communities (e.g. elderly, disadvantaged), protection of the environment, provision of health services etc, need to understand the potential risks and impacts on their ability to provide services. This includes identifying potential opportunities associated with these emerging risks, for example, new funding opportunities may eventuate in research and innovation around new areas of community need and support.

Chapter 18 Environmental, Social and Governance (ESG) provides more insight into the role of boards in managing sustainability risks and developing response strategies.

Similarly, it is critical that NFPs are aware of both the risks and opportunities generated by social media. The nature and volume of (mis)information spread through social media (and the speed at which this can occur) creates enormous reputational risk that can significantly impact any organisation's 'social licence to operate'. This is a particularly high risk for NFPs that are often in highly competitive funding environments. Conversely, the opportunities that social media can create for NFPs is also large and somewhat untapped. Awareness, support and even fund raising activities can be more quickly and effectively achieved through the reach and power of social media.

As for all organisations, directors need to ensure that the NFP entity has in place a detailed risk management plan that is reviewed regularly. The board or sub-committee will often have responsibility for identifying risks and mitigation strategies, and endorsing actions when issues emerge.

*Efficient and effective ability to monitor progress using agreed Key Performance Indicators (KPIs)*

In many NFP entities, the expectation of transparent and timely disclosure of performance is critical to ensuring ongoing viability, by demonstrating progress towards ongoing positive contributions to member/constituent and public benefit.

Measuring progress against objectives via sound planning and governance processes is, therefore, critical for any NFP entity to maximise the opportunities for ongoing funding and support from stakeholders.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## RECEIVING ASSURANCE

Assurance over NFP entities sits with different assurance and investigative bodies within the regulators that apply to the NFP entity.

Incorporated Associations in Australia are governed by each state and territory's Associations Incorporations Act. The auditing and reporting requirements are established by each local jurisdiction and, therefore, reference to the relevant legislation is required. For example, in Victoria, an annual audit is required, but only if revenue is greater than \$1,000,000. The auditor must be a registered company auditor, a member of CPA Australia or CA ANZ, or a person otherwise approved by the Registrar – Section 99 2(d) of the *Associations Incorporated Reform Act 2012*.

## Useful resources:

- AICD, The Not-for-Profit Governance Principles, <http://aicd.companydirectors.com.au/resources/not-for-profit-resources/not-for-profit-governance-principles>
- Australian Charities and Not-for-Profit Commission <https://www.acnc.gov.au/>
- Pearce, R, 2020, Exit the federation? New governance structures emerging in NFP organisations, <https://thinkinsightadvice.com.au/new-governance-structures-nfp-organisations>

## For further information please contact:

**Stephen Isaac****Partner, Audit****[stephenisaac@kpmg.com.au](mailto:stephenisaac@kpmg.com.au)**

## • FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 5. Proprietary Limited Companies

Proprietary limited (proprietary) companies are the most common company type in Australia. This chapter outlines the key differences between proprietary companies and other company types.

## In this chapter

- Key differences between public companies and proprietary companies
- Approaches to governance
- Financial statements requirements
- Governance and Income Tax
- Crowd-sourced funding

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Has the company adopted a constitution or is it governed by the Corporations Act 'Replaceable Rules'?
2. Is there an overarching shareholders' agreement or trust deed (for those proprietary limited companies that act as trustee of a trust) to be considered in conjunction with the company constitution/ Replaceable Rules?
3. If the company pre-dates the mid-1990s, has the board considered proposing the adoption of a new constitution to the company member(s)?
4. If the company is a wholly-owned subsidiary, does the company's constitution include the relevant clause to support this?
5. If the company is a family enterprise, does the company's share capital structure adequately facilitate the long-term succession of the company to the next generation?
6. If the company intends to avail itself of crowd-sourced funding, is it correctly structured to do so?
7. If the company is part of a larger group structure, is an up-to-date group structure chart maintained and readily available/accessible?
8. Has the company adequately maintained its financial records, minute book and statutory registers?
9. Has the company adequately documented and implemented a tax governance framework?
10. Is the company required to prepare, audit and/or lodge annual financial statements?
11. If the company is availing itself of ASIC relief from the requirement to prepare, audit and/or lodge annual financial statements, does the company adhere to the ongoing relief requirements?
12. If the company is required to lodge financial statements with ASIC or has constituent documents dated after 1 July 2021, have directors considered the new General Purpose Financial Statement reporting requirements?



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board has not given adequate consideration to (or review of) the insurance of the company and its officers against possible liabilities.
- The family enterprise has not given due consideration to the governance of the family versus the governance of the business.
- Multiple subsidiaries exist in the group, but there is no up-to-date group structure readily available (and it is unclear who is responsible for maintaining it).
- Financial records and/or inter-group transactions are not properly documented.
- An ASIC directorship search reveals multiple out-of-date and/or inconsistent details for a director.
- The company's memorandum and articles of association pre-date the mid-1990s and no consideration has been given to their review and/or adoption of a new constitution.
- The directors are unaware of (and/or do not refer to) the existence of an overarching shareholders' agreement or trust deed.
- The company is not adequately structured for the long-term strategic goals or succession planning of the enterprise.
- If the company is availing itself of ASIC relief from the requirement to prepare, audit and/or lodge annual financial statements, the directors do not ensure that the company continues to satisfy the ongoing relief requirements.
- The Board has not reconsidered its financial reporting requirements since 1 July 2021.
- No tax governance framework is documented or implemented.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## KEY DIFFERENCES BETWEEN PUBLIC COMPANIES AND PROPRIETARY COMPANIES

The majority of registered companies in Australia are proprietary limited companies. Like public companies, proprietary companies offer a limited liability to its members. However, there are a number of key differences between public and proprietary limited companies, including:

- Proprietary companies are limited by shares (or be an unlimited company with a share capital)<sup>110</sup> and are 'for profit' in nature (ie they cannot be used for not-for-profit purposes, unlike public companies that can be limited by guarantee and registered as not-for-profit organisations with the ACNC)
- They are not permitted to offer/sell shares directly to the public that would require disclosure under Chapter 6D of the Corporations Act
- They are limited to a maximum of 50 (non-employee) shareholders
- They are not able to list on the ASX and, therefore, are not subject to the ASX Listing Rules
- Directors may be permitted to vote on matters where there is a personal material interest being considered at a directors' meeting<sup>111</sup>
- They are subject to reduced requirements under the Corporations Act, including:
  - No requirement to have more than one director
  - Facility for a sole director and member company<sup>112</sup>
  - No requirement to appoint a company secretary
  - No requirement to hold an AGM
  - Possible exemption from preparing, auditing and lodging financial statements with ASIC.

<sup>110</sup> Corporations Act 2001, Section 45A(1) Note 2; Section 112(1)

<sup>111</sup> Corporations Act 2001, Section 194.

<sup>112</sup> Corporations Act 2001, Section 198E.

The majority of these reforms were made to the corporations legislation. Therefore, companies whose Memorandum and Articles of Association (M&As) refer to pre-1990s corporate legislation and, as a consequence, may not be able to avail of these reduced requirements. In such instances, the company's M&As may need to be amended or repealed and replaced by the adoption of a modern constitution document.

It is important to note that the reduced requirements under the Corporations Act do not lessen the company and directors' exposure under other legislation, eg Work Health & Safety legislation. Directors must familiarise themselves with the responsibilities arising from other legislation and regulations, and should consider insuring against liabilities, where possible and appropriate.

## APPROACHES TO GOVERNANCE

The governance of a proprietary company can vary immensely depending on its structure and purpose. Regardless of the simplicity of the company structure, all directors are still subject to their fiduciary duties, including but not limited to:

- the duty to act in good faith and exercise power for a proper purpose
- the duty to exercise skill and care.

They are also subject to other statutory duties, including the duty not to trade while insolvent.

### Director remuneration

In respect to directors' remuneration, the constitution should set out the mechanisms for the approval and reporting of directors' remuneration. If the Replaceable Rules, Section 202A(1) or 202C of the Corporations Act have been followed, the total amount to be paid to directors should be approved by the company by resolution. Constitutions may contain more specificity concerning the approval and reporting mechanisms.<sup>113</sup>

<sup>113</sup> Refer to AICD Directors' fees, 2017, <https://aicd.companydirectors.com.au/resources/director-tools/practical-tools-for-directors/board-composition/directors-fees>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Sole director/member**

A sole director/member company is the simplest of company structures. The Corporations Act includes a number of clauses that relate specifically to these companies. For example, Section 201F of the Corporations Act sets out the governance provisions for the circumstances that arise in the death or incapacity of the sole member/director.<sup>114</sup>

**Trustee companies**

It is common for trusts to appoint a corporate trustee, rather than individual trustees. This applies to private family trusts, unit trusts and self-managed superannuation funds. The management of the trustee company's affairs will typically parallel those of the underlying trust, however, the assets of the entity will lie in the trust rather than the company.

Section 19 of the Superannuation Industry (Supervision) Act 1993 requires superannuation fund trustee companies to adopt a constitution that specifically notes that the company's sole or primary purpose is to act as trustee of the fund. The trustee company's constitution must also prohibit the company from distributing income or property to its members.<sup>115</sup> Importantly all directors of a self-managed superannuation fund (SMSF) trustee company must also be trustee company shareholders and all trustee company shareholders must be trustee company directors too for an SMSF to be compliant under Australian Income Tax Law.

Directors identification number<sup>116</sup> requirements apply equally to directors of trustee companies as they do to directors of operating companies. These are discussed further in [Chapter 9 Structuring an Effective Board](#).

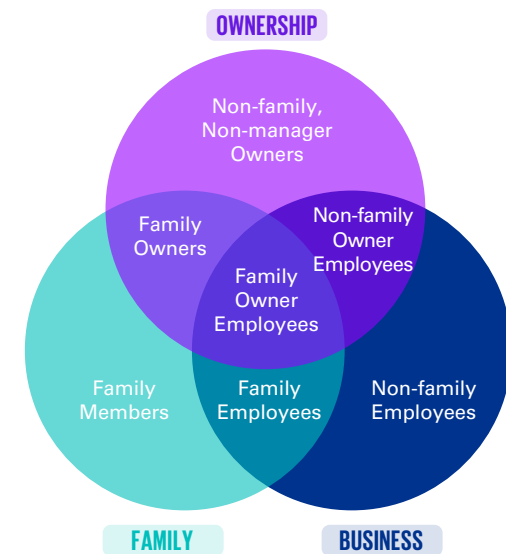
<sup>114</sup> Corporations Act 2001, Section 201F

<sup>115</sup> Refer to ASIC, Special Purpose Companies, <https://asic.gov.au/for-business/registering-a-company/steps-to-register-a-company/special-purpose-companies/>

<sup>116</sup> Refer to ABRS, Director Identification Number, <https://www.abrs.gov.au/director-identification-number>

**Family enterprises**

Family enterprises can often take the form of a proprietary company. The governance of the family can be challenging due to three interdependent and overlapping stakeholder groups being family, ownership and business. Good practice seeks to implement a framework that recognises long term success depends upon healthy functioning governance across all three key groups. Clarity and alignment within the family business system, depicted in the diagram below, enables the family to work cohesively towards its collective aspirations, and balance the needs and goals of individuals with the needs and goals of the collective family, the owners and the family business.

**Three-circle model of the family business system<sup>117</sup>**

<sup>117</sup> Renato Tagiuri and John A Davis, 1996, Family Business Review, Bivalent Attributes of the Family Firm, refer to <https://journals.sagepub.com/doi/abs/10.1111/j.1741-6248.1996.00199.x>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

It is important to clearly differentiate between the roles of owners, those in the business and other stakeholders in a family system. A family charter is often complemented by a shareholders' agreement and/or a family constitution document governed by a possible Family Council or Advisory Board. These additional layers of governance support the long-term strategy and succession planning for the family enterprise.

Family Business Governance Model



Underpinned by...				
<ul style="list-style-type: none"> <li>• Binding Financial Arrangements</li> <li>• Trusts</li> <li>• Wills</li> <li>• Family Council</li> </ul>	<ul style="list-style-type: none"> <li>• Family Constitution                             <ul style="list-style-type: none"> <li>– Statement of principles and rules, not binding</li> <li>– Pre-agreed rules</li> <li>– Family Charter, values</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Shareholders Agreement                             <ul style="list-style-type: none"> <li>– Directorships</li> <li>– Buy/sell mechanisms</li> <li>– Delegated authorities</li> <li>– Rights of owners</li> <li>– Succession plan</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Board Charter                             <ul style="list-style-type: none"> <li>– Skills matrix</li> <li>– Roles &amp; responsibilities</li> <li>– KPIs</li> <li>– Delegated authorities</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Roles &amp; job descriptions for family and non-family members</li> <li>• Authority &amp; accountabilities</li> <li>• Goals</li> <li>• Performance development &amp; management of family and non-family members</li> </ul>

Pitfalls of nepotism, inequality and blurred boundaries commonly arise as the family enterprise matures, and can become more pronounced at times when the family enterprise is going through a significant change, such as a transition to the next generation. It is important that advisers to the family enterprise recognise these pitfalls are not uncommon and work with the family and the family enterprise to educate and guide decision-making.

Wholly-owned subsidiaries

Wholly-owned subsidiaries differ in nature by virtue of being owned and controlled by a parent company. The parent company can be another Australian company or a foreign-registered company.

Directors of large groups should ensure that an up-to-date group structure is maintained and readily available, and assign responsibility for it to an appropriate director or member of management.

The Corporations Act specifically allows a company's constitution to include a provision to assist with subsidiary director duties.<sup>118</sup>

118 Corporations Act 2001, Section 187.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Section 187 of the Corporations Act provides that the directors of a wholly-owned subsidiary can be taken to be acting in good faith in the best interests of the subsidiary if:

- the constitution of the subsidiary company expressly authorises the director to act in the best interests of the parent company and
- the director acts in good faith in the best interests of the parent company and
- the subsidiary is not insolvent at the time of the director's acts and does not become insolvent because of the director's acts.

Details of delegated authorities are usually captured in the corporate group's delegations policy. However, a group's delegations of authority may not provide clarity on whether the directors of a subsidiary company have a right to approve major transactions. In such cases, directors should seek clarification from the owner of the group delegations policy. A failure to consider important transactions undertaken by the subsidiary company could potentially place directors in breach of their duty to exercise skill and care.<sup>119</sup> Directors should also take care that loan agreements and debt forgiveness between group entities is also adequately documented.

Directors who are appointed to multiple companies' boards should ensure that any changes to their personal details are notified to ASIC (and other relevant regulators and authorities) in a timely manner, for all affected entities. The periodic purchase and review of an ASIC directorship search is a useful exercise in this regard.

<sup>119</sup> Refer to the Governance Institute of Australia, Guidelines for directors of wholly-owned subsidiary companies, <https://web.governanceinstitute.com.au/home/>

## FINANCIAL STATEMENTS REQUIREMENTS

Section 286 of the Corporations Act requires all companies' financial records to be kept for at least seven years after the transactions covered by the records are complete. They must correctly record and explain the company's transactions, financial position and performance, and allow true and fair financial statements to be prepared. This obligation exists regardless of whether the company's books and records are maintained in-house or outsourced to a third party, and whether they are electronic or not.<sup>120</sup>

Even if the company's records are held by someone else (eg an accountant), the directors, as company officeholders, are still responsible for providing copies to auditors or anyone entitled to inspect the records.<sup>121</sup>

Section 292 of the Corporations Act outlines which companies must prepare annual financial reports and directors' reports. A 'large' proprietary company must prepare and lodge with ASIC a financial report, a directors' report and an auditor's report<sup>122</sup> within four months after the end of the company's financial year.<sup>123</sup> The financial report, directors' report and auditor's report must also be given to members within these four months.<sup>124</sup>

*Definition of 'large' company or group*

A proprietary company is 'large' if it meets at least two of three thresholds listed in the below table at the end of a financial year. The current thresholds replaced those from 2007 on 1 July 2019.

<sup>120</sup> Refer to ASIC, Directors and Financial Reporting, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

<sup>121</sup> Refer to ASIC, What books and records should my company keep?, <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>

<sup>122</sup> Corporations Act, Section 301(1).

<sup>123</sup> Corporations Act 2001, Section 319(3)(b).

<sup>124</sup> Corporations Act 2001, Section 315(4).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

	Threshold
Consolidated revenue for the financial year of the company and the entities it controls*	\$50 million
Value of the consolidated gross assets at the end of the financial year of the company and the entities it controls*	\$25 million
Employees^ of the company and the entities it controls	100 employees

\*Control is determined based on whether accounting standards require the company to prepare financial statements in relation to a consolidated entity

^ Part-time employees are counted as an appropriate fraction of the full-time equivalent

A 'small' proprietary company is only required to prepare, audit and lodge financial statements with ASIC if it is controlled by a foreign registered company (and its financial information is not consolidated into the financial statements of the foreign registered company, registered scheme or disclosing entity) or if the company is directed to do so by ASIC, or by 5 percent or more of their shareholders.<sup>125</sup>

Financial reporting obligations for certain proprietary companies significantly changed from 1 July 2021 with the introduction of AASB 2020-2 "Removal of Special Purpose Financial Reports for Certain For Profit Private Sector Entities". Where proprietary companies are required under legislation to prepare financial statements in accordance with Australian Accounting Standards or 'accounting standards', or their constitutions or other key governance documents (such as bank lending agreements), commencing or amended on or after 1 July 2021, require preparation of financial statements in accordance with Australian Accounting Standards, these companies will be required to prepare Tier 2 General Purpose Financial Statements (GPFS).

Where directors of proprietary companies have relied on preparing special purpose financial statements (SPFS) in the past, it is recommended that directors and advisors revisit the reporting/non-reporting entity classification and ensure that their reasoning for continuing SPFS is comprehensively documented or whether indeed GPFS are now required.

<sup>125</sup> Corporations Act 2001, Section 292.

**ASIC relief relating to financial statements**

In certain circumstances it is possible for proprietary companies to avail themselves of exemptions from the requirements to prepare, audit and/or lodge financial statements with ASIC. ASIC relief instruments include:

- ASIC Corporations (Foreign-Controlled Company Reports) Instrument 2017/204 (formerly ASIC Class Order 98/98)<sup>126</sup>
- ASIC Corporations (Wholly-owned Companies) Instrument 2016/785 (formerly ASIC Class Order 98/1418)<sup>127</sup>
- ASIC Corporations (Audit Relief) Instrument 2016/784 (formerly ASIC Class Order 98/1417).<sup>128</sup>

<sup>126</sup> ASIC Corporations (Foreign-Controlled Company Reports) Instrument 2017/204 available at <https://www.legislation.gov.au/Details/F2017L00307>

<sup>127</sup> ASIC Corporations (Wholly-owned Companies) Instrument 2016/785 available at <https://www.legislation.gov.au/Details/F2016C01085>

<sup>128</sup> ASIC Corporations (Audit Relief) Instrument 2016/784 available at <https://www.legislation.gov.au/Details/F2016L01542>

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The ASIC website<sup>129</sup>, ASIC Regulatory Guide 58 “Reporting by registered foreign companies and Australian companies with foreign shareholders”<sup>130</sup> and ASIC Regulatory Guide 115 “Audit relief for proprietary companies”<sup>131</sup> provide further guidance in relation to the requirements for proprietary companies wishing to avail themselves of the relief.

It is important to note that ASIC relief instruments do not exonerate any company from the requirement to prepare or audit financial reports if directed to do so by ASIC<sup>132</sup> or its shareholders.<sup>133</sup> Nor does the relief exempt the company from the requirement to retain financial records.<sup>134</sup>

If the board resolves that the company is eligible to avail itself of relief under a specific ASIC Instrument, it should review the relevant ASIC Instrument at least annually and ensure that the company continues to comply with the ongoing Instrument requirements.

## GOVERNANCE AND INCOME TAX

Directors and advisors should be aware of the ATO's Private Group review programs and be cognisant of the issues that are likely to attract attention. Private groups are becoming a greater focus for the ATO, as they are often confronted by the same issues as larger businesses and corporations however face a host of other issues arising from the private nature of their business and ownership. These issues include the complexities of family dealings and the consequences of employing different ownership structures.

<sup>129</sup> Refer to ASIC, Lodgement of financial report (INFO 31), <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/lodgement-of-financial-reports/>

<sup>130</sup> Refer to ASIC, Regulatory Guide 58, June 2020, Reporting by registered foreign companies and Australian companies with foreign shareholders, <https://download.asic.gov.au/media/5619359/rg-58-published-19-june-2020.pdf>

<sup>131</sup> Refer to ASIC, Regulatory Guide 115, June 2020, Audit relief for proprietary companies, <https://download.asic.gov.au/media/5689855/rg115-published-19-june-2020-20200727.pdf>

<sup>132</sup> Corporations Act 2001, Section 294.

<sup>133</sup> Corporations Act 2001, Section 293.

<sup>134</sup> Corporations Act 2001, Section 286.

The ATO is now devoting significant resources to assuring the taxation and superannuation obligations of private groups. Critical to achieving a ‘justified trust’ rating with the ATO is having a robust tax governance framework in place. Directors should ensure they have clear processes and procedures within a corporate governance framework to support the proprietary company's tax decision making and manage tax and super risks.

Proprietary company directors, like their public company counterparts, are individually personally liable to pay any outstanding liability where a company that they are a director for fails to meet obligations pertaining to pay as you go tax (PAYG), the superannuation guarantee charge and the goods and services tax (GST).

## CROWD-SOURCED FUNDING

Crowd-sourced funding (CSF) is a financial service where start-ups and small businesses raise funds, generally from a large number of investors that invest small amounts of money. A provider of CSF services must hold an Australian Financial Services (AFS) licence.

The Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Act 2018 took effect from 19 October 2018 and makes further changes to the law to extend the CSF regime to eligible proprietary companies. Under the CSF regime, eligible proprietary companies will be able to make offers of their shares, via an intermediary CSF service, using an offer document.<sup>135</sup>

<sup>135</sup> Refer to ASIC, Crowd-sourced funding, <https://asic.gov.au/regulatory-resources/financial-services/crowd-sourced-funding/>

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The Act includes requirements for proprietary companies wishing to use the CSF regime, including that the company must:

- maintain a minimum of two directors
- have their financial reports audited once they raise \$3 million or more from CSF offers
- comply with the existing related party transaction rules that apply to public companies.<sup>136</sup>

There are obligations and investor protections that apply to CSF offers, including:

- an investor cap of \$10,000 per annum per company for retail investors
- the provision of a CSF offer document containing minimum information and a prescribed risk warning
- a five-day cooling-off period.<sup>137</sup>

ASIC's Regulatory Guide 261 "Crowd-sourced funding: Guide for companies" is a guide for companies seeking to raise funds through CSF.<sup>138</sup>

## Useful references

- ASIC information sheet (INFO 183) 'Guide Directors and financial reporting' available at <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>
- ASIC information sheet (INFO 76) 'What books and records should my company keep?' available at <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>

<sup>136</sup> Refer to ASIC, Crowd-sourced funding, <https://asic.gov.au/regulatory-resources/financial-services/crowd-sourced-funding/>

<sup>137</sup> *ibid*

<sup>138</sup> Refer to ASIC, June 2020, Regulatory Guide 261, Crowd-sourced funding: Guide for companies, <https://asic.gov.au/media/5702668/rg261-published-19-june-2020-20200727.pdf>

- ASIC information sheet (INFO 79) 'Your company and the law' available at <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>
- Governance Institute of Australia's 'Difference between private and public company structure under the Corporations Act' chart available on its website (for members only) [www.governanceinstitute.com.au](http://www.governanceinstitute.com.au).
- Corporations Amendment (Proprietary Company Thresholds) Regulations 2019 available at <https://www.legislation.gov.au/Details/F2019L00538>
- Key facts: AASB 2020-2 Amendments to Australian Accounting Standards – Removal of Special Purpose Financial Statements for Certain For-Profit Private Sector Entities [https://www.aasb.gov.au/admin/file/content102/c3/AASB2020-2\\_KeyFacts\\_03-20.pdf](https://www.aasb.gov.au/admin/file/content102/c3/AASB2020-2_KeyFacts_03-20.pdf)
- ATO's Tax governance guide for privately owned groups <https://www.ato.gov.au/Business/Private-ownership-and-wealthy-groups/Tax-governance/Tax-governance-guide-for-privately-owned-groups/>
- Renato Tagiuri and John A Davis, 1 June 1996, Bivalent Attributes of the Family Firm.

## For further information please contact:

**Robyn Langsford****Partner,****Family Business & Private****[rlangsford@kpmg.com.au](mailto:rlangsford@kpmg.com.au)**



# 6. Indigenous Culture

Australian businesses operate on land that is rich with history. Boards have an important role to play in creating policies and culture which not only advance reconciliation and pay respect to First Nations people, but also increase economic equity.

## In this chapter

- Understanding First Nations culture to strengthen governance
- The role of the board in advancing reconciliation and economic equity
- Acknowledgement of Country
- Governance considerations for Indigenous organisations

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Does the organisation have a Reconciliation Action Plan?
2. How does the organisation recognise and celebrate the traditions and culture of the First Nations people of the countries where we operate?
3. Is the board equipped to engage confidently with First Nations' stakeholders?
4. Do directors, executives and staff demonstrate cultural competency?
5. What programs are in place to promote procurement and partnering with Indigenous corporations?
6. Are goals to increase First Nations representation across the workforce being achieved?
7. Has the board considered how governance may need to evolve to better support objectives pertaining to diversity and inclusion with regard to First Nations people?

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Acknowledgements of Country are seldom made and/or are not respectfully delivered.
- Directors display a lack of appreciation for the cultural values of First Nations people.
- The importance of respecting First Nations heritage is not communicated or actively demonstrated by the board or the executive.
- Inability to attract or retain First Nations staff.
- No partnerships or contracts have been established with any Indigenous organisations.

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## UNDERSTANDING FIRST NATIONS CULTURE TO STRENGTHEN GOVERNANCE

The focus of this chapter is twofold.

1. Support directors in incorporating policies and practices which embrace the full richness of Australia's culture and support reconciliation in the organisation.
2. Highlight how governance in Indigenous organisations may be different in certain aspects. There is much to learn from those that came before, especially as the world increases focuses on ESG. Whilst most of the corporate governance frameworks in OECD countries have only relatively recently incorporated aspects of culture, it is observed through the Indigenous Governance Toolkit (described as "an online resource developed for Indigenous nations, communities, individuals and organisations searching for information to build their governance")<sup>139</sup> that Indigenous governance has culture in the centre of how governance is approached.

## THE ROLE OF THE BOARD IN ADVANCING RECONCILIATION AND ECONOMIC EQUITY

The board sets the tone for the organisation through policies created (what it does) but also through words and actions (what it says). Accordingly, the board should be examining how policies (and related key performance indicators) can be adapted to drive necessary change which embraces the culture and heritage of all people connected to where the organisation operates and has an impact. For some organisations this may require a cultural change program to fast track the change required, especially where the organisation wants to be a leader in this area. At a minimum, whole of organisation cultural awareness training to support policies being implemented is considered better practice in building common understanding and appreciation.

<sup>139</sup> Refer to Indigenous Governance Toolkit at <https://toolkit.aigi.com.au/>



### Case Study – Microsoft Australia

Microsoft Australia's Managing Director, Steven Worrall, identified that his staff across Australia would benefit from Arrilla (a majority Indigenous-owned organisation in which KPMG has invested) providing training on how to confidently engage with Indigenous suppliers, stakeholders and businesses. Steven Worrall describes the benefits derived from this training in a video on the KPMG website<sup>140</sup> and, in summary, he states that the training fostered an understanding of Indigenous culture, a sensitivity to diversity, and a greater sense of inclusiveness, as well as decreasing unconscious bias.

Commercially, by breaking down stereotypes about Aboriginal and Torres Strait Islander people and businesses, Microsoft Australia's staff were enabled to more readily engage with Indigenous companies and suppliers. The flow on benefits of this increased economic engagement (e.g. including increased economic activity of Indigenous businesses), will continue to generate positive results across the communities Microsoft works with.

As with any cultural change, unless the board actively engages and is seen to be changing in how it operates, positive sustainable change is unlikely to occur. Ian Hamm (a Yorta Yorta man from Shepparton in central Victoria) spoke at the AICD's 2021 Australian Governance Summit encouraging more diversity in the boardroom to provide a "*better understanding of the social contract*" that organisations are part of.

<sup>140</sup> KPMG, Microsoft Australia: driving Indigenous culture competency in the workplace, <https://home.kpmg/au/en/home/insights/2019/01/microsoft-australia-indigenous-cultural-competency-workplace-client-story.html>

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

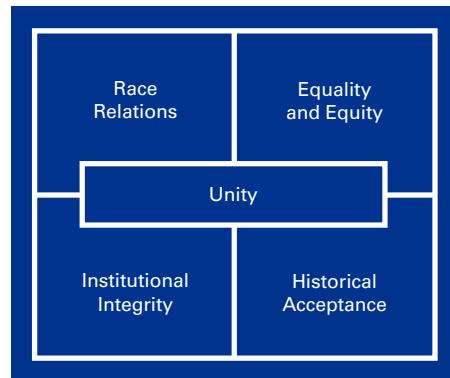
## APPENDICES

## CONTACT US

**Reconciliation**

Supporting reconciliation is one way that leading organisations are delivering on the aforementioned social contract. Reconciliation Australia describe reconciliation as being “about strengthening relationships between Aboriginal and Torres Strait Islander peoples and non-Indigenous peoples, for the benefit of all Australians.”<sup>141</sup>

Reconciliation Australia describe that reconciliation is based (and measured) on the five dimensions shown in the diagram below:



Source: Reconciliation Australia<sup>142</sup>

To bring reconciliation to life within organisations, at the time of writing this, over 1,100 organisations have developed Reconciliation Action Plans (RAPs) to embed the principles and purpose of reconciliation. Connected to ESG objectives, most organisations with RAPs proudly promote this fact, building awareness of the reconciliation imperative whilst also potentially benefiting from the incidental commercial benefit.

Making a decision to pursue a RAP is an investment and the implementation of actions needed may see policies and even potentially strategic objectives needing to be adapted. Accordingly, it would be expected that the decision to develop a RAP would be a matter reserved for the board to decide upon.

<sup>141</sup> Refer to Reconciliation Australia at <https://www.reconciliation.org.au/reconciliation/>

<sup>142</sup> *ibid*

**ACKNOWLEDGEMENT OF COUNTRY**

Acknowledgement of Country stems from the traditions of Australia’s First Nations people who historically would seek permission before entering another’s Country. Those to whom the Country belonged would in turn welcome the visitor to their Country. In the same way as the visitor would respect any customs and traditions of the Country being visited, and give thanks for being allowed to visit, it is considered good practice to include acknowledgment and heartfelt appreciation for a Country and its people at the start of any meeting or event.

Note that only Traditional Owners, or Aboriginal and Torres Strait Islander peoples who have been given permission from Traditional Owners to welcome visitors to their Country can deliver a Welcome to Country.

Reconciliation Australia recommends that the local Aboriginal Land Council or Native Title representative body can advise on organising a Welcome to Country by a Traditional Owner in the area where a gathering is occurring.

Directors should set the example for demonstrating their recognition of the heritage of the land that they are meeting on by consistently ensuring that a meaningful acknowledgement is included at the commencement of all gatherings and that this does not feel like an empty box-ticking exercise. Some organisations provide standard wording to be used in acknowledgements of Country which is one way to ensure a consistent message is delivered. Reconciliation Australia recommends the wording used could include something like the following:

## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

*"I'd like to begin by acknowledging the Traditional Owners of the land on which we meet today. I would also like to pay my respects to Elders past and present."*

or

*"I'd like to begin by acknowledging the Traditional Owners of the land on which we meet today, the (people) of the (nation) and pay my respects to Elders past and present."<sup>143</sup>*

To identify the Traditional Owners of the land that the meeting is occurring on, the map of Indigenous Australia provided by AIATSIS can be consulted.<sup>144</sup>

One way to make the delivery meaningful is to bring any learnings gleaned about the Country and its people into the acknowledgement. This has the added benefit of also educating the audience thereby furthering understanding of culture and heritage.

## GOVERNANCE CONSIDERATIONS FOR INDIGENOUS ORGANISATIONS

It is important to recognise an organisation's governance history and determine how Indigenous governance will be incorporated into its future governance practices. As mentioned before, Aboriginal and Torres Strait Islander people consider culture fundamental to governance. Their cultural values, traditions, rules and beliefs, although they may differ between communities and groups, continue to be fundamental to how they govern themselves. Consideration as to how to embed Indigenous cultural values should be at the forefront of developing and adapting an organisation's governance.

<sup>143</sup> Refer to Reconciliation Australia at <https://www.reconciliation.org.au/acknowledgement-of-country-and-welcome-to-country/#:~:text=An%20Acknowledgement%20of%20Country%20is,Strait%20Islander%20peoples%20to%20Country.&text=Aboriginal%20and%20Torres%20Strait%20Islander%20peoples%20may%20also%20wish%20to,other%20First%20Nations%20peoples%20present>.

<sup>144</sup> Refer to AIATSIS, Map of Indigenous Australia, <https://aiatsis.gov.au/explore/map-indigenous-australia>

## CATSI Act and ORIC

Indigenous groups may benefit from becoming a corporation and a separate legal entity. These groups are able to be incorporated under a Commonwealth, state or territory law depending on the individual circumstances. The Corporations (Aboriginal and Torres Strait Islander) Act 2006 (CATSI Act) allows the Office of the Registrar of Indigenous Corporations (ORIC) to provide regulatory assistance and education. ASIC has set out the key differences between the CATSI Act and the Corporations Act covering members; directors; shares/debentures; types of corporations; financial services limitations; internal governance rules; regulatory assistance; registration requirements; reporting; merits review process; native title and fees <sup>145</sup>, the key ones impacting directors are:

<sup>145</sup> Refer to ASIC, The CATSI Act and the Corporations Act – some differences, <https://download.asic.gov.au/media/4907483/fact-sheet-catsi-act-vs-corp-act.pdf>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

	Corporations Act	CATSI Act
<b>Directors</b>	<ul style="list-style-type: none"> <li>– Any person can be a director; they don't need to be a member.</li> <li>– A proprietary (private) company must have at least one director, but doesn't need to have a secretary. The director and secretary (if there is one), must usually live in Australia.</li> <li>– A public company must have at least three directors and at least one secretary. At least two of the directors and one secretary must usually live in Australia.</li> </ul>	<ul style="list-style-type: none"> <li>– Corporations can have a rule in their rule book that allows people who are not members to be directors. However, the majority of directors must:               <ul style="list-style-type: none"> <li>– be Aboriginal or Torres Strait Islander</li> <li>– be members of the corporation</li> <li>– not be employees of the corporation.</li> </ul> </li> <li>– The minimum number of directors is three and the maximum number is 12. Corporations can apply to the Registrar for an exemption if they want more than 12 directors.</li> <li>– The majority of directors must usually reside in Australia.</li> <li>– Large corporations must have a secretary. Small and medium corporations have a contact person.</li> </ul>
<b>Internal governance rules</b>	A company can follow the replaceable rules in the Corporations Act or adopt their own constitution.	<p>An Aboriginal and Torres Strait Islander corporation must have a rule book which, at a minimum, contains:</p> <ul style="list-style-type: none"> <li>– the objectives and name of the corporation,</li> <li>– frequency of directors' meetings and</li> <li>– a dispute resolution process.</li> </ul> <p>The corporation may adopt the replaceable rules in the CATSI Act or modify or replace them</p>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

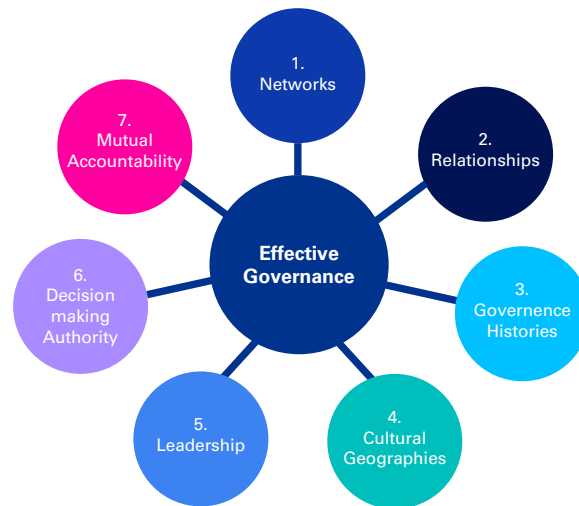
GLOSSARY

APPENDICES

CONTACT US

**Cultural-based governance principles**

The Indigenous Governance Toolkit describes Indigenous governance as “a networked form of governance. It is based on thick pathways and layers of relationships and connections between people, places and things, past, present and future”<sup>146</sup> Based on this, Indigenous people frequently apply the cultural-based principles in the diagram below to design their governance frameworks.



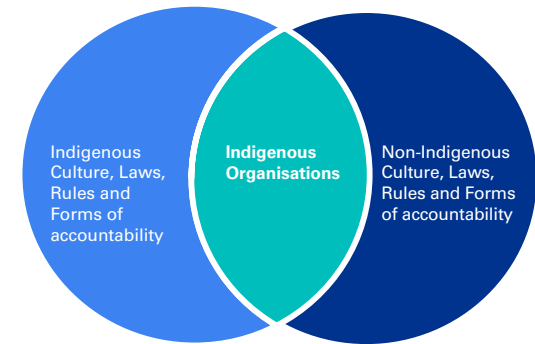
Indigenous Governance Principles in Australia (Source: Indigenous Governance Toolkit<sup>147</sup>)

As decisions are made on the organisation’s governance structure, the board and management should consider the Indigenous traditions and values which are important to them and use these principles to reflect priorities.

<sup>146</sup> Refer to Indigenous Governance Toolkit, <https://toolkit.aigi.com.au/toolkit/2-1-indigenous-governance-and-culture>

<sup>147</sup> Ibid

As the diagram below illustrates, the Indigenous Governance Toolkit recognises that Indigenous organisations are required to find a way for the governance framework to integrate both internal requirements (the rules that govern their networks and communities) and external requirements (the rules that govern the external stakeholders which support their community or organisation).



The Two-Way Accountability of Indigenous Organisations And Governing Bodies (Source: Indigenous Governance Toolkit<sup>148</sup>)

This is achieved by creating governance structures which are innovative and robust to cater for the two systems of governance. Equally there are benefits for non-indigenous organisations to consider how their frameworks may need to flex to work better with Indigenous organisations.

<sup>148</sup> Ibid



## FOREWORD

## • THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- Ted Talk on delivering an Acknowledgement of Country that really means something, Shelley Reys AO [https://www.youtube.com/watch?v=zxo18\\_7BDt4](https://www.youtube.com/watch?v=zxo18_7BDt4)
- Indigenous Governance Toolkit, <https://toolkit.aigi.com.au/> (1)
- Office of the Registrar of Indigenous Corporations, <https://www.oric.gov.au/> (2)

For further information please contact:



**Glen Brennan**

**Partner, Indigenous Services**  
**KPMG Enterprise**  
**[glenbrennan@kpmg.com.au](mailto:glenbrennan@kpmg.com.au)**

# Governance Accountability

---

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 7. Accountability to Shareholders

Listed public companies are often jointly owned by a relatively large number of separate shareholders, including both individual and institutional shareholders. Individual shareholders (and potential shareholders) have different investment objectives, which are based on varying degrees of financial and commercial understanding, literacy, competency and market intelligence.

## In this chapter

- Protecting shareholders' rights
- The board's role
- Shareholders' responsibilities
- The directors' role in investor relations
- Institutional shareholders' role in governance
- Effective Annual General Meetings (AGMs)
- Statutory reporting
- Statutory reporting content
- Annual Report
- Directors' report
- Directors' declaration
- Auditor's report
- Other disclosures in the annual report
- Concise version of annual reports
- Half-year reports
- Audit
- Audit committee
- Continuous disclosure
- Investor decision-making
- The board's role in business reporting

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

- **GOVERNANCE ACCOUNTABILITY**

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Does the chair and directors play an active role in the investor relations program?
2. Are mechanisms in place to capture market intelligence and investor feedback? This may include social media as a dynamic new data source.
3. Is the chair always well prepared for questions from the floor at the Annual General Meeting (AGM)?
4. Are there sufficient skills and experience amongst audit committee members to effectively review statutory reporting obligations?
5. Does the board have a process to ensure that all statutory reporting obligations are met in a timely manner?
6. Is there a continuous disclosure policy approved by the board and linked to the spokesperson policy?
7. Does the board regularly review the effectiveness of its business reporting and communication in assisting investor decision-making?
8. Is the reporting and communication strategy/ investor relations strategy part of the annual strategy development program?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

- **GOVERNANCE ACCOUNTABILITY**

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board is not aware of the identity or views of major investors.
- Major marketplace concern regarding executive remuneration incentives.
- The AGM is a major public relations challenge.
- There is no social media policy, monitoring or escalation procedures for unfavourable events.
- The investor relations manager has no contact with the board.
- There is no strategy of how to handle private equity approaches.
- Institutional investors publicly voice concerns regarding some of the organisation's governance practices.
- The ASX expresses concern regarding the timeliness of the organisation's market disclosures.
- The organisation's business model is not clearly articulated in external communications.
- The linkage between financial and non-financial reporting is not evident in external communications.
- A significant protest vote against the company's remuneration report.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The notion of accountability to shareholders is at the core of any corporate governance framework. Shareholders are certainly becoming more active in asserting their rights and many boards are responding by trying to engage with their shareholders more effectively. Nevertheless boards must balance the equitable treatment of shareholders and the protection of their rights against the need to create sustainable shareholder value.

## PROTECTING SHAREHOLDERS' RIGHTS

A basic principle of corporate governance is that it should protect shareholders' rights. These rights typically relate to, but are not limited to:

- Declaring dividends in the best interests of shareholders.
- Receiving information pursuant to the company's continuous disclosure obligations.
- Approving changes to the company's constitution, articles of association or similar governing documents.
- Nominating and appointing directors.
- Receiving continuous disclosure of material developments in the company's affairs.
- Calling a general meeting of shareholders, and/or proposing a resolution to be considered at a general meeting.
- Voting at the AGM.
- Obtaining an independent valuation of their securities.
- Inspecting the minute books for members' meetings.
- Suing the corporation for wrongful acts.

## THE BOARD'S ROLE

Governance authorities suggest there are some key board roles in protecting shareholders rights. These include:

- Maintaining a detailed understanding of shareholders' rights that are set out in the Corporations Act, the ASX Listing Rules and other relevant legislation, together with the company's constitution and board policies.
- Maintaining up-to-date knowledge of the company's nominee shareholders and, to the extent possible, their underlying beneficial shareholders.
- Ensuring shareholder communication is open and transparent.
- Ensuring debate on contentious issues is embraced and prepared for.
- Implementation of shareholder proposals approved by a majority of votes/proxies cast at a general meeting.

## SHAREHOLDERS' RESPONSIBILITIES

Shareholders have different investment objectives; some invest for short-term gain, some for long-term value and others for socially responsible reasons. Companies with an effective approach to investor relations will understand the objectives of different investor groups and key individual investors. Communication and active engagement with shareholders generate feedback on investor concerns. Certain shareholders, particularly some institutional shareholders, are becoming more assertive in protecting their own rights and are taking various measures to influence the companies in which they invest. These measures include:

- Communicating with the company openly and transparently.
- Adopting a clear, comprehensive and pragmatic view of what constitutes good corporate governance.
- Understanding and monitoring company performance and providing feedback to the company.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- Teaming with like-minded shareholders to exert a collective influence.
- Lobbying and targeted activism.
- Engaging with the company's board in times of crisis, or with regard to major transactions, such as takeovers, mergers and private equity approaches, and capital raisings.
- Adopting consistent positions, where appropriate, on particular issues and voting accordingly.
- Publishing governance guidelines.



## Case Study - ASIC v Healey [2011] FCA 717 (Centro)

The directors of Centro companies signed-off on financial reports with material errors; classifying short-term liabilities as long-term liabilities. The Federal Court found that in approving the financial statements, the directors had failed to discharge their duties with due care and diligence under sections 180(1), 344 and 601FD of the Corporations Act. The Centro decision reaffirms that whilst directors are not expected to possess specialist financial or accounting expertise, or to be involved in the day-to-day management of the company, they are expected to have the necessary level of competence to read and understand financial statements. Directors must independently and critically examine the accuracy and content of financial reports in the context of their knowledge of the company's affairs and activities, and cannot abrogate their responsibilities by placing sole reliance on management or external advisers, no matter how competent they appear to be.

Another case that has reinforced the behaviour expected of directors is the James Hardie case of *ASIC v Hellicar*.



## Case Study – ASIC v Hellicar [2012] 247 CLR 345 (James Hardie)

The non-executive directors approved a misleading announcement on the ASX that stated the company had fully funded its liabilities that related to asbestos disease when, in actual fact, there was a funding shortfall. The High Court held that the directors of James Hardie had contravened their duties of care.

## Shareholders convening meetings

Section 249D of the *Corporations Act 2001 (Corporations Act)* requires directors of a company to call and arrange to hold a general meeting at the request of members with at least 5 percent of the votes that may be cast at a general meeting. In addition, if members with at least 5 percent of the votes that may be cast at a general meeting call and arrange to hold a general meeting, then those members who called the meeting must pay the expenses in relation to calling and holding the meeting.<sup>149</sup>



## Case Study – Woolworths Ltd v Getup Ltd [2012] FCA 726; 90 ACSR 670

210 members requested the directors of Woolworths call a general meeting in order to put forward a special resolution to change its constitution to prevent ownership of poker machines. Woolworths requested an injunction for the meeting be held at the AGM as the meeting would have led to the incurrence of an additional \$400,000 in expenses. The Court did not consider a deferral to lead to substantial injustice and allowed Woolworths to defer the requisitioned meeting until its next AGM.

<sup>149</sup> Corporations Act 2001, Section 249F.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Shareholder and political activists have used the calling of general meetings as a platform to help promote political and social responsibility, notwithstanding the proposed resolutions might have a very low prospect of success or do not seek to maximise shareholder returns.

### Remuneration and the two-strikes rule as a vehicle for shareholder activism

There has been a substantial increase in shareholder voting against remuneration reports for ASX300 companies with the last three years' results as follows:

- 2018 – 20 companies (6.7 percent)
- 2019 – 24 companies (8.0 percent)
- 2020 – 25 companies (8.3 percent)

These votes are made not only as a means of signaling dissatisfaction with remuneration amounts or structures, but also to indicate shareholder expectations of the company's financial performance, governance and compliance have not been met.

Under the Corporations Act, the directors of a company are to be paid the remuneration that the company determines by resolution.<sup>150</sup> However, for public companies director remuneration does not require member approval if it is reasonable.<sup>151</sup>

Voting against a publicly-listed company's remuneration report has been a relatively recent encroachment that was prompted when the two-strike rule was brought about in 2011. Put simply, all directors can potentially face re-election without a resolution being held under Section 203D of the Corporations Act.<sup>152</sup> Under the two-strikes rule, when more than 25 percent of shareholders vote against the remuneration report for two consecutive years at the AGM, a 'spill motion' will be put to the company to spill the positions of all directors.

<sup>150</sup> Corporations Act 2001, Section 202A(1) (replaceable rule).

<sup>151</sup> Corporations Act 2001, Section 211

<sup>152</sup> Corporations Act 2001, Section 203D.

That is, all positions vacated and a vote cast on whether to reappoint the board within 90 days.<sup>153</sup>

The two-strikes rule functions as a vehicle for shareholders to express their disapproval of directors' remuneration via the introduction of a 'spill meeting'.<sup>154</sup> More broadly, it is a mechanism that activist shareholders can draw upon to indicate general discontent with the board and its performance. As part of the aftermath of the Royal Commission into the Misconduct in the Banking, Superannuation and Financial Services Industry, several Australian financial services firms received a 'first strike' against their remuneration report. Prior to this, the 50 percent vote against Commonwealth Bank's report in 2016 was the historical record for an ASX100 company. However, this was surpassed by AMP in 2018 with a 61 percent vote against its remuneration report,<sup>155</sup> Westpac with 64 percent<sup>156</sup> and NAB with 88 percent.<sup>157</sup> This activism garnered immediate action by many companies to overhaul their remuneration schemes and governance. See Myer Case study below.

<sup>153</sup> Note also the restrictions that apply under sections 200-200J of the Corporations Act to termination payments by companies incorporated in Australia (and their associates) to those who hold a managerial or executive office in the company or in a related body corporate.

<sup>154</sup> Corporations Act, Sections 250U-250Y. Under that rule, if 25% of the votes cast at two consecutive AGMs oppose the adoption of the remuneration report, then at the second AGM, shareholders can require that the board stand for re-election at a further general meeting to be held within 90 days. Shareholders can exercise this power if 50% or more of votes cast at the second AGM are in favour of a "spill". The requirement to stand for re-election does not apply to the managing director or any director appointed since the remuneration report was approved by the board.

<sup>155</sup> Alice Uribe, 'AMP shareholders deliver historic first strike against AMP', The Australian Financial Review (Online), 10 March 2018 <<https://www.afr.com/business/banking-and-finance/amp-shareholders-deliver-historic-first-strike-against-amp-20180510-h0zvki>>

<sup>156</sup> Stephen Chalmers and Michael Janda, 'Westpac shareholders hit bank with first strike against executive pay', ABC News (Online), 12 December 2018 <<https://www.abc.net.au/news/2018-12-12/westpac-shareholders-hit-bank-with-first-strike/10610882>>.

<sup>157</sup> Stephen Bartholomeusz, 'Banker's pay: There can only be one winner in this battle', The Sydney Morning Herald (Online), 27 March 2019 <<https://www.smh.com.au/business/banking-and-finance/banker-s-pay-there-can-only-be-one-winner-in-this-battle-20190327-p517zq.html>>.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US



## Case Study – Myer

In late 2021, the board of directors of Myer narrowly avoided a board spill as their largest shareholder, Solomon Lew, who had a 15.7 percent stake joined with other shareholders to vote against the company's remuneration report (37 percent against) for the second consecutive time resulting in a spill motion. However, the spill motion did not receive majority support meaning that the board were saved from having to stand for re-election.

As reported in The Sydney Morning Herald, Mr Lew had increased his shareholding earlier in the year with the intention of using his shareholding to drive a restructure of the board.

It is worth noting however that as reported in Minter Ellison's report on the 2020 AGM season declares, "The lack of appetite to spill a board since the introduction of the 'two-strikes' rule highlights the importance of board stability to shareholders."<sup>158</sup>

## THE DIRECTORS' ROLE IN INVESTOR RELATIONS

The board's role in formal investor relations continues to evolve. Many non-executive directors are now seeking to become more active in their companies' investor relations programs.

The investor relations function continues to increase in strategic importance. Investor relations teams have increasingly become responsible for communications, not only with the investment community, but also with internal stakeholders such as the board of directors, management and employees, by becoming responsible for, or at least influencing, coherent company messaging.

<sup>158</sup> MinterEllison, February 2021, Key trends to emerge from the 2020 AGM season, <https://www.minterellison.com/articles/key-trends-to-emerge-from-the-2020-agm-season>

Boards are exposed to a number of risks if their organisation has inadequate investor relations expertise; regulatory risk (continuous disclosure and class actions), poor/lack of communication of strategy and performance to investors, and expectation for information to be publicly available in liquid markets for accuracy of share price valuation. Large companies operate in multiple dynamic, volatile markets and jurisdictions, with diverse investors with different goals requiring different communication strategies. Additionally, the risk of misleading and deceptive information being publicised on social media heightens companies' obligations to meticulously inspect their sources of information and make proper corrections. Boards need to understand their shareholders and shareholder segments, communicate their strategy appropriately, its performance and ESG activities and ensure the strategy is aligned to the company's best interests (being the interests of their shareholders as a whole).

At a minimum, and in conjunction with the board chair's traditional investor relations responsibilities, the board should approve any policies that control investor relations engagement risks. The board should also provide input into, and approve, the investor relations strategy as well as regularly monitoring investor relations activities. This strategy typically addresses an organisation's approach, performance targets and accountabilities for:

- shareholder and key stakeholder analysis and engagement planning
- shareholder services (including share registry and transactional support)
- investor targeting initiatives
- shareholder and key stakeholder communications
- media and public relations initiatives (including brand and reputation management)
- market intelligence and feedback mechanisms.

The ASX has recently begun to focus more on producing investor relations tools for ASX listed companies.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## INSTITUTIONAL SHAREHOLDERS' ROLE IN GOVERNANCE

Several sets of best practice principles have been published, addressing the responsibilities of institutional investors. One such example includes the International Corporate Governance Network's (ICGN) *Statement of Principles on Institutional Investor Responsibilities*,<sup>159</sup> which sets out its view of the responsibilities of institutional investors in relation to their external role as shareholders and also in relation to internal governance. With respect to voting responsibilities, the ICGN suggests that institutional investors should:

- disclose an annual summary of their voting records, together with their full voting records in important cases
- seek to reach a clear decision, in favour or against, for each resolution on which they are expected to
- disclose details of any outsourcing of ownership responsibilities (including the names of agents to whom they have outsourced, together with a description of the nature and extent of outsourcing and how it is regularly monitored).

*Asset Owner Stewardship Code*

The Australian Council of Superannuation Investors (ACSI) released the Australian Asset Owner Stewardship Code on 17 May 2018.<sup>160</sup> It is the first guidance developed specifically for Australian asset owners in their role as equity holders in Australian-listed companies. The Code was established to increase the transparency and accountability of asset owners (including superannuation funds, endowments and sovereign wealth funds) when exercising their ownership rights in order to uphold value creation in their investments and ultimately protect and boost long-term investment performance for their beneficiaries.

<sup>159</sup> International Corporate Governance Network (ICGN), *Statement of Principles for Institutional Investor Responsibilities*, September 2013

<sup>160</sup> Australian Council of Superannuation Investors (ACSI), *Australian Asset Owner Stewardship Code* (2018). <https://acsi.org.au/wp-content/uploads/2021/10/ASSET-OWNER-CODE-stewardship.pdf> stewardship.pdf

Signatories to the Code are required to disclose details of essential stewardship activities including: voting, engagement, policy advocacy and the selection, appointment and monitoring of external asset managers. The disclosure requirement holds asset owners responsible for active ownership that will take into account ESG risks and opportunities, drive direct and collaborative engagement with investees and demonstrate awareness commitment to macroeconomic and regulatory issues.

## EFFECTIVE AGMS

AGMs are governed by the Corporations Act (Part 2G.2), the company's constitution and common law. In the case of meetings of listed companies public companies must hold an AGM of shareholders.<sup>161</sup>

For many public companies the AGM is a major exercise in shareholder communication and investor relations. The AGM offers shareholders a unique opportunity to question the board, express their views on company performance and suggest changes to company governance and operations.

As well as a forum for communication and discussion, the business of the AGM primarily considers the financial report and auditor's report, together with resolutions to approve the directors' report, and an advisory resolution for adoption of the remuneration report<sup>162</sup>, and may include consideration of the appointment and remuneration of the auditor and the election of directors.<sup>163</sup> Where the business of the meeting relates to the election (or re-election) of directors, shareholders will expect those directors to address them at the meeting.

Recommendation 9.3 of the ASX Principles also recommends that an external auditor attend the AGM and is available to answer questions from security holders at the meeting.

<sup>161</sup> Corporations Act, Section 250N.

<sup>162</sup> Corporations Act, Section 250R(1) and (2).

<sup>163</sup> Corporations Act, Section 250R

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The following are some key considerations for AGMs:

- A hostile AGM is rarely the result of spontaneous combustion. Boards in touch with shareholder concerns will anticipate and embrace debate on contentious issues.
- Boards and management should spend time trying to anticipate specific shareholder questions and develop appropriate responses. Speakers should be identified in advance to respond to specific issues.
- Difficult or contentious questions can sometimes be short-circuited by raising and answering them in the annual report, or in the formal chair's address to the meeting.
- Shareholders can be invited to submit questions prior to the AGM.
- Shareholders should be able to access a webcast of the meeting; this is generally done by ASX 50 Companies.
- The chair should be thoroughly familiar with the AGM agenda and meeting procedures, and have developed an approach for dealing with difficult or hostile 'responses' from the floor of the meeting.
- The chair must allow a reasonable opportunity for members to ask questions about or make comments on the management of the company.<sup>164</sup>

Under certain circumstances, shareholders can also compel directors to call extraordinary general meetings of shareholders,<sup>165</sup> or seek to have resolutions added to the meeting agenda.<sup>166</sup>

In response to a request from the Government for advice on the role of the AGM, in September 2012, the Corporations and Markets Advisory Committee (CAMAC) released a discussion paper entitled *The AGM and Shareholder Engagement*. Over 35 submissions were received in relation to this review and an updated version was released in December 2012.

<sup>164</sup> Corporations Act, Section 250S.

<sup>165</sup> Corporations Act, Section 249D.

<sup>166</sup> Corporations Act, Section 249N.

The updated paper provides useful guidance on shareholder engagement (including the regulation of proxy advisers), the purpose and format of the annual report, and the function and format of the AGM.<sup>167</sup>

COVID-19 disrupted businesses in many ways but one such disruption was the ability to hold AGM in an environment where people were not able to gather in large groups. Temporary measures introduced to overcome this obstacle were made permanent in February 2022 with the Corporations Amendment (Meetings and Documents) Bill 2021 passing through Parliament. In addition to enabling the use of technology to distribute and execute documents, this Bill allows for AGMs to be conducted physically and virtually (if permitted by the entity's constitution) as well as applying a hybrid approach of both physical and virtual.

An important factor in making use of technology for virtual or hybrid meetings is that all shareholders continue to have the equivalent opportunity to participate that they would experience were they attending the meeting physically. To this end, ASIC has provided guidance on how questions and voting (polls to be used rather than a show of hands) should be handled, how to support investors in accessing the meeting virtually and also what to do when technical problems arise.<sup>168</sup>

Given that questions will now be able to be asked in writing via technology platforms utilised for the meetings, it is a positive step forward for inclusion of a cohort of the investor population who previously may have remained unheard in such forums.

<sup>167</sup> Corporations and Markets Advisory Committee, 'The AGM and Shareholder Engagement', September 2019, [http://www.camac.gov.au/camac/camac.nsf/byheadline/pdfdiscussion+papers/\\$file/agm.pdf](http://www.camac.gov.au/camac/camac.nsf/byheadline/pdfdiscussion+papers/$file/agm.pdf)

<sup>168</sup> Refer to ASIC, August 2021, ASIC guidelines for investor meetings using virtual technology, <https://asic.gov.au/about-asic/news-centre/news-items/asic-guidelines-for-investor-meetings-using-virtual-technology/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## STATUTORY REPORTING

Shareholder and investor communication starts with statutory reporting. For ASX listed companies in Australia, statutory reporting is based on:

- The Corporations Act and Corporations Regulations.
- Australian Accounting Standards, including interpretations (based on International Financial Reporting Standards (IFRS® Standards) issued by the Australian Accounting Standards Board (AASB)).
- ASIC Legislative Instruments that apply to the organisation.
- ASX Listing Rules.
- ASX Corporate Governance Principles and Recommendations 4<sup>th</sup> Edition.

The key elements of the statutory reporting portfolio for listed companies include:

- A half-year report, a preliminary final report and an annual audited financial report and directors' report (including the remuneration report).<sup>169</sup>
- An annual Corporate Governance Statement and accompanying Appendix 4G.<sup>170</sup>
- Notices for AGM.<sup>171</sup>
- Additional disclosure requirements involving takeovers and new share issues.

<sup>169</sup> See Chapter 2M of the Corporations Act and Chapter 4 of the ASX Listing Rules as to the content requirements of the half-year, preliminary final and annual reports. ASX also requires quarterly reports in certain circumstances (for instance, for mining companies or where a company has been listed under the 'assets test' requirement that half or more its total tangible assets are cash or readily convertible to cash) – ASX Listing Rule 4.7B

<sup>170</sup> ASX Listing Rule 4.7.3, 4.7.4 and 4.10.3

<sup>171</sup> Including notices of meeting (Corporations Act, Section 249J-L) and notices of resolutions (Corporations Act, Section 249O).

Whilst it is common practice for the board to allocate the oversight of statutory reporting to its audit committee, or equivalent, it is unable to abrogate its ultimate responsibility for the accurate and thorough preparation and timely release of statutory reports. Consequently, all directors need to understand not only the content of the reports, but what reports are required and by which authorities.

ASIC guidance suggests if directors take on a role with special responsibilities, such as the chair of an audit committee or the role of an executive director, you must discharge the increased responsibilities expected of directors in such positions with appropriate care and diligence.<sup>172</sup>

Boards need to exercise appropriate due diligence in matters of financial disclosure. False or misleading statements could leave directors personally liable under the Corporations Act, the ASIC Act and Australian Consumer Law.

Boards should also insist that effective systems are in place to ensure all formal shareholder and investor communications (including financial reports):

- Result from a designated approvals process.
- Include all the information required by the relevant laws and standards.
- Adhere to statutory timing requirements.
- Follow the format prescribed by the relevant laws and standards.
- Produce information that is accurate and not false or misleading (including by way of omission).

Some companies may also have reporting requirements to overseas regulators. For example, the US Securities and Exchange Commission (SEC) requires foreign registrants to file a number of reports and documents, including the comprehensive Form 20-F Annual Report of a Foreign Private Issuer.

<sup>172</sup> Refer to ASIC, Information Sheet 183 (INFO 183), Directors and Financial Reporting, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Unless members specifically elect to receive a hard or electronic copy of the annual financial report, companies or schemes can provide the annual financial report (or concise report) to its members by making it readily accessible on a website and by directly notifying members in writing that it has done so.<sup>173</sup>

### ASX Corporate Governance Principles and Recommendations (4th Edition)

The changes in the 4th Edition of the ASX Corporate Governance Principles and Recommendations primarily focused on culture, values and trust.

Principle 8.2 specifically addresses disclosure of remuneration policies and practices for directors; both executive and non-executive, and other senior executives.

In addition, the modification of Recommendation 4.3 in this edition shifted from ensuring validation of the financial reports to allowing investors to be satisfied about the integrity of a wider-ranging suite of information that they may use for their investment decisions. The recommendation is thus that “a listed entity should disclose its process to verify the integrity of any periodic corporate report it releases to the market that is not audited or reviewed by an external auditor.”<sup>174</sup> “Periodic corporate report” is defined in the glossary as “an entity’s annual directors’ report, annual and half yearly annual statements, quarterly activity report, quarterly cash flow report, integrated report, sustainability report, or similar periodic report prepared for the benefit of investors.”

### STATUTORY REPORTING CONTENT

Detailed guidance on the contents of the financial statements and notes to the financial statements can be obtained from KPMG’s Financial Reporting Centre.<sup>175</sup>

<sup>173</sup> Corporations Act, Section 314(1AA).

<sup>174</sup> ASX Corporate Governance Council, ASX Corporate Governance Principles and Recommendations (2019), 4th Edition.

<sup>175</sup> Refer to KPMG, Financial Reporting Centre, <https://home.kpmg/au/en/home/insights/2021/03/financial-reporting-centre.html>

## ANNUAL REPORT

Depending on the entity’s structure and jurisdiction, there are varying reporting requirements that must be adhered to. Directors should be aware of the reporting requirements and obligations applicable to the jurisdiction in which they operate. For example, a publicly listed entity in Australia is required to adhere to the statutory reporting requirements outlined in the previous section and any other applicable legislation relating to the entity type. For this reason, the contents of an annual report should include, at a minimum:

- Full set of financial statements, as defined by AASB 101, including the statement of financial position, statement of profit and loss and other comprehensive income, statement of cash flows, statement of changes in equity and explanatory notes.
- Directors’ report (including the remuneration report).
- Directors’ declaration.
- Auditor’s report and independence declaration.
- Corporate governance statement (listed entities have the option of making disclosures on their website or within the annual report. If an entity includes its corporate governance statement on its website; it must lodge a copy of the statement with ASX to have a permanent record as its effective date each year (listing rule 4.74). Also, the annual report must include the website address where the corporate governance statement can be located.)

Increasingly, however, companies are choosing to include additional material in their annual reports. Emerging areas of optional reporting include sustainability, diversity, corporate citizenship and global taxation summaries, which are being used to not only satisfy stakeholder demands for extra information, but also as a proactive step in the stakeholder management process.

*ASIC Regulatory Guide 230 – Disclosing non-IFRS financial information* outlines financial information presented other than in accordance with accounting standards (i.e. non-IFRS financial information) and sets out guidance on how to use “underlying profit” and other non-statutory financial information disclosure.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DIRECTORS' REPORT

The directors must prepare a directors' report made in accordance with a resolution of the directors, which is signed by a director.<sup>176</sup>

The directors' report requirements are dependent on the nature of the company.<sup>177</sup> The required reporting obligations will vary for companies which are listed, limited by guarantee, large proprietaries and listed or unlisted registered schemes.

For listed entities, the annual remuneration report must be included in the directors' report, detailing the remuneration arrangements, payments and policies for directors and other key management personnel.<sup>178</sup> The remuneration report is subject to a non-binding advisory vote at the AGM by shareholders, however, there are consequences of an 'against' vote on the remuneration report following the introduction of the 'two strikes' rule in 2011. This gives shareholders a right to vote on a board spill resolution if 25 percent or more of 'no' votes are recorded against the company's remuneration report in two successive AGMs. Generally, information that would unreasonably prejudice the company need not be disclosed in the directors' report (although if material is omitted, the report must say so).<sup>179</sup> When considering if the unreasonable prejudice exemption is available, directors should refer to ASIC's *Regulatory Guide 247 – Effective disclosure in an operating and financial review*.<sup>180</sup>

Amongst other disclosures, a listed entity must give details of its operations, financial position, business strategies and prospects for future financial years. ASIC's *Regulatory Guide 247 – Effective disclosure in an operating and financial review* sets out guidelines for these disclosures.<sup>181</sup>

<sup>176</sup> Corporations Act, Section 298.

<sup>177</sup> Corporations Act, Section 300A – regarding specific information to be provided by listed companies.

<sup>178</sup> Corporations Act, Section 300A.

<sup>179</sup> Corporations Act, Section 299(3).

<sup>180</sup> ASIC, 2019, *Regulatory Guide 247 (RG 247) – Effective disclosure in an operating and financial review*, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-247-effective-disclosure-in-an-operating-and-financial-review/>

<sup>181</sup> Ibid

## DIRECTORS' DECLARATION

The directors' declaration<sup>182</sup> should include a solvency statement and mention of whether the financial statements and notes have been prepared in accordance with the Australian Accounting Standards, International Financial Reporting Standards, the Corporations Act, and provide a true and fair view of the financial performance of the entity for that reporting year. For listed entities, a resolution must be passed by the directors before the declaration is signed by a director (most commonly the chairman). Before the declaration is made, both the CEO and CFO must also give a declaration<sup>183</sup> regarding the veracity of the financial statements and notes and, in accordance with Recommendation 4.2 of the ASX Principles, certify that in their opinion it has been formed on the basis of a sound system of risk management and internal control which is operating effectively. The ASX Principles also extend this obligation of CEOs and CFOs to the financial statements for any period, not just the financial year.

When forming its opinion on the solvency of the company for the directors' declaration, a board is obliged to consider the debts of the company as at the date of the statement, not merely those debts included in the balance sheet as at balance date. ASIC believes the directors' declaration should contain a prospective element encompassing expected future debts that will compete for payment with existing debts. For this reason, directors should obtain all relevant information so that they can form an opinion about the company's solvency.<sup>184</sup>

The basis of a board's resolution on solvency should be minuted. If all directors do not support the resolution, the resolution should indicate this fact. Those dissenting from the resolution should be identified and their reasons stated. A board may qualify its statement. This could occur, for example, if there is a material uncertainty about the company's ability to renegotiate loans for repayment.

<sup>182</sup> Corporations Act, Section 295(4).

<sup>183</sup> Corporations Act, Section 295A.

<sup>184</sup> ASIC, 1992, *Regulatory Guide 22 (RG22) – Directors' statement as to solvency*, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-22-directors-statement-as-to-solvency/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A qualified statement will not of itself limit the liability of directors, nor will it operate as a substitute for the proper discharge of their duties.

When a holding company wants to take advantage of the ASIC legislative instrument giving accounts and audit relief to wholly-owned subsidiaries, the directors of the holding company must consider the solvency of the entire group of companies subject to the class order, not just that of the holding company.<sup>185</sup>

## AUDITOR'S REPORT

An auditor must report to members on whether the auditor is of the opinion that the financial report is in accordance with the Corporations Act, including compliance with Australian Accounting Standards and International Financial Reporting Standards, and that the financial report provides a true and fair view of the financial position and performance for the financial year.<sup>186</sup>

The auditor's report must also describe any defect or irregularity in the financial report and any deficiency, failure or shortcoming relating to:

- obtaining all information, explanations and assistance necessary for the conduct of the audit
- keeping sufficient financial records to enable a financial report to be prepared and audited
- keeping other records and registers required by law.<sup>187</sup>

The auditor must also provide the directors with a written declaration as to the auditor's independence.<sup>188</sup> Most commonly, this declaration is carried over to the annual report for inclusion within the directors' report.

<sup>185</sup> ASIC, relief for wholly-owned entities under ASIC Corporations (Wholly-owned Companies) Instrument 2016/785, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/relief-from-corporate-finance-provisions/relief-for-wholly-owned-entities-under-asic-corporations-wholly-owned-companies-instrument-2016-785/>

<sup>186</sup> Corporations Act, Section 308.

<sup>187</sup> Corporations Act 2001, Section 307B and Section 308(3).

<sup>188</sup> Corporations Act 2001, Section 307C.

For general purpose financial reports of listed entities, the auditor's report describes key audit matters. Key audit matters are those matters that, in the auditor's professional judgement, were of most significance in the audit of the financial report of the current period. Key audit matters are selected from matters communicated with those charged with governance.

## OTHER DISCLOSURES IN THE ANNUAL REPORT

The ASX Listing Rules require listed entities to produce a corporate governance statement which describes the extent to which an entity has followed the recommendations set out in the ASX Principles during the relevant reporting period.<sup>189</sup> The ASX Principles are not prescriptive, but a company that does not follow the recommendations must explain why, on an 'if not, why not' (or 'report or explain') basis. A company can publish its corporate governance statement in its annual report or provide a link to where the statement is located, or otherwise provide a separate copy of its corporate governance statement to the ASX at the same time that it provides its annual report.<sup>190</sup> In addition to providing its corporate governance statement (whether in the annual report or otherwise), a listed entity must also provide an Appendix 4G at the same time as it provides its annual report. The Appendix 4G serves a dual purpose. It acts as a key designed to assist readers to locate the governance disclosures made by a listed entity in its corporate governance statement and also acts as a verification tool for listed entities to confirm they have met the disclosure requirements of ASX Listing Rule 4.10.3.<sup>191</sup> In addition to statutory disclosures, many companies include additional information in their annual reports, such as overviews of business strategies and key drivers, and non-financial performance measures, and they convey these areas using snapshots, charts, artwork and photographs. Whilst often published under a separate report, many organisations are moving towards using the annual report to disclose their ESG achievements and compliance record, and to report on ESG initiatives.

<sup>189</sup> ASX Listing Rule 4.10.3.

<sup>190</sup> ASX Listing Rule 4.7.4.

<sup>191</sup> ASX Listing Rule 4.7.4, See also ASX Guidance Note 9: *Disclosure of Corporate Governance Practices*, paragraph 8: The Requirement for an Appendix 4G.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

In approving the content and format of annual reports, boards should keep in mind the following points:

- as far as directors are concerned, the annual financial reporting parts of annual reports are legal documents<sup>192</sup> – compliance with the legal requirements remains a key consideration for any board
- awareness of annual reporting 'best practice' for the nature and extent of disclosure, and for the presentation of information
- good reports usually incorporate a straightforward, logical and accurate account of the company's performance, together with a simple explanation of how the company intends to tackle the opportunities and problems confronting it
- whether it is more suitable to make the annual report readily available online or to distribute hard copies to shareholders.

In considering what additional disclosures may be appropriate, directors should refer to ASIC's *Regulatory Guide 230 – Disclosing non-IFRS financial information*.

The auditor's responsibilities with regard to other financial or non-financial information (other than the financial report and the auditor's report thereon) included in an entity's annual report are to read this other information and consider whether there is a material inconsistency between this other information and the financial report and the auditor's knowledge obtained in the audit.

## CONCISE VERSION OF ANNUAL REPORTS

The Corporations Act permits all companies to distribute to shareholders 'concise versions' of their annual reports.<sup>193</sup> The concise report must be prepared in accordance with AASB 1039 Concise Financial Reports, and must contain some discussion and analysis of the position and results of the company to accompany the concise financial statements. The concise report must be audited and a full report must be provided to members if they request it.<sup>194</sup>

<sup>192</sup> Corporations Act 2001, s 295–300.

<sup>193</sup> Corporations Act, Section 314(1)(b) and Section 314(2).

<sup>194</sup> Corporations Act, Section 314.

This form of delivery is less common due to the availability of critical reports on the company website.

## HALF-YEAR REPORTS

A disclosing entity must prepare a financial report and directors' report for each half-year and have the financial report audited or reviewed.<sup>195</sup>

The half-year report may be either reviewed or audited, although in Australia a half-year report would only be audited in exceptional circumstances. Accordingly, the level of assurance provided by the auditor is dependent on the directors' choice.

	Half-year review	Half-year audit
Level of assurance	Limited	Reasonable
Scope of work completed	Lower	Higher
Type of work completed	Generally extends only to inquiry of management and analytical procedures on financial information.	Extensive. Includes evaluating accounting systems, testing and obtaining third party evidence.
Risk of not detecting errors	Greater	Lower

<sup>195</sup> Corporations Act, Section 302.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## AUDIT

An audit (as opposed to a review) is an examination of financial information. It is designed to obtain sufficient, appropriate evidence so the auditor can express a positive opinion that the financial report provides a 'true and fair' view of the company's financial position and performance. The auditor draws on evidence from company and external sources, using, where appropriate, the company's internal controls and results obtained from substantive procedures. An audit provides a high, but not absolute, level of assurance on the financial information.

A review (as opposed to an audit) indicates that, based on the limited procedures performed, nothing has come to the attention of the auditor that indicates the financial report does not comply with the law. A review adds some degree of assurance to the financial statements, although considerably less than the level achieved by an audit.

The auditor must also describe any defect or irregularity in the financial report and any deficiency, failure or shortcoming relating to:

- obtaining all information, explanations and assistance necessary for the conduct of the audit
- the keeping of financial records sufficient to enable a financial report to be prepared and audited
- the keeping of other records and registers required by the law.<sup>196</sup>

Where applicable, the auditor must provide details of why the financial report does not so comply.<sup>197</sup>

## AUDIT COMMITTEE

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. The ASX Principles also suggest that a listed entity have an audit committee.<sup>198</sup>

<sup>196</sup> Corporations Act, Section 309.

<sup>197</sup> Corporations Act, Section 309(4) and (5).

<sup>198</sup> ASX Corporate Governance Principles and Recommendations, 4th Edition, Recommendation 4.1.

Audit committees are discussed in detail in [Chapter 11 Board Committees](#) however some information is included below in relation to the audit committees role in the matters addressed in this chapter.

Boards should ensure that the internal governance systems include adequate involvement of the external auditor, internal audit and the board audit committee. The terms of reference of the audit committee should include a role in the review of significant corporate reporting, including financial disclosures before sign-off by the full board.

While the existence of an audit committee does not alter the need for directors to take responsibility for the financial reports, with the ultimate responsibility for a company's financial statements resting with the board, audit committees can play an important role in the financial reporting process and in supporting and promoting audit quality.<sup>199</sup> A separate audit committee can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to the corporate reporting process.

The audit committee typically focuses on a limited range of key issues for statutory reporting purposes. It should review:

- any significant accounting and reporting issues, including professional and regulatory announcements, and understand their effect on the company's financial statements
- all half-year and annual financial statements of the company, and any other periodic disclosures, that require approval of the board (the process typically culminates in a detailed page-by-page review by the audit committee of these reports with the external auditor and management present)
- the written statements provided by the CEO and CFO for Australian reporting purposes (under s 295A of the Corporations Act and Recommendation 4.2 of the ASX Principles)
- the processes, policies and procedures for compliance with the company's continuous disclosure obligations
- all related party transactions for potential conflicts of interest, providing approvals on an ongoing basis.

<sup>199</sup> ASIC Information Sheet 196 (INFO 196). <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/auditors/audit-quality-the-role-of-directors-and-audit-committees/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The commentary to Recommendation 4.1 of the ASX Principles sets out the role of the audit committee and the matters which it should consider and make recommendations to the board.

## CONTINUOUS DISCLOSURE

Disclosing entities (both listed and unlisted) are subject to continuous disclosure requirements. Unlisted disclosing entities should refer to ASIC's *Regulatory Guide 198 – Unlisted disclosing entities: Continuous disclosure obligations* for guidance on complying with their continuous disclosure requirements and also Section 675 of the Corporations Act. The continuous disclosure requirements of ASX listed entities are governed by the ASX Listing Rules and also Section 674 of the Corporations Act.

Pursuant to ASX Listing Rule 3.1,<sup>200</sup> a listed entity must immediately notify the ASX once it becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities, subject to the carve-outs to immediate disclosure set out in Listing Rule 3.1 A.

Under Listing Rule 3.1B, if ASX considers that there is, or is likely to be, a false market in the company's securities, then ASX may require the company to give ASX any information it asks for to correct or prevent that false market. The term "false market" refers to a situation where there is material misinformation or materially incomplete information in the market which is compromising proper price discovery. This may arise, for example, where there is false or misleading information circulating in the market, including a specific rumour or media comment affecting the company's share price.<sup>201</sup>

The ASX Principles recommend that companies establish and disclose written policies and procedures designed to ensure compliance with ASX Listing Rules disclosure requirements and to ensure accountability at a senior executive level for that compliance.<sup>202</sup>

<sup>200</sup> Corporations Act 2001, s 674 – requires listed disclosing entities to comply with ASX Listing Rule 3.1 on continuous disclosure.

<sup>201</sup> ASX Guidance Note 8: Continuous Disclosure: Listing Rules 3.1 – 3.1B, Section 6 Listing Rule 3.1B – correcting or preventing false markets.

<sup>202</sup> ASX Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 5.1.

Each board should establish and approve policies and procedures to ensure the company complies with continuous disclosure requirements and that this is linked with the spokesperson policy. Commentary to Recommendation 5.1 of the ASX Principles contains useful information for consideration when formulating a continuous disclosure policy. The policies and procedures for meeting the continuous disclosure requirements should be made publicly available, ideally by posting them on the company's website. A "balanced" approach to disclosure in reporting both positive and negative information should also be considered.

There are other channels aside from the ASX company announcements platform that facilitate reporting to the market. These include the company's investor presentations, road shows, annual reports and the company's website. However, it is important to note that where any market-sensitive information is proposed to be released to a section of the market (for instance, at an investor or analysts' briefing), such information must **first** be provided to the ASX in accordance with Listing Rule 3.1 before it can be released via any other channel.

Information is considered to be 'generally available' if: it consists of readily observable matter; or it has been made known in a manner that would, or would be likely to, bring it to the attention of people who would commonly invest in the relevant securities and, since it was made known a reasonable period for it to be disseminated among such people has elapsed; or it otherwise consists of deductions, conclusions or inferences made or drawn from such matters.<sup>203</sup> The ASX carefully monitors the interaction between disclosure and movements in either volume or the price of shares to identify aberrations that suggest either manipulation or deficient information to the market.

Guidance Note 8 – Continuous Disclosure: Listing Rules 3.1 – 3.1B clarifies the approach of ASX to interpreting and enforcing the continuous disclosure requirements under ASX Listing Rule 3.1, and when the ASX may refer a possible breach of that rule to ASIC.<sup>204</sup>

<sup>203</sup> Corporations Act, Section 676(2).

<sup>204</sup> ASX Guidance Note 8, Section 4.5" The meaning of "immediately"

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

In addition, the Guidance Note clarifies, among other things, the meaning of 'immediately', the 'reasonable person' test, earnings guidance and surprises, and the use of trading halts to manage disclosure issues.

Under Guidance Note 8, the meaning of 'immediately' is defined as meaning 'promptly and without delay', that is doing something as quickly as it can be done in the circumstances (acting promptly) and not deferring, postponing or putting it off to a later time (acting without delay).

There are criminal and civil penalties for breach of the continuous disclosure requirements. Directors may also contravene their duty of care and diligence<sup>205</sup> by not complying with the continuous disclosure obligations.

**2021 Changes to Continuous Disclosure Laws**

The Treasury Laws Amendment (2021 Measures No. 1) Bill 2021 was passed on 13 August 2021. This Bill seeks to permanently amend the continuous disclosure obligations in the Corporations Act 2001 (Cth) (Corporations Act) such that companies and their officers will only be liable in civil proceedings for alleged breaches of continuous disclosure obligations, where they have acted with 'knowledge, recklessness or negligence'.

The Bill introduces sections 674A and 675A into the Corporations Act and in summary specifies that companies and their officers who have prima facie contravened continuous disclosure requirements will not be liable for misleading and deceptive conduct (under sections 1041H of the Corporations Act and 12DA of the Australian Securities and Investments Commission Act 2001 (Cth)) unless it can be proven that the company or officer acted with 'knowledge, recklessness or negligence'.

The reforms are only in place for 2 years at which point a review by an independent expert is required to be undertaken. Action at that point will determine whether the reforms expire or are made permanent in their current form or with some amendment.

<sup>205</sup> Corporations Act 2001, s 180 (1). Also refer to Chapter 1 Directors' Legal Duties for more information.

It is hoped that the reforms will provide more confidence to directors on making disclosures to the markets without the fear of class action looming as a disincentive. However this bill does not change ASIC's ability to prosecute under ASX Listing Rule 3.1.

Ultimately, these changes shouldn't change the manner in which entities (and directors) ensure that continuous disclosure requirements are met. The same level of rigor and due diligence should be applied with clear records being maintained.

**INVESTOR DECISION-MAKING**

If companies are to maximise returns to their shareholders, they must not only create value, but be seen to have created value and provide prospects for value creation in the future. This is essentially a matter of communicating with shareholders, potential shareholders and third parties in a position to influence investors' share buying, retention and selling decisions.

Regular and effective reporting and communications between the company and these parties influences the decision-making of shareholders and potential investors.

It is, however, widely acknowledged that traditional information flows (e.g. general purpose statutory financial reporting) and engagement practices (e.g. AGMs) do not typically address the broad range of issues of concern to individuals and entities seeking to make timely, accurate and precise decisions on their investments, or potential investments, in the company. Therefore, companies need to address the limitations of traditional reporting to fulfil their intended purpose and seek ways to better inform investors.

A more contemporary model of business reporting and communication that creates reports based on what the company wants to communicate – and on what investors want and need to know – can ensure that shareholders will make the right decisions, at the right time, about the things that matter to the company, particularly investment opportunities.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Reporting and communication strategies should be directed to balancing the performance/reward equation and aligning business rewards – capital, licences to operate (including social licence) and reputation – with company performance.

Integrated reporting of this kind takes a more forward looking and holistic approach to articulate the organisation's:

- business strategy
- performance in executing the strategy
- insights about the drivers and risks threatening the successful execution of the strategy
- outlook for future performance if the strategy is well executed.

This model implies specific reporting on performance drivers, such as infrastructure, people, business processes, strategic management, risk management and governance performance, and the dynamic interplay between all of these factors.

Through integrated reporting, shareholders can gain an appreciation of the strength of the business model in terms of its:

- velocity (speed of business processes)
- vulnerability (to shocks from business risks)
- versatility (flexibility and agility in the face of changing external forces and market conditions)
- volatility (consistency of business processes in the face of change).

With integrated reporting, companies can also provide more detail and clarity over the broader health of the organisation and the challenges and opportunities it faces in the future, rather than just a summary and discussion on historic financial results. Integrated reports provide a clearer understanding of how the organisation creates and preserves sustainable value by focusing on governance, resource use and exposure, short, medium and longer term risk to value, and how they are being addressed, as well as strategic performance and future outlook.

In contrast to this, in traditional reports, the reader is not given sufficient information to assess a company's ability to execute its strategy in the future and whether past earnings are likely to be sustainable in the medium to long term.

However, reporting and communication must be underpinned by rigorous business modelling and measurement methodologies. The business modelling methodology is required to support clear and precise reporting of the business strategy and model in a form that can be easily understood and acted upon by key shareholders and investors.

Business reporting and communication methodologies and tools help organisations decide what to report, in what format, to whom and when. Among other things, the process requires a filtering mechanism centered on balancing the measurement power of particular key performance indicators, including those relating to risk management (an information supply perspective), and how and when key shareholders and investors can and should build strategy, performance insights and outlook into their decision-making models (an information demand perspective).

The reporting and communications strategy needs to detail how and when the organisation can enhance investment decision-making models and influence investment decision-making behaviours.

***The changing tide with integrated reporting***

The focus on ESG has seen increasingly more companies applying the principles of integrated reporting in which they explain how long-term value is created – in their financial communications

KPMG's 2021 report on the annual review of corporate reporting trends<sup>206</sup> reflects that those companies that have adapted their approach to corporate reporting to articulate the more holistic story of corporate purpose and commitment to a positive societal impact, backed by targets, measurable progress, and a plan to drive action, are reaping rewards.

<sup>206</sup> Refer to KPMG, June 2021, Corporate Reporting Trends, <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/asx200-corporate-reporting-trends-2021-report.pdf>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

These rewards include increased capital flows, the attraction and retention of staff in a tough war for talent and, operational efficiencies to support sustainable growth.

The survey from which the corporate reporting trends are derived showed that many companies still have much to do in terms of understanding their climate risk and opportunity, applying the Taskforce for Climate-related Disclosures (TCFD) Recommendations and then reporting their response and likely impact in their primary report, ahead of the new Climate Exposure Draft released in 2022 (with reporting against the Climate Exposure Standard likely to be required as soon as 31 December year-end).

Positively it was noted that 35 percent of the ASX200 were found to currently detail their climate impact with reference to the TCFD Recommendations in their primary report. Several more provide TCFD-recommended information in a supplementary report or online rather than in the annual report. However, 40 percent of ASX200 companies are not reporting on climate impact, let alone adopting TCFD. This means that when the new climate standard is introduced, these companies face a considerable amount of work to prepare for it.

Those who have already adopted TCFD – and there has been a significant increase in the numbers doing so in the past 2 or 3 years – will be much better placed to cope with the new standard.

On wider ESG reporting, which is the subject of huge interest both from regulators and investors, there is still room for improvement noted based on the 2021 review. Only around half, 47 percent, include meaningful metrics on performance in managing ESG matters for long term value.

Organisations should embed ESG in core strategy and report on performance aligned to it. Currently many still have a separate section on sustainability, including ESG, which is not well connected to group strategy and the creation of enterprise value. Interviews with directors and executives in the report explain how adoption of the Value Reporting Foundation's (IR) Framework not only helped them in presenting better how the organisation delivers sustainable enterprise value, but also delivered other market and business benefits.

The move to adopt integrated reporting must be led by the board and executive management to ensure that the full value is realised not only through improved external reporting, but also through alignment across the organisation.

## Global developments

This is a fast moving area, just in the year before this document, the following developments took place:

**Mar 2022** – ISSB release of the General Requirements and Climate Exposure Drafts.

**Nov 2021** – formation of the International Sustainability Standards Board (ISSB). Release of two prototypes for developing its first two exposure drafts.

**Nov 2021** – The FRC, AASB and AUASB released joint position on Extended External Reporting (EER) in Australia. Will adopt an extended external reporting (EER) regime within the current institutional framework in place for financial reporting. The Boards were not supportive, at this time, establishing a new body that would specialise in developing sustainability reporting standards.

**Nov 2021** – AASB issued an Invitation to Comment (ITC 48) to seek feedback on its position, as an initial step, to support the voluntary adoption of the recommendations put forward by the TCFD for EER.

**Dec 2021** – ASIC issues a statement welcoming the establishment of ISSB and its objectives, and endorses listed companies to use the TCFD recommendations as the primary framework for voluntary climate-related disclosures.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## THE BOARD'S ROLE IN BUSINESS REPORTING

Business reporting should accurately reflect and communicate the real corporate picture. Boards are in a unique position to step back from the day-to-day perspective of management and view the organisation from all perspectives. Boards should be able to assist in improving the quality of reporting by identifying any major gaps between what is being reported to shareholders and investors by management and what should be reported, whilst having regard to stakeholder needs, concerns, influences and decision-making behaviour.

Thus boards are actively seeking a new reporting framework to help them decide on what to report, when, to whom, in what format and why. However, there are many impediments to change including:

- the risk of litigation if forward-looking statements are not met
- the release of competitively sensitive information or information that may be subject to rapid change or volatility
- a lack of willingness on the part of competitors and industry participants to be more forthcoming with voluntary disclosures
- no agreed industry reporting standards
- concern that capital markets will not cope with/ synthesise the extra information
- markets being only interested in short-term performance.

There are a number of ways to improve business reporting, including:

- encouraging more direct involvement by the board
- aligning internal reporting with external reporting (statutory reporting, results announcements and investor presentations, corporate social responsibility reporting, and other more frequent reporting such as:

- pro-forma/non-GAAP earnings guidance, production reports or balanced scorecards looking at the performance of non-financial KPIs)
- improving consistency and clarity in the company's message (strategic goals/objectives) and the linkages between financial and non-financial reporting
- streamlining reporting and creating a balanced portfolio of reports
- educating shareholders on the implications and value of reporting changes
- using technology for reporting automation and diffusion (e.g. XBRL, web-based and real-time reporting, enterprise and data modelling).

The ASX Principles and Recommendations include a corporate reporting process recommendation, sitting within Principle 4, requiring disclosure of the process to validate corporate reports and to provide investors with appropriate information to make informed investment decisions (Recommendation 4.3). The commentary to the corporate reporting process recommendation notes that some entities use the principles of integrated reporting as a useful framework for preparing operating and financial reviews in Director reports.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- ASIC, 2012, Regulatory Guide 73, Continuous Disclosure Obligations: Infringement Notices, <http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-73-continuous-disclosure-obligations-infringement-notice/>
- IFRS Foundation, 2021, Climate-related Disclosures Prototype standard <https://www.ifrs.org/content/dam/ifrs/groups/trwg/trwg-climate-related-disclosures-prototype.pdf>
- Task Force on Climate-related Financial Disclosures (TCFD), 2021, Guidance on Metrics, Targets, and Transition Plans [https://assets.bbhub.io/company/sites/60/2021/07/2021-Metrics\\_Targets\\_Guidance-1.pdf](https://assets.bbhub.io/company/sites/60/2021/07/2021-Metrics_Targets_Guidance-1.pdf)
- ASIC, 2019, Regulatory Guide 247, Effective disclosure in an operating and financial review <https://download.asic.gov.au/media/5230063/rg247-published-12-august-2019.pdf>
- ASX Guidance Note 8: *Continuous Disclosure: Listing Rule 3.1 – 3.1B*, [https://www.asx.com.au/documents/rules/gn08\\_continuous\\_disclosure.pdf](https://www.asx.com.au/documents/rules/gn08_continuous_disclosure.pdf)
- Corporations Act 2001 (Cth).

For further information please contact:



**Patricia Stebbens**

**Partner, Audit, Assurance  
& Risk Consulting**  
[pstebbens@kpmg.com.au](mailto:pstebbens@kpmg.com.au)



**Peter Trace**

**Partner, CFO Advisory**  
[ptrace@kpmg.com.au](mailto:ptrace@kpmg.com.au)

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 8. Stakeholder Engagement

Stakeholder expectations are changing. Now more than ever, effective stakeholder engagement is critical to organisational sustainability. Boards and directors need to understand and respond to stakeholder issues and needs, and leverage their perspectives on the organisation's performance and direction.

## In this chapter

- Stakeholder engagement
- Why focus on engaging stakeholders?
- Stakeholder engagement at a board level
- Stakeholder engagement and strategy development
- Establishing an effective stakeholder engagement framework
- Reputational advantages of effective stakeholder management



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is the board comfortable that it knows who its key stakeholders are?
2. Is the organisation aware of all potential vulnerabilities?
3. Does the organisation have an understanding of all stakeholder issues?
4. Have stakeholders with the ability to affect strategic and business objectives been effectively engaged?
5. Does the organisation have clear and approved narrative and processes for engaging with stakeholders?
6. Have the risks of not engaging key stakeholders (financial and reputational) been considered and, if applicable, quantified?
7. Is the purpose of stakeholder engagement defined and well-understood across the organisation?
8. Is stakeholder engagement embedded into the organisation's vision, mission and strategy statements?
9. Does the organisation have a stakeholder engagement framework aligned with best practice?
10. Do relationship effectiveness measures exist for key stakeholders?
11. Is the board seeking and maintaining relationships with its key stakeholders at the leadership level?
12. Has the organisation considered making a public disclosure about stakeholder management and corporate social responsibility?
13. Is effective stakeholder management used as a strategic, preventive mechanism, rather than a responsive tool?
14. Is there an anonymous feedback mechanism beyond whistleblowing for stakeholders who frequently interact with the entity?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The organisation maintains no stakeholder mapping, prioritising or profiling information.
- Stakeholders are defined narrowly as clients and customers.
- In most decisions, stakeholders are not considered or consulted.
- The risk of not engaging stakeholders is not discussed or is often dismissed quickly by some board members.
- Dialogue with stakeholders mostly occurs in the event of disputes and negative media coverage.
- Online coverage of the organisation is mostly negative.
- Unclear leadership and board accountabilities for stakeholder engagement.
- The organisation is unaware or unprepared for the impact of social media and stakeholder activism.
- Board members do not hold strong or effective relationships with key stakeholders.
- Stakeholder engagement is not tracked, monitored or reported on.
- Stakeholder issues (opportunities and risks) and perceptions about the organisation are unknown or not documented and tracked, with no process to identify, review or anticipate vulnerabilities.
- There is no clear message or process for engaging with stakeholders.
- There is no stakeholder engagement plan with no framework or tactics in place.
- There is no stakeholder management structure with no systems in place.
- No understanding of how the organisation's positions may or may not intersect with the government or stakeholder agendas.
- There is a gap between internal facing and external facing organisational positions.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## STAKEHOLDER ENGAGEMENT

Stakeholder engagement is the process of identifying and involving the key groups of people and organisations who are affected by, or have the capacity to influence, the organisation's activities and operations.

Ordinarily, a board's direct involvement with its key stakeholder groups may be limited to the chair or the respective chairs of committees such as the audit committee or the sustainability committee. In extraordinary circumstances (e.g. crisis mode) the wider board may become involved in engagement activities and communication.

However, management is now turning to directors to tap into expertise and relationships to facilitate engagement, advocacy and lobbying with key stakeholders. Directors who possess 'change agent' competencies can be influential in championing particular courses of action. Recent Royal Commissions have highlighted just how influential an organisation's engagement with key stakeholders can be on company value and shareholders' interests.

Relevantly, corporate governance reform in the UK includes requirements for boards to understand and report on how stakeholders' interests have been considered in board discussions and decision-making.<sup>207</sup> While not yet a legal requirement in Australia, the UK corporate governance regime is influential in Australia<sup>208</sup> and may provide useful insight on the future of directors' duties with respect to stakeholders in Australia.

## WHY FOCUS ON ENGAGING STAKEHOLDERS?

Organisations exist in an environment of heightened scrutiny over the sustainability and integrity of their operations. In the same way that companies perceived as acting in a detrimental fashion can suffer loss, companies that collaborate with their stakeholder base can reputationally and financially benefit from a positive public image.

<sup>207</sup> Refer to The UK Corporate Governance Code, July 2018, s5 <https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf>

<sup>208</sup> Refer to for an example, the Banking Executive Accountability Regime which was heavily based on the UK's Senior Managers Regime

Other than reputational and public perception implications, certain revenue (i.e. government contracts) can be dependent on an organisation's fulfilment of sustainability, community relations and other stakeholder engagement criteria. For such arrangements, effective stakeholder engagement processes are essential in providing organisations with the ability to compete with their industry rivals.

## STAKEHOLDER ENGAGEMENT AT A BOARD LEVEL

Organisations with effective stakeholder engagement possess a common theme of a strong 'tone at the top'. Boards are responsible for setting the general policies and direction of the organisation. They shape the organisation's framework for accountability, and they should lead by example in fostering an outward-looking approach.

At a board level, stakeholder engagement should be defined as a core organisational value. Directors should identify the key risks associated with evolving societal expectations and set expectations with their executive management group around effectively engaging the stakeholder base. Further, the board should also consider their own interface with their stakeholders, including the integration of stakeholder issues into the AGM and public reporting.

## STAKEHOLDER ENGAGEMENT AND STRATEGY DEVELOPMENT

Stakeholders can provide a unique perspective on an organisation's performance, challenges and opportunities. Strong and effective stakeholder engagement provides boards with a range of views that might otherwise be missed in the strategy development and risk assessment processes.

A robust strategy development process involves exploring the macro and micro environment for current and emerging issues that could impact the organisation's operating model. Management and the board tend to have a good grasp of the local/micro influences. However, having the perspective of a stakeholders' external lens can provide the organisation with a unique input to inform strategy development and identification of risks and opportunities.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Stakeholders have their own agendas and issues, and will view an organisation through this lens, providing the opportunity to bring enormous value to the business. Effectively engaging with stakeholders can provide management and the board with the ability to see issues affecting the business in a different context and can often provide a different interpretation of what these issues could mean for the business.

## ESTABLISHING AN EFFECTIVE STAKEHOLDER ENGAGEMENT FRAMEWORK

To be effective, organisations require formalised stakeholder engagement strategies, plans and processes. A stakeholder engagement framework can help facilitate a consistent, integrated and effective approach. A stakeholder engagement framework may include:

- Objectives and guiding principles of engagement.
- Stakeholder models/maps and prioritisation.
- Responsibilities for developing and managing stakeholder (including agreed accountabilities for the board and management).
- Methods of engagement at various levels of involvement, such as newsletters, workshops and forums.
- Methods for gathering information on/from stakeholders (i.e. surveys, focus groups, interviews, etc.).
- Methods and accountabilities for monitoring and measuring stakeholder concerns, influences and sensitivities.
- Methods of evaluation for stakeholder engagement activities.
- Established positions on relevant public or industry specific policies.

The AA1000 series of Stakeholder Engagement Standards provide an internationally recognised framework to help organisations ensure stakeholder engagement processes are purpose driven, robust and deliver results, and form a basis for designing and implementing effective stakeholder engagement in a credible way.<sup>209</sup>

<sup>209</sup> For further information please refer to AA1000 Stakeholder Engagement Standard, <https://www.accountability.org/standards/aa1000-stakeholder-engagement-standard/>

## REPUTATIONAL ADVANTAGES OF EFFECTIVE STAKEHOLDER MANAGEMENT

A good corporate reputation is a prized asset that is earned over time. It can be a source of competitive advantage, influencing the level of engagement with the organisation by employees, customers, suppliers, shareholders, communities and other stakeholders. By way of contrast, failure to manage reputation can have a deleterious and prolonged effect on a business. Reputation damage affects directors' personal reputations, employee morale, investor confidence and company performance. Reputation risk has been identified as one of the most important risks an organisation faces. Loss of reputation can occur as a result of poor risk management processes across all risk areas, including compliance, finance, environmental considerations and operations. A robust and systematic enterprise-wide risk management strategy is essential to maintain an organisation's reputation.

An organisation's reputation is directly linked to the board's role in both strategy and risk. The board's starting point in developing a positive corporate reputation is the right 'tone at the top', fostering appropriate organisational values that drive culture. A reputation management system, underpinned by straightforward and open communications, protects this intangible but vital asset. Organisations should regularly measure and assess their reputation and social licence, benchmarking against previous assessments, competitors and like organisations.

**“It takes 20 years to build a reputation and 5 minutes to ruin it.”**

WARREN BUFFET

Despite the best risk-mitigation program, when things go wrong, a period of reputational volatility can ensue. Importantly, reputation is affected by the way an accident/incident is managed and/or the organisation's ability to react to and handle such a crisis. The company needs to prepare itself for potential crises with clearly documented crisis management plans. The media is a critical influencer of public opinion, especially in a crisis.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

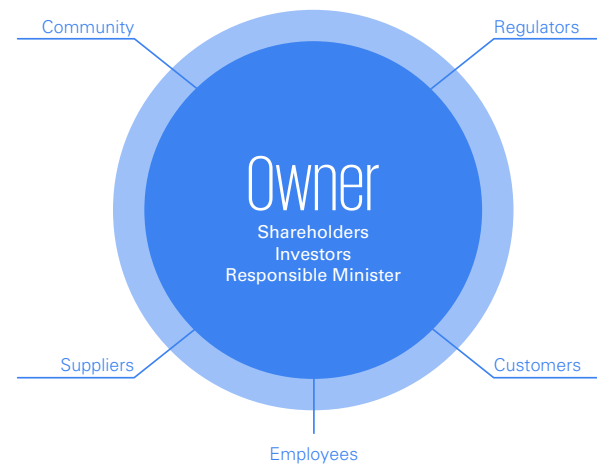
CONTACT US

Stakeholders

Stakeholders of organisations will differ depending on the nature, size and complexity of the organisation, however, stakeholders common to most organisations include:

- Community
- Regulators
- Suppliers
- Employees
- Customers
- Government – local, state, federal (beyond regulatory)
- Shareholders
- Investors
- Industry/advocacy/environmental bodies
- Media

The concerns of these stakeholders are not just financial, and extend to environmental, social and governance considerations and objectives.



COMMUNITY STAKEHOLDER ENGAGEMENT

Identifying, understanding and engaging with community groups interested in or impacted by an organisation is increasingly seen as a minimum requirement in today's landscape. The rise of social media has provided a platform for community members to instantly and publicly share feedback with organisations. Having a clear and direct approach to engaging with community groups has never been more important.

Some actions that directors can undertake to help their organisation manage and excel with their community stakeholders include:

- Requesting a report from management on the organisation's key community groups and the current engagement activity. Understanding the community's needs, issues and priorities.
- Assigning accountability for directors to engage and own the relationship between key community groups.
- Developing a community stakeholder engagement strategies and plans.
- Ensuring community stakeholders are engaged as part of the organisation's product/service/project development process.
- Ensuring feedback from community stakeholders is incorporated within board reporting.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

REGULATOR STAKEHOLDER ENGAGEMENT

The reputational and financial repercussions of regulatory scrutiny and action can be far reaching. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry provides a clear example of this, where intense regulatory scrutiny had significant impact on the reputation of many large financial organisations.

Building a constructive and trusting relationship with regulators is, therefore, in the best interests of an organisation's shareholders or owners. Given the potential impact that mismanagement of regulatory stakeholders may have, directors are increasingly seen as an important part of an organisation's regulatory stakeholder engagement strategy.

Directors can have bearing on this relationship in several key ways:

Role of directors with respect to regulatory stakeholders	Questions to ask
Ensuring a firm understanding of the organisation's key regulators.	<ul style="list-style-type: none"> <li>- What are the key regulators for the organisation/industry?</li> <li>- Do I understand the role and remit of each key regulator?</li> <li>- Am I familiar with each key regulator's objectives or stated focus areas? (e.g. 'crack downs' on certain areas of compliance).</li> </ul>
Understanding the key regulatory issues facing the organisation at any given time.	<ul style="list-style-type: none"> <li>- If approached by a regulator, do I have the requisite knowledge and understanding of the key regulatory issues facing the organisation to adequately respond?</li> <li>- Am I satisfied with management's reporting of regulatory issues?</li> <li>- Do I know who the key relationship managers are within the organisation for each key regulator?</li> </ul>
Setting and maintaining a culture of compliance throughout the organisation.	<ul style="list-style-type: none"> <li>- Am I familiar with the measures in place to manage compliance issues throughout the organisation?</li> <li>- Have directors or management recently interacted with frontline staff to understand the prevailing attitude towards compliance?</li> <li>- Do employee engagement surveys highlight any cultural issues?</li> <li>- See <a href="#">Chapter 21 Culture and Conduct</a> for further information on compliance culture.</li> </ul>
Establishing and demonstrating requirements for clear, open, transparent and truthful communications with regulators.	<ul style="list-style-type: none"> <li>- Am I role-modelling the behaviour I would expect from employees in my interactions and communications with regulators?</li> <li>- Have I witnessed (and corrected) any undesired behaviour or attitudes towards regulators?</li> </ul>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## SUPPLIER STAKEHOLDER ENGAGEMENT

Suppliers play a key role in enabling organisations to meet the needs of other key stakeholder groups, in particular customers and the broader community. This is especially so in competitive business environments, where there will be increased pressure to reduce costs while maintaining or improving the quality of the organisation's products and services.

Suppliers can be highly influential in the success (or otherwise) of an organisation. For example, an organisation that maintains a high profit margin at the expense of a key supplier that is struggling to maintain solvency may find itself in trouble in the long run. Similarly, any compliance, regulatory, legal and/or ESG issues that plague a supplier will often have a negative reputational impact upon the procuring organisation. A holistic approach must be taken when considering the needs of an organisation and its suppliers.

Some practical measures that directors may undertake to ensure the organisation is appropriately engaging and managing its suppliers include:

- Having visibility over suppliers' business practices and understanding how the organisation's business model may influence supplier behaviour or incentives.
- Ensuring the organisation maintains robust procurement processes that incorporate not only value for money factors, but also long-term sustainability, corporate reputation and any history of involvement with business practises below the standard expected by the organisation.
- Ensuring the organisation establishes mechanisms to measure and monitor suppliers' adherence to ESG policies and standards.

For further information on directors' role in ethical supply chains, see [Chapter 24 Human rights and modern slavery](#).



## Case Study - Takata Airbag recall

If you own a car in Australia, chances are you would have been required to replace the airbags as part of the large-scale Takata Airbag recall program overseen by the ACCC. The serious defect that impacts 1 in 4 cars in Australia has been associated with 24 deaths (one in Australia) and over 300 injuries worldwide.

The problem with Takata's airbags can be traced back to the 1990s, when the company transitioned to the use of an ammonium nitrate based inflator, which can become extremely unstable when exposed to moisture. Over time, the ammonium nitrate will degrade and can cause inflators to explode, sending shrapnel into the cabin of the car.

Takata originally notified safety regulators and car manufactures of concerns with airbag safety in 2008. However, a New York Times exposé alleged that the company held safety concerns as far back as 2004, but buried testing results instead of notifying regulators. Indeed, a 2017 US Department of Justice ruling said Takata "repeatedly and systematically falsified critical test data related to the safety of its products."

The ACC report that 99.9 percent of the more than 3 million airbags have been replaced under voluntary recall in Australia since 2009

For car manufacturers, this introduced significant costs to their businesses, with extensive recall programs requiring additional processes, oversight and brand damage management.

This case study serves as a clear example of the impact that unreliable suppliers can have on an entire industry. The reliance of many car manufacturers on one supplier has exacerbated the issue, with an international shortage of supply prolonging the recall and increasing the risk of further harm.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## EMPLOYEE STAKEHOLDER ENGAGEMENT

Unlike customer stakeholder groups, employee stakeholders' needs remain fairly universal across most organisations. To build a high performing culture that delivers the organisations purpose and promise to all its stakeholders, directors need to consider the following culture drivers:

- Leadership
- Values and behaviours
- Communication
- Governance
- Capability
- Structure
- Systems and Processes

For employees, job satisfaction usually requires:

- Fair remuneration and compensation
- Job security
- Respect, recognition and acknowledgement
- Alignment to the organisation's purpose and strategy
- Open and honest communication

Through corporate governance, boards have often had a fairly direct impact on employee interests. For example, boards will help establish, review, and approve the management and employee remuneration structure. Similarly, boards help set and maintain an organisation's culture, which will necessarily influence key job satisfaction factors, such as transparency of communication with employees and reward and recognition. Finally, risky decision-making at the board level may impact on an organisation's overall level of job security that it can offer employees.



### Case Study – 'Deliberate and systemic' underpayment of employees at 7-Eleven

In April 2016, the Fair Work Ombudsman (FWO) released its inquiry into 7-Eleven for the "deliberate and systemic underpayment of employees". The report summarised the FWO's investigation into allegations of significant underpayment of wages and falsification of employee records across 7-Eleven's franchisee network.

The FWO's investigation uncovered numerous instances of 7-Eleven Franchisees underpaying staff, falsifying employment records and enforcing "cash-back" programs (whereby staff are paid award rates, but required to pay back part of their salary to employers).

While the investigation and subsequent legal action has had significant impact on Australian employment law, this case study also serves as a cautionary tale for Boards and Directors.

The FWO's inquiry ultimately found that while 7-Eleven's approach to workplace matters appeared compliant on the surface, they failed to adequately identify and address deliberate non-compliance in practice. In particular, the FWO pointed towards a business model that restricted franchisees control over business expenses (aside from wages) and a culture of "complicity", coupled with an audit program that was inadequate to detect illegal or fraudulent work practises.

Interestingly, the FWO found that while the uncovered contraventions of employment law were restricted to the employee and employer (i.e. the franchisee), 7-Eleven (as the overarching franchisor) has "moral and ethical responsibility for what has occurred within its network and is capable of preventing it occurring again."

These underlying key contributing issues clearly form part of an organisation's key corporate governance responsibilities, which Directors and the Board play a critical role in establishing and monitoring. Indeed, Russel Withers, 7-Eleven's Chairman at the time, resigned midway through the investigation in 2015.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## • GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## CUSTOMER STAKEHOLDER ENGAGEMENT

Customers play a key role in the financial and reputational success of an organisation. Increasingly, organisations are taking a customer-centric approach to decision-making. This approach ensures the organisation's strategy and values, through to end products and services, are aligned to the expectations and requirements of its customers.

Customer stakeholder group interests are unique and will differ from industry to industry and organisation to organisation. However, several underlying interests will apply to most companies:

- Value
- Quality
- Customer Care
- Ethical products and services

## Useful references

- Global Reporting Initiative, GRI G3, Sustainability Reporting Guidelines, <https://www.globalreporting.org/standards/>
- Hall, J., 2008, Environmental Liabilities – Directors and Officers Beware, Keeping Good Companies, Vol. 60 No. 3, pp 169–173
- AICD, 2018, Dealing with regulator and other stakeholders – whose job is it anyway? <https://aicd.companydirectors.com.au/membership/the-boardroom-report/volume-16-issue-6/dealing-with-the-regulator-and-other-stakeholders-whose-job-is-it-anyway>
- Zollinger, P, 2009, Stakeholder Engagement and the Board: Integrating Best Governance Practices – Global Corporate Governance Forum, [https://www.ifc.org/wps/wcm/connect/bac56797-a3a7-4e24-90f6-efa9ab7363e0/FINAL%2BFocus8\\_5.pdf?MOD=AJPERES&CVID=jtCwtno](https://www.ifc.org/wps/wcm/connect/bac56797-a3a7-4e24-90f6-efa9ab7363e0/FINAL%2BFocus8_5.pdf?MOD=AJPERES&CVID=jtCwtno)

## For further information please contact:

**Josh Faulks**

**Director, Reputation Advisory,  
Customer Brand and  
Marketing Advisory**  
[jfaulks@kpmg.com.au](mailto:jfaulks@kpmg.com.au)

# Governance Leadership

---

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 9. Structuring an Effective Board

Whether it be starting a new company or changing organisational structures, structuring an effective board is a challenging undertaking. The structure, composition, and internal dynamics of boards can affect the performance of individuals and the board collectively.

## In this chapter

- Governance framework
- Code of conduct
- Skills and expertise
- Boardroom diversity
- Board size
- Finding and appointing new directors
- Appointment process
- Director induction
- Director professional development
- The first 100 days
- Board evaluation
- Director remuneration
- Listed companies remuneration
- Re-election and rotation of directors
- Board succession planning
- Director tenure
- Access to company records

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

### When establishing from the beginning –

1. Is there a structured plan, with timeframes and accountabilities, on how to establish the board?
2. Is the board considering its frameworks for communication with stakeholders in the first 100 days?

### At the beginning and thereafter –

3. Are candidates/current directors able to commit sufficient time to discharge board duties?
4. Is there an appropriate induction program (including committee induction) for new directors?
5. Are the directors sufficiently familiar with the company's operations, performance, values and aspirations?
6. Is there a nomination committee charged with the responsibility of director succession planning, or alternatively, does the board have a robust process to enable orderly board succession?
7. Has the board adequately considered its approach to diversity including, where appropriate, the formulation of relevant policies?

8. Beyond having the right mix of skills, experience and background present on the board, does the composition complement the culture, engagement and style of the board?
9. Is a contingency plan established in the event that the chair has to step down unexpectedly?
10. Has the board properly considered the overarching strategy of the organisation and taken account of changes that are likely to occur in the short to medium term (for example changes to strategy, changes in the external environment) when determining its desired size and mix of skills/experience/backgrounds?
11. To the extent there are gaps in desired skills and experience that reside on the board, has the board adequately considered whether and how the board might benefit from the professional development of current board members?
12. Is the board setting the tone at the top along with the culture and monitoring this?
13. Does the board regularly review its own performance and the effectiveness of its governance processes?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- On establishment – no advice is being sought from experts or directors who have experience in establishing a new board.
- Not everyone agrees on the priorities and what is required from the board (at establishment phase and ongoing).
- The board comprises mainly inexperienced directors and limited induction programs are in place.
- Accountabilities and delegations are unclear and not documented.
- No board instruments have been presented for endorsement (at establishment) or for review (ongoing).
- The board is too large or small compared with similar organisations.
- The board does not periodically review its skills and competencies or align its skills matrix to the company strategy.
- Board appointments are decided by the chair with little input from other directors.
- Limited consideration is given to the diversity of the board in its structure/composition and thought-process/decision-making processes.
- No consideration is given to fixed-term directorships.
- No consideration is given to the composition of, delegation to and reporting from board committees.
- Directors do not receive a letter setting out the terms and conditions of their appointment.
- No formal board induction is provided to new board members or this is insufficient.
- Board discussions are dominated by a small cohort of directors.
- The board finds it difficult to make decisions with consistent carry-over of agenda items from one meeting to the next resulting.
- Directors appear to be over-stretched and unable to dedicate sufficient time to their roles.
- Overuse of external advisers occurs due to skill gaps on the board.
- Directors are not provided with, or fail to engage with, professional development opportunities.
- There is no board evaluation/review process (or it is not documented or known to the board).
- There is a failure to appreciate the implications of the two-strikes rule on the directors' remuneration report or to anticipate members' reaction to the remuneration report.
- No consideration is given to the enforcement of accountability for non-remunerated directors.
- There is a lack of ongoing board succession planning.
- Directors have difficulty accessing company information in a timely manner.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## GOVERNANCE FRAMEWORK

Effective boards are boards that are able to consistently and constructively make proactive decisions that ensure the sustainable success of their organisation. Effective board composition is the bedrock of an effective board, helping to limit the potential for board complacency criticised in the APRA CBA report.<sup>210</sup> ASX Corporate Governance Principles and Recommendations Principle 2 commentary states that “a high performing, effective board is essential for the proper governance of a listed entity.”<sup>211</sup>

In practice, the company's governance embodies a complex range of structures (frameworks, policies, and processes) balanced against the appropriate mix of skills, behaviours, and practices.

A well-designed governance framework will help the board to be effective and fulfil its role by:

- instilling the desired behaviours that underpin the company's core values and drive the cultural ‘tone from the top’
- giving an audience to ‘the customer voice’ and the voice of other key stakeholders
- instilling confidence in shareholders and the public that the company is well-governed
- ensuring that directors' competencies and skills are appropriate given the company's current and future strategic requirements
- empowering the board to act to its best capability by having the appropriate mix of skills, expertise, experience and diversity of thought
- clarifying the roles, responsibilities and delegation of powers of individual directors, the board, its committees, and management
- matching the skills and expertise of individual directors with board and committee responsibilities

<sup>210</sup> APRA Prudential Inquiry into The Commonwealth Bank of Australia report (April 2018) [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)

<sup>211</sup> ASX Corporate Governance Principles and Recommendations (4th edition).

- ensuring that directors have access to an induction program and ongoing professional development
- implementing sound risk management practices and controls in line with the organisation's risk appetite
- facilitating the evaluation and review of the board, chair, CEO, and management
- embedding processes that facilitate the board's oversight and constructive challenge of management
- including transparent mechanisms for the enforcement of accountability by the board and management
- aligning the remuneration strategy with the shareholders' expectations, rather than encouraging short-term profits and self-interest, thereby safeguarding the shareholders' interests
- enabling the efficient and effective reporting of quality information on a timely basis between directors, the board and its committees, the company executives, the organisation as a whole, and wider stakeholders.

Recommendation 2.1 of The ASX Corporate Governance Principles and Recommendations suggests that the board of a listed entity have a separate nomination committee (of a majority of independent directors), as it can be “an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to decisions regarding the composition of the board”. The nomination committee should have a charter which “clearly sets out its role and confers on it all necessary powers to perform that role. This will usually include the right to seek advice from external consultants or specialists where the committee considers that necessary or appropriate”. If the company does not have a nomination committee, then the entity should “disclose that fact and the processes it employs to address board succession issues and ensure that the board has the appropriate balance of skills, knowledge, experience, independence and diversity to enable it to discharge its duties and responsibilities effectively.” Further information on committees can be found in [Chapter 11 Board Committees](#).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

As Governance practices continue to come under the spotlight following the Hayne Royal Commission and the APRA CBA report, in November 2018 ASIC introduced the Corporate Governance Taskforce. This taskforce was established to undertake targeted reviews of corporate governance practices in large listed entities and to “allow ASIC to shine a light on ‘good’ and ‘bad’ practices observed across these entities.”<sup>212</sup> To date one report has been produced by this Taskforce. The report addresses ASIC’s observations on director and officer oversight of non-financial risk in large and complex financial services companies.<sup>213</sup> In summary, the followed findings are contained within the report:

- “All too often, management was operating outside of board-approved risk appetites for non-financial risks, particularly compliance risk. Boards need to actively hold management accountable for operating within stated risk appetites.
- Reporting of risk against appetite often did not effectively communicate the company’s risk position. Boards need to take ownership of the form and content of information they are receiving so that they can adequately oversee the management of material risks.
- Material information about non-financial risk was often buried in dense, voluminous board packs. It was difficult to identify key non-financial risk issues in information presented to the board. Boards should require reporting from management that has a clear hierarchy and prioritisation of non-financial risks.
- The effectiveness of board risk committees (BRCs) could be improved. BRCs should meet more regularly, devote enough time and be actively engaged to oversee material risks in a timely and effective manner.”<sup>214</sup>

<sup>212</sup> ASIC, 2018, An ASIC update by John Price, Commissioner, <https://asic.gov.au/about-asic/news-centre/speeches/an-asic-update-by-john-price-commissioner/>

<sup>213</sup> ASIC, Corporate Governance Taskforce, Director and officer oversight of non-financial risk report, <https://asic.gov.au/regulatory-resources/find-a-document/reports/corporate-governance-taskforce-director-and-officer-oversight-of-non-financial-risk-report/>

<sup>214</sup> ASIC, 2019, ASIC releases report on director and officer oversight of non-financial risk, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-271mr-asic-releases-report-on-director-and-officer-oversight-of-non-financial-risk/>

ASIC Chair, James Shipton, made the following statements in the accompanying media statement:

*“While there is no “one size fits all” solution to these findings, boards need to proactively identify and assess their own characteristics and processes. Though the review examined companies in the financial services industry, many of the lessons learned can be applied to most public companies in other sectors of the economy”.*

*“Our report concludes with a series of questions that all public companies might ask themselves. Not all will be relevant to every company, but many will be. We urge boards of all large listed companies to read this report and review their governance practices and accountability structures with reference to our findings”.*<sup>215</sup>

## CODE OF CONDUCT

Recommendation 3.2 of the ASX Corporate Governance Principles and Recommendations suggests that boards of listed companies should have and disclose a code of conduct for its directors, senior executives, and employees that “articulates the standards of behaviour expected from directors, senior executives and employees” and ensure(s) that “the board or a committee of the board should be informed of any material breaches of the entity’s code of conduct as they may be indicative of issues with the culture of the organisation”.<sup>216</sup>

The commentary for Recommendation 3.2 also includes a list of “suggestions for the content of a code of conduct” which is a useful point of reference.<sup>217</sup>

<sup>215</sup> Ibid

<sup>216</sup> Refer to Principle 3.2 of ASX Corporate Governance Principles and Recommendations (4th edition) <https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf>

<sup>217</sup> Ibid

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Recommendation 3.2 is supplemented by the introduction of a newer Recommendation 3.1 (introduced in the most recent, 4th edition) which states that “a listed entity should articulate and disclose its values”. The recommendation commentary notes that “a listed entity’s values are the guiding principles and norms that define what type of organisation it aspires to be and what it requires from its directors, senior executives and employees to achieve that aspiration”.

## SKILLS AND EXPERTISE

The board should collectively possess a sufficient range of competencies to effectively deal with the issues and opportunities the company faces. It should be comprised of individuals who bring to the boardroom a range of skills and know-how in relevant areas. Their individual strengths should complement each other.

The competencies required for any particular board will vary considerably, depending on its industry, strategy, the company’s development stage and the environment in which it operates. The types of generic technical skills and competencies required on a board might include:

- accounting and finance
- business judgement
- industry knowledge
- government knowledge
- legal knowledge
- employment/industrial relations knowledge
- environment/sustainability knowledge
- leadership
- strategy/vision
- risk management.

With technological advancements and the risk of cyber attack being front of mind for boards, many boards are also looking for technology skills. Similarly, COVID-19 resulted in some boards bringing health related skills into the boardroom for the first time.

Similarly, given the increased focus on conduct risk and other non-financial risks as noted before. These new areas of focus increase the onus on directors to possess the appropriate behavioural competencies, as well as the traditional technical skills. Behavioural attributes include:

- emotional intelligence
- curiosity
- an appreciation for diversity of thought, backgrounds, expertise and experience
- authenticity
- transparency in decision-making and communication
- self-awareness and accountability
- willingness to reflect, learn and adapt
- ability to challenge and question in a constructive manner
- sense of rigor and ability to enforce accountability in an appropriate manner
- humility to know that they will not have all the answers.

## Board skills matrix

Recommendation 2.2 of The ASX Corporate Governance Principles and Recommendations states that companies should have and disclose a ‘board skills matrix’ setting out the mix of capability and diversity that the board currently has, or is looking to achieve, in its membership.

The Recommendation commentary notes that there is no prescribed format for a board skills matrix. It can set out either the mix of skills that the board currently has or the mix of skills that the board is looking to achieve in its membership or both. Whichever format it follows, the listed company should explain what it means when it refers to a particular skill in its board skills matrix and the criteria a director must meet to be considered to have that skill.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

In addition to a technical competency assessment, the skills matrix should ideally also include an analysis of the current or desired behaviours to help the board function as an effective decision-making body.

The skills matrix is a useful tool to identify gaps in the collective board's skills (which should be addressed by appointing new members or providing professional development to existing directors) as well as succession planning.

Disclosing the board skills matrix also "gives useful information to investors and helps to increase the accountability of the board in ensuring it has the skills to discharge its obligations effectively and to add value".<sup>218</sup>

## BOARDROOM DIVERSITY

The ASX Corporate Governance Principles and Recommendations have long focused on the importance of independent directors as their appointment plays a fundamental role in a board's diversity. Recommendation 2.4 specifically states that "a majority of the board of a listed entity should be independent directors". Whilst the appointment of a majority of independent directors to the board of a non-listed company may be impractical, the importance of the board's diversity as a whole should not be overlooked.

The economic arguments for more board diversity have been identified in various widely publicised studies. Interestingly, these studies demonstrate a correlation between increased diversity at higher levels of the organisation and stronger organisational and financial performance.<sup>219</sup>

<sup>218</sup> Refer to commentary for Principle 2.2 of ASX Corporate Governance Principles and Recommendations (4th edition)

<sup>219</sup> See for example – Gender Diversity and Corporate Performance, Credit Suisse Research Institute, August 2012; The Bottom Line: Corporate Performance and Women's Representation on boards, Catalyst, October 2007; Australia's Hidden Resource: The economic case for increasing female participation, Goldman Sachs JB Were, November 2009

In structuring the board to add value from diversity, a company should consider the mix of skills, backgrounds, experience, expertise, age, gender and perspectives of its directors that would be necessary to meet the unique requirements of the company. An emphasis on director diversity should yield a number of key benefits:

- an increase in the intellectual resources of the board and lessen the reliance on the authority of key individuals
- derive value from previously unrecognized or overlooked opportunities
- enhancement of the board's ability for reflection and decision-making capabilities, thus lessening the risk of 'group-think', 'dulling of the senses' or the 'chronic ease' criticised in the APRA CBA report
- a stronger sense of board authenticity and connection with customers, employees and other stakeholders, helping to set the cultural 'tone from the top' and critical to the company's 'social-licence to operate' and
- improving skills to constructively challenge and hold management to account, reducing the chance of over-confidence in management and the company's performance as a whole, particularly with regard to risk management.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

To encourage companies to foster a governance culture that embraces diversity, Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations requires listed entities to:

- have and disclose a diversity policy
- set measurable objectives for achieving gender diversity in the composition of the board, senior executives and the workforce generally
- charge management with designing, implementing and maintaining programs and initiatives to help achieve those measurable objectives
- review with management and disclose at least annually:
  - the measurable objectives set by the board, particularly for achieving gender diversity
  - the progress towards achieving those measurable objectives
  - the adequacy of the entity's programs and initiatives in that regard
  - whether the review referred to above has taken place
  - note the respective proportions of men and women on the board, in senior executive positions and across the whole workforce (or if the entity is a 'relevant employer' under the Workplace Gender Equality Act, the entity's most recent 'Gender Equality Indicators', as defined in and published under that Act).<sup>220</sup>

If the entity was in the S&P/ASX 300 index at the commencement of the reporting period, the measurable objective for achieving gender diversity in the composition of its board should be to have not less than 30 percent of its directors of each gender within a specified period.

<sup>220</sup> Recommendation 1.5(c) of the ASX Corporate Governance Principles and Recommendations (4th edition).

The inclusion of a specific target follows the KPMG ASX review which suggests that "diversity policies are most effective when a listed entity sets numerical targets to be achieved within a specified timeframe, outlines the initiatives it is introducing to help meet those targets".<sup>221</sup> According to the commentary for Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations "non-numerical objectives such as "introducing a diversity policy" or "establishing a diversity council", and aspirational objectives such as "achieving a culture of inclusion", while individually worthwhile, are unlikely to be effective in improving gender diversity unless they are backed up with appropriate numerical targets".

The ASX recommendations specific focus on gender diversity is supported by reference to Bankwest Curtin Economics Centre's 2020 report *More women at the top proves better for business*, which observes that an increase of 10 percentage points or more in female representation on the Boards of Australian ASX-listed companies led to a 4.9 percent increase in the company market value. These companies also had a 12.9 percent increase in the likelihood of outperforming the sector on three or more performance and profitability metrics.<sup>222</sup>

The Australian Institute of Company Directors (AICD) tracks new board appointments on a quarterly basis. They report that as at 30 November 2021, the percentage of women on boards of ASX200 companies was 34.2 percent, with 41.8 percent of the new board appointments of ASX200 being woman and no boards in the ASX200 without women.<sup>223</sup>

<sup>221</sup> Refer to KPMG ASX Corporate Governance Council Principles and Recommendations on Diversity: Analysis of disclosures for financial years ended between 1 January 2015 and 31 December 2015 <https://www.asx.com.au/documents/asx-compliance/asx-corp-governance-kpmg-diversity-report.pdf>, cited in commentary for Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations (4th edition).

<sup>222</sup> Bankwest Curtin Economics Centre, *More women at the top proves better for business* <https://bcec.edu.au/media/more-women-at-the-top-proves-better-for-business/>

<sup>223</sup> AICD, Women on ASX 200 Boards (at 30 November 2021) <http://aicd.companydirectors.com.au/advocacy/board-diversity/statistics>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

CGI Glass Lewis, one of the major proxy advisors in Australia, updated its guidelines in 2021 to state it would consider voting against companies in the following circumstances:

- if 6 or more Directors, less than two women on Board and
- if 5 or less Directors, less than one woman on Board.<sup>224</sup>

The commentary of Recommendation 1.5 also states that boards of listed entities should also “have regard to other facets of diversity in addition to gender when considering the composition of the board. In particular, having directors of different ages and ethnicities and from different cultural or socio-economic backgrounds can help bring different perspectives and experiences to bear and avoid ‘groupthink’ in decision making.” *Box 1.5: Suggestions for the content of a diversity policy*<sup>225</sup> in the commentary may prove helpful to those boards formulating or updating diversity policy.

The introduction of Recommendation 9.1 into the 4th edition, which requires a listed entity to disclose the processes it has in place to ensure that its directors of a different primary language (to that of the other directors and the language used in key documents) understand and can contribute to the discussions at board meetings and understand and can discharge their obligations in relation to key documents highlights the challenges that diversity can entail and how processes are required to ensure that inclusion is achieved as well as diversity.

Diversity is a key cornerstone to a dynamic, effective board. A board should be able to illicit the skills required to adapt, embrace change, co-operate with key stakeholders to proactively respond to challenges, identify and exploit opportunities, harness its social licence to operate and build long-term sustainable success. Boards and directors that fail to embrace diversity (in all its forms) will become less relevant and influential.

<sup>224</sup> CGI Glass Lewis 2021 Policy Guidelines, <https://www.glasslewis.com/wp-content/uploads/2021/07/Voting-Guidelines-Australia-GL.pdf?hsCtaTracking=1b56c341-10c5-43bb-b5bb-c78db1cdd52f%7C7feec965-69fe-4885-82ce-44afabe48c70>

<sup>225</sup> Refer to commentary for Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations (4th edition).

## BOARD SIZE

The Corporations Act specifies that public company boards should have a minimum of three directors.<sup>226</sup> ASX Corporate Governance Principles and Recommendations Principle 2 states that “a listed entity should have a board of an appropriate size, composition, skills, commitment and knowledge of the entity and the industry in which it operates, to enable it to discharge its duties effectively and to add value” and that the board “should be of sufficient size so that the requirements of the business can be met and changes to the composition of the board and its committees can be managed without undue disruption. However, it should not be so large as to be unwieldy”.

In practice, the optimum size for any particular board will reflect several factors, including the:

- size and complexity of the company and its operations
- range of competencies and behavioural skills needed to handle the evolving circumstances and needs of the board and company as a whole
- need, if required, to achieve an appropriate mix of executive and non-executive directors
- need, if required, to allow for the appointment of nominee directors by institutional investors
- number and nature of board committees (audit committee, nomination committee, etc.)
- need to raise a quorum.

<sup>226</sup> Corporations Act 2001, Section 201A(2).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## FINDING AND APPOINTING NEW DIRECTORS

Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations suggests that “to promote investor confidence, there should be a formal, rigorous and transparent process for the appointment and reappointment of directors to the board”.

The recommendation commentary states that “the process for recruiting a new director, including evaluating the balance of skills, knowledge, experience, independence and diversity on the board and, in the light of this evaluation, preparing a description of the role and capabilities required for a particular appointment” is part of the role of the nomination committee. When searching for a new director, the nomination committee should thoroughly review the existing board’s strengths and weaknesses, skills and experience gaps, current age range and gender composition, and its ambitions for the future. The outcome of this process will be a brief containing detailed selection criteria approved by the board. There are numerous organisations that can assist with independent board skills assessments, as well as a range of tools and templates designed to provide guidance on better practice approaches.<sup>227</sup> All boards should adopt a proactive, systematic and transparent approach to board appointments, and develop a succession plan. The nomination committee should have specific responsibility for identifying suitable candidates, working at least 9-12 months ahead of anticipated board vacancies.

The Corporations Act imposes no educational or specific qualification requirements for directors, although the following people are excluded from holding office as a director:

- an undischarged bankrupt cannot act as a company director, or participate in the management of a company without the permission of a court<sup>228</sup>

227 Examples include Governance Institute of Australia <https://www.governanceinstitute.com.au> and Australian Institute of Company Directors <https://aicd.companyDirectors.com.au>

228 Corporations Act 2001, Sections 206B(3) and 206G.

- anyone convicted of certain offences cannot act as a director within 5 years of their conviction or release from prison, without the permission of a court<sup>229</sup> and
- anybody disqualified from managing a company as a result of a court order.

Depending on the industry in which a company operates, there may be other regulatory requirements relevant to director appointments emanating from sources other than the Corporations Act. For example, corporations regulated by APRA need to ensure compliance with CPS 510 Governance and CPS 510 Fit and Proper. Government entities are subject to different appointment processes (including candidate selection), which are outlined in the entity’s Enabling Act.

The ASX Listing Rules require that entities which are applying for listing to satisfy the ASX that each director or proposed director, the CEO or proposed CEO (if the CEO is not a director) and the CFO or proposed CFO, is of ‘good fame and character’.<sup>230</sup> Whilst this is a formal requirement that applies to companies that are seeking to be listed, the ‘good fame and character’ requirement is something that all companies should consider when appointing new directors.

The introduction of Director Identification Numbers from November 2021 will result in every director having an identification for life that will need to be recorded whenever they become a director.

Individuals are required to have a director identification number if they are a director or an alternate director who is in that capacity (“an eligible officer”) of:

- a company, a *registered* Australian body or a registered foreign company under the *Corporations Act 2001* (Corporations Act)
- an Aboriginal and Torres Strait Islander corporation registered under the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (CATSI Act)<sup>231</sup>.

229 Corporations Act 2001, Sections 206B(2) and 206G.

230 ASX Listing Rule 1.1, Condition 20.

231 ABRS, 2021, Who needs to apply and when, <https://www.abrs.gov.au/director-identification-number/who-needs-apply-and-when>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The transitional deadlines are as follows for application of an identity number which should then be shared with the relevant entity that the director is director of:

Date you become a director	Date you must apply
On or before 31 October 2021	By 30 November 2022
Between 1 November 2021 and 4 April 2022	Within 28 days of appointment
From 5 April 2022	Before appointment

Extensions have been provided for directors who are directors of Aboriginal and Torres Strait Islander corporation in accordance with the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (CATSI Act). The deadlines for these directors are:

Date you become a director	Date you must apply
On or before 31 October 2022	By 30 November 2023
From 1 November 2022	Before appointment

## APPOINTMENT PROCESS

*Initial appointment*

There are some limitations on who can be appointed as a director. For example, an individual must be at least 18 years old. A person who is disqualified from managing companies can only be appointed as a director if the appointment is made with the permission granted by ASIC or leave granted by a court.<sup>232</sup>

Directors are normally appointed by a resolution<sup>233</sup> passed by members at a general meeting of the company. Directors must provide a signed consent to act to the company prior to being appointed.<sup>234</sup>

<sup>232</sup> Corporations Act 2001, Section 201B.

<sup>233</sup> Refer to Corporations Act 2001, Section 201G for legislation regarding approval of Director appointment by members.

<sup>234</sup> Corporations Act 2001, Section 201D.

Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations recommends that a listed entity should undertake appropriate checks before appointing a person or putting forward a candidate to security holders for election as a director, and provide security holders with all material information in its possession relevant to their decision to elect or re-elect a director (including a summary of information that should be provided to help security holders make an informed decision).<sup>235</sup>

For new appointments, the board should provide the security holders with details of the candidate, including:

- biographical details, including relevant qualifications, experience and skills
- material directorships currently held by the candidate and
- potential conflicts of interests and close personal ties that may influence the candidate's judgment.

These details are particularly relevant for proposed independent director appointments, and as such, require a statement by the board as to the whether it supports the election of the candidate and their rationale. The committee would also "usually include checks as to the person's character, experience, education, criminal record and bankruptcy history"<sup>236</sup> and the introduction of Director Identification Numbers does not remove this requirement to perform appropriate due diligence.

<sup>235</sup> Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations (4th edition).

<sup>236</sup> Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations (4th edition).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Depending upon the company's constitution, the existing directors may also be able to appoint directors usually to fill casual vacancies.<sup>237</sup> If appointed in this manner, public companies must confirm the appointment by resolution at the company's next AGM.<sup>238</sup> In the case of a proprietary company governed by the Replaceable Rules, the appointment must be confirmed by the company within 2 months of the time the appointment is made;<sup>239</sup> ASIC must be notified within 28 days of an appointment. Listed companies must comply with the relevant ASX Listing Rule requirements, (some of which may also be included in a company's constitution), which include, for instance, the requirement to hold director elections each year and director rotation requirements.<sup>240</sup>

**Director letter of appointment**

When a new director has consented to the appointment, they should receive a letter of appointment setting out the key terms and conditions of the appointment. The form of the agreement will differ depending on whether the director holds an executive or non-executive position. There are a number of guides<sup>241</sup> as to what should be included in appointment letters, although this will generally depend on the size, structure and individual circumstances of the company. Listing Rule 3.16.4 requires an entity to disclose the material terms of any employment or service contract (or any variation to it) with the CEO (or equivalent) and any of its directors. For a general guide of what should be included in a non-executive director or executive director (or other senior executive) agreement, refer to the ASX Corporate Governance Principles and Recommendations commentary to Recommendation 1.3.

<sup>237</sup> Corporations Act 2001, Section 201H.

<sup>238</sup> Corporations Act 2001, Section 201H(3).

<sup>239</sup> Corporations Act 2001, Section 201H(2).

<sup>240</sup> See specifically ASX Listing Rules 14.3, 14.4 and 14.5.

<sup>241</sup> Refer to AICD guidelines on letter of appointment for Directors [https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/nfp/pdf/05446-7-5-6-appointment\\_a4\\_web.ashx](https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/nfp/pdf/05446-7-5-6-appointment_a4_web.ashx), ACNC guide on letter of appointment for responsible persons <https://www.acnc.gov.au/tools/templates/letter-appointment-for-responsible-persons> and Governance Institute of Australia's 'Good Governance Guide — Letters of appointment for non-executive Directors: suggested contents' and 'Letter of Appointment' template available at <https://www.governanceinstitute.com.au/>

**Director due diligence**

The role of the company director has become increasingly onerous and time consuming with directors bearing increased responsibility and liability. It is critical for prospective directors to undertake their own due diligence on the companies they are invited to join, to ensure they can make a useful contribution and effectively discharge their duties.

Prior to accepting a board appointment, an individual should:

- investigate the particular company and the industry in which it operates
- gather information about the people in leadership roles and arrange to speak with key directors and senior management
- review documentation supplied by the company, such as company policies and strategy
- be satisfied that they are equipped with the requisite skills and knowledge to properly discharge the responsibilities of a director and
- assess their ability to contribute the requisite technical and inter-personal skills to enable them to build effective working relationships with the rest of the board and the executive team.

Board members must have a personal contingency plan to deal with the additional time constraints and commitment required during a particularly busy or challenging period for an entity, whilst balancing other work and personal commitments. Going one step further, directors should consider how they would handle an unanticipated surge in workload from other board roles.<sup>242</sup>

The AICD's *Director Tools: Board composition – evaluating an organisation before joining* is a useful point of further reference.<sup>243</sup>

<sup>242</sup> Refer to AICD, 2018, Final round of Royal Commission hearings, <https://aicd.companydirectors.com.au/membership/membership-update/final-round-of-royal-commission-hearings>

<sup>243</sup> AICD, Evaluating an organisation before joining, <http://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/2019/individual/07236-5-1-evaluating-an-organisation-before-joining-fa.ashx>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DIRECTOR INDUCTION

In light of the Hayne Royal Commission there should be a concerted focus on getting directors 'up to speed' as quickly as possible.<sup>244</sup> The need to get new directors 'up to speed' as quickly as possible relates not only to directors' due diligence, but also to the induction provided by entities, as induction programs make it more likely that new directors can make an immediate contribution.

Director induction programs are designed to make the most out of a director's existing knowledge base by filling any knowledge gaps, typically concerning the company's industry, the competitive landscape and technical issues, as well as familiarising the director with all aspects of the company, including risk management. Increasingly, induction is also recognized as a key tool in a company's ethical framework, used to instil the desired cultural values and behaviours of the organization. Professional development aids the reinforcement of those values and principles.

There is no prescriptive formula for what should be included in an induction program. The elements of the program should be tailored to take account of the appointee's knowledge and experience, and will vary depending on company structure, processes and the major issues it faces.

Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations suggests that a company should have an induction program in place for new directors. Recommendations 1.4 and 2.1 of The ASX Corporate Governance Principles and Recommendations suggest that it is the responsibility of the company secretary and the nomination committee to organise and facilitate the induction and professional development of directors.<sup>245</sup> An induction program for a new director may include the following:

- **corporate information** – mission statement, values and code of conduct, strategic and business plans, financial accounts, legal and regulatory frameworks, major shareholders, corporate communications, overview of the company's competitors and industry information, risk profile and appetite, company history and product information
- **governance framework** – board charter/governance statement, annual agenda, selected board packs, full details of directors, committee structures, Board process, assurance providers, resources available, key stakeholders, procedures for sign-off of financial statements and items requiring approval outside of board meetings
- **management information** – names and background of senior management, organisational and management structure outline, etc.
- **legal and accounting training** – if a new director is not familiar with the legal framework that governs the entity and/or if the director does not have accounting skills or knowledge<sup>246</sup> and
- **technology training** – to optimize the use of dashboards and other technology in the boardroom. Technology training at the induction stage may also facilitate the directors' adoption of new technology in the future.

Both the AICD and Institute of Community Directors provide free guidance on their website regarding the typical matters covered in an induction pack.<sup>247</sup>

Typically, a combination of written materials, coupled with presentations and activities, such as meetings and site visits, will provide the appointee with a realistic picture of the company's position and the challenges it faces. It will also serve to foster a constructive relationship between the new director and their fellow directors and senior management. In addition to the provision of induction materials, it is also important to schedule interviews with key senior executives to gain an understanding of the entity's structure, business operations, history, culture, and key risks.<sup>248</sup>

<sup>244</sup> Refer to AICD, 2018, Final round of Royal Commission hearings, <https://aicd.companydirectors.com.au/membership/membership-update/final-round-of-royal-commission-hearings>

<sup>245</sup> Recommendations 1.4 and 2.1 of the ASX Corporate Governance Principles and Recommendations (4th edition).

<sup>246</sup> Refer to Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition)

<sup>247</sup> Refer to Institute of Community Directors <https://communitydirectors.com.au/check-lists/checklist-for-an-effective-induction>

<sup>248</sup> Refer to commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

An induction to board committees, with particular emphasis on those board committees which the new director will join, should not be overlooked. An induction pack containing relevant documents such as committee charters, annual agendas, copies of minutes, plus a full briefing by the relevant committee chair will help the new director gain an appreciation of the major issues.

## DIRECTOR PROFESSIONAL DEVELOPMENT

As well as providing induction programs for new directors, boards should also encourage and finance continuing director education.

Through the board evaluation process, areas will be identified where further education may enhance board and individual director effectiveness. The board should ensure that resources are budgeted to provide appropriate educational opportunities for directors. The chair should address the developmental needs of the board as a whole, plus those of individual directors, with the company secretary playing a key role in facilitating the process.

The commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations recommends that professional development for directors should be considered where gaps are identified and they are not expected to be addressed in the short term by new appointments.<sup>249</sup> The commentary further notes that "the board or nomination committee should ensure that directors receive briefings on material developments in laws, regulations and accounting standards relevant to the entity". As the need to interpret and critique non-financial reports becomes increasingly relevant, boards would also be wise to broaden the scope of such briefings and director training programs to include integrated reporting. The development of behavioural skills to help embed the cultural "tone from the top" is also likely to become increasingly important.

Professional development requires an ongoing commitment from individual directors to continually reflect, learn, challenge and adapt.

<sup>249</sup> Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

Directors with long tenures can often feel that they know the business and their role well enough to not require ongoing education, however, the reverse is often the case. Such complacency is a key component of the 'chronic ease' and over-reliance on key individuals repeatedly criticised of CBA in the APRA CBA report.<sup>250</sup> Complacency and over-confidence can quickly make directors – and their organisations – irrelevant. Directors who do not value and engage in professional development are red flags for any board.

## THE FIRST 100 DAYS FRAMEWORK

Directors appointed to newly formed boards are required to oversee the challenging task of establishing a functioning boardroom and effective corporate governance structure. The first 100 days framework provides a high-level roadmap of the key activities and deliverables needed to establish an effective board within a target timeframe of 100 days. It can be applied for new boards or used as a checklist for existing boards.

The framework begins by establishing a direction and clear set of priorities for the newly established board. During this stage, the board should document its plan, and establish timelines and accountabilities around achieving its milestones.

Importantly, the board should then consider its risk management – setting its overall 'risk appetite' and documenting what it considers are the critical risks facing the organisation. With these considerations in mind, the board should then define its target operating model, appoint its key management personnel and endorse policies to guide the organisation.

While this is occurring, the board should be engaging shareholders and key stakeholders and overseeing the development of an accountability and compliance framework.

<sup>250</sup> Refer to the Executive Summary, Sections 2.2.2, 2.2.3, 9.2.6 and 9.2.7 and of APRA Prudential Inquiry into The Commonwealth Bank of Australia report (April 2018) [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

First 100 days framework

Governance priorities	Risk profile	Operating model	Stakeholder framework	Compliance
<ul style="list-style-type: none"> <li>- Terms of reference</li> <li>- Charter and annual agenda</li> <li>- Financial compliance</li> <li>- Legal and compliance duties</li> <li>- Retained authorities</li> <li>- Delegations/ CEO limitis</li> <li>- Code of conduct</li> <li>- Strategic plan</li> </ul>	<ul style="list-style-type: none"> <li>- Risk mangement policy</li> <li>- Risk workshop</li> <li>- Agree and validate critical risks</li> <li>- Risk register</li> <li>- Risk monitoring and mitigation</li> <li>- Risk reporting framework</li> </ul>	<ul style="list-style-type: none"> <li>- Policies:                             <ul style="list-style-type: none"> <li>- Conflicts of interest</li> <li>- Regulatory compliance</li> <li>- Privacy</li> <li>- Whistleblower &amp; Fraud</li> <li>- Media/crisis/incident</li> <li>- Continuous disclosure</li> </ul> </li> <li>- Target operating model</li> <li>- Key appointments CEO/ CFO</li> </ul>	<ul style="list-style-type: none"> <li>- Communication policy</li> <li>- Internal/shareholders/ community/government</li> <li>- Shareholder relations</li> <li>- Mapping &amp; tiering</li> <li>- Engagement plan</li> <li>- Consultation model</li> <li>- Shareholder and consumer participation forums</li> </ul>	<ul style="list-style-type: none"> <li>- Compliance framework</li> <li>- Internal and external auditor appointment</li> <li>- Audit and risk committee</li> <li>- Consequence and breach policy</li> <li>- Reporting &amp; oversight</li> <li>- Board performance assessments</li> </ul>
Leadership & strategy	Risk management	Peformance & monitoring	Stakeholder engagement	Accountability & audit
<i>Informed discussions and decisions, not an endless stream of surprises.</i>	<i>Proactive, strategic tool, not a reactive function.</i>	<i>Healthy culture supported by strong policies, not an inconsistent 'tone at the top'.</i>	<i>Active stakeholder consultation, not disengagement from the process.</i>	<i>Tailored assurance and reporting, not a 'one size fits all' approach.</i>

BOARD EVALUATION

As previously stated in the 'Finding and appointing new directors' section of this chapter, Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations states that "to promote investor confidence, there should be a formal, rigorous and transparent process for the appointment and reappointment of directors to the board." The reappointment of directors is inextricably linked to the evaluation of the board.

Board evaluation is also a useful process in identifying the critical success factors for improving the effectiveness and efficiency of the board and its committees. It encourages directors to examine their own contribution and, when expertly facilitated, can improve working relationships between directors.

Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations recommends that a listed entity should have,

and disclose, a process for periodically evaluating the performance of the board, its committees and individual directors, and should disclose whether the performance evaluation was undertaken in accordance with that process during the reporting period.<sup>251</sup> Other standards, including Australian Standards Good Governance Principles AS 8000-2003 and Prudential Standard CPS 510 Governance include similar recommendations.

The commentary for Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations suggests that the nomination committee should consider implementing a plan for evaluating the balance of skills, knowledge, experience, independence and diversity on the board. The rationale for this approach is that such an evaluation will enable the identification of specific skills that will best increase board effectiveness.

<sup>251</sup> Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations also notes that the board or nomination committee should regularly assess/evaluate whether the directors as a group have the skills, knowledge and experience to deal with new and emerging business and governance issues. These may include cyber security, AI and data analytics, climate change, conduct and culture related matters.

**Evaluation of non-executive directors and the chairperson**

Principle 2 of The ASX Corporate Governance Principles and Recommendations emphasises the importance of the board's ability to evaluate the independence of its independent directors. Recommendations 2.3 and 2.4 focus specifically on independent directors. The wording of *Box 2.3 – Factors relevant to assessing the independence of a director* of The ASX Corporate Governance Principles and Recommendations has seen a number of amendments since the 3rd edition to simplify the wording and expand the factors for consideration when evaluating a director's independence and is a useful point of reference.<sup>252</sup>

The commentary for Recommendation 2.1 also suggests that the board or nomination committee should "regularly review the time required from a non-executive director and whether directors are meeting that requirement".<sup>253</sup> The time committed by directors was also one of the governance-related issues highlighted during the Hayne Royal Commission. It may be argued that the increasing demands of governing large and complex corporates has resulted in the need for non-executive directors to dedicate more time to their roles, in order to sufficiently discharge their duties. Consequently there is some debate about the scope for directors to hold multiple board roles.<sup>254</sup>

<sup>252</sup> Refer to commentary for Recommendation 2.3 of The ASX Corporate Governance Principles and Recommendations (4th edition)

<sup>253</sup> Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations (4th edition).

<sup>254</sup> Refer to Section 1.1.1 of the 'AICD's Essential Director Update:18' <http://aicd.companyDirectors.com.au/-/media/cd2/resources/events/essential-Director-update/pdf/06729-10-edu-essential-Director-update-2018-handbook-a4-web.ashx>

The commentary for Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations specifies that "a suitable non-executive director (such as the deputy chair or the senior independent director, if the entity has one) should be responsible for the performance evaluation of the chair, after having canvassed the views of the other directors".

**Evaluation of senior executives**

Recommendation 1.7 of the ASX Corporate Governance Principles and Recommendations states that "it is essential that a listed entity has in place a proper process for regularly reviewing the performance of its senior executives and addressing any issues that may emerge from that review". According to the Recommendation "a listed entity should:

- have and disclose a process for evaluating the performance of its senior executives at least once every reporting period and
- disclose for each reporting period whether a performance evaluation has been undertaken in accordance with that process during or in respect of that period".

**The evaluation process**

Some of the issues to consider when designing an evaluation include:

- the type of assessment and evaluation process to be used (e.g. qualitative, quantitative or a combination of both)
- the scope of assessment and evaluation
- who should perform the assessment and evaluation process (in-house, chair, external independent facilitator) and
- the timing and frequency of the assessment and evaluation.

A gap analysis between how the board or committee actually works and good board practice is a useful starting point for any evaluation. Conducting regular board and committee evaluations also sends a signal to the marketplace that the company is serious about governance and enhancing its performance. Shareholders and proxy voters are beginning to take more notice of whether companies engage in this practice.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The commentary for Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations states that “the board should consider periodically using external facilitators to conduct its performance reviews”. Consequently, it is now increasingly common for companies to engage an external consultant to facilitate a board review at least every 2 years, with an internal review usually facilitated by the chair every other year. As well as offering independence, an external expert facilitator can help to shine a light on previously unthought-of aspects of the evaluation process that will glean further opportunities for board development and succession planning.

The board or nomination committee can address gaps identified during the evaluation process through professional development and/or succession planning (both of which are covered separately in this chapter).

## DIRECTOR REMUNERATION

Directors are not entitled to payment for services unless this is provided for in the constitution of the organisation or approved in a resolution of shareholders. The Act provides that “the directors of a company are to be paid the remuneration that the company determines by resolution”.<sup>255</sup> The company ‘may’ also pay the directors’ travelling and other expenses that they properly incur:

- In attending directors’ meetings or any meetings of committees of directors
- In attending any general meetings of the company
- In connection with the company’s business.<sup>256</sup>

The Corporations Act provides that member approval is not required to approve the remuneration of a director of a public company.<sup>257</sup>

<sup>255</sup> Corporations Act 2001, Replaceable Rule Section 202A(1).

<sup>256</sup> Corporations Act 2001, Replaceable Rule Section 202A(2).

<sup>257</sup> Corporations Act 2001, Section 211.

Executive remuneration continues to be a hot topic globally and in Australia, particularly in light of the Hayne Royal Commission findings and the APRA CBA report. Both criticized the financial services industry’s remuneration policies, incentivised sales practices and culture and questioned the adequacy of boards’ oversight of remuneration structures.<sup>258</sup>

The process for determining levels of remuneration for directors is complex and involves balancing the interests of a number of stakeholders. A balance needs to be struck between attracting, motivating and retaining highly skilled directors, and paying an appropriate level of fees that properly reflect the responsibilities of the directors, the size and complexity of the company and its operations, the industry sector, the shareholders’ vote on the remuneration at the AGM (and likelihood of a two strikes occurring against the remuneration report), the time commitment required of the director, the director’s qualifications and experience and any other duties to be carried out within the role (e.g. chair of certain board committees).

The ASX Corporate Governance Principles and Recommendations also recommends that a board of a listed entity should have a separate remuneration committee as an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to remuneration decisions. The commentary to Recommendation 8.1 also sets out which matters the remuneration committee should consider when making recommendations to the board.<sup>259</sup>

Companies should clearly distinguish and separately disclose the policies and practices regarding the structure of non-executive directors’ remuneration from that of executive directors and senior executives.<sup>260</sup>

<sup>258</sup> Refer to Section 1.1.1 of the ‘AICD’s Essential Director Update: 18’ <http://aicd.companyDirectors.com.au/-/media/cd2/resources/events/essential-Director-update/pdf/06729-10-edu-essential-Director-update-2018-handbook-a4-web.ashx>

<sup>259</sup> Recommendation 8.1 of the ASX Corporate Governance Principles and Recommendations (4th edition). Refer to chapter 3.4 for further information on committees.

<sup>260</sup> Recommendation 8.2 of the ASX Corporate Governance Principles and Recommendations (4th edition).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The ASX Corporate Governance Principles and Recommendations provide some useful guidance on formulating remuneration policies and practices for both executives and non-executives, in the commentary to Recommendation 8.2. It is critical that the board establishes a process by which directors can determine both their structure and remuneration levels in an objective manner.

It is important to ensure that a director is being paid fairly and appropriately in light of the specific responsibilities and risks associated with the role, their memberships on particular committees, the time required to discharge their duties to the company and the size and complexity of the business as a whole. This should involve reviewing the director's remuneration annually, and can include a peer group benchmarking review, if warranted.

**Listed companies remuneration**

Shareholders of public companies generally approve an upper limit or pool of fees for the board as a whole in general meeting. The board then determines how this is distributed to individual directors. Many companies obtain by resolution an upper limit to the total amount to be paid on an ongoing basis and then infrequently seek to have this increased. Usually companies do not allocate this total amount. A listed company will need to have sound reasons for seeking an increase to this amount.<sup>261</sup>

**Non-executive director remuneration**

For listed companies, the company must obtain shareholder approval for any increase to the maximum aggregate of non-executive director fees, from which fees to non-executive directors for their participation on the board and board committees should be paid (inclusive of superannuation).<sup>262</sup>

Non-executive director compensation should be:

- determined by the board and disclosed completely to shareholders
- aligned with the long-term interests of shareholders and
- at a level to adequately compensate directors for their time and effort.

Non-executive directors should normally be remunerated by way of fees, in the form of cash, non-cash benefits, superannuation contributions or salary-sacrifice shares. The AICD supports the view that individual directors should have the freedom to nominate the proportion of their total remuneration that falls into each category.<sup>263</sup> As a general rule, compared with executives, non-executive directors should not receive options or bonus payments which are dependent on the satisfaction of performance conditions, as this can bias their judgment in favour of short-term performance. Non-executive directors should not be provided with retirement benefits (other than superannuation), as entitlements to benefits that accrue over time may discourage directors from retiring or resigning from the board at the most appropriate time.

Some boards also pay a travel allowance where board meetings are held internationally and directors are required to commit to significant travel time to attend meetings.

Many argue that directors should build a material share ownership in the company to directly link directors' interests to those of the shareholders. There is an increasing trend towards companies adopting policies requiring or encouraging non-executive directors to acquire a minimum shareholding in the company. If it is a listed company, the ASX should be notified of those shareholdings within the required timeframe,<sup>264</sup> noting blackout periods that should be detailed in the listed entity's trading policy.

The GIA provides some useful guidance and basic principles that should be considered in establishing a non-executive director share ownership policy.<sup>265</sup>

<sup>263</sup> GIAs, Good Governance Guide: Director remuneration – non-executive share ownership, 2012.

<sup>264</sup> Corporations Act 2001, Section 205G.

<sup>265</sup> GIA, Good Governance Guide: Director remuneration – non-executive share ownership, 2012.

<sup>261</sup> AICD, 2017, Directors' fees, <https://aicd.companydirectors.com.au/resources/Director-tools/practical-tools-for-Directors/board-composition/Directors-fees>

<sup>262</sup> ASX Listing Rule 10.17.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Larger organisations will often develop a fee system that compensates directors according to the number of sub-committees in which they participate, and whether they participate as the chair or member. Some further issues to take into account when setting fees are the company's current policy with regard to board fees, the experience and knowledge of the potential director, the indicative level of remuneration being paid to directors in comparative companies (of size and industry) and the size and complexity of the business.

In some circumstances, such as takeovers and mergers, directors may be required to spend considerably more time reviewing proposals or responding to the situation. In these circumstances, it has become more common for directors to receive additional remuneration to take account of the extra time.

Volunteer board members, including directors of government entities, are often entitled to claim 'reasonable' expenses. The specific details will be outlined in the letter of appointment, supported by the relevant board charter or Enabling Act (whichever applies).

**Executive director remuneration**

It is increasingly acknowledged that executive director remuneration should be structured to achieve two main purposes, to:

- align the interests of shareholders and directors and
- reward executives for their contribution towards the achievement of company objectives.

Remuneration for executive directors (and other executives) should include an appropriate balance of fixed remuneration and short and long term performance-based incentives. Commentary to Recommendation 8.2 of the ASX Corporate Governance Principles and Recommendations sets out those guidelines for executive remuneration.<sup>266</sup>

<sup>266</sup> Box 8.2 / Suggested guidelines for: Executive remuneration; Non-executive director remuneration, ASX Corporate Governance Council's, Corporate Governance Principles and Recommendations, 4<sup>th</sup> Edition.

**Remuneration Report – two strikes rule**

Listed companies must account annually for directors' fees as well as the remuneration paid to senior management under Section 300A of the Corporations Act.

The Act was amended from 1 July 2011 to provide for the 'two strikes' rule in relation to the remuneration report. At the AGM, the shareholders must vote approval or otherwise of the remuneration report. The first strike is when a company's remuneration report receives a 'no' vote of 25 percent or more. Where this occurs, the company's subsequent remuneration report must explain whether shareholders' concerns have been taken into account, and either how they have been taken into account or why they have not been taken into account.

The 'second strike' occurs where the company's subsequent remuneration report receives a 'no' vote of 25 percent or more. Where this occurs, shareholders will vote at the same annual general meeting to determine whether the directors will need to stand for re-election within 90 days. If this resolution passes with 50 percent or more of eligible votes cast, then the 'spill meeting' will take place within 90 days. At the spill meeting, those individuals who were directors when the report was considered at the most recent annual general meeting will be required to stand for re-election (other than the managing director, who is permitted to continue to run the company).<sup>267</sup>

The number of ASX300 companies receiving a strike on their remuneration report in recent years has been as follows:

- 2018: 20 companies (6.7 percent)
- 2019: 24 companies (8.0 percent)
- 2020: 25 companies (8.3 percent)

While this represents an upward trend, at the time of writing this, a lower number of strikes are expected to be received for 2021.

<sup>267</sup> AICD, Director Remuneration, <https://aicd.companydirectors.com.au/resources/all-sectors/Director-remuneration>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The most common reasons observed for remuneration report strikes are as follows:

- Executive bonus outcomes are not aligned with business performance/shareholder outcomes
- Overall quantum of remuneration is too high
- The executive remuneration structure viewed as inappropriate (e.g. incentives are not performance tested, ad-hoc awards are paid, Boards apply upward discretion in a manner deemed too generous)
- Overall dissatisfaction with performance of the company or Board (e.g. shareholders using the remuneration report resolution as an opportunity to demonstrate discontent with company matters more broadly, rather than just on executive remuneration)

The GIA website provides further guidance in relation to managing members' expectations on remuneration-related resolutions and dealing with the fall-out of a second-strike.<sup>268</sup>

**Not-for-profit companies remuneration**

Not-for-profit organisations may or may not pay directors. Some not-for-profits take the view that directors should see their contribution as service to the community and hence receive no remuneration outside of reasonably occurred expenses. Others, usually larger, not-for-profits take the view that they expect a considerable workload from directors and are seeking directors with high levels of skills. The AICD's 2021 not-for-profit survey found that although the proportion of directors receiving some remuneration, expenses or an honorarium for their roles has increased, the expectation for their roles has intensified during the pandemic with an increased time commitment.<sup>269</sup>

<sup>268</sup> Refer to Governance Institute of Australia, Guidelines on managing voting exclusions on remuneration-related resolutions and Managing the requirements of a second strike, <https://web.governanceinstitute.com.au/home/>

<sup>269</sup> AICD, 2021, Not-for-Profit Governance and Performance Study, <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/nfp/pdf/not-for-profit-governance-and-performance-study-2021-a4-web.ashx>.

When a not-for-profit company is a registered charity, the provisions of the Corporations Act, the Australian Charities and Not-for-profits Commission Act 2012, and the Australian Charities and Not-for-profits Commission (ACNC) Governance Standards must be considered. While not specifically mentioning payment to directors, the ACNC Governance Standard 2 is relevant:

“Charities that have members must take reasonable steps to be accountable to their members and provide them with adequate opportunity to raise concerns about how the charity is governed”.

Under this Governance Standard it can be expected that the charity will seek members approval of the total amount of the proposed directors' remuneration and provide details, usually as part of the annual report, as to what payments were made to directors. In short, although not legally required, it is recommended that not-for-profits which pay directors adopt many of the practices concerning approval and reporting as apply to listed companies.<sup>270</sup>

**RE-ELECTION AND ROTATION OF DIRECTORS**

For non-listed companies, the requirement and terms of the re-election of directors is dependent on the company's constitution.

For listed companies, ASX Listing Rules 14.4 and 14.5 require all directors, other than the managing director, to stand for re-election at the company's AGM at least once every three years. ASX Listing Rule 14.3 requires that a company must accept nomination for the election of directors up to 35 business days prior to the AGM, unless the company's constitution provides otherwise.

Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations recommends that for directors standing for re-election, the board should provide the security holders with details of the term of office currently served by the director and, if the candidate standing for re-election is to be an independent director, a statement to that effect and a statement by the board as to whether it supports the re-election of the candidate and its reasons why.

<sup>270</sup> Australian Charities and Not-for-Profits commission (ACNC), Meet governance standards, <https://www.acnc.gov.au/tools/topic-guides/governance-standards>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The board should also consider the evaluation of the candidate's independence when providing details. Further details can be found in the 'Board Evaluation' section of this chapter.

## BOARD SUCCESSION PLANNING

Board succession planning challenges boards to anticipate and plan for their future needs. It should be a continuous process that is regularly considered by the board so that changes in the board composition can be anticipated and planned for in advance.

Its role in the company's strategic success has increased in significance due to the increased pressure for non-executive directors to limit the number and tenure of directorships<sup>271</sup> and for boards to actively monitor the length of service of each director, as independent from management and substantial holders who are perceived to be potentially compromised over time.<sup>272</sup>

Recommendation 2.1 of The ASX Corporate Governance Principles and Recommendations sees "board succession planning generally" as one of the roles of the nomination committee.

Board succession planning is built on:

- an assessment of the challenges and opportunities facing the company, now and in the future (and therefore strongly aligned to the strategy development process)
- an analysis of the core skills, competencies and behaviours that are required, both immediately and in the future, for both the board and its committees
- an evaluation of the skills, competencies and behaviours of existing directors, including their strengths and weaknesses, skills and experience gaps, current age range and gender composition, and length of tenure

<sup>271</sup> Refer to Section 1.1.1 of the 'AICD's Essential Director Update: 18' <http://aicd.companyDirectors.com.au/-/media/cd2/resources/events/essential-Director-update/pdf/06729-10-edu-essential-Director-update-2018-handbook-a4-web.ashx>

<sup>272</sup> Refer to 'Box 2.3 – Factors relevant to assessing the independence of a Director' of the ASX Corporate Governance Principles and Recommendations (4th edition).

- assessments of existing directors' performance and
- assessments of non-executive directors' independence.

Recommendation 1.5 of The ASX Corporate Governance Principles and Recommendations states that gender diversity should also be a relevant consideration in succession planning.

## Succession planning for chairperson

In developing a succession plan, the chair's role needs to be considered by the board or nomination committee. In instances where the current chair's retirement date is known, plans can be set in place to identify a new chair, either internally or externally.

Companies should also have a contingency plan for the chair's role, in the case of some unexpected event. Previous cases of simultaneous vacancies in the roles of both the chair and managing director are a reminder to all boards of the consequences of such unplanned disruptions to a board's succession.

## DIRECTOR TENURE

KPMG Enterprise's report "*Secrets to success of the ASX 300+: Six priorities of opportunity and challenge research of ASX300+ companies*" found that in 2016 companies with a chairperson of ten years or more tenure delivered significantly better financial performance in terms of revenue growth<sup>273</sup> compared to the rest of the group surveyed. This helps to understand the resistance to challenge these long-held appointments and potentially disrupt the company's successful financial strategy. However, as identified in the report, a key challenge facing these companies is the risk of becoming stale through a lack of diversity of thought and opinion.

<sup>273</sup> Refer to Priority Six-Tenure and Remuneration, key findings of KPMG Enterprise's report *Secrets to success of the ASX 300+: Six priorities of opportunity and challenge* <https://assets.kpmg.com/content/dam/kpmg/au/pdf/2017/secrets-to-success-asx-300-mid-market-enterprises.pdf>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

As stated in the Succession Planning section of this chapter, the commentary for Recommendation 2.1 of ASX Corporate Governance Principles and Recommendations states that “board renewal is critical to performance”. There is a danger that long-standing directors become entrenched and lose their ability to consider issues from an impartial and objective standpoint. Tenure has been cited as one of the key criteria for evaluating the independence of NEDs in the ASX Corporate Governance Principles and Recommendations;<sup>274</sup> for this reason, many listed companies adopt a director tenure policy providing for a maximum term of office (e.g. 9 years), with any extension being subject to annual approval. A company's constitution can also provide for situations in which a director's office is to be vacated at any given point in time (e.g. unsoundness of mind).

A director may resign by giving notice in writing to the company, unless the company's constitution provides otherwise.<sup>275</sup> The company must notify ASIC of the resignation within 28 days.<sup>276</sup>

Removing a director who is unwilling to leave is a difficult situation. By law, the directors of a public company cannot pass a resolution requiring a director to vacate office;<sup>277</sup> only by resolution of a general meeting can the company remove a director.<sup>278</sup> The law prescribes a process for the removal in which the director has a right to put their case to the members.<sup>279</sup>

<sup>274</sup> Refer to Recommendation 1.6 of ASX Corporate Governance Principles and Recommendations (4th edition).

<sup>275</sup> Corporations Act 2001, Replaceable Rule Section 203A.

<sup>276</sup> Corporations Act 2001, Section 205B(5).

<sup>277</sup> Corporations Act 2001, Section 203E.

<sup>278</sup> Corporations Act 2001, Section 203D.

<sup>279</sup> Corporations Act 2001, Section 203D(4).

## ACCESS TO COMPANY RECORDS

The Corporations Act provides that directors (both current and former) have a legally enforceable right of access, at all reasonable times, to the company's books for the purposes of a legal proceeding:

- to which the director is a party
- which a former director proposes to bring in good faith and
- which a director has reason to believe will be brought against them.<sup>280</sup>

This right extends for a period of 7 years after the person ceases to be a director of the company, and also includes the right to inspect the company's financial records.<sup>281</sup>

It is generally established practice for:

- directors not to retain individual copies of board papers and
- a deed of access between the company and each director to be executed.

<sup>280</sup> Corporations Act 2001, Section 198F(1).

<sup>281</sup> Corporations Act 2001, Section 198F(2).



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The board could consider adopting an information policy which provides that the company secretary holds a complete set of board and committee papers. Under this policy, directors should be entitled, on request, to access board papers for the period during which they were a director, even if they have ceased to be a director. Increasingly, such papers are being held electronically, with approval granted to directors, enabling easy access and avoiding the need for the retention of papers by individual directors.

The Governance Institute of Australia also recommends that it is good governance to execute a deed between the company and a director, which sets out the rights of the director to access board papers and/or company information and how such information may be used.<sup>282</sup>

<sup>282</sup> Refer to GIA's Good Governance Guide 'Director and ex-Director access to company information' available on <https://www.governanceinstitute.com.au/>

## Useful references

- Corporations Act 2001
- ICSA Guidance Note, 2021, Due Diligence for Prospective Directors.
- AICD, Appointing a new Director: Role of the Board, [https://aicd.companyDirectors.com.au/-/media/cd2/resources/Director-resources/Director-tools/pdf/05446-5-1-Director-tools-rob-appointing-new-Director\\_a4\\_web.ashx](https://aicd.companyDirectors.com.au/-/media/cd2/resources/Director-resources/Director-tools/pdf/05446-5-1-Director-tools-rob-appointing-new-Director_a4_web.ashx)

## For further information please contact:

**Andrew Holland**

**Director,**  
**Performance & Reward**  
**[aholland1@kpmg.com.au](mailto:aholland1@kpmg.com.au)**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 10. Company Leadership

Most boards would agree that one of their most important governance roles is hiring and possibly replacing the CEO. After all, the CEO is responsible for the day-to-day operations of the organisation and is instrumental in both the development and execution of corporate strategy.

## In this chapter

- CEO and executive management
- Executive remuneration
- Role of the CEO
- Executive service agreements

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Does the board have confidence in the skills and capabilities of the CEO and the senior management team? What process or approach is in place to help to objectively validate this view?
2. How does the CEO encourage and support the talent pipeline through attraction, development and retention of high potential employees?
3. What is the 'tone at the top', as understood and experienced by layers below?
4. Does the board have in place a robust and fit-for-purpose succession readiness program that is ready to support a CEO replacement process at any time and is supported by internal executive talent development?
5. Prior to the appointment of a new CEO, does the board (through the chairman or nomination committee) conduct a rigorous succession evaluation process?
6. Is the CEO's view regarding senior management team members and other talented people with strong leadership qualities considered?
7. Does the board have a CEO and senior management succession plan that is regularly (e.g. semi-annually) considered and reviewed for relevance, given the operating environment of the organisation at the time of review (such that talent is considered in the context of the current and prospective operating environment)?
8. Are concerns about the CEO's performance discussed with the CEO and appropriately documented?
9. Does the board have a transparent process for determining management remuneration?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The CEO selection process was conducted largely in-house within a pool of board members' friends and business associates.
- Support and confidence in the CEO is divided amongst board members.
- The CEO does not have KPIs or they are often not being met.
- Remuneration setting is discussed mostly privately.
- CEO performance appraisal is conducted infrequently and informally.
- No contingency plan or succession plan exists for the current leadership structure; or the plans that do exist lack substance and meaningful engagement (i.e. box checking).
- The CEO seems focused mostly on achieving their own remuneration targets.
- There is no senior executive development plan in place.
- There is no regular review or external assessment of senior executive talent.
- The board has restricted or no access to senior management.
- The board is often drawn into operational matters due to lack of confidence in and/or capability of the executive.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## CEO AND EXECUTIVE MANAGEMENT

The CEO should be involved in nearly all board discussions and input into decisions, where appropriate. They should also have meaningful delegated authority to enable the execution of the enterprise's strategy. The CEO is pivotal to establishing and reinforcing to all stakeholders the 'tone' of what is expected of the enterprise to all stakeholders; they play a key role in representing the organisation to external parties.

It is usual practice for a CEO to establish an executive management team (or similar) which will:

- provide support to the CEO
- exchange information and ideas
- constructively develop and implement strategies and management frameworks
- provide input on the organisation's direction
- influence the organisation at all levels.

Building a strong executive management team is essential for organisational success. Factors associated with strong organisational leadership include:

- respective board and management roles and responsibilities clearly delineated and articulated in writing
- board protocols covering directors' access to executive managers outside of board meetings
- a CEO that provides appropriate direction, mentoring, support and guidance to executive management team members
- executive management team members who are empowered to share leadership responsibilities
- executive management team members who are rewarded for organisational, business unit and individual performance, based on behavioural standards displayed and value creation outcomes

- management succession and development plans that cover all key positions, based on competencies, behaviours and experience to achieve the strategic vision
- full disclosure of conflicts of interest.

**“Leaders establish the vision for the future and set the strategy for getting there; they cause change. They motivate and inspire others to go in the right direction and they, along with everyone else, sacrifice to get there.”**

DR JOHN KOTTER, KONOSUKE MATSUSHITA PROFESSOR OF LEADERSHIP, EMERITUS (HARVARD BUSINESS SCHOOL)

## ROLE OF THE CEO

It goes without saying that, as a company's most senior officer, the CEO is critical to the performance of the enterprise. The scope of activities and responsibilities assigned to the CEO are broad and far-reaching. Through their attitudes and behaviours, CEOs are instrumental in reinforcing the 'tone' of their organisations.

An effective CEO:

- leads with clear purpose and actions this purpose through providing clarity to the organisation
- actively develops direct reports and sponsors organisation-wide people development
- is consultative, as well as courageous, in making the decisions needed
- always acts with integrity
- drives strategic vision and innovation
- is resilient in the face of setbacks
- successfully adapts to the company's everchanging circumstances
- demonstrates high-level business acumen
- meets immediate performance targets without neglecting longer-term growth opportunities

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The titles CEO and managing director (MD) are often used interchangeably. In theory, a CEO does not necessarily have a seat on the company's board, whilst the MD is, by definition, a director.

**Delegated authority**

In putting its relationship with the CEO on a sound footing, a board needs to formulate a CEO's job description and define the criteria for the CEO's performance-based remuneration (usually led by the chair). There should also be a formal statement delineating the boundaries between board and management responsibilities, including the board's retained authorities and those delegated to management (which is usually set out in the board charter). A high-performing board will invest time and effort in constructing an active partnership with the CEO and senior management. It will not be a relationship based mainly on supervision but one in which the board engages with the CEO and senior management to achieve outstanding results.

**Outside directorships**

Traditionally, the CEOs of many of Australia's leading companies were invited onto the boards of other public companies. The only real restriction on this practice was the avoidance of overt conflicts of interest. This practice was not considered exceptional, and was seen as a good training ground for public company directors. In recent times, as a consequence of both the size of current CEO remuneration packages and the scope of their responsibilities, this has often made outside directorships untenable.

Recent trends show examples of CEOs who are coming to the end of their management tenure may look to find an unrelated non-executive directorship. Proxy advisors appear to be comfortable with this approach for transitioning CEOs.

Former CEOs can make excellent non-executive directors in other companies. However, many who have made the move report that there is a considerable transition from being a CEO wielding considerable power and influence to the collegiate and consensus-based role of the non-executive director.

This is where having a clear understanding of the role of a director (versus being part of the executive team) is crucial for both the board and management to effectively do their jobs.

It is no longer common practice for retiring CEOs to remain on their boards in a non-executive capacity, or for retiring CEOs to assume the chair's role as it then raises issues of independence. According to the ASX Principles, a director who was previously employed in an executive capacity by the company (or another group member) will generally not be considered independent unless a period of at least three years has lapsed between the director ceasing such employment and serving on the board.<sup>283</sup>

**CEO succession planning**

The purpose of succession planning is to ensure the board always has available a number of successor candidates in the event that the incumbent CEO departs suddenly and unexpectedly. Ideally, succession planning should start from day one of a new CEO's appointment.

Each company's needs are unique and change over time, as does the available pool of talent from which a new CEO may be drawn. The board should ask the CEO to provide an assessment of the key internal contenders and what is being done to develop their strengths and overcome any limitations in order to prepare them for being succession-ready.

Some companies approach succession planning by considering different contingencies, ranging from crisis management (e.g. if something untoward were to happen to the CEO, could the company continue to operate successfully?) to long-term issues such as attraction, development and retention of individuals to be future leaders.

<sup>283</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2014, Recommendation 2.3, Box 2.3 which sets out the 'Factors relevant to assessing the independence of a director'. In each case, the board must assess the materiality of each such factor and determine whether the director has the capacity to bring an independent judgement to bear on issues before the board and to act in the best interests of the entity as a whole.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

At the heart of CEO succession planning is the notion that the board and the CEO work in cooperation to attract, develop and retain high performers who can be tried and tested prior to possibly being offered the CEO role in the future.

**Selecting a CEO**

The selection of a CEO is the most important task a board can undertake. It is also probably the most difficult. Boards should drive the succession process, although normally in collaboration with the incumbent CEO. Boards sometimes select a CEO heir-apparent well in advance of the incumbent CEO's planned departure.

For organisations with good succession planning, the selection of a CEO may appear almost automatic with a suitable successor long identified. However, as executives become more mobile and the typical CEO's job tenure continues to shrink, conventional succession planning may not identify an unequivocally acceptable internal candidate. Many boards will feel they have an obligation to look beyond a company's own executive ranks if they are to find the best available CEO.

The board must ensure that robust processes are adhered to in the lead-up to the appointment. Experience suggests that the probability of a successful outcome is enhanced if boards follow a structured appointment process.

Confidentiality is critical throughout the appointment process. Any breach will deter potential candidates and reflect poorly on directors and the company as a whole.

**CEO tenure**

CEOs are increasingly under the spotlight with boards being prepared to replace them if they consider that their CEO is not performing, or believe that future performance may not be up to the level expected.

Investment in the CEO and management team is crucial for the creation of sustained shareholder wealth. The Harvard Law School Forum on Corporate Governance note in their article titled CEO Succession Plans in a Crisis Era that "replacing an ill-chosen or

short-tenured CEO leads to a loss of \$1.7 billion in shareholder value in addition to a loss of organizational confidence and momentum".<sup>284</sup> For this reason, directors need to commit considerable time and effort to selecting a new CEO. This should be supplemented by appropriate mentoring, development, encouragement and support; a role often fulfilled by the chair of the board.

When CEO performance concerns arise, these should be discussed and addressed promptly. If it is clear that the CEO is not delivering and needs to be replaced, then the board should act without delay. Whilst the cost of replacing a CEO is considerable, the cost of not acting can be devastating.

**CEO appraisal**

The CEO performance appraisal is an important board responsibility and should take place on an annual basis. This appraisal provides:

- important feedback to the CEO about his/her performance
- increased understanding of the CEO's concerns and views on the achievement of corporate objectives
- a forum to build a healthy relationship between the board, especially the chair, and the CEO
- a framework for the CEO to further develop capabilities
- a forum to reinforce accountability, transparency and the responsibilities of the CEO
- an opportunity to identify and address early warning signs of possible difficulties
- an opportunity to discuss any future plans the CEO may have (e.g. retirement).

<sup>284</sup> Posted by Rusty O'Kelley, Margot McShane, and Justus O'Brien, Russell Reynolds Associates, on Sunday, July 26, 2020. <https://corpgov.law.harvard.edu/2020/07/26/ceo-succession-plans-in-a-crisis-era/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A robust appraisal process should be established that reflects the company's unique circumstances. This work is generally the responsibility of the remuneration committee, which will make recommendations to the entire board.

A more accurate picture of CEO performance can be gained by incorporating the views of several groups. For example, directors, senior executives, institutional shareholders, customers, suppliers and other key stakeholders will all have a view on the CEO's performance. This must be handled sensitively and all comments treated confidentially to uphold the integrity of the appraisal process.

Both quantitative and qualitative indicators may be included to assess the CEO's leadership behaviour and performance goals, which are fundamental to sustained organisational performance. Using financial and company performance measures alone are inherently problematic. There are an array of factors outside the direct control of the CEO that can affect company performance. A CEO may be performing strongly when the company is not and vice versa. Also, shareholder value can be measured from a number of perspectives, with startlingly different end results. In any event, CEO performance should be measured not only against short-term company financial performance, but also on the CEO's own performance, especially against agreed key performance indicators and corporate strategic objectives.

## EXECUTIVE REMUNERATION

Executive remuneration is a topic that usually elicits much discussion and controversy. ASX Principle 8 provides that a company should remunerate fairly and responsibly. In determining a remuneration policy, the board needs to:

- ensure that remuneration is set at levels that appropriately reward, motivate and incentivise management to execute company strategy
- demonstrate a clear relationship between senior executives' performance and remuneration
- ensure that the remuneration policy is understood by investors.

Executive remuneration should include an appropriate balance of fixed and variable remuneration. Commentary to Recommendation 8.2 of the ASX Principles sets out the guidelines for executive remuneration, including:

- fixed remuneration should be fair in light of legal, labour and market conditions and relative to the scale of business operations
- variable remuneration should be clearly linked to specific performance targets, appropriate to the company's objectives, goals and risk appetite
- equity-based payments may be an effective form of remuneration to align executives' incentives with long-term company performance
- termination payments must be agreed in advance and no payment should be made in the case of misconduct.

Executive remuneration has been the subject of much debate and increasing focus in recent years, which culminated in the introduction of the 'two strikes' rule and other remuneration reforms to the Corporations Act in 2011.<sup>285</sup>

Listed companies are subject to a strict disclosure regime. Section 300A of the Corporations Act requires listed companies to make specific and comprehensive annual disclosures regarding the company's remuneration framework and the remuneration arrangements for the key management personnel (KMP). Companies that fail to effectively communicate their remuneration practices and policies to shareholders will risk attracting a 'no' vote on their remuneration report. Other common reasons for a negative vote include:

- a lack of transparency
- insufficiently demanding performance hurdles for at-risk remuneration
- excessive remuneration quantum
- insufficient alignment of remuneration with shareholder experience
- remuneration not reflecting company performance.

<sup>285</sup> Corporations Amendment (Improving Accountability on Director and Executive Remuneration) Act 2011 (Cth)



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

There continues to be a tendency for 'vanilla' approaches to executive remuneration designed not to raise the ire of proxy advisors and shareholders as a result of the 'two-strikes' rule.

The 'vanilla' approach typically sees executive remuneration delivered in the following components:

- Fixed remuneration (e.g. salary, superannuation, fringe benefits)
- Variable remuneration, consisting of:
  - Short term incentive (e.g. at-risk remuneration with payout levels determined based on performance or share price improvement over a 12-month period against metrics set by the board)
  - Long term incentive (e.g. at-risk remuneration with payout levels determined based on performance or share price improvement over a 3-5 year period against metrics set by the board).

The challenge for boards is to identify and implement a remuneration framework which best supports the organisation's ability to achieve its unique business strategy.

Shareholders demand that the process for setting remuneration be transparent and as detailed in [Chapter 11 Board Committees](#), certain procedures are required to be followed when engaging a remuneration consultant to provide a recommendation in relation to the quantum or elements of KMP remuneration to ensure that the remuneration consultant is free of undue influence by the KMP to whom the remuneration recommendation relates.<sup>286</sup>

Other measures implemented by the Australian Government in response to perceived corporate excess included the significant tightening of restrictions relating to termination payouts or 'golden handshakes'. Termination payments for regulated executives cannot exceed one times an executive's base salary without shareholder approval being obtained.<sup>287</sup>

<sup>286</sup> Corporations Act 2001, Section 300A(1)(h)

<sup>287</sup> Corporations Act 2001, Sections 200B and 200F

## EXECUTIVE SERVICE AGREEMENTS

With more rigorous disclosure requirements, the board's approach to negotiating the terms of CEO and senior executive service contracts is more open to challenge by the media and shareholders.

The board has the difficult task of striking a balance between the need to attract and retain senior executives with protecting company interests by not paying excessive remuneration. Most importantly, the process by which executive service agreements are set up must be transparent and beyond reproach.

The remuneration committee is usually vested with the responsibility of providing recommendations to the board in relation to the key terms of executive service agreements and remuneration arrangements on appointment. It is important that there is sufficient expertise within the ranks of the remuneration committee to effectively advise the board on these matters. The board is ultimately responsible for ratifying the appointment of the CEO, and thus it should retain sign-off authority.

It is important that the process adopted ensures the executives for whom contracts are being negotiated remain at arm's length (i.e. instructions on the preparation of the contract should be given directly to solicitors or consultants by the remuneration committee). This does not preclude the CEO and other senior executives from making submissions to the remuneration committee about their own contracts or making recommendations on the remuneration of their direct reports.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The preparation of an executive service agreement is complex. Professional advisers should be engaged who can ensure that the contract reflects what has been agreed and that the contract accords with the law. Any drafting of contracts needs to consider the regulatory framework and the company's governing documents, including the:

- Corporations Act (particularly Part 2D.2)
- ASX Listing Rules
- industrial relations, employment and WHS legislation
- company constitution
- company remuneration policies
- company strategy.

For general guidance of what should be included in an executive service agreement, refer to the ASX Principles commentary to Recommendation 1.3.

Listing Rule 3.16.4 requires an entity to disclose the material terms of any employment or service contract (or any variation to it) with the CEO (or equivalent) and any of its directors.

## Useful references

- KPMG, 2021, Insights into Remuneration Reporting <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/insights-into-remuneration-reporting.pdf>
- KPMG, 2022, Remuneration and the E in ESG - does Australia need to play catch up?, <https://newsroom.kpmg.com.au/remuneration-e-esg-australia-need-play-catch/>

## For further information please contact:

**Andrew Holland**

**Director,  
Performance & Reward  
aholland1@kpmg.com.au**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 11. Board Committees

Board committees can enhance the oversight provided for companies. As increasingly more is being required from boards, greater use is being made by committees to help all directors better perform their duties and discharge their responsibilities in an effective and efficient way.

## In this chapter

- Types of committees
- Benefits of committees
- Committee charters
- Committee annual agenda
- Committee induction framework
- Committee meeting agenda and minutes
- Committee size and composition
- Committee/board interaction and reporting
- Committee evaluation
- Typical committees of the board
- Audit committee
- Risk committee
- Remuneration committee
- Nomination committee
- Sustainability committee
- Other common committees
- Special purpose committees

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Do the committees in place help the board focus on the key risks and issues facing the organisation?
2. Are board committee charters approved by the board and reviewed annually?
3. Are board committees comprised of a majority of independent directors?
4. Are the chair of the board and the chair of the audit committee different people?
5. Are the chair of the board and the chair of the remuneration committee different people?
6. Does each board committee have the expertise and experience to properly advise the full board?
7. Are there an appropriate number of directors with accounting or financial expertise on the audit committee?
8. Does the audit committee meet without management present in order to question the external and internal auditors?
9. Does the board critically scrutinise and question the information provided, and recommendations made, by a board committee, even when endorsed by 'experts'?
10. Are non-financial risks given as much attention as financial risks in risk committee meetings?
11. Are separate committees required in order to address ESG and/or other emerging requirements?
12. Is the board informed of any issue upon which committee members are not in full agreement?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Board committees lack terms of reference or charters.
- Certain committees are not resourced with appropriately skilled people.
- The audit committee meets only when required by internal or external auditors.
- Minutes are not taken at committee meetings or the minutes are not distributed regularly to members.
- The audit, nomination or remuneration committee involve mostly executive directors due to the unavailability of independent directors.
- The audit committee has little to do with assessing internal control systems and coordinating with the internal audit function.
- Only financial risks are discussed in the risk committee.
- Similar sized companies or competitors have established additional committees that the company is yet to establish.
- There is irregular reporting to the board from the chairpersons of the committees.
- There is insufficient detail provided by the committee chairman for the issues to be appropriately considered.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## TYPES OF COMMITTEES

The most common board committees are the:

- audit (and risk management) committee
- nomination committee and
- remuneration committee.

Depending on circumstances, additional committees, including ad hoc committees, may be established to deal with other pertinent matters, oversee specific projects or focus on key risk areas for the organisation.

Types of additional committees can include sustainability, safety, technology, research and development and special purpose (e.g. takeover and merger). However, in general terms, the number and scope of board committees will depend upon the size and complexity of the organisation.

## BENEFITS OF COMMITTEES

Board committees can produce a number of benefits, such as:

- allowing directors to use their limited time more efficiently and effectively to do board work
- acting as a filter in summarising complex issues and recommending courses of action
- sending a positive signal to investors that major issues are being dealt with by the company and
- allowing independent directors to gain a comprehensive understanding of the business.

The ASX Principles suggest that having separate audit, risk and remuneration committees can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed in those areas.<sup>288</sup>

<sup>288</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Commentary to Recommendations 2.1, 4.1 and 8.1

Where committees are separated, it is important that there are common members such that information transfers between committees and discussions supporting decisions to be made are well informed.

Unless prohibited by a company's constitution, directors have the power to delegate any of their powers to a committee.<sup>289</sup> Such delegations are documented in the board minutes and also generally set out in the committee charters as well.

It is imperative that all board committees adopt the same type of systematic planning and processes as the full board, including having:

- a written charter
- an annual agenda and
- meeting papers and minutes prepared.

Committees should report regularly to the board through a verbal report by the committee chair, as well as through a detailed report and/or committee minutes in the board papers. Committees should also review their charters and membership at least annually, with any recommend changes reported back to the full board.

Some of the challenges associated with board committees include:

- ensuring that the committee is comprised of directors with the appropriate expertise and resources to provide the full board with high quality advice and
- the legal question of whether a higher standard of care will apply to directors, who are vested with the responsibility of investigating particular issues and making recommendations to the full board.

## COMMITTEE CHARTERS

The starting point for any board committee is a formal charter or terms of reference. The charter helps committee members understand their duties and responsibilities and how these can be reconciled with the expectations of the full board and the organisation's stakeholders.

<sup>289</sup> Corporations Act 2001, Section 198D.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A typical committee charter covers:

- the committee's purpose, responsibilities and duties
- the authority of the committee (including delegations by the board)
- the committee structure and terms of appointment for the chair and members
- meeting requirements and procedures (e.g. frequency of meetings, quorum, voting and minutes)
- access to company personnel and independent external advisers
- members' skills and experience requirements
- board reporting requirements
- committee assessment process.

For an example of an audit committee charter (including further detail on the types of key matters which are typically covered), refer to example [Appendix 3 Audit committee charter](#).

Committee charters should also be posted on the organisation's website and the key features included in the governance statement in the annual report in accordance with the ASX Principles.

## COMMITTEE ANNUAL AGENDA

An annual agenda provides the framework to manage the committee's time, resources, meeting frequency and the matters considered by the committee.

An effective annual agenda:

- reflects a complete picture of the committee's roles and responsibilities
- is aligned with the board annual agenda to ensure integration of the board and its committees
- provides a summary of the committee's key activities
- prevents meetings being 'crowded-out' by peripheral issues
- ensures the committee's insights and expertise are fully utilised.

The annual agenda brings the committee charter to 'life' as it drives the committee's:

- activities
- meeting agendas
- information requirements.

For more information, refer to the example audit committee annual agenda set out in [Appendix 5 Audit committee annual agenda](#).

Discussion on the annual agenda solicits the involvement of committee members concerning the nature and timing of agenda topics. The committee's annual agenda also helps to determine non-committee members who should be invited (including management and external advisers) to meetings and identifies potential conflicts of interest.

## COMMITTEE INDUCTION FRAMEWORK

Audit and other board committees have significant responsibilities. It is not sufficient for committee members to have only a rudimentary knowledge of the specific matters under consideration. Committees cannot provide meaningful protection for shareholders unless their committee members are in a position to challenge management. To do this effectively, they must have the skills, knowledge and expertise, and be supported by access to independent advisers. A formal induction framework for new committee members is essential. Induction should comprise the provision of an information package with key business documentation, training sessions and meetings with key business executives. [Appendix 4 Audit Committee Induction Framework](#) provides a detailed listing of inclusions in the audit committee induction framework.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## COMMITTEE MEETING AGENDA AND MINUTES

Each committee meeting agenda should be prepared with reference to the committee's charter and annual agenda. The committee chair and company secretary should take responsibility for the content of the agenda, seeking input from committee members, the CEO and senior management, where practicable.

The process of setting the agenda should involve:

- consideration of content
- ordering of items
- allocation of time for each item
- deciding on invitees.

Careful preparation of the agenda will enhance the committee's productivity by focusing the committee's attention on the critical matters requiring examination and discussion. Committee minutes must be a complete and accurate record of the resolutions adopted and recommendations made by a committee, evidencing that the committee has acted with due care.

The company secretary, or delegate, is responsible for maintaining a complete set of committee papers, including minutes of meetings, meeting agendas and supporting papers.

Committee draft minutes should be circulated to members after meetings and to all directors for information as soon as possible after the meeting (KPMG suggests that good practice is to do this within 14 days).

Approval of minutes should coincide with the next meeting of the committee.

## COMMITTEE SIZE AND COMPOSITION

While the size of a committee varies according to the organisation, a sufficient number of members with the necessary knowledge and expertise should be present in any committee. KPMG suggests that for large organisations, audit committees should be made up of at least four members to allow sufficient diversity of skills and experience.

In determining the appropriate size for each committee, the board should take into account the:

- complexity and geographic diversity of the organisation
- nature and extent of its responsibilities
- knowledge and experience required of committee members
- minimum number of members to allow a workable quorum
- numbers needed to encourage robust and insightful debate.

The ASX Principles indicate that the audit, nomination and remuneration committees should:

- consist of a majority of independent directors (and in the case of the audit committee, should consist only of non-executive directors and be chaired by an independent director (who must not be chair of the board)
- have at least three members.<sup>290</sup>

Committees usually deal with technical matters, such as financial reporting standards, risk management and executive remuneration. Therefore, ensuring committee members have the relevant skills and experience, as well as access to expert advice, is paramount.

<sup>290</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendations 4.1, 2.1 and 8.1 and Commentary.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## COMMITTEE/BOARD INTERACTION AND REPORTING

Board committees are an effective forum for investigating and reviewing important issues in more detail than the full board's agenda normally allows for.

The board should expect the reports it receives from its committees will be:

- complete, but concise
- timely
- accurate
- compiled with integrity.

Whilst the committee may complete background work and make recommendations to the board, or act where the delegation to the committee permits, the overall responsibility for decisions always remains with the full board.

It is, therefore, essential for directors to:

- question the committee chair and members when the committee report is being presented
- not blindly rely on any information or advice provided (even 'expert' recommendations)
- challenge whether the organisation's culture is appropriate, including the 'tone at the top', from a control perspective
- be informed of any issues on which committee members were not in total agreement
- confirm that any external parties (e.g. auditors) have been effective in providing the required assurance.

## COMMITTEE EVALUATION

Board committees, like their parent boards, should be evaluated on a regular basis to improve their effectiveness. Disclosure of the process of evaluating the performance of both the board and its committees is recommended by the ASX Principles.<sup>291</sup>

The focus of the evaluation assessment should include looking at the committee's:

- structure, role-clarity and authority
- composition, skill-sets and development
- leadership, relationships and processes
- nature and scope of work.

A typical assessment process includes:

- a self-assessment survey
- interviews with committee members, as well as management and assurance providers
- a review of the quality, quantity and relevance of information coming to, and emanating from, the committee.

The assessment's outcome should be a report providing an objective, balanced evaluation of the committee's effectiveness, highlighting specific areas for improvement.

As a good governance measure, committee evaluations should be performed on an annual basis (even if only informal). Individual assessments of committee chairs should be undertaken regularly by the chair of the board, and by the committee chair for individual committee members.

<sup>291</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendations 1.6.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## TYPICAL COMMITTEES OF THE BOARD

The most typical committees are laid out below. It's important to note however that committees may be named differently and often might be combined to meet the needs of the board and the organisation (e.g. an audit and risk committee in one organisation may be a risk and audit committee in another and an audit, risk and governance committee in a third yet all cover the same areas). The most commonly understood committee names are used below, consistent with the ASX Principles and Recommendations.

## Audit committee

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. Recommendation 4.1 of the ASX Principles also suggests that a listed entity have an audit committee.

Stakeholder expectations of audit committees have increased significantly, both in Australia and internationally.

The commentary to Recommendation 4.1 of the ASX Principles lists those matters for which the audit committee should make recommendations to the board. Most audit committees perform the following functions:

- reviewing financial statements and other financial information distributed externally
- monitoring company financial reporting to ensure compliance with the Corporations Act, ASX Listing Rules and other regulatory requirements
- reviewing the nomination and performance of the external and internal auditors
- making recommendations relating to the appointment and removal of external and internal auditors
- overseeing and considering the effectiveness of internal control systems

- assessing the performance and objectivity of the internal audit function.

It is fundamental that the audit committee has the technical skills and expertise to discharge its responsibilities and the members exercise independent judgement. Above all, audit committee members must act with integrity and honesty.

ASX Principles suggest that the audit committee should include members who are financially literate and consist of at least three members, all of whom are non-executive directors and a majority of whom are independent directors.<sup>292</sup>

The external auditor performance evaluation must be based on the committee's view of the external audit process and should include assessments from management and internal audit.

The external auditor should also be given the opportunity to discuss the findings of the committee's evaluation.

Where an audit committee is not established, it is crucial the company put in place an alternative means of scrutinising the financial reporting system and the board allocates appropriate time to this function.

Audit committees should continually seek to improve their effectiveness through improving and updating committee agendas. Greater focus should be given to material issues rather than 'checklists' that add little or no value. Audit committees should always be seeking better information flow, through high quality resources and greater internal transparency.

As economic uncertainty, globalisation and geopolitical turbulence continues, KPMG have identified Audit Committee priorities, as outlined below.

<sup>292</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendation 4.1 and Commentary; KPMG, 2019 Priorities for Boards and Audit Committee, KPMG, on the 2022 audit committee agenda, <https://home.kpmg/us/en/home/insights/2022/03/2022-issue1-article1.html>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- Risk management is a top concern for audit committees, with the complexity and interconnectivity of risk, creating a need for multi-dimensional risk analysis and treatment, rather than the traditional two-dimensional, linear approach most organisations currently apply.
- Internal audit can maximize its value to the organisation by focusing on critical risk (operational and financial) and the adequacy of the company's risk management processes generally.
- Tone at the top, culture and short-termism are major challenges and focus on ethics and compliance is important.
- CFO succession planning and bench strength in the organisation continue to be weak spots.
- Audit committee effectiveness hinges on understanding the business.
- Consider how the company's disclosures (including non-financial disclosures such as those pertaining to ESG) can better tell the company's story—and that of the audit committee's.
- Reinforce audit quality and set clear expectations for the external auditor.
- Stay apprised of global tax developments and risks and recognize that tax has become an important element of ESG.
- Understand how technology is impacting the finance function's talent, efficiency, and value-add.

**Risk committee**

Recommendation 7.1 of the ASX Principles recommends that the board should have a committee to oversee the management of risk. If a risk committee is established, its charter needs to be developed with reference to the intersection between its duties and those of other committees, particularly the audit committee.

KPMG's model of risk governance considers risk from two angles – risk content and risk process.

Risk content involves the identification of specific enterprise-level risks that threaten the company's existence, strategy and business model. Risk process refers to how the organisation identifies, evaluates, assigns responsibility and reports on risk content.

Risk committees generally have the following responsibilities:

- endorsing the risk management policy for approval by the board
- overseeing the establishment and implementation of the risk management framework
- reviewing management's plans for mitigation of the material risks faced by the company
- monitoring emerging risks and changes in the risk profile
- promoting awareness of a risk-based culture.

The commentary to Recommendation 7.1 of the ASX Principles lists those matters on which the risk committee should make recommendations to the board.

Recommendation 7.2 suggests that the board or the risk committee annually review the company's risk framework and disclose at the end of each reporting period whether or not such a review has taken place.

KPMG recommends that in reviewing material business risks against risk appetite that the risk committee should also understand what assurance is being received from the three lines (refer to [Chapter 15 Receiving Assurance](#)) so as to be informed as to whether determinations pertaining to the rigor of the control environment used to determine risk ratings have been tested.

The ultimate responsibility for risk oversight rests with the full board, regardless of whether or not a separate risk committee is established.<sup>293</sup>

293 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendation 7.1.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Remuneration committee**

The Listing Rules require ASX listed companies in the S&P/ASX 300 Index to have a remuneration committee comprised solely of non-executive directors.<sup>294</sup> Recommendation 8.1 of the ASX Principles also recommends that a listed entity have a remuneration committee of at least three members.

A remuneration committee provides support and advice to the board on:

- the company's remuneration framework, recruitment, retention and termination policies and procedures for senior executives, including the process for setting remuneration and assessing performance
- the level and composition of a senior executive's remuneration
- superannuation arrangements
- the remuneration framework for directors.<sup>295</sup>

The commentary to Recommendation 8.1 of the ASX Principles lists those matters for which the remuneration committee should make recommendations to the board.

Companies should limit the use of executive directors serving on the remuneration committee in order to address the potential for, or perception of, conflict of interest. The committee can consult with individual executives on remuneration policies generally, but no individual should be directly involved in deciding their own remuneration.<sup>296</sup>

A key task of the remuneration committee is to monitor levels of remuneration across relevant industries, and the economy as a whole, in order to ensure the company's remuneration policies are effective in attracting, retaining and motivating the people integral to its success.

<sup>294</sup> ASX Listing Rule 12.8

<sup>295</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendation 8.1 and commentary; Governance Institute of Australia, The Role of the Remuneration Committee, Good Governance Guide.

<sup>296</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Principle 8.

A remuneration report must be included in each annual report, and there must be an advisory non-binding (subject to the 'two strikes' rule) shareholder vote on the remuneration report at the AGM.<sup>297</sup>

Remuneration committees are increasingly engaging external consultants to advise on remuneration arrangements, and must take into account the relevant Corporations Act requirements which apply to such engagements<sup>298</sup>. In summary, these require that:

- The details of the remuneration consultant be disclosed together with related fees and whether the consultant provided any other services to the entity for the financial year. If other services were provided the nature and amount payable is required to be disclosed such that independence of the consultant is transparent.
- The appointment of remuneration consultants be made directly by the Remuneration Committee (or the Board) to avoid undue influence from key management personnel (conflict of interest).
- The Board must include a statement in the Annual Report to the effect that they are satisfied recommendations have been made by the consultant free from undue influence from the key management **personnel** to whom the recommendation relates. This should include how they arrived at this determination.

**Nomination committee**

Recommendation 2.1 of the ASX Principles suggests that the board should establish a nomination committee to oversee a formal, rigorous and transparent process for the appointment and reappointment of directors to the board.<sup>299</sup> In smaller companies, this function may be performed by the full board or combined with the remuneration committee.

<sup>297</sup> Corporations Act 2001, Section 250R

<sup>298</sup> Corporations Act 2001, Section 300A (1)(h). See Chapter 3.2 (Company Leadership)

<sup>299</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendation 2.1.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Nomination committees are generally responsible for:

- devising criteria for directorship (including membership of board committees)
- identifying suitable candidates for appointment to the board
- undertaking appropriate succession planning for the board and the CEO as well as providing oversight in relation to succession planning of the executives more broadly
- developing and managing the process for the performance evaluation of the board, committees and directors.

The commentary to Recommendation 2.1 of the ASX Principles lists those matters for which the nomination committee should make recommendations to the board.

Prior to recruiting new directors, the committee would typically undertake a formal process of reviewing the balance and effectiveness of the existing board, identifying the skills and experience needed and considering board candidates who might best provide them.

Ensuring robust board and committee succession plans are in place and that these plans are effective in delivering directors with the required expertise, is another key role of the nomination committee.

Developing a pipeline of future potential board candidates, meeting certain criteria and making contact with such individuals in advance, is an effective method to ensure robust board and committee succession. Although the CEO should be involved in the work of the committee, they should not be involved in its decision-making processes.

In the oversight function pertaining to executive succession planning, the nomination committee can play a key role in ensuring that the organisation is identifying and supporting high potential individuals. They are also well positioned to support diversity and inclusion policies in the same way.

## Sustainability committee

A sustainability committee can help reduce matters on the board's agenda by addressing issues such as integrated corporate reporting and the impact of the organisation on the environment and community (in essence meeting ESG expectations as discussed in [Chapter 18 Environmental, Social and Governance \(ESG\)](#)). Since the inclusion of Recommendation 7.4 of the ASX Principles regarding disclosure of material exposure to environmental or social risks,<sup>300</sup> Sustainability Reports and Integrated Reporting have increased, driven largely by the focus on ESG matters. To this end, an increasing number of organisations are forming board committees to assist the board in handling specific matters with high relevance to the business, such as health, safety and wellbeing, environmental and social matters. Sustainability committees assist the board in areas such as:

- establishment of the ESG strategic position and related policies as well as oversight over the governance frameworks which will support the strategy
- compliance with applicable legal and regulatory requirements associated with health, safety, environmental and societal matters (including human rights, modern slavery)
- the preparation of a sustainability report for inclusion in the annual report.

The industry and nature of the company's activities will be the most significant influence on the need for such a committee and the nature of the material issues it covers.

300 KPMG, Survey of Sustainability Reporting 2020, <https://home.kpmg/xx/en/home/insights/2020/11/the-time-has-come-survey-of-sustainability-reporting.html>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Other common committees**

A number of other committees often exist and are frequently chaired by directors of the board to provide additional oversight on key risk areas, for example:

- Health, safety and wellbeing committee – often used in high risk industries such as mining, petroleum and health, where staff are placed in complex production or service environments.
- Information technology (IT) steering committee – generally in place where there is a significant reliance on information technology, such as call centres, emergency response services and technology service providers.
- Research & development committee – often found where revenue generation is dependent on ongoing research activity, such as in the pharmaceutical and mining industries.

**Special purpose committees**

Special purpose committees are usually established to consider a specific matter and tend to have a limited life span. Nevertheless, the committee's charter or terms of reference should be approved by the full board and the committee should follow the same operating principles as other board committees.

Special purpose committees are often formed to deal with one-off events including:

- takeovers, mergers, acquisitions or divestments
- major builds, capital projects or system upgrades
- reputation matters
- first-time adoption of significant laws, regulations, industry codes and organisational standards.

**Useful references**

- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.
- Appendix 3 Example audit committee charter
- Appendix 4 Example audit committee induction framework
- Appendix 5 Example audit committee annual agenda

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 12. Investment Management

Entities such as asset and wealth managers (superannuation funds, investment managers and banks), insurers, health funds and organisations which invest funds to meet both short and long terms obligations, have the task of prudently investing funds whilst balancing the need to obtain a reasonable return with managing the portfolio so that it operates within the agreed risk appetite and tolerance.

This must be achieved within a robust risk and reporting framework to achieve compliance with applicable regulatory requirements.

## In this chapter

- The role of the board
- Investment committees
- Investment framework
- Risk appetite
- Risk tolerance
- Investment strategy
- Asset allocation
- Financial risk management
- Investment policy
- Investment performance and risk management reporting
- Outsourcing – fund managers and external providers

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Are directors convinced that the risk appetite is aligned with management's risk appetite for each investment/financial risk?
2. Does the Investment Policy make sense intuitively, including articulating the rationale for a particular investment strategy?
3. Do the investment mandates given to service providers, such as fund managers, align to the Investment Policy?
4. Is there a process to monitor compliance with the Investment Policy – including by outsourced service providers?
5. Is the investment selection process documented and undertaken by appropriately qualified investment management staff?
6. Would it be useful to employ an external specialist advisor to provide advice on asset allocation strategies?
7. Is there separation of duties between the custodian, fund manager and asset consultant (e.g. it is preferable for the asset consultant not to be providing investment products)?
8. Is investment management performance regularly reviewed and critically examined?
9. Is investment management performance exceeding index-based performance – because if it is not – then why is the organisation paying additional fees for 'active management'?
10. Are investment management fees and custodian fees regularly reviewed and periodically tested to the market?
11. What information is available in relation to investment risk (e.g. investment risk ratios, value at risk, stress testing, counterparty risk)?



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Lack of a formal, documented and comprehensible Investment Policy. It should be easily understood by a competent, but non-technical director.
- There is not an Investment Strategy directing the investment activities.
- The Investment Policy and Strategy have not been reviewed for over three and one year respectively.
- An investment performance benchmark is either deemed not appropriate or is not established.
- The performance of external managers is not measured or reviewed.
- There appears to be inadequate segregation of duties, inadequate controls and breach reporting is either not formalised or is inadequate.
- There are large variances in reported performance over periods.
- There is a lack of independent verification of performance or compliance with the Investment Policy.
- Non-compliance with Investment Policy – which may be consistent in nature or not be detected in a timely manner.
- Management is very defensive when asked logical questions or becomes aggressive towards third parties, such as auditors, when reasonably challenged.
- There is a high dependence on one key individual in terms of the management of funds.
- There is confusion at the Investment Committee in terms of interpreting various reports or advice received from parties, such as an asset consultant.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

This chapter provides guidance to directors who are responsible for overseeing investment governance, operations and processes. Due to the need for brevity, as well as the complexity of various regulatory environments, this chapter covers the general issues associated with better practice investment governance, rather than specific regulatory requirements. Further references that provide more detail are provided at the end of the chapter.

## THE ROLE OF THE BOARD

Ultimately the board is responsible for investment management, including the overall investment beliefs and philosophy, the investment strategy, investment policy and associated risk appetite and tolerance.

Even though the board may delegate these responsibilities, either in whole or in part, to a board committee, such as the Investment Committee, or rely on the advice of an asset consultant, the board is still ultimately responsible for investment management.

## INVESTMENT COMMITTEES

The investment committee traditionally tends to be a board committee, rather than a management committee, and is responsible for the investment strategy, as delegated by the board. The investment committee would also be responsible for the monitoring of investment performance and either approving investment decisions or recommending investment strategies to the board in line with its charter and delegations. Further details regarding board committee composition and structures are provided in [Chapter 11 Board Committees](#).

## INVESTMENT FRAMEWORK

The investment framework supports the organisation's process for formulating an investment strategy. An investment framework includes the governance, policies, systems, processes and people to operate and oversee the management of investments, including the management of the investment and financial risks.

## RISK APPETITE

The collective risk appetite of the organisation is a key determinant in the construction of the investment portfolio. It is important that the risk appetite of the board and management are aligned (which is often not the case) and, ultimately, it is the board's risk appetite which is paramount.

Risk appetite is driven by a number of factors, including:

- the values of the organisation and the types of investments it is, and is not, willing to make
- the amount of funds available for investment (i.e. the greater the amount the more diverse and sophisticated the investment choices)
- the period of time over which funds are available (i.e. generally, short-term equates to a lower risk, longer term enables greater risk. Exceptions to this include long-term bank deposits where the longer term risk is generally low)
- what the uses for the funds are (e.g. capital expenditure, supporting financial liabilities)
- the ability to withstand volatility in the investment portfolio (i.e. less than one in X years chance of negative returns)
- capital requirements (i.e. for insurance companies, higher risk investments require higher levels of capital)
- the complexity of investments
- the capability and experience of the investment framework, including personnel
- the requirement to make regular dividends/distributions to share/unit holders
- restrictions on certain types of asset class, based on ethical, social or environmental risks (e.g. the tobacco industry) and
- investment diversity guidelines for the portfolio, including minimum credit ratings of investment counterparties.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Once the risk appetite has been agreed then the investment selection/asset allocation process can commence.

## RISK TOLERANCE

Risk tolerance sits hand in glove with the risk appetite of the organisation. Risk appetite focuses on defining the boundaries within which investments are made. It is a higher-level statement that defines the amount of risk the organisation is willing to take in order to meet its investment objectives. Risk tolerance is the degree of volatility that the organisation is willing to accept within the parameters of its risk appetite.

For example, an organisation's risk appetite statement may state that it does not accept risks that could result in a 'significant loss in revenue'. A risk tolerance statement would then go on to define the specific levels of acceptable variation within that risk (e.g. the organisation may only accept a 10 percent loss in revenue from a particular asset class in any given period e.g. a year).

The questions to consider in the development of the organisation's risk tolerance statement are, therefore, inherently linked to those used to develop the risk appetite.

## INVESTMENT STRATEGY

The investment strategy is the key document defining the strategic investment objectives, and the guiding framework and principles determined by the board to be appropriate for the organisation's broader operating strategy. Its key components include:

- Investment purpose and the alignment of organisational values to the investment strategy (e.g. 'ethical' investment principles).
- Asset allocation principles – such as how the portfolio will be constructed in order to meet the desired risk/return outcome.

- Risk management guidelines – including clear risk appetite and risk tolerance targets.
- High-level policy statements, including the monitoring framework that details what will be monitored and the specific measures in place to track performance.

## ASSET ALLOCATION

To implement the investment strategy, the organisation should have an asset allocation process in place which includes robust due diligence. Asset allocation involves dividing an investment portfolio among different asset categories/classes. This is a crucial step to ensure that investments selected are aligned to the organisation's investment objectives, including risk appetite and tolerance.

The due diligence process should consider historical returns for particular asset classes and the volatility of return/value of the instrument (i.e. risk) over various time periods. Considering these factors can be insightful and assist in identifying correlations between assets, while helping to dispel common preconceptions about various assets. For example, some assets may be considered to have low returns, but when looked at over the long term, they perform well with low volatility, providing a form of capital protection.

Another relevant example in asset allocation is where funds are needed in the short term and a loss cannot be tolerated. Therefore, the logical asset allocation would be to defensive assets such as cash, term deposits and short dated fixed interest securities, all of which impacts the return that can be achieved.

Many research and academic articles indicate that asset allocation is a key driver of returns, rather than stock or security selection – hence the importance of having a robust framework and process in place to determine asset allocation.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Having allocated assets, an organisation should also have arrangements in place for the ongoing management and monitoring of its investment strategy. Depending upon the value of funds invested, this may include asset allocation rebalancing processes, exposure management arrangements (i.e. derivatives and currency), investment transition arrangements, processes to monitor investments and valuation procedures. It is critical that the reporting framework to monitor investments provides directors with meaningful information in a timely manner.

## FINANCIAL RISK MANAGEMENT

When directors are overseeing the investment process, they need to be mindful of the financial risks associated with the investment process and not just the asset allocation decision.

A robust risk management framework needs to be established and implemented to address the risks arising from the investment of funds. These risks would include:

- liquidity risk (ensuring that investments can be readily converted to cash, if required, without suffering a significant loss or that sufficient cash is held as part of the investment portfolio)
- credit risk (the risk of loss resulting from counterparty default)
- market risk (the risk of loss in value of investments due to the adverse effects of movements in interest rates, equity prices, foreign exchange rates, commodity prices, etc)
- operational risk (the risk of loss resulting from errors in the processing of transactions, a breakdown in the control environment or errors or failures in systems)
- reputational risk (the risk of damage to the reputation of the organisation due to the nature of the investment or loss in value of the investment – particularly important for Government and widely owned organisations) and

- environmental, social and governance risk 'ESG' (the risks associated with failing to meet ethical, social and environmental expectations that generate a loss of business value through stakeholder activism, and perceptions of the organisation's misalignment of its business to the broader societal values. In addition, ensuring the appropriate approach is taken to govern the risk management decisions and activities).

Financial risk management arrangements would typically comprise a range of tools for risk measurement and analysis that are commensurate with the investments of the organisation. One very good example of this is the use of stress testing and scenario analysis, which can assist the organisation to identify and assess potential risk exposures that may threaten the likelihood of achieving investment objectives. Stress testing should be a forward-looking assessment of possible risk factors. Importantly, the outputs from stress testing should enable directors to make informed decisions on the management of the portfolio to enhance returns and reduce financial risk.

## INVESTMENT POLICY

Having determined the investment beliefs and philosophy, objectives, strategy, risk appetite, risk tolerance and approach to financial risk management, it is important that this is documented in the Investment Policy.

The fundamental importance of an Investment Policy is that it provides the framework for an organisation to achieve its investment objectives (as defined in the investment strategy) and seeks to avoid unacceptable outcomes. The policy ensures that the risk appetite and philosophy of the organisation are reflected in its investment activities.

The purpose of the policy is to provide general guidance regarding the investment objectives, specific guidance on strategies to achieve the investment objectives, and to provide a mechanism to control management behaviour and reduce bias and potential errors arising from decision making.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

An Investment Policy should address the key areas of:

- the investment objectives, philosophy, risk appetite and risk tolerance, including an explicit mandate for values-led / ethical investment strategies (e.g. addressing ESG including, for example, not investing in gaming, tobacco)
- the asset allocation strategy and the rationale by which those objectives are to be pursued
- guidelines on investment exposures and maturity periods
- guidelines on counterparty exposure limits
- liquidity requirements
- the mandates with which underlying investments must comply and, in the case of pooled investments, the guidelines in place for the selection and contracting of managers and how they align to the organisation's investment mandate
- any socially responsible investments and prohibited investments
- the benchmarks against which the performance of investments and managers are to be assessed
- the valuation approach and methodology for unlisted or illiquid investments
- the methodology for deciding and disclosing proxy voting decisions
- the reporting required to be provided to the investment committee and the board and
- the responsibilities of various stakeholders, including the board, investment committee and management.



## Case study – Ethical investment

In February 2014, Transfield Services (Transfield) made a commercial decision to broaden its services and invest in the management of detention centres. With large government contracts on offer for the management of controversial detention centres, both in Australia and offshore, the Transfield board saw the potential for large, stable returns. These contracts eventually were estimated to contribute up to 15-20 percent of the company's revenue (in the wake of lost revenue from the declining resources sector), and saw an increase in Transfield stock price of up to 140 percent.

However, only 18 months after the investment decision, Transfield were facing a major issue, with many of its shareholders withdrawing their investment in Transfield due to claims of abuse within the detention centres. Under the confidentiality clauses of the Government contracts, the company was unable to answer questions from investors about the abuse claims, making it difficult to transparently disclose how the company undertook the operation of the centres.

As a result of the perceived lack of transparency, together with the instigation of Senate hearings to investigate the claims on the back of public and political pressure, Transfield stock dropped in value by 45 percent.

Whilst commercially, the investment decision was sound, aligned with the board's investment metrics and had a short term positive impact on shareholder value, ultimately, a lack of consideration of social, political and contractual drivers undermined the return and potentially caused significant financial and reputational damage through divestment of Transfield stock by key shareholders.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## INVESTMENT PERFORMANCE AND RISK MANAGEMENT REPORTING

Having executed the investment strategy, the investment performance and risk management reporting will need to be undertaken to measure the performance of investment activities against the investment objectives and benchmarks. At a detailed level, this will involve comparing the performance of investments and managers to agreed benchmark indices. Other considerations include:

- frequency (usually a minimum of monthly reporting)
- documentation – the reporting process should be documented in procedures
- detail/content (e.g. manager performance, compliance, portfolio values, credit risk and other risks)
- format, such as the use of an 'Investment Report Dashboard' and
- distribution (i.e. executive management, middle office/compliance function, investment committee etc.).

## OUTSOURCING – FUND MANAGERS AND EXTERNAL PROVIDERS

Depending upon the size of the funds available for investment, the outsourcing of various activities may be appropriate. This could include the outsourcing of investment activity to fund managers, the use of asset consultants to determine asset allocation and the use of a custodian for the settlement and recording of investment transactions. However, there are also risks arising from the outsourcing of activities which needs to be recognised and managed.

Outsourcing and the use of external providers should also take into account:

- the benefits of outsourced investment management given the capabilities of in-house staff and the complexity of investments
- the nature of asset classes invested in
- the scale and size of investments
- system requirements to support outsourced arrangements
- the use of index funds versus active investment manager funds
- external manager assessment, selection and monitoring processes and
- the custody and investment administration requirements.

It is also important that the 'mandates' given to investment service providers, particularly fund managers, are consistent with the Investment Policy. It is not uncommon for an Investment Policy to prohibit the use of derivatives, only to find a fund manager using derivatives – because it is not prohibited in the mandate provided to the fund manager.

Critically, an organisation can outsource its investment activities, however, it cannot outsource its legal accountabilities and responsibilities. Directors and investment committee members should also consider APRA's prudential standard SPS 231 in relation to outsourcing for more specific guidance.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- Certain industries such as Superannuation, Health and Insurance are subject to various regulatory requirements relating to the management of investment funds. For example, superannuation funds and insurance entities are regulated by APRA and ASIC and health entities are regulated by APRA.
- The regulation of these industries also provides guidance for other organisations. For example, on the topic of Investment Governance, APRA has released a prudential standard (SPS 530) and related guidance notes (SPG 530).
- Australian Prudential Regulatory Authority (APRA), <http://www.apra.gov.au>

For further information please contact:



**Paul Travers**

**Director,  
Treasury Services  
[ptravers@kpmg.com.au](mailto:ptravers@kpmg.com.au)**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 13. Productive Meetings

Meetings of directors should be forums of informed discussion and decisions – not an endless stream of surprises.

## In this chapter

- Duties related to board and committee meetings
- Meeting papers
- Meeting procedures
- Decision-making process
- Decision-making outside the boardroom
- In-camera sessions
- Boardroom conduct
- Technology
- Confidentiality
- Independent professional advice
- Board minutes
- Meeting evaluation



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is the number and length of board meetings sufficient to allow the board to effectively discharge its duties and responsibilities?
2. Are board members able to access the previous meeting's board minutes with ease and review these prior to the next board meeting?
3. Are all board members provided sufficient time to review the board papers prior to entering the meeting?
4. Is the chair clearly accountable for the agenda's content, with all directors and committee chairs having the opportunity to contribute?
5. Does the board agenda allow sufficient time for strategic discussion?
6. Are in-camera sessions made appropriate use of to focus the board on what is required from them and any key concerns?
7. Are communication channels used by the board to conduct its business secure and confidential?
8. Is the size of the meeting group appropriate, having regard to the purpose of the meeting, and are all attendees directly relevant?
9. Is regular feedback and evaluation of the effectiveness of meetings provided to board members?
10. Does the board manage actions arising from board minutes, with outstanding actions being reviewed at each board meeting?
11. Is the board undertaking critical self-assessment to identify opportunities for improvement?
12. Has the board allowed sufficient time for committee reporting such that they are satisfied delegated authorities are being executed appropriately?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Board or subcommittee meetings are not scheduled on a regular basis.
- Meeting agendas and materials are sent out with little time for review or director contribution.
- Board members do not read board papers prior to attending the meeting.
- Board papers are voluminous and don't always relate to the key agenda items.
- Board papers are regularly changed at the last minute.
- The company secretary provides incomplete or untimely distribution of board meeting minutes after meetings.
- Directors attend less than 50-75 percent of meetings held (depending on the nature of the organisation).
- Many issues discussed carry over to the next meeting.
- Attendee and absentee lists are kept irregularly and sometimes are not noted in the minutes.
- There is no information sharing portal set up for the board and directors rely on emails and handouts to communicate and store information.
- Often meetings are closed without an agreed set of actions.
- There are very few or no non-executive director/'in-camera' sessions.
- At the end of each meeting a review of the effectiveness of that meeting is not undertaken before closing.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DUTIES RELATED TO BOARD AND COMMITTEE MEETINGS

Directors are expected to prepare for, attend and contribute meaningfully to board meetings in order to discharge their director duties. A director's meeting attendance record is often taken into consideration by proxy advisers when determining whether to make a recommendation to shareholders supporting a director's re-election to the board.

Unless the company's constitution provides otherwise, the quorum for a directors' meeting is two directors, and the quorum must be present at all times during the meeting.<sup>301</sup>

Boards need to be aware of the requirements relating to the conduct of board meetings imposed by formal documents such as the board charter and company constitution.

**Chair**

The chair plays a central role in the effective functioning of meetings, maintaining responsibility for leadership of the board and its efficient organisation and functioning. The chair is responsible for setting the board agenda and ensuring adequate time is available for discussion of all items. It is important that the chair leads and facilitates discussions, encourages the participation of other members, ensures that all directors have a say, and conducts meetings in an effective manner.<sup>302</sup> The chair must ensure the board's time is used to focus on the most important issues and that the discussion is open, collegiate and relevant to the agenda items.

The role of a strong chair includes encouraging all directors to:

- identify and challenge their biases
- engage in active debate
- listen to internal alarm bells and give them a voice
- have the courage to speak up

<sup>301</sup> Corporations Act 2001, Section 248F.

<sup>302</sup> Australian National Audit Office, Public Sector Audit Committees: Independent Assurance and Advice for Chief Executives and Boards, August 2011.

- challenge management, where appropriate
- not to back away when a difficult issue arises and
- promote clarity of purpose.

**Company secretary**

The company secretary is instrumental in ensuring meetings run smoothly. An efficient company secretary is proactive and will anticipate the needs of directors.

With respect to board meetings, the company secretary should ensure:

- the board agenda and briefing materials are completed and distributed in a timely manner
- appropriate personnel have been invited to the meeting
- presentations are concise and highlight significant issues
- the chairman is appropriately briefed and supported
- the meeting venue and location is appropriate and secure
- audio-visual and other equipment is operational and
- expert advice is available when required.

In boards where no company secretary exists, these duties often reside with management and the chair. Many organisations appoint administrative staff members to assist with the preparation and distribution of board documents, however, the responsibility for ensuring that this occurs remains with the chair.

**Board committees**

Board committees provide an effective way of distributing work between directors and allow for more detailed consideration of important issues than would be possible during scheduled board meetings. Committees allow directors sufficient opportunity to focus on relevant matters without having to compromise the limited time available during full board meetings.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Committee meetings should apply the same governance protocols as those described in this chapter for board meetings.<sup>303</sup>

**Meeting attendance**

As a part of their duties and responsibilities, directors should be present for board and appropriate committee meetings. Absenteeism will never excuse a director from their duties to the company.

To facilitate participation, directors may attend in person, via teleconference or video-conference.

Directors who are unable to attend a meeting should ensure their apology is given in advance and noted in the minutes. In the case of public companies, attendance is measured and documented in the annual directors' report. If there are repeated absences on the part of a director, the chair may need to meet with the director to ascertain their future availability and commitment. In some circumstances it may be in the company's interest for the director to resign.

To facilitate the effective conduct of the meeting, it is important to:

- establish and circulate a clear and appropriately detailed agenda in advance
- consult with any independent advisers or members of management whose participation is required, and limit attendance at board or board committee meetings to the extent necessary
- establish an appropriate meeting environment (including style, location, room size and seating)
- ensure the meeting begins and ends promptly at the scheduled times
- be aware of particular customs, rules and etiquette for the meeting.

<sup>303</sup> See Chapter 11 (Board committees) for a further discussion of board

**Meeting frequency and duration**

The *Corporations Act* does not prescribe the number of directors' meetings that must be convened. Both the frequency and duration of meetings are factors which influence the quality of board output. The board must agree on the frequency and duration of meetings required for it to effectively address all matters listed in its annual agenda.

In Australia, boards previously held monthly meetings. However, there is a growing trend suggesting that longer duration bi-monthly meetings, in addition to specific strategy meetings, may be more effective. As the business environment is constantly evolving, and information and issues arise more quickly, the more traditional frequency and structure of meetings may also need to be reconsidered. Board agility is an important factor in enabling issues to be considered when they arise, rather than waiting for the next board meeting. In these instances, mechanisms for formally considering board matters can be leveraged, such as teleconferencing/videoconferencing for an ad-hoc meeting or circular resolutions.

Public companies are required to include in their annual report the number of board and committee meetings held each year and the attendance of each director at these meetings.<sup>304</sup>

The length of the meeting should be sufficient to give appropriate attention to all issues at hand. When planning the agenda for a long meeting, it may be useful to consider whether splitting the meeting into two shorter meetings would be more appropriate. If the meeting must be kept to a single session, scheduling breaks is vital to keep participants focused, attentive and productive.

A meeting should only be held if it is necessary. If the same information could be covered in an email or report, for example where all agenda items are information sharing, a meeting should be avoided. As meetings are costly, the outcome must be valuable enough to justify holding the meeting.

<sup>304</sup> Corporations Act 2001, Sections 300(10)(b) and 300(10)(c).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The replaceable rules in the Corporations Act provide that a director can call a directors' meeting by giving reasonable notice to every other director.<sup>305</sup> It is crucial that board members have sufficient notice of forthcoming meetings. Circulation of a list of prearranged dates is sufficient notice and typically a convenient practice.

**Meeting preparation**

Careful preparation of the agenda enhances the board's productivity and supports its strategic and oversight role. The board meeting should be an opportunity for directors to add value to the discussion and not be informed on the issues for the first time.

The purpose of the meeting should be communicated amongst members in advance, allowing sufficient time to become familiar with the proposed agenda and undertake any research required. In order for a meeting to be productive, a strategically defined purpose should be linked to specific plans and outcomes.

The chair must also review the board papers prior to any meeting to identify any potential conflicts of interests for board members and raise these with the individual prior to the meeting. This relies on ongoing, open dialogue between the chair and other board members regarding potential conflicts of interest.

**Agenda**

A board meeting agenda enables directors to be fully informed of issues to be proposed and discussed at the meeting, reducing the time required on briefing at the beginning of a meeting. It should be referenced to the annual agenda, which identifies matters to be periodically included on the board agenda.

The chair, working with the company secretary, should be accountable for the agenda's content. Input should be sought from directors, the CEO and senior management, and the chairs of board committees. Setting the agenda should involve consideration of content, the ordering of items, the allocation of time for each item and deciding on invitees.

<sup>305</sup> Corporations Act 2001, Section 248C.

High-priority items should be scheduled first and it is essential to clarify which items are for decision (resolution), discussion, noting or information purposes. A timed agenda will assist directors in recognising the relative significance of each issue and ensure the meeting finishes on time.

**MEETING PAPERS****Review of papers prior to the board meeting**

Board meetings are a place for discussion and decision-making. To make effective use of the often limited time available, all board papers should be read prior to the meeting, with questions and comments noted and ready to be raised. A well-functioning board will distribute a complete set of board papers at least one week prior to the meeting. This pack will include:

- an agenda with all items for discussion, noting and decision clearly noted, together with the timing allocated for each item (as in indication of importance)
- a copy of the prior meeting minutes for approval
- list of outstanding action items
- copies of any committee reports being tabled
- copies of all regular reports (e.g. financial reports, performance reports, compliance reports and risk reports). These should be in a consistent, succinct and clear format with content that directly aligns to the organisation's strategic and operational KPIs and
- relevant information to support specific agenda items.

Many boards are often inundated with volumes of reading prior to board meetings, making it almost impossible for directors to do the required pre-reading and digest the relevant information. High volumes of board papers are symptomatic of:

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- Management being unaware of what information the board requires. If there is no clarity regarding matters requiring board consideration, issues that need to be escalated or how the information requested relates to strategic objectives and KPIs, there is a tendency for management to 'give them everything' in the hope of meeting expectations.
- Management attempting to overwhelm the board with irrelevant information in the hope of distracting time and discussion away from known problem areas.
- The board being unable to articulate to management the key information that they need to support their decision-making processes. Directors and boards that request large amounts of supporting data can often be lacking clarity in direction or confidence in their decision making.

In each scenario, it is up to the board to set the criteria and basis of information to be provided. Board papers should strike an appropriate balance between quality and quantity, and should be concise documents that fully present the information the board will require to comprehend all issues and make appropriately informed decisions (where a decision is required). They should be prepared to strict standards in terms of presentation and content, share a consistent format and include the date, version reference, author and reviewer's name and title. The purpose of each paper should also be clearly indicated. Directors should establish clear criteria for what matters should be raised at board level and why. Once that has been established, directors should then be willing to challenge the quantity and quality of papers provided by management. Poor papers are a major cause of bad board decision-making and create a difficulty in reaching a consensus.

The content of papers should reflect the following comments provided in section 3.1.3 of the Hayne Final Report:

"Boards must have the right information in order to discharge their functions...When I refer to boards having the *right* information, I am not referring to boards having *more* information. As I noted earlier, it is the quality, not the quantity, of information that must increase. Often, improving the *quality* of information given to boards will require giving directors *less* material and more information".

**Access to meeting papers**

Technology is rapidly moving into boardrooms, with the digital distribution of board papers becoming commonplace. Electronic communication methods facilitates the exchange of timely and accurate information between board members however, the adequacy of the security of data sharing and storage technology (email, Sharepoint and Dropbox-type applications) should be carefully considered when exchanging highly sensitive and confidential company information. The use of online portals for hosting board papers and other company materials has grown substantially as a secure and efficient way of facilitating the board process. Electronic delivery allows relevant information required for decision-making to be delivered rapidly and economically.

Electronic portals are commonly used by boards to securely post and retain materials, including board minutes, policy documents, agendas and other core documentation. Further uses include providing updates on the activities of board committees, enabling real-time communication and collaboration between board members, and facilitating information sharing between directors and management. Uploading, organising and editing materials online is typically much more time efficient than sorting, printing, stapling and distributing papers.

The way in which directors access such information has changed too. Most boardrooms now have board members using a digital device (tablet or laptop) and accessing the portal for board documentation in the meeting. Digital devices which include authentication controls and encryption offer a considerable security improvement over traditional hard copy distribution. However, professional advice may be warranted regarding security and document retention concerns where information is downloaded from portals, or saved from emails, onto personal devices.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## MEETING PROCEDURES

It is the role of the chair to ensure that meetings are run to time and that all matters are discussed and actioned appropriately. It is the responsibility of directors to ensure that they work with the chair to achieve these objectives.

Agendas should include time for ensuring a quorum is present, declaration of any conflicts of interest before opening the meeting to discussion of specific agenda items, approval of prior meeting minutes and a review of outstanding action items.

## DECISION-MAKING PROCESS

The emphasis in the boardroom is on consensus decision-making, which focuses on securing the agreement of the full board. If unable to reach a consensus, the board should state the reasons for this and endeavour to solve the issues or find further information required to make a decision.

The board and management should agree on having a number of predetermined elements included in all material proposals for board decision. It is important these elements are seen as guidance, and that management exercises common-sense and business acumen in deciding what information to provide to the board.

The following elements at a minimum should be considered in material proposals for informed decision-making:

- alignment with strategic direction
- values and behaviours
- financial and reputational impact and considerations
- economic and financial assumptions
- key risks and dependencies
- legal and regulatory obligations
- availability of resources (internal and/or external)

- ethical and environmental dimensions (eg, directors should consider 'should we', not just 'can we')
- shareholder and stakeholder perspectives
- description of due diligence completed
- benefits or outcomes are measurable and can later be tested
- contingencies to deal with unexpected developments and
- monitoring and accountability mechanisms – in particular, are actions being addressed in a timely manner.

## DECISION-MAKING OUTSIDE THE BOARDROOM

In some situations, decisions need to be taken before the next scheduled directors' meeting. It is usually permissible to circulate a resolution for approval by directors without the need to convene a meeting, though this process should be reserved for urgent matters or more procedural matters. Unless the company's constitution provides otherwise, the resolution must be signed by all directors entitled to vote on the matter and it is deemed as being passed when the last director has signed.<sup>306</sup> Even so, best practice requires that a written resolution of the directors is passed unanimously (that is, it must be signed by all directors and not just a majority), as a written resolution of directors does not otherwise provide an adequate forum for further discussion on the issues at hand should one or more directors be inclined to vote against the resolution. Separate copies of the document may be used for signing, provided the wording of the resolution and statement is identical in each copy.<sup>307</sup>

There are some matters for which a rotary/circulating resolution is not permissible, for example where the directors make a declaration of solvency prior to a voluntary winding up. Here, there is a requirement that directors have formed an opinion on solvency at 'a meeting of directors'<sup>308</sup> (which could be held virtually). Typically, most matters are best dealt with at a directors' meeting where appropriate discussion can take place.

<sup>306</sup> Corporations Act 2001, Section 248A.

<sup>307</sup> Corporations Act 2001, Section 248A(2).

<sup>308</sup> Corporations Act 2001, Section 494.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Once the resolution has been passed, it must be entered into the minute book and noted at the next meeting of directors.

## IN-CAMERA SESSIONS

Non-executive directors should consider the benefits of meeting without the presence of management. These meetings are known as 'in-camera' sessions, and can be held when non-executive directors consider it appropriate to convene without the presence of the other directors. Most often this is at the start or the end of each board meeting, so as to allow free flowing and candid discussion. Directors tend to find that having the in-camera session as standard on the agenda that any angst from management is reduced. Further, starting each meeting with an in-camera session allows the chair to identify any key concerns that directors may be seeking to gain an understanding of in the board meeting.

The types of subjects that could be usefully discussed at an in-camera session include:

- CEO performance and remuneration
- relationships between directors
- relationships with management and assurance providers
- director performance issues
- 'tone at the top' concerns
- whistleblower issues relating to senior management
- confidentiality issues
- potential conflicts of interest
- independence concerns relating to assurance providers and
- sensitive matters affecting management and/or assurance providers.

Whether there should be minutes of an 'in-camera' meeting is up to the board and will depend on the nature of the discussion. Some organisations allow their minutes to simply state that an 'in-camera' meeting took place, while others may be more descriptive.

Any formal actions that arise from an 'in-camera' session should be documented, allowing outcomes to be tracked in subsequent meetings.

## BOARDROOM CONDUCT

While each board will have its own particular boardroom style, there are basic principles of good boardroom practice and etiquette:

- punctuality and attendance for the full meeting
- full attention should be given to listening and contributing to the discussion and
- well-timed and adequate breaks should be scheduled, and catering provided, especially for long meetings.

Boardroom conduct and behaviour has a significant impact on board effectiveness, yet it is one of the most difficult things for boards to deal with. Negative behaviours such as lack of engagement, aggression, dominance, bullying and exclusiveness entering the boardroom can distract directors from their responsibilities, creating rifts, factions or divisions that can take considerable time and effort to resolve. In particular, the non-essential use of mobile phones should be discouraged during board meetings.

It is in the best interests of individuals – and the organisation – for boards to engage in collegiate, constructive and respectful behaviours.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## TECHNOLOGY

A directors meeting can be called or held using any technology, provided that all directors consent.<sup>309</sup>

This is obviously useful when a director cannot physically participate in a meeting. Emergency meetings called at short notice are a case in point. Whilst the use of meeting technology for virtual meetings can eliminate many hours of travel time for directors located interstate or overseas, face-to-face meetings are often preferred, especially where contentious matters are to be discussed. It is fundamental where technology is used, that it is secure (particularly given the commercially sensitive nature of discussions), reliable and fully functional.

KPMG recommends that at least two meetings a year be conducted face to face, in addition to any strategy dedicated sessions such that the directors are able to form a connection and build a level of trust that is sometimes more difficult to achieve in a virtual meeting.

## CONFIDENTIALITY

Consistent with their fiduciary duties, directors are expected to maintain the confidentiality of the deliberations of the board and its committees. Confidential company papers must remain secure. It is recognised as best practice for directors to return meeting papers to the company secretary after the meeting, who will then arrange for the secure destruction of surplus copies.

Several fundamental security recommendations include:

- encrypting documents
- installing password-protection mechanisms for all electronic equipment
- activating automatic locking after periods of inactivity on electronic devices and
- careful use of PINs for conference calls.

<sup>309</sup> Corporations Act 2001, Section 248D.

## INDEPENDENT PROFESSIONAL ADVICE

When one or a number of directors have concerns about the advice given to the board in relation to an issue, the board may need to seek independent professional advice to properly discharge its responsibilities.<sup>310</sup> The board should have authority to obtain advice, reports or opinions from expert advisers, as deemed necessary, at the expense of the company. Controls should be in place to ensure the process is properly managed.

## BOARD MINUTES

The *Corporations Act* provides that a company must keep a record of the proceedings and resolutions of directors' meetings, including meetings of a committee of directors, and any decisions taken outside the meeting, such as those passed by a rotary/circulating resolution.<sup>311</sup>

The company secretary is responsible for preparing the minutes from notes taken at the meeting, and should provide a draft copy to the chair within an agreed reasonable time frame. KPMG recommends that this should not exceed 5 days. The minutes must be posted in the minute book (which can be digital) within one month of the meeting and signed within a reasonable time by the chair of the meeting or the chair of the next meeting.<sup>312</sup>

Minutes should be compiled very carefully and with appropriate detail, with due regard to the fact that minutes provide evidence of what has occurred in meetings and can be used as documents with legal significance in instances of litigation. With an increasing responsibility on directors to be able to show they have properly undertaken their duties, proper minutes can protect directors in this respect.

It is therefore essential that directors give the process of reviewing and approving the minutes the level of attention it warrants, rather than simply treating it as an administrative exercise. Once signed, minutes are evidence of a proceeding, resolution or declaration to

<sup>310</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Commentary to Recommendation 1.1.

<sup>311</sup> Corporations Act 2001, Sections 251A(1)(b) and 251A(1)(d)

<sup>312</sup> Corporations Act 2001, Sections 251A(1)(b) and 251A(1)(d).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

which it relates (unless the contrary is proven).<sup>313</sup> Criminal penalties can be imposed for the falsification of records.<sup>314</sup> Minutes may be used in court to prove or disprove that directors have fulfilled their duties (as was evidenced in the James Hardie case).

If errors are subsequently detected in signed minutes, directors may pass a resolution at a future meeting to correct them. The directors may agree not to proceed with an agreed course of action as set out in the signed minutes. In these circumstances, it will be necessary for the directors to pass a resolution to rescind previous resolutions.

The minutes should always be formally approved at the next meeting if they have not previously been formally approved by all the members of the board. If the minutes are amended at the next board meeting, this should be reflected in the minutes of the subsequent meeting.

The company is responsible for safely and indefinitely keeping the minute books at the company's registered office, principal place of business or another place approved by ASIC.<sup>315</sup> Minutes can be stored in a bound or loose leaf format or electronically, as long as they can be reproduced in a printed form.<sup>316</sup>

The level of detail included in the minutes will vary from company to company. General inclusions would be:

- company name
- meeting location, date and commencement time
- chair and attendee names, including those physically present and those participating through the use of technology (e.g. teleconference)
- apologies
- presence of a quorum
- minutes of the previous meeting
- directors' declarations of personal interest

<sup>313</sup> Corporations Act 2001, Section 251A(6).

<sup>314</sup> Corporations Act 2001, Section 1307.

<sup>315</sup> Corporations Act 2001, Section 251A(5).

<sup>316</sup> Corporations Act 2001, Section 1306.

- proceedings and resolutions (including a brief outline of material factors in reaching a decision)
- title, version reference and date of all papers tabled
- directors' disclaimers or objections
- action plans, timelines and responsibilities for implementation
- closure time and
- signature of the chairman (at the subsequent meeting).

The original minutes with the amendments noted should be retained to demonstrate compliance with section 251A of the Corporations Act, and to avoid any suggestion of destruction of company records in contravention of section 1306 of the Corporations Act.

## MEETING EVALUATION

The meeting should conclude with a review of decisions reached and the related actions, in order to increase accountability among directors. All participants should be fully aware of what is expected of them. Following the meeting, the company secretary should ensure the minutes are circulated quickly in order to allow directors to promptly respond.

Requesting feedback on the meeting will provide valuable insights into how future meetings may be made more productive.

## Useful references

- Australian Institute of Company Directors and Governance Institute of Australia, Joint statement on board minutes (2019), <https://www.governanceinstitute.com.au/advocacy/thought-leadership/joint-statement-on-board-minutes/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 14. Strategy and Planning

Boards are responsible for ensuring the company is sufficiently agile to respond to changes in the business and economic environment and be able to take advantage of emerging opportunities.

## In this chapter

- Corporate strategy
- Defining the board's role in strategy
- Defining the chair's role in strategy
- Defining the committee's role in strategy
- Understanding shareholder value
- Sustainable competitive advantage
- Thinking strategically
- Stakeholder involvement in strategic planning
- Strategic risk
- Strategy review
- Using the 'balanced scorecard'

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. At the start of the strategy development process, does the board provide management with directional guidelines?
2. Has the board and management defined shareholder value and how it is measured?
3. Does management ensure that all strategic initiatives presented to the board are designed to enhance shareholder value, but with appropriate consideration of other relevant stakeholders?
4. Do the board and senior management hold an annual strategic planning day(s) to discuss and approve strategic objectives?
5. Does the board challenge and question management to achieve better strategy formulation based on mutual respect, open and honest communication and candid debate?
6. Does the board incorporate risk management into its strategic decision-making process?
7. Does the strategy include scenario analysis such that the strategy can easily pivot when scenarios change?
8. Does the board drive management to develop a business model that provides the organisation with a competitive advantage?
9. Are the strategic options presented by management based on robust and thorough analysis using established tools and methodologies?
10. Does management have an environment scanning process to capture new technologies, consumer trends, competitor tactics and other significant external changes?
11. Are the views of key stakeholders taken into account in the strategy development process?
12. Are different strategic options considered prior to a final decision being made by the board?
13. Does the board ensure that there is a rigorous process in place to translate the strategy into action through corporate budgeting and planning?
14. Have board and management considered using the 'balanced scorecard' approach to measure the organisation's performance?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board accepts management's strategy without in-depth probing or questioning.
- The board does not fully understand the nature and implications of the proposed strategy.
- The external environment is not fully considered in strategy development.
- Not all directors attend the meeting when the strategy is discussed and approved.
- The risks inherent in strategy are not identified or managed.
- Strategic decisions are not adhered to or are revisited excessively.
- The mechanisms for measuring shareholder value are not fully understood.
- Board meetings are not strategically focussed.
- There is little time devoted to non-financial performance measures.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## CORPORATE STRATEGY

The performance dimension of a board's role focuses on business strategy and the pursuit of shareholder value.

The nature and extent of the board's participation in strategy depends on the company's size, industry and particular circumstances. It is, however, essential that cooperative and interactive strategic planning processes are instituted which enable boards and management to:

- make, review and assess strategic decisions
- understand the key drivers of company performance
- align the company's strategy, operations and external environment
- understand potential risks and incorporate risk management into strategic decision-making.

## DEFINING THE BOARD'S ROLE IN STRATEGY

At the end of the day, it's management's strategy. But the long-held view that the board's role is limited to reviewing, understanding, and signing off on the strategy is giving way to deeper board engagement. Increasingly complex business conditions demand it, investors and stakeholders expect it, and ASIC and other professional bodies have urged boards to be more strategic, focusing on future performance, as well as compliance. Many directors believe strategy to be their most important sphere of activity, with their input having a significant influence on company performance.

Directors can have a meaningful impact on the strategy process. Factors to assist in enabling this include:

- strong knowledge of the company's operating context
- allocating sufficient time to consideration of strategic issues
- board time not being overly taken up with compliance issues
- executives being willing to incorporate director input
- having a dedicated forum for participation (such as a specific strategic planning workshop)

- management discussing options with directors rather than presenting a 'final' strategy.

However, the foundational element is the board providing clarity on what the risk appetite of the organisation is. Without this, it is very difficult to assess whether a strategy is too bold, too timid or has hit the right balance.<sup>317</sup>

Reviewing, adding value to and approving the strategy are crucial to the board's governance role and KPMG's experience in talking to boards and undertaking board performance assessments is that directors almost always would like more time on strategy. Unfortunately with an increased focus on compliance, it has been strategy that has been allocated less time on the board agenda notwithstanding that this is often the area in which directors feel that they add the most value.

Boards need to be seen by management as a strategic resource that contributes to superior company performance. Through the board's unique position, directors can contribute by providing:

- market information and industry trends
- experience and expertise accumulated during their professional careers
- new perspectives and fresh ideas
- an independent and objective viewpoint.

These strengths, combined with management's in-depth company knowledge and experience, mean that collaborative decision-making often leads to better strategy. Directors are more likely to add value to the strategy process if they possess a strong understanding of the company and its environment, have strong meaningful working relationships with each other, as well as the management team, and are able to communicate and exchange information.

<sup>317</sup> This is discussed in more detail in Chapter 17, Risk Management

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DEFINING THE CHAIR'S ROLE IN STRATEGY

Chairs KPMG spoke to as part of a global 2019 survey emphasized three key areas of focus for chairpersons as they facilitate their board's engagement in the strategy process, from strategy development and evaluation to monitoring strategic execution and recalibrating strategy as necessary:

- **Setting expectations** with the CEO and directors for the board's engagement in strategy
- **Planning the setup** and staging of board strategy discussions and providing the backdrop to drive the right focus and dynamics
- **Building consensus** about the proposed direction of the strategy—the fifty-thousand-foot view

The chairs also emphasized a number of specific elements and practices that are pivotal to quality boardroom discussions about strategy, e.g., diverse and dissenting views, having a vivid picture of the future, and focusing on critical alignments:

- Encourage the board, CEO, and management to develop a vivid picture of the future, where the industry and competition are headed and its impact on strategy
- Insist on diverse and dissenting points of view, including third-party input
- Assess whether the company's strategy process enables the company to recalibrate strategy as needed while maintaining critical alignments
- Work with committee chairs to maintain the alignment of board and committee structure and governance processes with strategy
- As part of the board evaluation, assess whether the board has the right composition and leadership to effectively engage in strategy

## DEFINING THE COMMITTEE'S ROLE IN STRATEGY

As boardroom leaders, committees can offer a unique perspective on strategy. At least annually, consider the company's strategy through the committee lens; revisit committee responsibilities, work plans, and evaluations to help ensure alignment with the company's strategy and its drivers.

- **Nomination committees** should be focused squarely on board composition and talent. "Do we have the talent around the boardroom table to effectively evaluate the strategy? Is the board fit for purpose and able to help guide the company into the future?" More broadly, consider with the remuneration committee whether the company has the right talent to implement the strategy.
- **Remuneration committees** should ensure that remuneration plans are synchronized with strategy, particularly as strategies change in light of industry transformation and disruption. Old metrics and incentives may no longer relate to the new strategy. Is the organisation attracting and retaining the talent required to execute its strategy?
- **Audit committees** may need to sharpen their focus on capital investments and capital allocation as well as the overall culture and control environment, particularly as the strategy changes.
- **Other committees** – Is a new committee needed? As the operating environment gets more complex, an additional committee—for example, to oversee technology, risk, or public policy—might make sense. Although, this needs to be considered in light of whether the board has the bandwidth and necessary skill sets for an additional committee.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## UNDERSTANDING SHAREHOLDER VALUE

The board and management must ensure all strategic initiatives are designed to enhance shareholder value, balanced with appropriate consideration given to other relevant stakeholders and overall ESG objectives. Shareholders define value from a different perspective to the company. To shareholders, value may be simply the dividends or cash equivalents they receive, plus the increase (or decrease) in the market value of their shareholdings over the life of their investment. Companies require more objective measures of shareholder value that are independent of the volatility and ambiguity of market valuations. It is important for boards to define and measure shareholder value. This definition will guide decision-making at all levels of the organisation.

## SUSTAINABLE COMPETITIVE ADVANTAGE

The fundamental aim of corporate strategy is to provide an organisation with sustainable competitive advantage. This refers to the unique value-creating processes that set an organisation apart from its competitors. Sources of competitive advantage may include:

- use of a leading edge business model
- innovation
- effective use and sharing of assets and resources, such as patents and other intellectual property, corporate reputation and physical locations
- dynamic product lines
- the collective skills and experience of the executive and management team
- a lock on the market or customer base
- strong focus and differentiation.

Most competitive advantages are short-lived because environments change rapidly. Creating sustainable competitive advantage over the long-term necessitates that companies be flexible and responsive. In fact, organisational agility and the ability to re-deploy organisational resources to take advantage of opportunities can be a sustainable competitive advantage in itself.

## THINKING STRATEGICALLY

Thinking strategically is distinct from strategic planning. Whereas strategic planning is often a formal process, driven by analysis and consideration of different strategic options, strategic thinking is a more continual, creative process whereby individuals let go of the detail and approach problems from a broader perspective. Boards are removed from the everyday running of the company and are therefore, in an ideal position to employ strategic thinking.

Boards should develop a culture of strategic thinking that can be assisted by:

- creating a climate where strategic thinking is a valued activity
- challenging and evaluating the processes for developing strategy, not just the strategies themselves
- upholding high expectations for strategic plans
- setting aside adequate time and resources to discuss strategy in a meaningful way
- establishing methodologies, tools and policies for strategic decision-making and monitoring management adherence to them
- ensuring all company decisions align with the strategy.

## STAKEHOLDER INVOLVEMENT IN STRATEGIC PLANNING

A critical step in the strategic planning process is engaging with key stakeholders. A company's stakeholders are those groups who affect and/or are affected by the company and its activities, such as investors, lenders, analysts, employees and customers. In leading organisations, stakeholder engagement has migrated from an optional consideration to an integral part of the business strategy.

Boards face ongoing scrutiny and increasingly high expectations from stakeholders. As part of their responsibility for governance oversight, directors need to identify and understand the expectations of the company's stakeholders, which may vary across industries and are continually changing.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The ASX Principles suggest that to make ethical and responsible decisions, companies should not only comply with legal obligations, but should also consider the reasonable expectations of their stakeholders.<sup>318</sup> It is considered good practice to incorporate stakeholder views into the strategy development process, whether directly through consultation with stakeholder representatives, or by indirectly acknowledging their goals when generating strategy. Stakeholders bring expert advice or represent the interests of groups that can have a major effect on the success of the strategy. A diverse range of views and ideas can lead to more innovative problem solving. There should also be enhanced communication and trust, leading to mutual understanding and collaboration, and reduced legal and reputational risks and associated costs.

## STRATEGIC RISK

Boards must identify, assess and manage the risks inherent in any strategic plan. Strategic plans often do not achieve their desired aims, are poorly executed, or fail to keep pace with changes to the business environment.

Directors have a duty to satisfy themselves that an effective strategic risk management plan is in place and is being followed. Such plans should:

- identify and evaluate strategic risks
- consider non-financial in addition to financial risks
- consider emerging risks and trends
- reflect the organisation's risk appetite
- measure what is happening
- be aligned with the organisation's delegation of authorities
- prepare for, and take appropriate corrective action.

<sup>318</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Principle 3.

Boards must try to balance both short and longer-term strategic risk. Strategic risk increases as the time horizon expands – the longer the timeframe, the more unpredictable it becomes, and thus the more sophisticated the organisation's risk management capabilities need to be. Many organisations develop scenarios that deal with a variety of alternatives to mitigate this problem. Risk management is an increasingly vital part of organisational accountability and strategic decision-making. Accordingly risk and strategy feed each other as emerging and existing risk informs strategic direction and then the strategy informs what strategic risks will need to be managed.

## STRATEGY REVIEW

Strategy needs to be continually reviewed. It is the board's responsibility to conduct a thorough analysis of current strategy and progress towards the agreed objectives, and to evaluate company performance in light of these objectives. A board will normally review the strategic direction at least annually, with an increasing trend to half-yearly reviews. Strategies should also be subject to reviews to ensure they remain appropriate to the organisation's needs. There is a danger that organisations become complacent in their strategy, making incremental adjustments whilst their environments continue to change rapidly. More agile competitors will quickly overtake companies that merely react to the environment, rather than challenging, questioning, and even influencing it.

In addition, boards need to be vigilant in assessing company performance in achieving the strategy. Periodic reporting from management (such as a quarterly report card incorporating exception reporting) can help the board quickly come to terms with what is not working and why. Boards need to ensure that sufficient funds and resources are provided to enable an organisation to achieve its strategic goals.

It is important that the board receives the appropriate facts and information to make an accurate assessment. Financial and operational reports are a good starting point, but the board also requires non-financial performance indicators. These may include indicators of customer satisfaction, employee engagement, health, safety and wellbeing and community involvement.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The board is there to look objectively at company strategy and make the tough decision to change a company's course when it is no longer viable.

Rather than trying to predict the future, the board can ensure the organisation's capabilities and resources are sufficient to manage uncertainty and that strategic plans are flexible. In-built flexibility is promoted by:

- scanning the environment constantly and keeping abreast of changes that could materially affect the achievement of strategic objectives
- exploring how environmental shifts will impact on strategy
- inviting subject matter experts to address the board and senior management
- ensuring accurate and timely information reaches the board and is discussed candidly by directors and managers by scheduling 'break-out' sessions to allow the board to critique the current strategy.

## USING THE BALANCED SCORECARD

The balanced scorecard method is used by many companies globally as a better practice approach to setting performance measures and subsequently measuring actual performance. The idea of a balanced scorecard arises from the fact that financial measures are the end result of a range of other activities and processes taking place in companies. To increase sales, cut costs, lift margins, raise profits and improve return on investment, companies must do things such as engage in activities, processes, programs and projects. Directors must get behind the financials to discover these value drivers. They must learn to measure the value drivers if they are to manage them.

The balanced scorecard approach recommends that boards view their business from many perspectives.



**Financial perspective** – how does our performance look to shareholders? Are we adding value?



**Customer perspective** – how do customers see us?



**Internal business perspective** – what must we excel at?



**Innovation and learning perspective** – can we continue to innovate and create value?



**Community and environment** – how do we meet all stakeholder expectations?

Using a balanced scorecard approach, companies set themselves goals or business objectives for each perspective. They then select the measures that best calculate progress in achieving these goals. These goals and measures should be geared to the circumstances of individual companies.

The balanced scorecard provides a performance information framework that allows companies to evaluate the effectiveness of their strategy. The balanced scorecard methodology has been promoted mainly as a management process, but it makes an excellent reporting framework for company boards.

## Useful references

- ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations*, 4th edition, 2019.
- AICD, Strategic Plan Development, Role of the board, [https://aicd.companydirectors.com.au/~media/cd2/resources/director-resources/director-tools/pdf/05446-5-14-mem-director-rob-strategic-plan-development\\_a4-web.ashx](https://aicd.companydirectors.com.au/~media/cd2/resources/director-resources/director-tools/pdf/05446-5-14-mem-director-rob-strategic-plan-development_a4-web.ashx)
- KPMG, 2019, Facilitating the board's engagement in strategy, <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2019/12/facilitating-the-boards-engagement-in-strategy.pdf>
- Governance Institute of Australia, Journal: Governance Directions, Volume 74- Number 3, 3 ways your attitude to risk might be holding back your strategy by Rosie Yeo, <https://web.governanceinstitute.com.au/resources/governance-directions/volume-74-number-3/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 15. Receiving Assurance

Whilst the board may understand its business risks well, without comprehensive assurance the board has no way of knowing that the business is managing these risks appropriately.

## In this chapter

- The role of assurance
- The role of the audit committee
- Internal risk and compliance frameworks
- Internal audit
- External audit
- Assurance over sustainability reporting
- Analytics and assurance
- Artificial Intelligence (AI) in assurance
- Other assurance providers

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is the board/audit committee satisfied with management's assurances in relation to the company's risk management and internal control and compliance systems?
2. Does the board receive regular independent assurance on the effectiveness of the business risk management framework and controls?
3. Has an assurance map been developed that provides a consolidated view on how assurance across the organisation's key processes and/or risks is obtained?
4. Does the external auditor test and challenge elements of the financial reporting, disclosure, risk and control environment?
5. Does the board receive assurance over other non-financial disclosures made by the company (e.g. Environmental, Social and Corporate Governance (ESG) related disclosures)?
6. Is the board, through the audit committee, satisfied that the internal audit function is operating effectively and efficiently?
7. Is the internal audit plan clearly linked to the most current risk profile, and is the risk profile updated based on audit findings and outcomes?
8. Are remedial actions resulting from weaknesses identified by assurance activities monitored by the audit committee?
9. Are management invited to the audit committee to discuss key assurance outcomes (e.g. high or critical rated assurance findings) with the board?
10. Does the audit committee have a defined escalation process in place for any critical risks identified in assurance activities?
11. Does the board and relevant committees have the right skills and experience to provide oversight and challenge to the internal and external auditors?
12. Do both the external and internal auditors meet with the Chair of the audit committee without management attending, as well as have the opportunity to present at each audit committee meeting?
13. Are there board approved charters in place for the roles and accountabilities of the external and internal auditors?
14. Is the assurance planning aligned with risk management and strategic planning?
15. What insights can assurance provide about the organisation?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- A assurance map does not exist to indicate any gaps in assurance provided.
- Assurance is limited to financial processes only.
- The board does not review the risk profile and internal audit plan on a periodic basis.
- The assurance findings do not align with the perceived control framework effectiveness on which the overall risk profile is based.
- Uncertainty exists over the processes supporting management attestations.
- The internal audit function appears to be under-resourced or projects are being cancelled or delayed by management.
- Recommendations made by assurance providers are not being tracked and implemented.
- The audit committee reports to the board do not provide an overview of the internal audit work plan and outcomes.
- The board becomes aware of significant accounting disagreements between management and the external auditors.
- The external auditors are not present when the board considers the annual financial statements.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## THE ROLE OF ASSURANCE

Assurance can be described as an assessment process from which a level of confidence over the matter under review can be gained. Boards should obtain comprehensive assurance on the effectiveness of their organisation's business risk management and compliance frameworks, and the controls applied to manage these.

Assurance can be sought by the board for dual purposes, as a means of gaining comfort over the implementation and effective management of **internal** controls over organisational risks, and, to provide **external** stakeholders with an independent assessment of how well an organisation is meeting mandatory or voluntary performance and reporting standards.

Assurance can take a number of forms including:

- system-based reporting produced from the implementation of risk and compliance frameworks
- management attestations and assurances
- internal audit
- external audit
- other independent assurance providers (e.g. actuarial, WH&S, independent experts).

## THE ROLE OF THE AUDIT COMMITTEE

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. Recommendation 4.1 of the ASX Principles also suggests that a listed entity have an audit committee. The commentary to Recommendation 4.1 lists those matters which the audit committee should make recommendations to the board regarding.

The audit committee's key duties and functions relating to internal audit include:

- reviewing the internal audit charter to ensure the appropriate organisational structures, authority, access and reporting arrangements are in place

- assisting the board to ensure senior management establishes and maintains adequate and effective internal controls
- overseeing the scope and effectiveness of the assurance systems established by management to identify, assess, manage and monitor the various business risks arising from the organisation's activities
- reviewing the scope and coverage of the internal audit plan, annual work plan, and monitoring progress
- advising the board on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- reviewing internal audit reports and advising the board on significant issues identified and the actions taken (including the identification and dissemination of good practice)
- monitoring management's implementation of internal audit recommendations
- assisting the board to oversee that appropriate controls are in place for the monitoring of compliance with laws, regulations, supervisory requirements and relevant internal policies
- periodically assessing the performance and objectivity of the internal audit function
- making recommendations for the appointment (or if necessary, the removal) of the head of internal audit.

The audit committee should be involved in setting the internal audit's functions and goals. These should be incorporated into the internal audit charter or in an appropriate service level agreement. The internal audit charter defines the audit committee's expectations for the internal audit function.

Typically, the audit committee should expect the following components to be included in the internal audit charter:

- role and scope of work
- responsibility and accountability

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

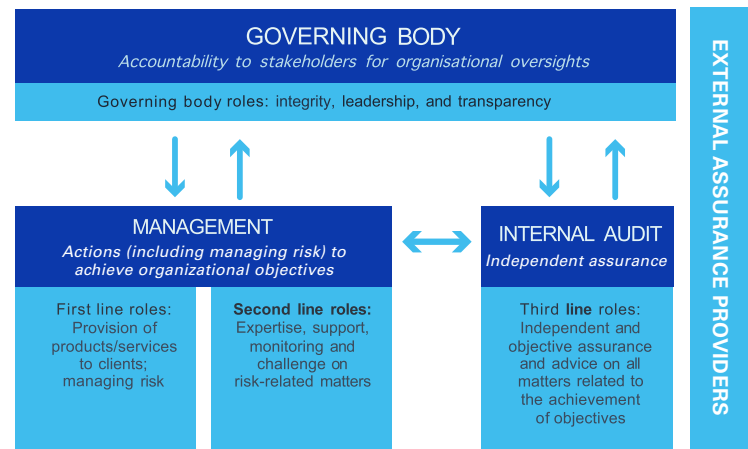
- objectivity and independence
- operating principles
- reporting, including an overview of reports to be completed throughout the year
- quality of service, including management feedback.

It is common practice to combine the audit and risk committees which serves to even further align the assurance activities with the risk management functions.

INTERNAL RISK AND COMPLIANCE FRAMEWORKS

Most organisations establish a control environment that is commonly referred to as 'the three lines model' or 'three lines governance model' (previously, 'three lines of defence'). The Institute of Internal Auditors illustration of this model is included below.

The IIA's Three Lines Model



**KEY:** ↑ Accountability, reporting | ↓ Delegation, direction, resources, oversight | ↔ Alignment, communication, coordination, collaboration

Source: the IIAs Three Lines Model – An update of the Three Lines of Defence

The three lines works on the basis of establishing controls within different layers of the organisation, starting at the operational level as the first line, where controls are in place to manage day-to-day risks (e.g. the bank teller validating a customer's identity when they withdraw cash to help mitigate fraud risk). The second line relies on oversight functions within the business, which establish and oversee systemised governance approaches that support the first line. For example, the Finance team of the bank checking transactions to ensure that the correct identification from the customer was sought during the withdrawal and that a reconciliation of funds withdrawn for the day is regularly performed to identify any potential errors. The third line is independent assurance over these processes, where reviewing and testing by an independent party is performed and reported to the board (potentially through and audit committee or similar), identifying any errors or control weaknesses.

Boards should obtain a level of assurance or comfort on the soundness of the systems of management controls over key risks from risk management reporting. The degree of assurance will depend upon the robustness of the risk management process. Boards should understand this process well and ensure that it is regularly reviewed and updated. At least in theory, receiving attestations from management allows the board to regularly satisfy itself about the veracity of the company's outputs, processes and systems and controls.

The scope of these attestations can include:

- the integrity of the financial reports
- effective risk management, internal compliance and management control systems over financial reporting risks and material business risks
- compliance with company policies and regulatory requirements.

The Corporations Act and ASX Principles formalise the management sign-offs relating to the financial reports. Section 295A of the Corporations Act requires the CEO and CFO of a listed company to provide the board with an annual written declaration and sign-off that the company's financial records have been properly maintained,

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

the annual financial statements comply with accounting standards and give a true and fair view of the company's financial position and performance.

Further, the ASX Principles recommend that the declarations required under section 295A extend to include a declaration from the CEO and CFO that the financial statements have been formed on the basis of a sound risk management system and internal controls which are operating effectively. It also extends the need for the declaration to apply to the financial statements for any financial period, not just the financial year end.<sup>319</sup>

The ASX Principles also recommend that a listed entity should disclose:

- if it has an internal audit function, how the function is structured and what role it has or
- if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.<sup>320</sup>

An internal audit function can assist a listed entity to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and continually improving the effectiveness of its risk management and internal control processes.<sup>321</sup>

## INTERNAL AUDIT

An effective internal audit function plays a key role in helping the board, through the audit committee, to discharge its governance responsibilities. As such, the audit committee needs to satisfy itself that internal audit is functioning effectively and efficiently.

A strong relationship between the audit committee and the entity's internal auditors enables the committee to meet its responsibilities and carry out its functions. Internal audit should be a major source of information to the audit committee on the performance of the entity.

Australia's position in the global market, changes to corporate governance requirements and the dramatic changes in the business operating environment have increasingly brought about a need for the board, through its audit committee, to seek broader assurances, beyond financial matters, in a range of areas, including core operations, major projects and/or transformation initiatives, health, safety and wellbeing; environment; security; information systems and human resources to name a few. These quality assurance needs have broadened the traditional internal audit function. The new-style internal audit model is aligned directly with corporate strategy and focuses on specific risks that influence organisational success.

Internal audit has a multifaceted role to play in the enterprise risk management (ERM) arena. The Institute of Internal Auditors in Australia notes that internal audit's core role with regard to ERM is to provide objective assurance to the board on the effectiveness of an organisation's ERM activities to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively. In addition, many companies are looking to internal audit to support strategic business objectives. That effort extends to ERM activities such as:

- risk identification and prioritisation
- alignment of people, processes and systems with the business strategy
- definition of key performance indicators
- analysis and quantification of risk factors in new business ventures and strategies
- understanding the shared risks among various projects and initiatives.

<sup>319</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, commentary to Recommendation 4.2

<sup>320</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Commentary to Recommendation 7.3

<sup>321</sup> Ibid



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Internal audit's role, its knowledge of the organisation's key risks, and its enterprise-wide view enable it to bring an important perspective and discipline to an ERM effort.

Forward-thinking organisations are those that do not view compliance risk management as a cost of doing business, but rather as a strategic investment that is critical to business resilience, efficiency and success. This trend towards strategic compliance risk management requires a bespoke approach to the design and development of compliance arrangements. A one size fits all approach to the design of compliance arrangements is not always appropriate or practical.

**Risk-based internal audit plan**

In reviewing the internal audit plan, audit committees need to consider the risk profile and determine the areas where internal audit can provide assurance. In making this judgement, directors need to be aware that, where the internal audit function is in-house, there may be some issues that will require coverage by additional specialists through an independent third party review. The audit committee should ensure the internal audit team has used a formal process to define and prioritise risks and plan its work accordingly. A risk-based internal audit plan can prioritise the key risks subject to audit and allocate focus over the internal audit cycle. The plan should also be flexible so that emerging risk issues can be incorporated into the program.

**Scope, procedures, coverage and timing**

The proposed scope, procedures, coverage and depth of the internal audit plan, and particularly any restrictions on the scope of the internal audit plan, should be fully discussed and debated by the audit committee before being approved. The audit committee should ensure that strategic business risks have been evaluated and assessed with respect to determining the audit procedures and scope. The audit committee should consider the timing of proposed audit work and prioritise, where necessary.

**Internal audit results**

Regular communication by the internal audit function with the audit committee is critical, especially with regard to the completion of reported findings and recommended improvements. A timetable for regular meetings and proposed internal audit report completion dates should be included in the internal audit plan. The audit committee should have mechanisms for facilitating confidential exchanges with the internal auditor. This can be by way of the audit committee chair meeting with the head of the internal audit function outside audit committee meetings, or meetings (adjunct to the formal committee meeting) between the audit committee and the internal auditor 'in-camera' (without management present).

The reporting to the audit committee should not cease when the internal audit report on findings is tabled. Rather, the internal auditor should report to each meeting on whether actions agreed to be taken to remediate the weaknesses noted have been completed to an acceptable level by the due dates. This enables the audit committee to understand whether the risks identified have been mitigated, or whether further resources need to be applied to achieve resolution. Internal audit functions may elect to leverage governance, risk, compliance (GRC) technological tools (software) to facilitate the capturing, monitoring and reporting of findings and agreed management actions.

**Operational changes and new developments**

Audit committees and the internal audit function need to keep abreast of developments affecting its activities and internal audit work. The internal audit function should be responsive to changing needs, striving for continuous improvement and monitoring integrity in the performance of its activities.

**Budget, staffing and resources**

The audit committee should ensure the internal audit function is appropriately staffed and resourced. To allow for full accountability, the budget should include a detailed analysis of time and/or cost per project. If a third party provider acts as the internal auditor, an engagement letter should also be signed to formally set out the mechanism for developing and agreeing a plan and budget.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

So as to enable internal audit to extend into all aspects of the business, as well as to create opportunities for talented staff to understand assurance and risk management, some progressive organisations utilise "guest auditors" from within the operations to join the internal audit team and provide subject matter expertise into the topic being audited.

## EXTERNAL AUDIT

The external auditor, as an independent party with knowledge of the entity's financial affairs, is in a position to provide the board (through the audit committee) with independent insight into the effectiveness of the organisation's risk management, internal control, financial reporting and legislative compliance frameworks. As such, the external auditor can be an important contributor to good governance.

One of the key functions performed by the external auditor is the audit of the company's annual financial report. The auditor must report to members on whether, in the auditor's opinion, the financial report complies with the Corporations Act, accounting standards and gives a true and fair view of the financial position and performance of the company.<sup>322</sup> The auditor must also provide the directors with an independence declaration – i.e. a declaration that, to the auditor's knowledge and belief, that there have been no contraventions of the auditor independence requirements under the Corporations Act or any applicable professional code of conduct in relation to the audit.<sup>323</sup>

Other functions carried out by an external auditor will also generally include evaluating elements of the control environment covering financial reporting and providing suggestions to improve the effectiveness of financial control, management and reporting and disclosure.

The audit committee typically has significant engagement with the external auditor throughout the year. Some of the key functions performed by the audit committee in assisting the board in its oversight of the external auditor include:

- developing and implementing procedures for the selection, appointment and rotation of the external auditor
- recommending to the board the appointment or (if necessary) the removal of the external auditor
- reviewing and (if appropriately authorised under the delegations framework) approving the terms of engagement and the reasonableness of the audit fees prior to the commencement of the audit
- reviewing and (if appropriately authorised under the delegations framework) approving the external auditor's proposed audit plan and audit approach, including materiality thresholds
- assessing the performance and objectivity of the external auditor.<sup>324</sup>

The Auditing and Assurance Standards Board (AUASB) is an independent statutory agency of the Australian Government which is responsible for developing, issuing and maintaining auditing and assurance standards. The AUASB Standards establish requirements and provide explanatory material on the responsibilities of the auditor and the assurance practitioner, as appropriate, when performing audits, reviews, assurance or related services engagements.<sup>325</sup> Directors on an audit committee should have a general understanding of the standards and how these apply to the external auditor in the external audit process.

Section 250RA of the Corporations Act requires an auditor of a listed entity to attend the entity's AGM and be available to answer questions from shareholders relevant to the audit.<sup>326</sup> For those listed entities established outside of Australia, Recommendation 9.3 recommends that the entity should ensure that its external auditor attends its AGM and is available to answer questions from security holders relevant to the audit.

<sup>322</sup> See Part 2M.3 Division 3 of the Corporations Act generally as to the audit and auditor's report. See also Chapter 3 (Accountability to shareholders).

<sup>323</sup> CA 307C

<sup>324</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Commentary to Recommendation 4.1.

<sup>325</sup> Refer to Auditing and Assurance Standards Board, <http://www.auasb.gov.au/Home.aspx>

<sup>326</sup> Section 250T of the Corporations Act.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Communication with the external auditor**

It is important that the audit committee communicates to the external auditor any matters relevant to the planning and completion of the audit. At the start of each annual external audit cycle, the audit committee needs to consider the external auditor's overall audit strategy, including the planned levels of materiality and proposed resources to execute the external audit plan, and evaluate whether it appears consistent with the scope of the external audit engagement. It should also consider the seniority, expertise and experience of the external audit team.

Throughout the external audit engagement, the audit committee should challenge management and the external auditor about the:

- risks of material misstatement
- impact of changes in the business environment
- critical accounting principles
- subjective and judgemental areas of accounting
- quality of financial reporting and disclosures
- changes to accounting standards.

**ASSURANCE OVER SUSTAINABILITY REPORTING**

Although it is not currently a requirement for boards to receive independent assurance on sustainability reports, an increasing number of companies recognise that independent assurance provides confidence to both internal and external stakeholders regarding the credibility, reliability and relevance of data reported. This is reflected in the adoption of ASX Principle 7.4, which requests listed entities to disclose in the annual report any "material exposure to economic, environmental and social sustainability risks, and if it does, how it manages or intends to manage those risks". In response, obtaining assurance over these risks is an increasing trend. More recently this has also extended into boards receiving assurance in relation to its organisation's sustainability related claims and commitments.

**ANALYTICS AND ASSURANCE**

In the last few years, there has been a focus on enhancing the role of assurance to provide insights into the business which go beyond the effectiveness of an organisation's control environment. Technological software has progressed to analyse full populations of data which can allow for:

- the stratification of data sets to provide an informative breakdown by various sub-groups
- trends across various periods, detailing effectiveness of the control environment across time
- Correlation of control environment effectiveness to events occurring in the organisation (e.g. organisation restructures, implementation of new systems, departure of key personnel etc.).

As the role of internal audit evolves over the next few years, the capability to provide assurance over a full population should be a requirement, as opposed to being a 'value add'. Substantive testing on selected samples across the year will no longer be enough to provide the board and other subcommittees with the oversight required to effectively understand and make decisions with regards to an organisation's control environment. It is, therefore, important to enquire about the how internal audit is able to provide analyses over population sets of data, minimising the manual effort required to test samples. This is not to say that manual testing has no place in the future, rather, effort should be undertaken to investigate exceptions and provide thoughtful analyses from the data provided which can complement traditional auditing techniques.

**ARTIFICIAL INTELLIGENCE (AI) IN ASSURANCE**

AI has the ability to provide useful information to internal auditors and boards if it is used and managed well. The benefits of AI include:

- Enhancing and quickening the process of data collection through machine learning, natural language processing and robotics
- Assisting in conducting repetitive tasks and assisting auditors in the validation of information and
- Converting data to useful information to aid decision making.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Despite increased automation of many activities, human input is still required to analyse the data and information; however, the time required for traditional auditors to 'crunch numbers' will be significantly reduced as AI evolves.

## OTHER ASSURANCE PROVIDERS

A number of different assurance providers can be used by management across its business operations. This can cover quality, clinical, training, safety and regulatory compliance type audits or reviews being routinely conducted by many businesses.

An assurance map can be a useful tool for the board to outline the key business processes as a source of assurance, as well as expose any gaps or duplication in assurance activities. The board should be kept informed of all important findings from these assurance activities and have a formal escalation process in place. A commonly observed approach may take the form of a company policy where "all assurance audits with a finding rated as critical must be tabled with the chair of the audit committee within one working day of identification, and all assurance reports tabled with the audit committee when final".

## Useful references

- Australian Government – Auditing & Assurance Standards Board, [www.auasb.gov.au/Home.aspx](http://www.auasb.gov.au/Home.aspx)
- The Institute of Internal Auditors, [www.iaa.org.au/Home.aspx](http://www.iaa.org.au/Home.aspx)
- The Institute of Internal Auditors, The IIAs Three Lines Model, An update of the Three Lines of Defence, [https://iaa.org.au/sf\\_docs/default-source/technical-resources/the-iias-three-lines-model--an-update-of-the-three-lines-of-defence.pdf?sfvrsn=4](https://iaa.org.au/sf_docs/default-source/technical-resources/the-iias-three-lines-model--an-update-of-the-three-lines-of-defence.pdf?sfvrsn=4)

## For further information please contact:



Jonathan Ho

Director, Governance,  
Risk & Controls Advisory (GRCA)  
[jho5@kpmg.com.au](mailto:jho5@kpmg.com.au)

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 16. Tax Governance & Transparency

Tax governance is at the heart of tax management, and as ESG principles continue to increase in relevance, so does tax governance and tax transparency. Tax governance can and should be considered together with the performance of tax functions in support of business objectives.

## In this chapter

- Overview of Tax Governance
- Director's Responsibilities
- Recent Developments and Trends in the Market
- Future Direction

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is there a formalised tax control framework/policy setting out governance and risk management for tax that has been endorsed by the board?
2. Does the framework/policy include the organisation's Tax Risk Appetite in relation to strategic and operational risk? How is the Tax Risk Appetite documented and communicated?
3. Is the tax control framework/policy published internally and externally?
4. Is the tax risk management escalation model formally documented, such as the definition of significant transactions/events/risks (identification, assessment and escalation including when to seek external tax advice)? Is it clear when the board should be involved on tax risks?
5. Are the roles and responsibilities/delegation for tax governance and risk management documented in the board/sub-committee charters?
6. Does the company have a board skills and competency matrix covering tax?
7. Is a tax briefing included in the tax induction programme for new board directors?
8. Is the board regularly reported on tax compliance, legislative developments that may have an impact on the organisation and tax risks including trends (e.g. tax risk register/enterprise risk register that includes tax risk)?
9. Is periodic internal control testing conducted to assure the board that the internal control framework is robust enough to effectively manage tax risk?
10. Are directors aware of their personal liability exposures for unpaid PAYG, GST and superannuation guarantee charge?
11. How recently has there been a determination of the level of tax transparency reporting by the company? Especially for groups with international presence, has the evolution in global trends including specific recent EU developments been considered?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Tax risk management and governance framework is not formalised/established.
- Tax strategy/policy/framework is not reviewed regularly and/or endorsed by the board.
- Tax Risk Appetite is not incorporated in the overarching risk appetite statement.
- Tax risk management escalation is not formally documented or established.
- Roles and responsibilities for tax governance and risk management are not formalised.
- The board is not informed of tax risks and taxation developments.
- Internal control framework is not tested periodically.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## OVERVIEW OF TAX GOVERNANCE

Tax governance can be described as implementing controls that support business objectives whilst exhibiting agility and resilience, and supporting compliance.<sup>327</sup> Setting a tax strategy, putting in place a governance framework including processes and controls and taking steps needed to bring it to life are the building blocks to success. Establishing the right operating model for your tax function is key.

In Australia, the importance of demonstrating tax governance measures are in place has experienced a step change. The Australian Taxation Office (ATO) has established a tax governance benchmark through its Justified Trust methodology, which is being reviewed formally through its Top 100 and Top 1000 compliance and certain Private Group programmes. 'Justified Trust', an Organisation for Economic Cooperation and Development (OECD) concept, aims to strengthen community confidence that taxpayers are paying the correct amount of tax.

In January 2017 the ATO released an expanded Tax Risk Management and Governance Review Guide (ATO Guide), which was updated in April 2018.<sup>328</sup> The ATO Guide establishes a series of expectations of taxpayers in the design and operation of tax risk management and governance. In July 2020, the ATO also released a GST Governance, Data Testing and Transaction Testing Guide (ATO GST Guide)<sup>329</sup> going into more detail in respect of GST related controls. In April 2022 the ATO issued supplementary guidance<sup>330</sup> on third-party data controls for organisations in the investment sector.

<sup>327</sup> Refer to KPMG, 2020, Everything Matters: Governance & Performance in Tax, <https://home.kpmg/au/en/home/insights/2020/09/governance-performance-tax.html>

<sup>328</sup> Australian Taxation Office (ATO), 2022, Tax risk management and governance review guide, <https://www.ato.gov.au/Business/Large-business/In-detail/Key-products-and-resources/Tax-risk-management-and-governance-review-guide/>

<sup>329</sup> ATO, 2020, GST governance, data testing and transaction testing guide, <https://www.ato.gov.au/Business/Business-bulletins-newsroom/GST/GST-governance,-data-testing-and-transaction-testing-guide/>

<sup>330</sup> ATO, 2022, New third-party data governance guide: investment industry tax controls, <https://www.ato.gov.au/Business/Business-bulletins-newsroom/Public-advice-and-guidance/New-third-party-data-governance-guide-investment-industry-tax-controls/>

The benefits of establishing tax governance include:

- Increased comfort that tax outcomes are being consistently achieved within a defined risk appetite, with fewer surprises.
- Saving time through greater clarity in responsibilities and the procedures to occur across organisations.
- Addressing key person risks and save time through having in place documentation of the tax governance framework and key processes, controls and policies when team members change.
- Providing a structured approach to avoid complacency and identify process and other improvements.
- Providing a structured approach to identify the needs and build the business case to address tax data and tax technology needs as regulators globally invest in their own data technologies.
- Demonstrating purpose and care towards internal and external stakeholders, creating a positive legacy.

## DIRECTOR'S RESPONSIBILITIES

The ATO Guide sets out the responsibility of the Board for oversight and monitoring of organisation's governance processes and risk management frameworks with Management responsible for day-to-day operation.

In addition the Director penalty regime prescribes personal liability if a company does not meet its pay as you go (PAYG) withholding, goods and services tax (GST) or super guarantee charge (SGC) obligations.<sup>331</sup>

<sup>331</sup> ATO, 2021, Director Penalties, <https://www.ato.gov.au/Business/Your-workers/In-detail/Director-penalty-regime/>



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

*ATO model*

Following is a summary of the control model the ATO has defined as better practice and reviews taxpayers against. Over time the expectations continue to evolve and become more sophisticated.

<b>Board level controls</b>	Formalised tax control framework <b>BLC-1</b>	Roles & responsibilities of board clearly understood <b>BLC-2</b>	The board is appropriately informed <b>BLC-3</b>	Periodic internal control testing <b>BLC-4</b>
	<b>Roles &amp; responsibilities across organisation understood MLC-1</b>	Confidence in capacity and capability <b>MLC-2</b>	Significant transactions are identified <b>MLC-3</b>	Controls in place for data <b>MLC-4</b>
<b>Management level controls</b>	Record – keeping policies <b>MLC-5</b>	Documented control frameworks <b>MLC-6</b>	Procedures to explain significant differences <b>MLC-7</b>	Complete and accurate tax disclosures <b>MLC-8</b>
	Legal and administrative changes <b>MLC-9</b>			

■ ATO's initial focus areas      ■ Additional ATO initial focus area for GST

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## RECENT DEVELOPMENTS AND TRENDS IN THE MARKET

In the evolving COVID era which manifests a general theme of uncertainty and rapidly changing social norms and expectations, governments needing to fund taxpayer support programmes, together with changing operating models, the performance of tax functions will likely receive renewed attention, as with other functions. Similarly, it is anticipated that community attitudes towards taxation will change in response to COVID-19.<sup>332</sup>

This comes as organisations were already expanding their purpose and community stance, measures to build business and operational resilience and adoption of new technologies to acclimatize to growing global focus on trust in tax and tax transparency, the rise of purposive organisations and scrutiny by regulators. From a pure tax governance perspective over recent years there have been initiatives concerning automatic data exchange between countries, reporting requirements such as 'DAC 6' in Europe, guidance on board and management level tax controls such as from the ATO in Australia and public transparency of taxation information.

The global theme placing greater focus on tax governance is increasingly prominent. In December 2019 the Global Reporting Initiative (GRI) released a final standard for tax transparency. The standard addresses tax governance framework disclosure and is a significant development coming from one of the leading standard setters in sustainability reporting. Beyond transparency, groups have been responding in how they govern and manage tax. According to global KPMG benchmarking<sup>333</sup> 59 percent of respondent companies now assign tax responsibility to a board member (or board-level individual/committee), moving sharply away from historical practices of tax being relegated to specialists in a 'dark corner' of the organisation. The ultimate accountability rests with the Board of Directors.

<sup>332</sup> ATO, 2020, Taxation in the evolving post-COVID world, <https://www.ato.gov.au/Media-centre/Speeches/Other/Taxation-in-the-evolving-post-COVID-world/>

<sup>333</sup> Refer to KPMG, Global Tax Department Benchmarking, <https://home.kpmg/xx/en/home/insights/2021/02/global-tax-department-benchmarking.html>

Another notable international trend that can be observed in other jurisdictions in Asia and Europe is the development of specific views on tax governance frameworks directly but also indirectly through data requests.

In Australia, we have seen updates to the Tax Transparency Code (TTC) by the Board of Taxation.<sup>334</sup> Better practice now requires the inclusion of a "basis of preparation statement". Where external/audit assurance has not been obtained, this would also provide information on the internal processes undertaken to collate and verify the information in the TTC.

## FUTURE DIRECTION

Regulators are calling for increased sophistication of organisation's data level controls, and in the level of detail and consistency of framework and process controls. An area that is anticipated to require greater tax governance emphasis in the future is Transfer Pricing (TP). The tax governance enhancement opportunity here is to embed more controls to boost contemporaneous documentation and enhancement of the evidence of the governance process. When arriving at TP positions, the model for ongoing review and testing of the application of TP positions across an organization globally will become even more critical.

We would also expect continued demand for increased tax transparency. For instance at the end of 2021 the EU parliament passed legislation requiring mandatory publication of taxes paid on a country by country basis for groups operating in Europe.

<sup>334</sup> Refer to The Board of Taxation, Corporate Tax Transparency Code and Register, <https://taxboard.gov.au/current-activities/corporate-tax-transparency-code-and-register>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- KPMG, 2020, Everything Matters: Governance & Performance in Tax, <https://assets.kpmg/content/dam/kpmg/au/pdf/2020/everything-matters-governance-performance.pdf>
- ATO, 2018, Tax Risk Management and Governance Review Guide, <https://www.ato.gov.au/Business/Large-business/In-detail/Key-products-and-resources/Tax-risk-management-and-governance-review-guide/>
- ATO, 2021, Director Penalty Regime, <https://www.ato.gov.au/Business/Your-workers/In-detail/Director-penalty-regime/>
- Jeremy Hirschhorn, 2020, Taxation in the Evolving Post-COVID World, <https://www.ato.gov.au/Media-centre/Speeches/Other/Taxation-in-the-evolving-post-COVID-world/>
- KPMG, 2021, Global Tax Department Benchmarking, <https://home.kpmg/xx/en/home/insights/2021/02/global-tax-department-benchmarking.htm>

For further information please contact:



**Phil Beswick**

**Director,  
Deals, Tax & Legal  
pbeswick@kpmg.com.au**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 17. Risk Management

Ultimate responsibility for risk lies with the board. Consequently, risk management is a focus of the board and executive management.

## In this chapter

- Key concepts
- ASX Corporate Governance Principles and Recommendations
- AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines
- Risk and strategy
- Risk governance
- Risk culture
- Risk management policy
- The benefits of enterprise-wide risk management
- Risk appetite
- Crisis management
- Business continuity
- Organisational roles

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Are the relevant roles and accountabilities for governance, risk and compliance properly formalised and documented with appropriate interfaces in place?
2. Do the board share a common view of what the risk appetite is such that this may be consistently applied in decision making?
3. Are assurance activities based on appropriate and robust structures and aligned to the risk profile and appetite of the organisation?
4. Do board members appreciate the potential consequences of serious governance, risk and compliance failures?
5. Is sufficient focus paid to both non-financial and financial risks in discussions?
6. Are there early warning systems in place to alert the board and senior management to emerging risks?
7. Is there integration and alignment of risk management with strategic direction and planning?
8. Is the board aware of how management is using risk information and the risk appetite established by the board to inform decision making?
9. How are missed opportunities, or realised risk events, identified and discussed?
10. Does the board provide oversight on plans for crisis management and business continuity?
11. Is the board establishing the 'tone at the top' to reinforce and promote a risk aware culture?
12. Does the board have a good working knowledge of, and are they updated on changes to, the laws, regulations and Listing Rules relevant to the company?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The company's constitution is never, or rarely, referred to in board discussions/documentation.
- Risk management is not connected to corporate strategy.
- There is a disconnect between risks discussed at a board level (strategic risks), those reported in the annual report and the operational risks on which management focus. Risk management is positioned as a compliance and backroom exercise.
- Risk reporting and risk management plans are not challenged at board level.
- A strong risk culture is not embedded throughout the organisation.
- A risk appetite statement has not been developed and communicated.
- Risk issues are being brought to the attention of the board through media and stakeholders rather than management.
- The board cannot clearly describe its risk management processes.
- The Audit and Risk Committee(s) does not meet or report to the board on a regular basis.
- Focus is unduly placed on financial risks over non-financial risks.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## KEY CONCEPTS

Risk is 'the effect of uncertainty on objectives' (see AS/NZS ISO 31000:2018).

Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities while managing the potential adverse effects.

Enterprise-wide risk management is an organisation-wide approach to the identification, assessment, communication, and management of risk in a cost-effective manner – a holistic approach to managing risk.

Risk governance incorporates the processes necessary to bring reliable risk management information to the attention of the board.

Effective boards consider the robustness of risk governance systems, understand how they work, and to what extent they have the capacity to provide them with assurance.

## ASX CORPORATE GOVERNANCE PRINCIPLES AND RECOMMENDATIONS

Recognising and managing risk is a critical role of the board and management. Failure to do so may adversely impact on security holders and all other stakeholders.

Principle 7 of the ASX Principles recommends that companies should establish a sound risk management framework, to periodically review the effectiveness of that framework.<sup>335</sup> It makes the following recommendations:

- **Recommendation 7.1** – The Board of a listed company should have a committee or committees to oversee risk (this may be a stand-alone committee or combined with the audit committee)
- **Recommendation 7.2** – The board or a committee of the board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound; and

disclose, in relation to each reporting period, whether such a review has taken place

- **Recommendation 7.3** – A listed company should disclose if it has an internal audit function, how the function is structured and what role it performs; or if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes
- **Recommendation 7.4** – A listed company should disclose whether it has any material exposure to environmental or social risks and, if it does, how it manages or intends to manage those risks.

## AS/NZS ISO 31000:2018 RISK MANAGEMENT – PRINCIPLES AND GUIDELINES

AS/NZS ISO 31000:2018 (ISO 31000) sets out the principles for effective risk management and the key building blocks for an organisation to develop and embed a comprehensive risk management framework. The ISO 31000 standard is the better practice standard for managing risks and is commonly applied across private and public sector organisations in Australia. The objective of ISO 31000:2018 is to assist organisations to develop an enterprise-wide risk management strategy to effectively identify and mitigate risks and achieve organisational objectives. In order to achieve this, it adopts a strategic focus and emphasises the role of senior management and the integration of risk management across the organisation. Interestingly, ISO 31000 defines risk as "the effect of uncertainty on objectives" and as such does not focus purely on the down side of risk in the way that traditional risk management historically has. This aligns with the strategic focus of the standard whereby if an organisation is able to proactively manage its risk profile, risk may in fact represent an opportunity (or up side).

<sup>335</sup> ASX Corporate Governance Council, Corporate Governance Principles' and Recommendations, 4<sup>th</sup> edition, 2019, Principle 7.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

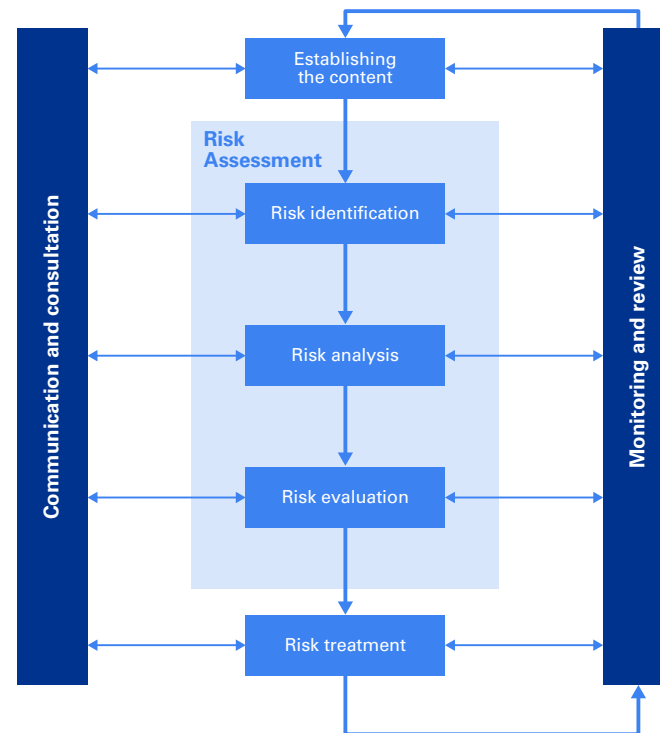
## GLOSSARY

## APPENDICES

## CONTACT US

The following diagram summarises the approach to risk management described in ISO 31000.

## Risk Management Framework



ISO 31000:2018

Whilst not mandatory, the principles and guidelines outlined in ISO 31000 are considered to be best practice from a high level to facilitate proactive risk management. All directors should understand these basic principles and, more importantly, how to ensure that they are being implemented effectively by management.

## RISK AND STRATEGY

Risk and strategy are essentially two sides of the one coin with the development of strategy subject to the risks that threaten its achievement. Despite the benefits of integrating these two key processes, many organisations struggle to do this and will typically identify the risks to their strategy after the strategy has been developed, rather than using an understanding of the risk environment to inform the strategy and then identifying risks to the strategy thereafter.

Experience suggests that organisations that make risk management an integral part of their strategy are more resilient in dealing with adverse events and uncertainty. Poor management of material business risks has been widely recognised as one of the key contributors to corporate failures during the global financial crisis (GFC). The latter provided useful lessons that listed entities can draw on to improve risk management and risk disclosures to stakeholders.

## RISK GOVERNANCE

Risk governance incorporates the processes and supporting systems necessary to bring reliable risk management information to the attention of the board. It encompasses the overarching risk management structure to facilitate the management of risks across an organisation. It includes the formal policies and procedures in place for key risk areas, disciplines and reporting. The increasing availability and options for integrated Governance, Risk and Compliance (GRC) systems has seen Australia begin to embrace the power of risk management technology at a faster pace which is providing an effective and efficient solution for risk governance.

Many audit committees today have oversight responsibility for the company's enterprise risk management process, as well as other major risks facing the company – including financial, operational, cyber security, IT, legal and regulatory compliance. Other organisations establish a separate risk committee to focus specifically on risk identification and management oversight issues (this is discussed further in [Chapter 11 Board Committees](#)).



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

RISK CULTURE

Establishing organisational culture is the responsibility of the board, and this includes developing, communicating and 'living' the organisation's risk management culture.

Culture can be difficult to define, however it is often thought of as 'the way we do things around here'. Whilst an organisation might have a best practice set of policies and processes in place to manage key risk areas of the business, they will be ineffective if they are not adhered to by staff.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Increasingly, regulators such as ASIC are interested in corporate culture and the impact that it has on business conduct and, therefore, financial consumer trust and confidence.<sup>336</sup> Whilst culture cannot be regulated, conduct can. In the context of risk, the conduct of employees is significant, as employee behaviours can quickly impact on financial performance and the business' reputation.

Risk management implementation not only requires significant effort, but also the creation of a risk management culture that is committed to managing risk within the boundaries defined by the board. The board must set the 'tone at the top', whilst management sets the 'mood in the middle'. Ensuring these behaviours are consistent requires a proactive approach. Key actions to establish a common risk culture include:

- communicating the board's vision, strategy, policy, responsibilities and reporting lines to all employees and stakeholders
- developing a clear risk appetite statement that communicates the end vision and benefits, and the acceptable thresholds within which decisions can be made by the business
- establishing a control environment that assigns responsibilities for risk management, and that has an effective and consistent measurement and accountability framework
- implementing training programs for risk management, that includes identifying and training 'risk champions', and developing a knowledge-sharing system
- communicating success stories and identifying quick wins.

## RISK MANAGEMENT POLICY

A listed entity established in Australia is required under the Corporations Act to include a discussion in the operating and financial review, contained in its directors' report of the main internal and external risk sources (including environmental and sustainability risks) that could adversely affect the entity's prospects for future financial years.<sup>337</sup>

<sup>336</sup> Refer to speeches by Greg Medcalf, John Price of ASIC regarding culture and ethics, available at [www.asic.gov.au/about-asic/media-centre/speeches](http://www.asic.gov.au/about-asic/media-centre/speeches)

<sup>337</sup> Corporations Act 2001, s 299A(1) and ASIC Regulatory Guide 247 (RG247) – Effective disclosure in an operating and financial review.

If a significant risk event occurs, the company may also have to disclose the occurrence and its impact pursuant to its continuous disclosure obligations under the Listing Rules.<sup>338</sup>

Risk management policies should reflect the company's risk profile and should clearly describe all elements of the risk management and internal audit function.<sup>339</sup> The policy should be an instrument to communicate the company's risk-management approach and should include, at a minimum:

- 'a definition of 'risk' and 'risk management' relative to the organisation
- goals and strategies for risk management
- the organisation's risk appetite/tolerance
- how risk management targets will be measured
- accountabilities for risk management.

## THE BENEFITS OF ENTERPRISE-WIDE RISK MANAGEMENT

The elements that comprise an ERM framework are defined in the graphic below. Potential benefits of having an integrated ERM framework include:

- better informed decisions
- greater management consensus
- increased management accountability
- greater ability to meet strategic goals
- reduced earnings volatility
- better allocation of resources, which may lead to increased profitability
- ability to use risk as a competitive tool
- more accurate risk adjusted pricing
- better contingency planning
- improved crisis response.

<sup>338</sup> See Chapter 7 – Accountability to Shareholders.

<sup>339</sup> Ibid.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT








18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Elements comprising an ERM framework

 <p><b>Risk Strategy &amp; Appetite</b></p>	<p>Alignment/Conscious decision to use risk management to enable the achievement of business plans, goals and strategic objectives. It includes a risk appetite statement supported by risk tolerances, limits and associated breach protocols to control risk levels throughout the organisation.</p>
 <p><b>Risk Governance</b></p>	<p>A structure through which an organisation directs, manages and reports its risk management activities. It encompasses clearly defined roles and responsibilities, decision rights, the risk governance operating model, and reporting lines.</p>
 <p><b>Risk Culture</b></p>	<p>Values and behaviors present throughout an organisation that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits. A strong risk culture helps to encourage strategic decisions that are in the long-term best interest of the organisation, its shareholders and employees.</p>
 <p><b>Risk Assessment &amp; Measurement</b></p>	<p>The activities in place that allow an organisation to identify, assess and quantify known and emerging risks. The risk assessment and measurement processes allow organisations to consider the extent to which potential events may have an impact on achievement of objectives. It encompasses qualitative and quantitative approaches, processes, tools and systems that organisations develop and implement to identify, assess, and measure risks.</p>
 <p><b>Risk Management &amp; Monitoring</b></p>	<p>Management's response to manage, mitigate, or accept risk. Risk management efforts create value through the use of risk and control information to improve business performance across the enterprise. Systematically monitoring the identified risks and management activities against established metrics permits timely proactive response where warranted. Management designs activities to assure stakeholders that risk management activities and controls are effective in managing risks that could have an impact on achievement of objectives (i.e. Integrated Assurance).</p>
 <p><b>Risk Reporting &amp; Insights</b></p>	<p>Reporting of risk and related information (e.g. mitigation activities) provide genuine insight into the strengths and weaknesses of risk management activity. Disclosure of risk management information to key stakeholders also supports the decision making processes. Effective risk reporting enhances the transparency of risks that could have an impact on achievement of objectives in a timely manner.</p>
 <p><b>Data &amp; Technology</b></p>	<p>Management of risk data that can be translated into meaningful risk information for stakeholders. It includes the development and deployment of risk management tools, software, databases, technology architecture, and systems that support risk management activities.</p>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## RISK APPETITE

Risk appetite is the amount of risk, at a broad level, that an organisation is willing to accept in pursuit of value. It will reflect the risk management philosophy and the organisation's capacity to take on risk. It is based on strategic objectives and stakeholder demands. The notion of risk appetite can add discipline and focus when responding to an uncertain and constantly shifting risk environment. A risk appetite statement can provide a decision-making framework for the strategic and operational handling of risk. As the appetite may vary across different parts of the business and different risk types, it is important that the appetite for each area and risk type is specified. For example the risk appetite for health, safety and wellbeing related risk is most commonly low however the appetite for innovation is high (so as to allow for a safe-to-fail and innovative culture). This then drives the resourcing into the control frameworks for each area accordingly.

Risk appetite, if embedded and used well, can support resource reallocation and cost reduction where needed. Setting Key Risk Indicators aligned to the risk appetite enables proactive risk management through early warning signals being monitored and reported.

## CRISIS MANAGEMENT

Companies should have crisis management plans in place. Such plans should include reference to the board's role during a crisis and should be considered as part of a board's risk management responsibility. Boards should insist that crisis management plans contain a robust communications element.

Without effective communication, companies may inflict additional damage on themselves including:

- losing control of the communications process
- allowing facts to be displaced by rumour and speculation
- reputational harm
- putting employee morale and trust at risk
- alienating shareholders, customers, suppliers and other stakeholders.

Contemporary risk management frameworks, including crisis management plans, should incorporate the mitigation of social media as a key function. Boards and senior management need to be prepared to manage and respond to social media.

## BUSINESS CONTINUITY

Planning for a disaster is considered essential practice as all businesses face the risk of a serious event occurring that can damage the organisation's ability to continue operating.

Business continuity management focuses on an organisation's responsiveness to an organisational or external crisis that puts its ongoing operation at risk. The aim is to foster and develop preparedness for all types of events that may significantly affect an organisation and enable a company to respond and resume normal business operations after they occur.

The ultimate goal of business continuity is to develop a response to events to enable the organisation to maintain its most critical operations, and survive all but the most extreme forms of operational disruption. The key elements of effective business continuity planning are flexibility and simplicity.

A well-prepared organisation will be able to make the right decisions at the right time, based not on rigid instructions contained in a detailed manual, but on tried and tested alternative ways of working.

These arrangements must:

- be integrated into everyday business
- look inside as well as outside the organisation
- be understood by employees and stakeholders
- be regularly and effectively tested to ensure they remain relevant.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## ORGANISATIONAL ROLES

*The Board*

The board is ultimately responsible for risk management. The board:

- approves the organisation's risk appetite as recommended by the audit and risk committee
- must regularly review and approve the organisation's risk management policy, and maintain oversight of the policy
- approves the risk management framework for the organisation
- receives regular updates about key risks, changes in risks and emerging risks from the audit and risk committee
- establishes board sub-committees (audit and risk committee) and evaluates committee performance.

*Chief Risk Officer*

It is common now for organisations to have appointed an organisation chief risk officer (CRO) or risk manager. The existence of a CRO centralises risk management, but also brings several other benefits. One is to understand the relationship between risks within separate business units that might not have been apparent before. This is becoming more important given the increasing diversity and complexity of global businesses in which a risk that appears acceptable to the manager of an individual business unit may be inappropriate from the point of view of the enterprise as a whole. Using a comprehensive risk matrix, CROs can identify such linkages across the business and manage them more effectively.

Another important way CROs can benefit the business is by enabling the organisation to make decisions based on a better appreciation of the relationship between risk and reward. CROs are most effective when they provide the board with a clear vision of where enterprise risks lie, help define a policy for distributing and offsetting those risks, and work to communicate that vision so that individual managers understand and support it.

The CRO provides a framework for risk management while decisions on what is acceptable risk fall to managers and employees in the frontline of the business.

*Risk Management Committee*

The ASX Principles recommend that the board of a listed entity has a risk committee in place to oversee risk and the risk management committee should review the entity's risk management framework at least annually (with disclosures as to whether such a review has taken place).<sup>340</sup> Many companies have established risk management committees, or have a combined audit and risk committee. This committee acts as an efficient mechanism for focusing the company on appropriate risk oversight, risk management and internal control. A risk committee can be an efficient and effective mechanism to bring the transparency, focus and individual judgment needed to oversee a company's risk management framework. For companies that do not possess a risk management committee (e.g. in the case of smaller boards where the same efficiencies may not necessarily be derived from a formal committee structure), board processes should raise the issues that would otherwise be considered by a risk management committee.

Generally the risk management committee will have a key role in the governance of risk and compliance, including:

- oversight of the risk management framework and its implementation
- considering and challenging risk reporting
- oversight of the compliance framework
- considering and directing management's response to key risk issues.

The commentary to recommendation 7.1 of the ASX Principles lists those matters for which the risk committee should be responsible for making recommendations to the board.<sup>341</sup>

<sup>340</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4<sup>th</sup> edition, 2019, Recommendations 7.1 and 7.2.

<sup>341</sup> Refer also Chapter 11 – Board Committees

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

- **GOVERNANCE LEADERSHIP**

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- ASIC, 2016, Good corporate culture, values and ethics, <http://asic.gov.au/about-asic/media-centre/speeches/good-corporate-culture-values-and-ethics/>
- ISO 31000:2018, Risk management – Guidelines
- KPMG, 2019, Risk Reimagined, <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/risk-reimagined-seize-opportunity-in-risk.pdf>

# Governance Oversight

---

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 18. Environmental, Social and Governance (ESG)

The rapidly expanding oversight responsibilities of directors over the impact the organisation has on the environment and society and how governance structures are established to maintain trust.

## In this chapter

- Key concepts
- Drivers
- Strategy
- Identifying material risks
- Reporting
- Governance and culture
- KPIs and targets
- Role of the board



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. What are the company's material environmental and social opportunities and risks? This will include consideration of impacts of areas such as climate, waste, biodiversity, water, health and safety of employees and the community, community engagement and investment, human rights and employee diversity and inclusion, and the overall governance of each of these areas.
2. Does the board have visibility of the company's strategy in relation to these material environmental and social opportunities and risks?
3. Is there a governance framework in place for managing social and environmental issues? Does responsibility lie with a 'C class' executive?
4. How does the company meet its obligations to investors to disclose on material environmental and social sustainability risks?
5. Does the company report publicly on environmental and social strategy, performance, governance and risks? Has the board ever read the report?
6. Does senior management report to the board on environmental and social issues? Are environmental and social targets aligned to broader business objectives?
7. If environmental and social data is reported externally, are these areas managed internally or is the external reporting just for show? Could the company be accused of 'green washing' in its external disclosures?
8. Is the company exposed to material environmental and social risks in its supply chain? How are risks in the supply chain identified and managed?
9. Which committee is responsible for oversight of social and environmental issues and their reporting? Is the board aware of its role and responsibilities in relation to these issues? Does it have sufficient knowledge to be able to challenge senior management?
10. Is the board aware of the true value of the company's operations – that is – when considering economic, social and environmental externalities, does the company make a positive or negative contribution? Does the organisational strategy consider these impacts?
11. Has the board performed a self assessment so as to determine whether governance practices are aligned with what stakeholders may expect?
12. How is the board's composition needing to adapt to be better positioned to respond to ESG?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- An absence of environmental or social considerations in the overall strategic business objectives.
- Environmental and social issues and costs are rarely reported, discussed or considered at board level, or publicly disclosed as part of the company reporting process.
- No executive is accountable for environmental and social issues.
- Social or environmental sensitivities impact corporate operations or share price.
- Social or environmental incidents occur with little warning.
- The organisation struggles to answer questions from investors and analysts which extend beyond corporate financial performance.
- ESG is mentioned to please external stakeholders but there is no structured plan on how to achieve objectives and implement the changes needed.
- The sustainability team spend most of their effort collecting data, but little action is taken.
- ESG data and information is not reliable, or not regularly collated or available.
- The board do not review or sign off any elements of the sustainability/ESG strategy or any performance reporting (internal or external).
- The business is working in an issues-rich space that has attracted the attention of activists.
- There is a lack of business knowledge of who the online advocates, activists and regular commentators about the business and its interests are, what their arguments are, and how influential and connected they are.
- There is an awareness that dedicated influencers are reaching influential actors, like politicians, regulators, shareholders and staff with criticisms of the business.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The corporate sustainability debate has evolved significantly in the last 2 years. No longer is corporate sustainability limited to the pressures on corporations to reduce their negative impact on the environment and communities in which they operate. The prevalence of corporate sustainability as a mainstream issue is evidenced by new regulatory requirements, shareholder activism, the continued emergence of integrated reporting, and the active involvement of the investment and analyst communities. The role of directors in this space is also evolving; it can no longer be ignored.

Growing stakeholder awareness, particularly in the investment community, is driving organisations to consider and address the ESG issues within their business. These non-financial risks are now having significant financial implications and, therefore, disclosure expectations with respect to the management and performance of material sustainability issues is also on the rise.

It has become more common for independent bodies (for example, the Australian Council of Superannuation Investors (ACSI)) to publish sustainability indices and reports that discuss commonly used sustainability frameworks aimed at improving the quality of sustainability related information provided by companies. These reports provide a number of benchmarks against which investors can comparatively assess company performance and are driving an approach to standardise sustainability disclosures. The number of ESG reporting frameworks has grown exponentially in the last 12 to 18 months, and often now the challenge faced by companies is not whether to report on ESG issues and data, but which reporting framework to report against. There is also an increasing amount of regulatory onus on companies and their directors to take responsibility for sustainability-related risks, and the potential impact on company performance. For example, the ASX Principles now recognise that a company's operations impact on a wide range of stakeholders and that an entity should be aware of the increasing calls globally for the business community to address the effects of environmental and social responsibility.

Recommendation 7.4 indicates that a listed entity should disclose whether it has had any "material exposure" to economic, environment and social sustainability risks, and to discuss how it intends to manage those risks. The definition of "material exposure" recognises that ESG risks, are inherently linked with economic and/or financial risk.

## KEY CONCEPTS

Institutional investors and analysts are today commonly applying ESG factors in their assessments of the long term performance of companies. Integrating ESG into the investment decision is to approach investing without sacrificing risk-adjusted return and creating value while also improving the long term return.

According to the *Global Sustainable Investment Alliance 2020 Report* (produced every other year), sustainable investing assets in the five major markets (Australia & NZ, Canada, Europe, United States, Japan), stood at \$35.3 trillion at the start of 2020, a 15 percent increase in 2 years and representing a 57 percent increase over the last 4 years. Responsible investment has continued to increase substantially since that report was published and now commands a sizable share of professionally managed assets in each region constituting 36 percent globally.<sup>342</sup>

The challenge for companies is the extent to which they 'internalise externalities' in their day-to-day and strategic decision making.

## DRIVERS

The key drivers of the enhanced focus on ESG are the increasing power of stakeholders, changing market dynamics and the emergence of regulations and standards. These are collectively referred to as the 'drivers of internalisation', as any one of these factors can result in an external impact on the organisation by changing to one which directly affects the operation and profitability of the company. For example, "green buildings" were once seen as niche, but have now become mainstream, due to market demand for these type of buildings.

<sup>342</sup> Global Sustainable Investment Review 2020, GSIA, <http://www.gsi-alliance.org/wp-content/uploads/2021/08/GSIR-20201.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

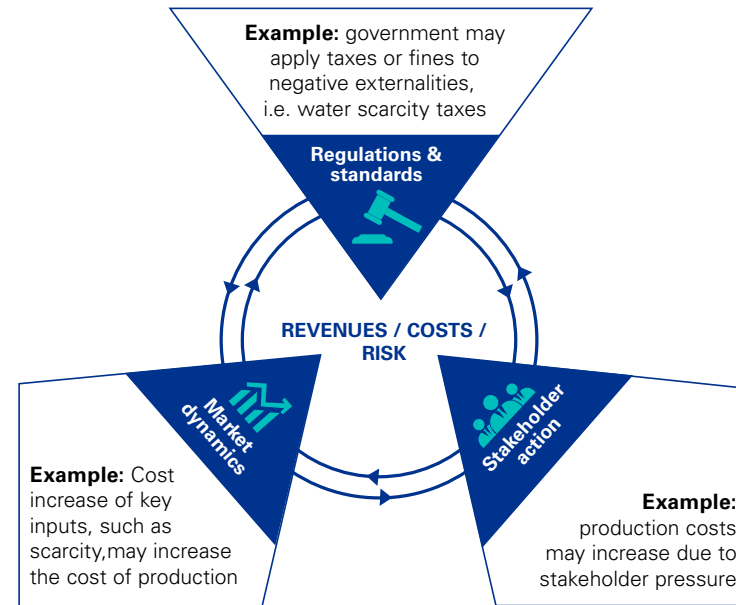
18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Drivers of Internalisation



The pressure to transparently demonstrate how ESG assessment criteria are utilised across governance, processes and reporting is largely due to stakeholder demands to understand more about the sustainability of a company and its key decisions. Investors and analysts are the stakeholders with the most direct impact on companies, but the indirect impacts are forever strengthening. The power of stakeholders has grown exponentially with the rise of social media and the knowledge is shared globally almost instantly.

Much of the value of companies today is inherent in intangible assets, such as brand names and reputation, rather than traditional tangible assets. These intangible assets are closely linked to ESG factors and their value can be readily destroyed if these factors are not managed.

There are also a growing number of regulatory requirements driving the increased focus on ESG issues, such as the Financial Services Council (Standard 20), the ASX Principles and the signatory requirements under the United Nations (UN) Principles for Responsible Investment (PRI). Regulatory requirements in other jurisdictions are also increasingly driving shareholder expectation of reporting in Australia.

Much of the current focus for investors and regulatory bodies is on responding to climate change.

The Task Force on Climate-related Financial Disclosures (TCFD) has become the cornerstone framework for addressing and reporting organisations' exposure to climate-related risks and opportunities. The move by networks and bodies such as the UN PRI and the UK Government to mandate TCFD-based reporting for signatories and companies in the UK, respectively, supports the global shift towards a more prudent and strategic integration of sustainable financial practice across the industry more broadly. The recommendations of the TCFD provide a framework for organisations to report consistent, comparable and voluntary disclosure to assist financial markets understand material climate-related risks and opportunities.<sup>343</sup> There is increasing legal precedent for companies to be obliged to report transparently on the impacts of climate change on the business. The Centre for Policy Development, in partnership with the Future Business Council, commissioned a legal opinion by Noel Hutley SC and Sebastian Hartford-Davis on instruction from Minter Ellison Lawyers in 2016, which indicates how Australian company law requires directors to consider and respond to climate change risks relating to their business.

343 Task Force on Climate-Related Financial Disclosures (TCFD), 2017, Recommendations of the Task Force on Climate-related Financial Disclosures, <https://www.fsb-tcfd.org/publications/final-recommendations-report/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

This interpretation falls under a director's obligation to act in the best interests of the organisation and ensure that all material risks are properly investigated and mitigated.<sup>344</sup>

Australian regulators ASIC and APRA, the AASB and the RBA are in alignment on the material and financial impact of climate change, and the recommended risk management integration and disclosure of climate-related risks and opportunities. These recommendations have primarily been made with reference to the fulfilment of directors' fiduciary duties under Section 180 of the Corporations Act (2001).

In March 2019 APRA announced its intention to increase scrutiny of how the financial sector is managing the financial risks related to climate change and expects to see continued adoption of the TCFD recommendations.<sup>345</sup> ASIC released RG 247, a guidance document citing climate change as one example of a systemic risk that could have a material financial impact, and encourages companies with material exposure to climate risk to report in-line with the TCFD recommendations.

The AASB also released Practice Statement 2, recommending that where companies believe investors might view climate risk as a material issue for the company, climate-specific impacts should be considered within the financial report (e.g. whether this would impact any impairment evaluations).

ASIC has taken action where it does not believe companies have made appropriate external disclosures about climate risk. In 2021, ASIC contacted several companies with a "please explain" letter, targeting companies that did not discuss climate risk as a key business risk in their financial report, when in ASIC's view climate risk was likely to have a material impact on those businesses.

Globally, other jurisdictions are taking steps to make TCFD and climate-risk reporting mandatory.

<sup>344</sup> Centre for Policy Development (CPD), 2016, Directors' duties and climate risk, <http://cpd.org.au/2016/10/directorsduties>

<sup>345</sup> APRA, 2019, APRA to step up scrutiny of climate risks after releasing survey results, <https://www.apra.gov.au/media-centre/media-releases/apra-step-scrutiny-climate-risks-after-releasing-survey-results>

The New Zealand government has made climate-risk related disclosures reporting mandatory for listed issuers, banks, general insurers, asset owners and asset managers from 2023, with the TCFD framework being used as a foundation for compliance.<sup>346</sup>

The United Kingdom has also enforced mandatory TCFD-aligned reporting for large companies from April 2022.

Other, non-mandatory reporting frameworks, such as the Global Reporting Initiative (GRI) and the Sustainability Accounting Standards Board (SASB) also exist and are increasingly being adopted to report on diversity, human rights and environmental policies. There have been a large number of other reporting frameworks that have been developed and published over the last few years, but in particular over the last 12 to 18 months. There have been moves made towards convergence of these different frameworks, most notably in the formation of the International Sustainability Standards Board (ISSB) which aims to develop a single set of sustainability reporting standards that can be applied globally, similar to the International Accounting Standards Board (IASB). In addition, the Paris Agreement made at the United Nations Framework Convention on Climate Change (UN-FCCC) Conference of Parties (COP-21) in December 2015, saw the world commit to limit global warming to well below 2°C above pre-industrial levels and to pursue efforts to keep it to 1.5°C. The Paris Agreement sends a clear signal to the private sector: a global political intention to shift to a low carbon, and ultimately zero carbon, future.

Since then, subsequent UN-FCCC Conferences of Parties (COP) were held with the latest being COP26 in Glasgow. At these meetings, world governments have focused on the development and implementation of the practical and technical aspects necessary to achieve the goals that were agreed under the Paris Agreement.

The latest COP26 was held against a backdrop of increasing recognition of the impacts of climate change and the need to implement real action to cut greenhouse gas (GHG) emissions, but with some governments still refusing to commit to clear actions or activities to meet the broad targets set at the conference.

<sup>346</sup> Refer to <https://environment.govt.nz/what-government-is-doing/areas-of-work/climate-change/mandatory-climate-related-financial-disclosures/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Key takeaways from COP26 included the development of the new ISSB and the release of the General Requirements and Climate Exposure Draft; world governments agreeing on the final day to 'reduce coal' fossil fuel production, with specific actions outlined by some governments to achieve this; confirmation that the Paris ambition to decrease to 1.5°C is still alive (government and private sector commitments tallied up to approximately 1.8°C); and a pledge to reduce methane emissions by 30 percent by 2030 (notably this was not agreed by Australia). Separate to climate change, there was also a pledge to end deforestation by 2030, with 110 countries committed including Brazil and Indonesia (where a significant amount of the deforestation takes place).

Given the wide-spread adoption and success of the TCFD to encourage transparent reporting on climate risk, this has led to the creation of the Task Force on Nature-related Financial Disclosures (TNFD), which aims to apply a similar framework for addressing and reporting organization exposure to biodiversity risk. It is expected that reporting against the TNFD will increase in coming years.



### Case Study – Volvo Group: The True Value of Volvo's electric buses

Volvo Group wanted to show leadership in the transport sector and the global sustainable development movement by quantifying the environmental and social value created by their electric buses. To do this, they calculated (using KPMG's True Value methodology), a true Total Cost of Ownership (TrueTCO), which took into account not only the financial costs and returns associated with building and operating electric buses, but also the environmental and social costs and returns.

For example, cost of ownership calculations traditionally only focus on direct acquisition and operating costs, such as vehicle leases, fuel, driver salaries, garage and maintenance costs. However, there are other, indirect/non-financial costs (and benefits) that are associated with electric vehicles, including:

- negative effects of noise and pollution on public health
- environmental impacts of manufacturing the fuel
- contributions to climate change
- time that passengers spend travelling.

Using proxies and measures such as greenhouse gas emissions comparisons (including carbon prices/taxes), noise and air pollution levels associated with electric versus diesel engines, fuel/energy consumption data and a value of time per hour per passenger (based on Government economic estimates), a true cost of ownership was calculated. The results indicated that the TrueTCO of an electric bus is lower than that of a diesel bus, by a significant amount.

The findings transformed the business case for electric buses. Using traditional accounting techniques, electric buses looked like a high cost, low return investment. However, when incorporating social and environmental costs and benefits, it was determined that Sweden could save up to approximately US\$225 million per year, of which US\$45 million could be savings in public healthcare costs. In addition, passengers could save 14 million hours of travel time per year and Sweden's carbon emissions could be reduced by 84,000 tons per year (approximately equivalent to the annual per capita emission of 15,000 Swedish citizens).

The benefits for Volvo? The analysis has helped Volvo to position itself as a leader in sustainability and the development of sustainable cities, enhancing its brand reputation and an opportunity to leverage this with Government and key stakeholders, thereby managing multiple risks and creating new opportunities.

*"The results of this analysis have the potential to change perceptions, influence decision makers and ultimately to transform urban environments worldwide."*

- Niklas Gustavsson, Chief Sustainability Officer, Volvo Group

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## STRATEGY

A comprehensive ESG strategic framework is part of the overall company strategic framework. Decisions as to the extent of the internalisation of externalities across the value chain should be taken at senior levels within an organisation, applying a risk management approach to minimising potential future costs and promoting the long-term sustainability of the organisation. At face value, ESG risks are largely non-financial, however, financial markets are increasingly costing in the value of ESG risks in investment decisions. Further, social and environmental issues inevitably result in economic impacts; it's just a matter of timing.

The key to understanding non-financial risks is to understand the integration and impact of these risks on the economic success or failure of an organisation, including:

- regulatory risk due to complex changes to the regulatory landscape
- reputational risk and damage to corporate reputation and value through adverse publicity
- competitive risk from fast changing market dynamics, uncertainty of supply, and price volatility of key inputs
- exposure to legal action through, for example, non-disclosure of environmental, social and governance information.

Oversight of the effective management of non-financial risks and opportunities is the responsibility of the board, and an increasing number of stock exchanges and Governments are seeking more public disclosure on ESG governance in recognition of this responsibility. A board should consider the relationship between non-financial and financial risks, and whether these are adequately identified and addressed by the company.

Effective oversight of an ESG framework also requires consideration and challenge on the extent of ESG integration into corporate strategic planning, both in the short and long terms. The board should ensure the ESG issues identified as most material to the organisation are connected to existing strategy and risk management processes.

## IDENTIFYING MATERIAL RISKS

Effective ESG risk management requires a robust mechanism for the identification and assessment of issues that are material to the organisation. Materiality with respect to ESG risks does, however, involve a more qualitative assessment of issues than is traditionally applied in financial reporting. The ASX Principles define material exposure as “a real possibility that the risk in question could substantively impact the listed entity’s ability to create or preserve value for security holders over the short, medium or long term.”<sup>347</sup>

Guidelines such as the Association of British Insurers on Responsible Investment in the UK recommend a regular review of ESG risks by the board of directors.

Directors should enquire of management whether a robust materiality assessment process and ESG risk assessment are in place, and how key non-financial and financial risks interact across their business. This includes understanding where the key non-financial exposures are across the organisations’ value chain and the potential subsequent cost/impact, such as costs arising from the impact of extreme weather events and reputational damage associated with human rights issues/claims. This assessment may also identify economic opportunities across the environmental and social impacts observed.

Identifying and understanding the material ESG issues, and the risks and opportunities they represent, is a critical part of promoting the long-term sustainability of the organisation. The board should enquire of management whether there is strong alignment between the materiality assessment process for ESG issues and the organisation’s existing risk management and strategy development processes.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

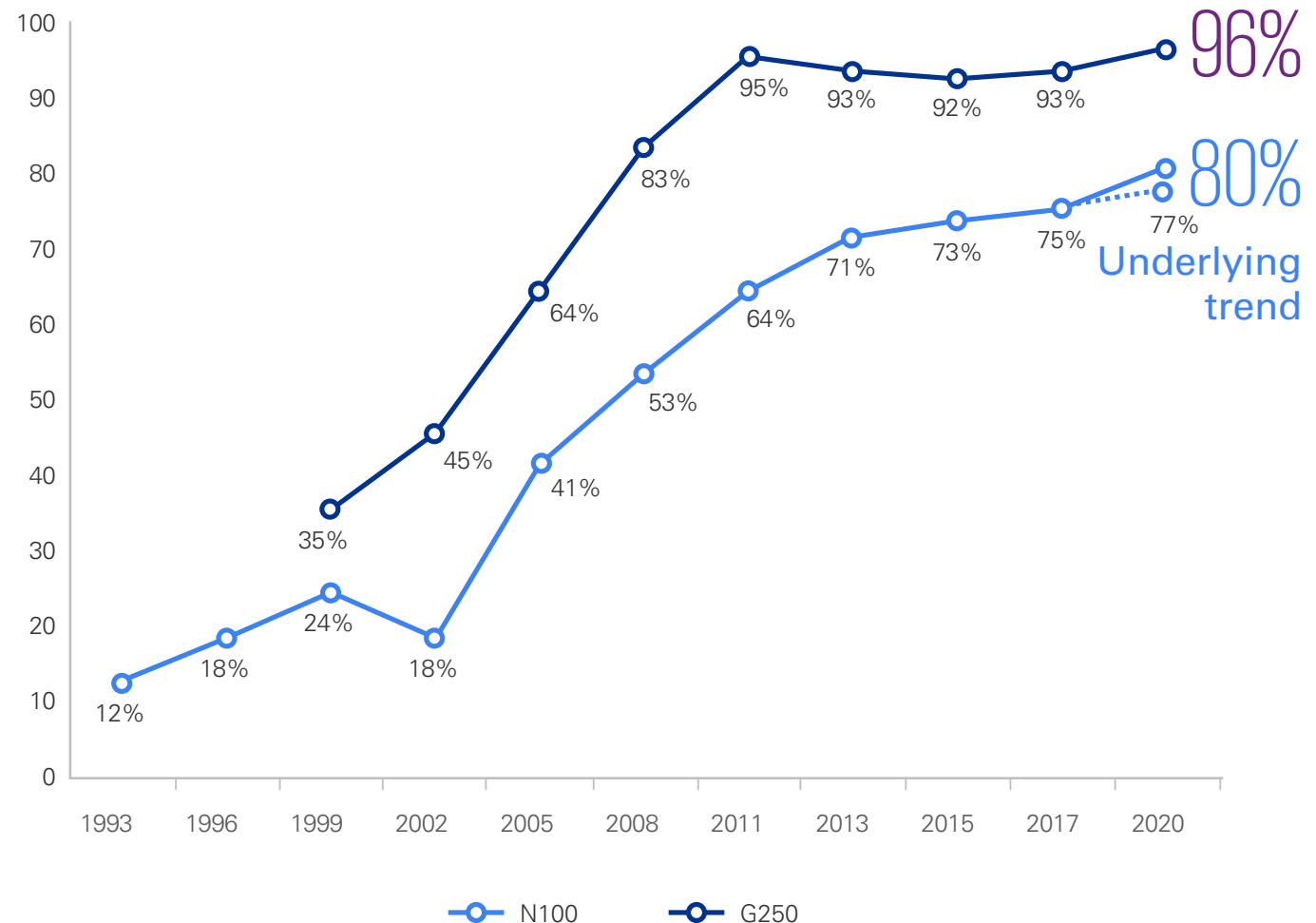
CONTACT US

REPORTING

Corporate Responsibility (CR) Reporting has now become the norm, driven by both regulation and stakeholder expectations. The below growth in CR reporting since 1993 shows that now over 90 percent

of the largest 250 global companies (G250) have been reporting on CR performance since 2011. In line with the global reporting trends, the CR reporting is now mainstream in Australia, with 98 of the ASX100 now reporting on sustainability as of 2020.

Growth in global sustainability reporting rates since 1993: N100 and G250





## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Since our first corporate reporting study was released in 1993, KPMG has continued to track the adoption of CR Reporting amongst major companies around the world. In 2020, the rate of CR reporting for G250 and N100 companies have increased to around 96 percent and 80 percent respectively.

The GRI framework is the most commonly used, with 67 percent of N100 reports and 73 percent of G250 reports applying it. Meanwhile, 19 percent of N100 and 17 percent of G250 companies are using stock exchange guidelines.

## GOVERNANCE AND CULTURE

Effective management of non-financial risks and opportunities requires a robust governance structure. The ESG framework should detail the governance arrangements in place to oversee the effective identification and management of ESG risks across the business, setting the tone at the top for the rest of the organisation.

While the board is ultimately responsible for the oversight of non-financial risk, this is more commonly undertaken by an executive or committee of the board responsible for the oversight of ESG matters. Regardless of the approach, clear reporting lines and responsibilities should be established and communicated. Some companies are choosing to set-up a specialised committee to oversee non-financial matters.<sup>348</sup>

It is the responsibility of directors to ensure they receive adequate and appropriate training and continuous development in order to ensure they are fully equipped to carry out their roles, make informed decisions and adequately challenge management in the area of ESG risk management. The ASX Principles recommend that a listed entity has a program in place to provide appropriate training and professional development opportunities for directors so they are able to maintain the skills and knowledge to perform effectively in their roles.<sup>349</sup> Having at least one board member with a demonstrated sustainability background or experience is now becoming one of the criteria that analysts are using in scoring company ESG performance for sustainability indices such as Bloomberg ESG.

348 See Chapter 3.3 Board Committees

349 ASX Corporate Governance Principles, 4<sup>th</sup> edition, 2019, recommendation 2.6

Boards are increasingly expected to promote and support a corporate culture which embeds the consideration of environmental and social issues into decision-making and performance throughout the organisation. The ESG governance framework should include clear expectations of how risk and opportunities are managed and who within the organisation is accountable. Raising the visibility and importance of the issues through specific KPIs for senior management that cascade down the organisation, is one way the board can set the tone and influence corporate culture.

## KPIs AND TARGETS

An effective way for directors to assess progress against identified material risks is to ensure management implement targets and KPIs associated with each material indicator. It is the responsibility of directors to ensure that management has implemented systems, procedures and controls to gather reliable and timely information about key environmental and social trends and issues.

Directors should understand and agree on management's selection of key performance indicators regarding environmental and social performance, and ensure periodic reviews take place of company and individual performance against these indicators. The board and management should engage in discussions over the types of performance indicators that need to be set, measured, rewarded and communicated. The indicators selected for assessment should be based on appropriate data collection and reporting systems, and, most importantly, should be relevant to the company's material ESG issues identified through its materiality assessment.

It is currently popular for companies to publish ESG targets, particularly in relation to climate change (e.g. setting targets to achieve net zero by 2050). But care should also be taken to ensure these targets are achievable and supported by real action. In 2021, a shareholder activist group took Santos to court to argue that it did not have a sufficiently clear and credible plan to support its plans to reach net zero emissions by 2040.<sup>350</sup>

350 Refer to The Guardian, 2021, Santos sued for 'clean fuel' claims and net zero by 2040 target despite plans for fossil fuel expansion, <https://www.theguardian.com/australia-news/2021/aug/26/santos-sued-for-clean-fuel-claims-and-net-zero-by-2040-target-despite-plans-for-fossil-fuel-expansion>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

There has been no outcome to the court case yet, but investors and analysts are becoming increasingly savvy and companies should ensure that their targets and external disclosures are achievable and realistic to avoid claims of greenwashing.

## ROLE OF THE BOARD

Ultimately the board is the G in ESG and plays a key role in leading a company's commitment to ESG issues and their consideration and integration across the organisation. This can be done by:

- recognising responsibility for ESG issues at board level and ensuring that ESG governance is appropriately delegated across the organisation
- providing clear strategic direction on ESG issues for the short and long term in order to allow for the development of a more detailed ESG framework
- monitoring the assessment and regular review of material issues
- oversight and challenge of management's financial and non-financial assessment of material risks
- challenging the performance of the company in relation to ESG targets and related KPIs
- establishing a corporate culture that supports the effective management of ESG related issues, in recognition of their importance to the long-term sustainability of the organisation
- oversight of the depth and breadth of ESG-related reporting and the alignment with recognised frameworks and initiatives
- requiring senior management approval and external assurance over ESG reporting in order to ensure confidence in the information and the business systems and processes from which it is sourced
- undertaking training to keep up to date with the evolving issue of ESG and to be able to lead and challenge management.

## Useful references

- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.
- KPMG, KPMG Sustainability Services <https://home.kpmg/au/en/home/services/advisory/risk-consulting/climate-change-sustainability-services/sustainability.html> KPMG, KPMG Survey of Corporate Responsibility Reporting 2020 <https://home.kpmg/xx/en/home/insights/2020/11/the-time-has-come-survey-of-sustainability-reporting.html>
- United Nations, Sustainable Development Goals, <https://sdgs.un.org/goals>
- Global Reporting Initiative, <https://www.globalreporting.org/standards/>

## For further information please contact:

**Tanya Kerkvliet**

Director, ESG  
tkerkvliet@kpmg.com.au

**Adrian King**

Partner in Charge,  
Climate Change & Sustainability  
Services, KPMG Australia

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 19. Private Equity

Private equity deals are now being transacted with heightened corporate governance expectations. Directors operating in this environment will need to understand their governance responsibilities, issues and priorities.

## In this chapter

- What is private equity?
- Australian Investment Council Limited (AIC)
- Pre-private equity considerations for boards
- PEC board considerations

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Are there protocols for managing conflicts of interest with participating directors and/or management?
2. Does the board understand the potential personal financial upside to management from a private equity (PE) deal?
3. Are protocols in place to secure independent review of any approach?
4. Should the board set up an independent sub-committee to lead decision-making and process-manage a potential transaction?
5. Does the board understand the position of key shareholders?
6. Should a broader sale process be initiated to maximise shareholder value?
7. Is the board clear on its requirements regarding when and what to disclose to the markets?
8. Does the board have a 'defence protocol' for a potential approach by a prospective bidder that enhances the company's responsiveness and mitigates potential risks?
9. Does the board discuss the approach or the proposed transaction in closed sessions without participating directors and management?
10. What will the impact of the PE approach have on the board's normal agenda?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board has in the past been caught unaware by PE bids.
- No strategy has been developed for dealing with PE bids and it is rarely discussed at board meetings.
- Continuous disclosure issues have been raised against the company over past PE bids.
- Directors' messages are inconsistent or unclear regarding their position on PE bids.
- Independent advisers are usually not engaged to examine PE submissions.
- Disclosure of directors and senior managements' interests is not clear.
- A lot of work needs to be undertaken for the company's financial, operational and commercial information to stand up to a due diligence process.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## WHAT IS PRIVATE EQUITY?

The term *private equity (PE)* covers a broad range of activities related to investing in unlisted companies. It may include taking listed companies private. It represents an alternative model to that of the dispersed ownership of a publicly listed entity.

The Australian Private Equity and Venture Capital market continues to recover after COVID-19, up 52.9 percent in a one-year period to end of June 2021, according to the Australian Investment Council Limited. At the end of Q2 2021, the Australian Private Equity and Venture Capital Index had a total value of \$30.3 billion raised by 109 deals.<sup>351</sup> According to BDO Australia, the top five deals with private equity involvement contributed to 66 percent of total deal value in the 2021 Financial Year.<sup>352</sup>

## AUSTRALIAN INVESTMENT COUNCIL LIMITED

AIC is a national association which represents the private equity and venture capital industries. AIC's members comprise most of the active private equity and venture capital firms in Australia. These firms provide capital for early stage companies, later stage expansion capital, and capital for management buyouts of established companies.<sup>353</sup> AIC and its members are subject to a Constitution, Code of Conduct and Code of Private Equity Governance. All members agree to observe these requirements upon acceptance of membership. All AIC private equity and venture investor firms are required to comply with the Code of Conduct, and where they do not, they must satisfy the 'if not, why not' test, consistent with the approach adopted within the ASX's Corporate Governance Principles.<sup>354</sup>

351 Australian Investment Council, Australian Private Equity and Venture Capital – The New Normal, <https://www.avcal.com.au/AIC/Articles/Blog/2021/11-November/Australian-Private-Equity-Venture-Capital-The-New-Normal>

352 BDO Australia, top deals, refer to <https://www.bdo.com.au/en-au/privateequity2021/deals>

353 Refer to <https://www.avcal.com.au/AIC/>

354 Ibid

## PRE-PRIVATE EQUITY CONSIDERATIONS FOR BOARDS

Boards need to be on the front foot when PE does come knocking. A plan of action developed beforehand regarding how to respond to a bid, be it from PE or anyone else, is a good idea.

Boards must not be too hasty in rejecting an informal takeover approach. Those who dismiss informal takeover approaches without engaging further (for example, seeking to negotiate an improvement in price and conditions) because they believe the indicative offer price is inadequate, only to find that industry conditions deteriorate or other circumstances arise that adversely impact the successful execution of their current strategy, leave themselves exposed to shareholder criticism. Pressure then mounts on the board to defend their earlier decision to not engage with the proponent of the informal takeover approach.<sup>355</sup>

Failure to achieve a materially better outcome for shareholders within a reasonable time of rejecting an indicative takeover proposal can attract further criticism from shareholders, with reputational implications for the directors.<sup>356</sup>

A board cannot leave the initial response to a PE approach to management, which is very likely to possess a conflict through its involvement in the transaction via a management buyout.

355 Refer to GIAs Governance Directions June 2015 Article "When a suitor comes calling: Key developments and trends in mergers & acquisitions".

356 Ibid

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The board's fiduciary duty is to continue to act in the best interests of shareholders as a whole. Directors should consider:

- understanding whether the PE approach is a 'sounding out' conversation or an immediate precursor to a bid
- obtaining market perceptions reports
- procuring up-to-date valuations (can set the tone for subsequent negotiations and discussions)
- arranging a panel of selected advisers (speaking with them in closed sessions without management)
- ensuring policies are appropriate and clear (e.g. conflict of interests)
- setting ground-rules (roles and responsibilities) for the board, chair, board committee and individual director involvement
- understanding the shareholder base (current and future) and the role a PE investor might have as a potential source of funding for future growth and expansion strategies
- establishing a due diligence process, particularly around the degree of access, if any, that may be granted to this or any other bidders, and areas of possible synergies from merging with potential bidders (which may be part of a defence/price maximisation strategy)
- providing institutional investors with enough information for them to do their own valuations.

Despite the focus and commitment in dealing with a PE approach, it will be business as usual at the frontline. The board also needs to consider the impact of an approach on its normal agenda. To assist with this, and to isolate directors who may have a conflict of interest, an ad hoc board committee can take control of the company's response to a PE offer.

This board committee should:

- comprise independent directors who are free of conflicts
- possess access to its own advisers who are also free of conflicts
- have appropriate authority
- pay careful attention to the documentation presented and produced (and if necessary, have the authority to obtain an independent fairness opinion/valuation)
- tightly monitor continuous disclosure and any transparency issues with price sensitive information during the transaction (including decisions on when to go public and the control and provision of confidential information by independent directors to the board and management)
- continuously monitor the market for other possible opportunities.

The committee needs to be open-minded, willing to take advice and consider all options and alternative strategies (defence strategies, further independent valuation, auction strategies and overcoming impasses).

The existence of the committee does not, however, relieve other directors of their obligations under the Corporations Act and ASX Listing Rules during PE activity. The key objective is to provide good counsel to shareholders on the PE proposal.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## PEC BOARD CONSIDERATIONS

In principle, Private Equity Committees (PEC) should observe many of the same governance practices adhered to by publicly listed companies.

The PEC board is typically structured in the best interests of the investee company. The composition of the PEC board will inevitably change with greater representation from the PE investor. Good practice includes maintaining an independent chair and ensuring that a majority of directors are independent. A PEC board consequently tends to be smaller due to the high cost of appointing independent non-executive directors. However, board appointees should continue to be individuals of appropriate competencies, skill and experience who can provide value and insight to the PEC. The relationship between the board and management should be clear and be supported by the appropriate documentation of roles and responsibilities, with effective conflict of interest policies. In some cases, the board develops and monitors a 'management agreement' between the investors, the board and management to assist this cause.

The board's charter depends on what the PE owners expect. This may also be dependent on what the lender(s) demand. Some roles and responsibilities may also, change (e.g. audit committee, company secretary, etc.).

As many PECs eventually re-emerge as publicly listed entities, PEC boards will be better served if their governance frameworks allow a seamless transition to public trading.

## Useful references

- Australian Private Equity & Venture Capital Journal, <https://www.privateequitymedia.com.au/journal/>
- Australian Investment Council's Code of Private Equity Governance and Code of Conduct, <https://www.aic.co/AIC/Our-Industry/Annual-Report-2021/Governance.aspx?WebsiteKey=cabac208-5371-45e7-b5cb-6d0d81afccd6>

### For further information please contact:



**David Willis**

**Partner, National Head of Private Equity, Transaction Services**  
[davidwillis@kpmg.com.au](mailto:davidwillis@kpmg.com.au)



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 20. Health, Safety and Wellbeing

Every workplace is exposed to work health, safety and wellbeing risks, no matter what industry they operate in, and employers (including directors) are responsible for the health and safety of all workers. Health and safety is fundamental for all organisations and begins with the board. Organisations should ensure they have robust systems and processes in place for compliance with Work Health and Safety (WHS) Legislation to effectively manage this risk.

## In this chapter

- Key concepts – health, safety and wellbeing
- Legislation
- Strategy
- Governance
- Organisational structures
- Due diligence
- Penalties
- Performance management
- What health and safety information should be provided to the board?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Does the board have oversight of a clear health, safety and wellbeing strategy with performance indicators and targets? Are these targets realistic and able to be measured effectively?
2. How does the board hold management accountable for implementing the health, safety and wellbeing strategy and policy, and ensure that the CEO meets the board's expectations?
3. How does the board demonstrate its commitment to a positive health, safety and wellbeing culture?
4. Does the board understand the legalities of the health and safety framework in which they operate?
5. Has the board received the appropriate training to enable it to challenge health, safety and wellbeing management?
6. Is there a culture that values and prioritises health, safety and wellbeing within the organisation?
7. What audits or assessments are undertaken to provide assurance over health, safety and wellbeing management processes?
8. How does the board ensure that it has obtained competent health, safety and wellbeing advice from management or other parties?
9. What information does the board receive about health, safety and wellbeing performance to make informed decisions?
10. Do directors understand their liabilities and responsibilities when it comes to ensuring the health, safety and wellbeing of their workforce?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- There are no board level objectives and targets for health, safety and wellbeing and/or the targets in place do not use the SMART principles for measuring objectives and targets.
- There is no vision / strategy or annual health, safety and wellbeing plan.
- There is no board oversight or appropriate level of engagement in the determination, development, endorsement, promotion and/or review of the organisation's health, safety and wellbeing strategy and policies.
- Health, safety and wellbeing information does not appear on the agenda for board meetings.
- Board members have not received appropriate information and training on their health, safety and wellbeing responsibilities.
- Board reporting of health and safety performance is based only on lagged indicators (e.g. number of incidents) rather than leading indicators (e.g. training and education hours on health, safety and wellbeing issues).
- Where there has been significant organisational change, the implications for health, safety and wellbeing have not been reported to the board.
- The company continues to have poor health, safety and wellbeing outcomes despite management's assurance that 'appropriate' controls are in place.
- Contradictory/counter performance indicators are being reported (e.g. workers compensation claims costs; and the frequency and duration of injuries are escalating yet other safety key performance indicators, such as lost time injury frequency rates, are improving).
- Material health, safety and wellbeing risks are ignored or undisclosed (e.g. contractor performance is ignored, where contractors contribute to the workforce, or where the company has overseas operations, these risks are undisclosed/ignored in reporting).
- Health, safety and wellbeing risks are not considered or existing risks are not adequately risk assessed within the organisation's risk management framework.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## KEY CONCEPTS – HEALTH, SAFETY AND WELLBEING

Organisations have a duty of care to ensure that any person affected by the company's undertakings remains safe at all times and their work activities are not prejudicial to their health – or the health of others.

Health, safety and wellbeing extends not only to the physical safety of the workforce, but also to mental health and wellbeing. Having a strong health and safety culture, and an embedded effective management system by which managers and workers demonstrate accountability, can result in significant benefits for an organisation. The failure of organisations to effectively manage health safety and wellbeing risks and performance has both human and business costs and, as such, should receive the same priority by directors as all other risks.

Health, safety and wellbeing governance is as important as any other aspect of governance, and is both core to an organisation's overall risk management function and a key responsibility of directors. This approach includes the identification, evaluation and control of risks and threats to the health, safety and wellbeing of workers, communities and supply chains.

## LEGISLATION

All directors have a legal imperative to ensure that the organisation which they represent remains compliant with relevant health and safety legislation.

In Australia, nationally harmonised health and safety legislation is in effect in most Australian States (except Western Australia and Victoria) and all Territories. Harmonisation is based on the development of "Model Work Health and Safety Bill" and "Model Work Health and Safety Regulations" that have been developed over a number of years by Safe Work Australia. The model Work Health and Safety (WHS) laws set out the key aspects of health and safety legislation that each State and Territory then adopts in their relevant WHS legislation. Safe Work Australia does not regulate state and territory WHS laws, which remain the remit of the relevant regulators in each jurisdiction.

The model WHS laws have been adopted by all states and territories as reflected in the respective legislation within each jurisdiction except for Western Australia and Victoria. Western Australia is currently in transition and consulting on options to implement elements of the model laws. Western Australia's new laws under the WHS Act and accompanying regulations will come into effect in 2022 Victoria has not amended its legislation as the laws were already reflective of nationally harmonised standards.

**Note:** References to the Model WHS Act, including relevant sections relating to specific obligations, will be referred to as the WHS Act throughout this chapter.

Under the WHS Act:

- 'Officers' have a clear, legal duty to be proactive and exercise due diligence on a day-to-day basis with respect to an organisation's health and safety obligations.
- An 'officer' is defined in Section 9 of the Commonwealth *Corporations Act 2001*. 'Officer' includes a director or secretary of a corporation and anyone who makes, or participates in making, decisions that affect the whole, or a substantial part, of a business or an undertaking.
- Continuous examination and due diligence is required by the officer to ensure the resources and systems of the business or undertaking are adequate to comply with the duty of care required under the WHS Act. This also requires officers to ensure that delegations are working effectively and they acquire, and keep up-to-date, their knowledge of health and safety matters.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media










## GLOSSARY

## APPENDICES

## CONTACT US

In addition, following several high profile incidents in Queensland in 2016, industrial manslaughter laws were introduced into both Queensland and the ACT. Other states and territories have since passed new industrial manslaughter legislation but laws differ

between the Australian jurisdictions that have implemented these provisions. The fines and years of imprisonment included in these laws is substantial and, in the case of Queensland, there is no fine option for individuals, purely imprisonment.

Model laws and regulation		Statutory authority
Model Work Health and Safety Bill Model Work Health and Safety Regulations		
Jurisdiction	Legislation and Regulations	Regulator
Federal	Work Health and Safety Act 2011 (Cth) Work Health and Safety Regulations 2011 (Cth)	
NSW	Work Health and Safety Act 2011 (NSW) Work Health and Safety Regulation 2017 (NSW)	
QLD	Work Health and Safety Act 2011 (Qld) Work Health and Safety Regulation 2011 (Qld)	
ACT	Work Health and Safety Act 2011 (ACT) Work Health and Safety Regulation 2011 (ACT)	
SA	Work Health and Safety Act 2012 (SA) Work Health and Safety Regulations 2012 (SA)	
NT	Work Health and Safety (National Uniform Legislation) Act 2011 (NT) Work Health and Safety (National Uniform Legislation) Regulations 2011 (NT)	
TAS	Work Health and Safety Act 2012 (Tas) Work Health and Safety Regulations 2012 (Tas)	
<b>NOTE:</b> Western Australia is currently in transition and consulting on options to implement elements of the model WHS laws. Victoria has not amended its legislation as its laws were already reflective of nationally harmonised standards.		
VIC	Occupational Health and Safety Act 2004 (Vic) Occupational Health and Safety Regulations 2017 (Vic)	
WA	Occupational Safety and Health Act 1984 (WA) Occupational Safety and Health Regulations 1996 (WA)	
NOTE: WA Government endorsed the development of new WHS Act 2020 and accompanying WHS regulations on 10/11/2020 which come into effect in 2022.		

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## STRATEGY

It is the duty of the board to ensure that the organisation has the right strategic direction for health, safety and wellbeing (including mental health). This must be underpinned by robust systems, processes, culture and people. Ultimately, boards are responsible for determining the organisation's high-level health, safety and wellbeing strategy and policy, which managers are then required to implement. The health, safety and wellbeing strategy and policy should also include consideration of all persons impacted by the organisation's activities, not just employees (e.g. contractors and visitors). However, board responsibility should go beyond the issuing of strategy and policy. It should extend to ensuring the effective implementation of the health safety and wellbeing policy by holding management accountable through policy planning, delivery, monitoring and review processes.

Comcare (the Commonwealth regulator for work health and safety in Federal workplaces) states that a "strong health and safety culture is key to profitability, sustainability, reduced compensation costs and other success measures. With an ageing workforce, the impact of chronic disease in the workplace and a competitive labour market, businesses using targeted strategies to build (and embed) health and wellbeing at work will have greater business performance and people outcomes" and that "measuring health and safety performance provides an insight into management and investment decisions".<sup>357</sup> Senior managers and executives have a duty to ensure their organisation complies with its duties and obligations under the WHS Act and the Safety Rehabilitation Compensation Act 1988. They have a duty to ensure work health and safety laws are integrated into everyday business. As part of the strategic direction, directors should consider and challenge the key performance indicators that underpin the company's strategy. For example, safety performance (particularly numbers of/nature of incidents) is often reported by management, yet there is little to no disclosure on health indicators and associated impacts (mental and physical wellness), which often have a much greater effect on a business performance.

<sup>357</sup> Australian Government Comcare, Senior managers and executives, <https://www.comcare.gov.au/roles/senior-managers>

## Culture, standards and values

The board should take ownership for key health and safety issues and be ambassadors for good health and safety performance within the organisation. Boards achieve this by upholding core values and standards, setting the 'tone at the top', 'walk the talk' and establishing an open culture across the organisation with a high level of communication on health and safety issues.

## Strategic implications

The board is responsible for driving the health, safety and wellbeing agenda. They have oversight and an understanding of the risks and opportunities associated with health, safety and wellbeing, including any market pressures which might compromise the values and standards – ultimately establishing a strategy to respond. In many workplaces, mental health issues such as stress, bullying and the impacts of domestic violence (also known as psychological injuries) are emerging as key risks to be managed as part of an organisation's health, safety and wellbeing strategy. According to "NSW Mentally Healthy Workplaces Strategy to 2022", the estimated cost to NSW due to mental illness at work is estimated at \$2.8 billion per year.<sup>358</sup> The Australian Work Health and Safety Strategy 2012–2022 identifies work-related mental health conditions as a priority.

Safe Work Australia has published a guide to help meet WHS duties to prevent harm to workers' psychological (mental) health. It provides a step-by-step process for eliminating or minimising psychological hazards so far as reasonably practicable as well as intervening early, and managing psychological injury. This guide states using a thorough and systemic approach can have significant business benefits including:

- decreasing business disruption and costs from work-related psychological injury
- improving worker motivation, engagement and job satisfaction so increasing

<sup>358</sup> Safe Work Australia, Australian Work Health and Safety Strategy 2012-2022, <https://www.safeworkaustralia.gov.au/system/files/documents/1902/australian-work-health-safety-strategy-2012-2022v2.pdf>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- productivity, reducing absenteeism and turnover, and ultimately helping your organisation achieve its business goals, and
- enhancing your reputation as an employer of choice.

**Most at risk occupations for mental health claims**

Safe Work Australia has published data on the most 'at risk' occupations for psychological injuries. These tend to be professions that involve a high degree of interaction with other people, in often challenging or traumatic situations, for example:

- defence force members, fire fighters and police
- school teachers
- automobile, bus, tram and rail drivers
- health and welfare support workers, including ambulance officers and paramedics
- prison and security officers
- social and welfare professionals.

**Performance management**

The board should ensure they it retains oversight of the key objectives and targets for health and safety management, and create an incentive structure for senior executives which drives good health and safety performance, balancing both leading and lagging indicators, and capturing both tangible and intangible factors. Non-executives (through the Remuneration Committee, where one exists) should be involved in establishing the appropriate incentive schemes.

**Internal controls**

The board should ensure health and safety risks are adequately managed and controlled, and that a framework is established to ensure compliance with the core standards. It is important that governance structures enable management systems, actions and levels of performance to be challenged. This process should utilise, where possible, existing internal control and audit structures, and be reviewed by the audit committee, or other suitable committee or board members, where necessary.

Recommendation 7.1 of the ASX Principles suggests that listed entities have a dedicated risk committee (which may be a combined audit and risk committee), addressing different elements of risk. Most organisations include oversight of health safety and wellbeing risk in the remit of the risk committee. In the absence of a risk committee, many organisations establish a dedicated committee to specifically oversee health, safety and wellbeing risks. These often include environmental and/or community risks as well (Health, Safety, Environment and Community (HSEC) committee). Under WHS legislation, a health and safety representative (also known as HSR) can request to establish a Health and Safety Committee providing it meets certain requirements as set out in the WHS legislation. The function of the committee is to help facilitate co-operation and consultation with work groups and/or through their HSRs in health and safety matters.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

## GOVERNANCE

### Director competence

All directors should have a clear understanding of the key health, safety and wellbeing issues characterising their organisation and be continually developing their skills, knowledge and understanding in this area. Knowledge of good health and safety governance structure and practice includes but not limited to the following.

- Liability of Directors and Industrial Manslaughter offences
- Workplace Health and Safety duties and obligations under the WHS Act
- Due Diligence – what is it and how do you demonstrate it
- Understanding the hazards and risks of business operations
- Knowing WHS Performance Metrics – Leading and Lagging
- Leadership and Culture
- Systems and processes for managing health, safety and wellbeing risks

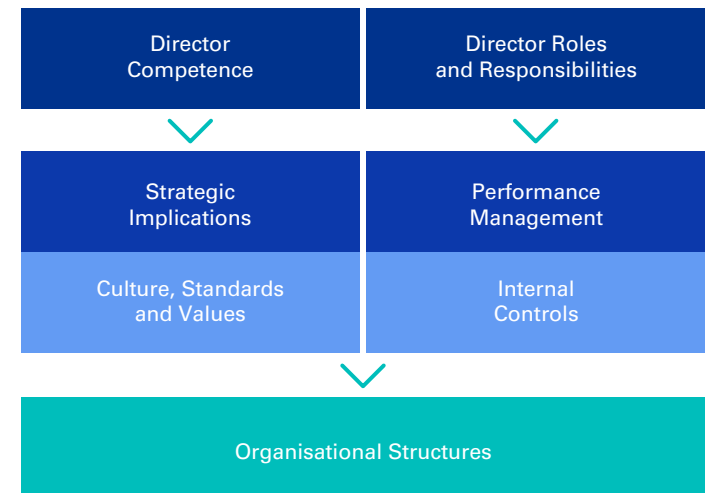
### Director roles and responsibilities

All directors should understand their legal responsibilities and their role in governing health, safety and wellbeing matters for their organisation. Their roles should be supported by formal individual terms of reference, covering, at a minimum, the oversight of the health, safety and wellbeing strategy development, setting of policies and standards, performance monitoring and oversight of an internal controls framework. Where applicable, directors should communicate to all levels in the organisation or within their scope of direct reports about their specific health and safety responsibilities, authority to act and reporting requirements.

## ORGANISATIONAL STRUCTURES

The board should integrate health, safety and wellbeing governance processes into the organisation's broader corporate governance structures, including the activities of the main board and its committees. In some cases, the creation of an additional board committee to consider health, safety and wellbeing matters may be relevant (as discussed above).

### Better Practice Framework for WHS Governance





## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## DUE DILIGENCE

Regardless of the size of the undertaking or the nature of the organisation's health, safety and wellbeing risk profile, it is important that directors, as officers, are fully informed of the relevant health, safety and wellbeing matters, up-to-date key information (e.g. COVID-19 changes) and the requirements that apply to them. This includes understanding their role in governing health, safety and wellbeing, as part of their broader responsibilities of good corporate governance.

Under WHS laws, the exercise of due diligence is the individual obligation of each officer or 'person conducting a business or undertaking' (PCBU). This means that each individual officer should consider how they will demonstrate compliance with their due diligence requirements contained in the WHS Act.<sup>359</sup>

*How do directors/officers demonstrate due diligence?*

In exercising due diligence, section 27 of the WHS Act requires officers to show that they have taken reasonable steps to:

1. acquire and keep up-to-date knowledge of work health and safety matters

2. gain an understanding of the nature of the operations of the business or undertaking of the PCBU and generally of the hazards and risks associated with the operations
3. ensure the PCBU has available for use, and uses, appropriate resources and processes to eliminate or minimise risks to health and safety arising from business operations
4. ensure the PCBU has appropriate processes in place for receiving and considering information regarding incidents, hazards and risks and responding in a timely way to that information
5. ensure the PCBU has, and implements, processes for complying with any duty or obligation of the PCBU under the WHS Act
6. verify the provision and use of the resources and processes referred to in dot points 3 to 5 above.

## PENALTIES

In Australia, significant personal penalties apply to a corporation, officer or PCBU who fails to exercise due diligence under the WHS Act (in the relevant jurisdictions to which the WHS Act applies). The individual penalties for a breach are:

Type of offence	Maximum penalty for corporation	Maximum penalty for officers	Maximum penalty for workers
<b>Category 1</b> offence – recklessness that leads to serious injury or death	\$3,000,000	\$600,000 or 5 years' imprisonment	\$300,000 or 5 years' imprisonment
<b>Category 2</b> offence – failure to comply with the duty leads to serious injury or death	\$1,500,000	\$300,000	\$150,000
<b>Category 3</b> offence – simple failure to comply with the duty	\$500,000	\$100,000	\$50,000

<sup>359</sup> Refer to Safe Work Australia, 2019, Model Work Health and Safety Bill, <https://www.safeworkaustralia.gov.au/system/files/documents/2003/model-whs-bill9-december2019.pdf>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Similar penalties apply in Victoria and Western Australia subject to the provisions of the relevant health and safety legislation in those jurisdictions.

**Industrial Manslaughter in Australia**

Where a worker is seriously injured or dies in the workplace, in these circumstances, as an employer, a director may be liable for industrial manslaughter penalties.

Industrial manslaughter laws differ between the Australian jurisdictions. They aim to prevent workplace deaths and deter employers from breaching health and safety duties owed to workers. Directors must understand how industrial manslaughter offences arise and establish effective work health and safety systems. The individual and body corporate penalties for industrial manslaughter are:

	Maximum penalty for individual	Maximum penalty for a body corporate
<b>New South Wales*</b>	25 years imprisonment	\$3,809,300
<b>*In NSW general criminal law of manslaughter applies</b>		
<b>Victoria</b>	25 years imprisonment	\$16,522,000
<b>Queensland</b>	20 years imprisonment	\$13,345,000
<b>Australian Capital Territory</b>	20 years imprisonment \$320,000 for an individual	\$1,620,000
<b>Northern Territory</b>	Life imprisonment for an individual	\$10,270,000
<b>Western Australia</b>	20 years imprisonment \$5,000,000 fine for an individual	\$10,000,000
<b>South Australia and Tasmania</b>	South Australia and Tasmania are not currently planning to introduce specific industrial manslaughter legislation.	

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**WHS exemption from D&O insurance**

Importantly, there is a permanent exemption from D&O insurance for WHS obligations. Under WHS legislation, an officer or PCBU cannot delegate to another person or company their obligation to devise, maintain and implement a safe and proper system of work. Consequently directors cannot insure against negligence.

**Examples of recent WHS convictions**

Date of conviction	Incident	Conviction
NSW 2021	Employee suffered a psychological injury at work following a fatality which the worker witnessed and was initially unfairly blamed for the fatality during the employer's internal investigation. The injuries sustained by the worker were accepted as having left the employee with at least 15% whole person impairment.	Worker's compensation claim approx. \$1 million for the injured worker.
QLD 2020	Company found failing to implement control measures that effectively separated mobile plant and pedestrian workers and failing to effectively supervise operators of moving plant and workers resulting in the death of a worker who was crushed by a forklift.	Company fined \$3 million for breach of health and safety duties under the WHS Act.  Two company directors sentenced to 10 months imprisonment, wholly suspended with an operational period of 20 months.
SA 2015	Truck company owner systematically ignored due diligence obligations, near miss reports, safety issues raised by its workers and failed to exercise due diligence or pay any heed to WHS legislation to repair faulty brakes which led to the death of one of its drivers.	Company owner found guilty of manslaughter and endangering life sentenced to 12 years imprisonment.
TAS 2022	Engineered stone benchtop manufacturer failed to comply with health and safety duties that resulted in workers being exposed to the risk of developing the incurable lung disease silicosis.	Company found guilty to health and safety breaches fined \$500,000.
VIC 2021	Civil construction company failed to provide a safe working environment and provide necessary supervision resulting in two workers being fatally injured when a trench collapsed.	Company found guilty of health and safety breaches fined \$550,000.
WA 2021	Two workers fell from height while they were installing roof sheets on a large machinery shed building on a farm without safety control measures in place. Neither of the workers were licensed for the work they were performing, and the worker who was killed did not hold a construction induction training certificate.	Company Director was sentenced to two years and two months imprisonment (18 months suspended) and fined \$2,250 for gross negligence causing death of a worker and serious injury of another.  Company was fined \$550,000 for gross negligence.
NT 2021	Company director fined after an unsupervised apprentice electrician was electrocuted on the job.  The 34-year-old fourth-year apprentice died while working with another apprentice on the roof of the Tennant Creek Fire Station in February 2019.	Company Director fined \$160,000 in the Alice Springs Local Court.  The company was convicted and fined \$80,000 for failing to comply with its health and safety duties under the WHS Act and the Company director was convicted and fined \$40,000.  The court also ordered the company to provide \$40,000 to NT WorkSafe as an enforceable undertaking to develop an electrical safety campaign.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## PERFORMANCE MANAGEMENT

Lost time injury (LTI) rates have become the cornerstone of mainstream injury/incident reporting and the benchmark against which organisational, industry and national comparisons are made. Although LTI rates are being applied to inform an ever growing range of health and safety problems and decisions, they also have a number of important limitations, such as a poor correlation with both the human and financial consequences of work related injury and illness.<sup>360</sup> There are also considerable variations in the definition of "lost time" across organisations, thereby making performance benchmarking comparisons difficult.

'Lagging' indicators such as LTI measure outcomes, however, may not provide sufficient information for successful management, nor provide appropriate information for due diligence purposes. For example, lagging indicators may provide information too late for management to respond.

In contrast, 'leading performance indicators' (LPIs), provide valuable information that helps the user respond to changing circumstances and take to action to achieve desired outcomes, or avoid unwanted circumstances. Examples of LPIs include:

- the number of hazards reported
- the number of workplace inspections or audits carried out
- the number of actions completed as a result of the inspections/ audits performed.

LPIs can play an important role in motivating continuous improvement, with a focus on areas that have the potential to cause an incident, before the incident itself is realised.

## WHAT HEALTH, SAFETY AND WELLBEING INFORMATION SHOULD BE PROVIDED TO THE BOARD?

Directors should ensure the appropriate level of information is being reported by management to the board. Reports should be inclusive of lead and lag indicators, and have sufficient information to support the board's decision making with respect to oversight of health and safety risk. The individual importance of health and safety for directors and the organisation's workforce, means that health and safety data should be supported by independent and objective assurance –

<sup>360</sup> Safework Australia, updated October 2020, Issues in the Measurement and Reporting of Work Health and Safety.

bringing a systematic, disciplined approach to health and safety risk management, control and governance processes.

For LPIs to be successful they need to be selected carefully, for example, targeting relevant and material issues and setting sufficient challenge. Setting an LPI and obtaining a 'good score' does not automatically improve performance. It is not only the numbers that are important, but the quality and application of the gathered information and the preventative measures put in place that makes the difference.

## Useful references

- Safe Work Australia <https://www.safeworkaustralia.gov.au/>
- Australian Government Comcare, <https://www.comcare.gov.au/>
- Issues in the Measurement and Reporting of Work Health and Safety: A Review, Safe Work Australia, November 2013.
- Guidance for Officers in exercising Due Diligence, Australian Government Comcare.
- Safe Work Australia Australian Work Health and Safety Strategy 2012-2022

## For further information please contact:



**Paul Rubotham**

**Director, Health & Safety,  
Audit, Assurance and Risk Consulting**  
[prubotham@kpmg.com.au](mailto:prubotham@kpmg.com.au)

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 21. Culture and Conduct

Boards are accountable for driving an organisation's culture by setting its values and a code of conduct underpinned by processes to ensure all employees demonstrate ethical behaviours to foster a culture of transparency and accountability.

## In this chapter

- Tone from the top
- Business ethics
- Organisational values and ethics
- Code of conduct
- Cultural issues
- Developing a 'learning culture' where 'bad news' is communicated
- Whistleblower policy
- Boardroom dynamics
- Information communications outside board meetings

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Are the company's policies and procedures supporting the realisation of the desired culture?
2. Is the code of conduct and compliance program regularly reviewed to determine if they need updating due to business, legal, or regulatory changes?
3. Has the organisation's ethics and compliance program been reviewed by outside consultants or experts for possible improvement?
4. Have any compliance investigations arisen from a cultural problem?
5. Is there a whistleblowing policy and program in place? How do you know that it is effective?
6. How do individuals receive the information required to understand the firm's core values, code of conduct and the specific policies, laws and regulations related to their jobs?
7. Has a corporate culture been developed and maintained that creates an environment of openness, honesty and the timely reporting of bad news?
8. How does management fully inform the board about potential or actual conflicts between the company's values and the business practices in countries where it operates?
9. What processes and practices are in place to promote ethical behaviour?
10. Does the company have in place processes to monitor and measure culture?
11. Does the board have access to data to assess whether the desired culture of the company is being realised?
12. Has the board considered how executive compensation aligns with the desired ethics and compliance culture?
13. What do the company's internal and external auditors' reports indicate about the organisation's culture? Has the board set an appropriate 'tone from the top'?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The board has 'power factions' that inhibit teamwork.
- The board always comes to a consensus quickly and easily with little or no discussion.
- The code of conduct has not been reviewed in recent years.
- There are a concerning number of internal and external complaints.
- The board receives limited reports or information regarding whistleblower policy.
- The board virtually 'ticks the box' with respect to recommendations from management.
- The board culture does not allow discussion of difficult, controversial or sensitive matters in the boardroom.
- Risk monitoring is not conducted with regards to doing business in higher risk countries.
- The board does not ask questions related to culture, ethics or conduct.
- The board and/or management are not respectful in discussions and reporting on matters involving the regulator(s).
- The importance of culture is not communicated or actively demonstrated by the board.
- Management is rewarded for what they have achieved with little consideration given to how this has been achieved.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

While the conduct of financial institutions at home and abroad has garnered considerable attention, a number of other industries have also had their fair share of poor press. Questionable practices in the construction sector, utilities and banking, as well as large retailers and their suppliers, have rocked the public's confidence time and again and led people to question the moral integrity of these organisations. Governmental bodies and agencies are similarly positioned. Concerns around bullying and harassment and a perceived lack of inclusiveness are giving these entities good reason to reconsider their own cultures.<sup>361</sup>

It is not surprising then that leading organisations have begun to reflect on the culture and sub-cultures of their organisations. They are intent on assessing whether issues exist, their underlying causes and what actions could be taken to either change or enrich their organisational culture.

However, it is also important to note that culture cannot be considered in isolation of a number of other tangible organisational initiatives. In particular, remuneration and incentives (decisions about remuneration and incentive structures have a direct influence on both leaders' and staff behaviour), accountability (clearly defined accountability with consequences for poor risk and customer outcomes drives the required message from management), governance, and, most importantly, leadership ('Tone from the Top').

## TONE FROM THE TOP

Whilst many organisations implement policies and frameworks that outline the conduct and behaviours expected of individuals, they are often initiated in response to legal requirements and other guidelines. Although it is important that an ethics and compliance program is in place, it must be more than just adherence to rules and policies. Instead, an ethical culture should be embedded into an organisation. Merely meeting legal requirements is unlikely to be sufficient to satisfy the ethical concerns of employees, clients, customers, shareholders and other stakeholders.

<sup>361</sup> Refer to KPMG, Risk Consulting: Organisation's cultural assessment and transformation, <https://assets.kpmg/content/dam/kpmg/ie/pdf/2017/07/ie-risk-cultural-assessment-transformation.pdf>

The commitment of the entire organisation is essential in order to design, develop and implement an effective corporate culture. It represents 'how we do things around here' and sets the basis of acceptable behaviours and cultural norms. Having policies in place is a start, but the real test of an organisation's culture is what happens in practice. There is often a marked difference between what is written in policy and how things are done in practice. Boards set the 'tone from the top', which influences the entire organisation. The board should ensure appropriate values, ethics and culture are upheld throughout the organisation.

Increasingly, there have been many examples of where organisational behaviour has been at odds with stated policies. In some instances it has been individual 'bad apples' that have 'spoiled' the entire organisation through discrete acts of unethical behaviour. However, more often, the issues are more systemic, where unethical conduct has represented a culture of complicity or risk taking that is at odds with the stated policies. Research has shown that ethical culture is often based on the behaviour of peers<sup>362</sup> and immediate managers.<sup>363</sup> Setting the right 'tone from the top' is therefore an important factor in shaping the ethical and behavioural standards that the organisation is willing to accept, including holding staff to account when these standards are not met – regardless of whether the poor conduct is reported publicly or not.

The 'tone from the top' refers to the character and behaviour displayed by leaders of an organisation that forms a model of appropriate conduct for every level of the organisation. Boards bear ultimate responsibility for their organisation's culture, including the values and ethical environment that underpin that culture. The 'tone from the top' should be underpinned by clearly articulated values and policies, a code of conduct, ongoing ethical awareness training and an ethics management process that is embedded across all the organisation's activities.

<sup>362</sup> Collins, F. (2006). Career Self-Interest and Concern for Others—The Effects of Co-Worker Attitudes on Fraudulent Behavior. *Accounting & The Public Interest*, 695-115.

<sup>363</sup> Schaubroeck, J. M., Hannah, S. T., Avolio, B. J., Kozlowski, S. W., Lord, R. G., Treviño, L. K., & ... Peng, A. C. (2012). Embedding Ethical Leadership Within And Across Organization Levels. *Academy Of Management Journal*, 55(5), 1053-1078. doi:10.5465/amj.2011.0064.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

It is also important to note that the dissemination and reinforcement of desired conduct and values is also important as, without an 'echo from the bottom' or staff engagement, the 'tone from the top' is of limited utility.<sup>364</sup>



### Case study – Lessons in culture from the Financial Services Royal Commission

Changing culture and governance was a centrepiece of the Hayne Royal Commission's Final Report. Commissioner Hayne directed that financial services entities are to take proper steps to assess the entities' culture and governance, identify any problems, deal with those problems and thereafter determine whether the changes made have been effective.

For many organisations, conducting a risk assessment and outlining remedial actions are already part of their ongoing activities. However, risk culture is a nebulous concept, and difficult to measure in any quantitative way outside of one-dimensional risk surveys. Demonstrating genuine effectiveness of culture change will be a challenge for many. Measuring the effectiveness of changes is made more challenging as organisational culture is built over time and is only changed slowly.

APRA has been directed to re-establish their culture supervisory capabilities, and to take a more active role in the supervision of culture including "assessing the cultural drivers of misconduct in entities". Organisations wanting to avoid close cultural scrutiny from APRA would do well to take steps to understand and deal with their cultural problems as the recommendation suggests a "risk based approach" given that cultural work can be resource intensive and therefore focused.

Culture is also addressed in the 4<sup>th</sup> edition of the ASX Principles, with principles and recommendations that focus on the link between culture, values and community expectations. The 4<sup>th</sup> edition includes significant changes to Principle 3, with an overarching view that it is imperative that listed entities align their culture and values with community expectations, to help address a declining trust in business so as to build long-term sustainable value for their security holders.<sup>365</sup>

Specifically, Principle 3 now provides that "a listed entity should instil and continually reinforce a culture across the organisation of acting lawfully, ethically and responsibly."<sup>366</sup> This is also consistent with the themes that emerged from the Royal Commission noted above as, the ASX Corporate Governance Council has expressly linked the themes of the ASX Principles and Recommendations with the outcomes of the Financial Services Royal Commission.

The specific recommendations under Principle 3 include having and disclosing:

- the entity's values
- a code of conduct
- a whistleblower policy and
- an anti-bribery and corruption policy.

## BUSINESS ETHICS

Business ethics refers to rules, standards, stated organisational values and behaviours that determine what is acceptable or unacceptable in specific situations. They are inextricably linked to notions of honesty, integrity, trust, accountability, transparency and social responsibility. Ethical conduct is a key factor in the long-term viability and success of organisations. Moreover, the reputations of individual directors and executives are tarnished when a business is seen not to have acted ethically, or has otherwise breached community standards.

<sup>364</sup> Group of Thirty, "Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform" (July 2015) at 13.

<sup>365</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Principle 3. 2019

<sup>366</sup> Ibid

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

An organisation's business ethics and corporate culture may be revisited in conjunction with a board review or a review of the organisation's remuneration practices. Perceived failures, adverse media exposure and episodes of high staff turnover are examples of possible catalysts for a re-awakening interest in business ethics and corporate culture; a tool to revitalise the organisation.

An effective business ethics process should generate real benefits, including:

- increasing the integrity of financial reports and information
- minimising the incidence and encouraging the reporting of fraud and other organisational misconduct
- creating confidence that unethical behaviour will be reported and addressed and
- producing a working environment that fosters pride, responsibility and a sense of both purpose and value.

The following is an example of a business ethics framework.

- A code of conduct that clearly and concisely articulates an organisation's values and behaviours.
- A code of conduct which underpins all organisational activities, sets out the organisation's employment practices, and provides direction on how management will manage the business.
- Ethics and awareness training should be delivered and reinforced regularly to all employees, and included in induction programs for new employees.
- Formal processes providing guidance to employees facing ethical dilemmas, and the mechanisms for reporting wrongdoing, and making suggestions about how business ethics can be improved.
- A performance management process that not only measures results, but considers how these results have been achieved.

## TRENDS

## Moving away from 'can we' to 'should we'

*APRA's Prudential Inquiry into the Commonwealth Bank of Australia (CBA), April 2018*

For nearly a decade the CBA had been using the word 'can' in its marketing campaigns, however, in April 2018 the prudential regulator, APRA, demanded that the question 'should we' be injected into the bank's culture in relation to all dealings with and decisions on customers.

The Inquiry Panel explored the concept of conduct risk management, which it noted in its simplest form "goes beyond what is strictly allowed under law and regulation ('can we do it?') to consider whether an action is appropriate or ethical ('should we do it?'). The Panel also noted that compliance functions globally have more recently been focused not just on evaluating with business units whether an activity or product is allowed under regulation ('can we?') but, critically, whether they should engage in such an activity or product in the first place ('should we?').

## ORGANISATIONAL VALUES AND ETHICS

Organisational values not only guide a company's people, but also create expectations on the part of external stakeholders about acceptable behaviour within the organisation. Strong values shared by both an organisation and its employees have been found to increase employee commitment and satisfaction. This in turn is said to lead to a strong culture.<sup>367</sup>

Once agreed, values should be embedded in documented policies and procedures, and then actively embraced and practised by all company personnel. An effective ethics and compliance program requires senior management leadership to entrench and uphold values, organisation-wide commitment, an effective communications system and an ongoing monitoring system.

<sup>367</sup> Adamoniene R et al, June 2021, influence of individual and organisational variables on the perception of organisational values.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## CODE OF CONDUCT

Good corporate governance is ultimately about personal and organisational integrity. Though this cannot be regulated, investor confidence can be enhanced if the company clearly articulates acceptable practices for directors, senior executives and employees.

Typically a code of conduct:

- spells out an organisation's values and principles
- reflects and shapes the organisation's culture
- makes transparent the value framework within which the organisation operates.

The ASX Principles recommend that companies establish a code of conduct that articulate the standards of behaviour expected of its directors, senior executives and employees and ensure that the board or board committee is informed of any breaches.<sup>368</sup>

Box 3.2 of the ASX Principles includes a detailed list of suggested matters which may be useful for consideration when formulating a code of conduct. Codes of conduct should reflect the company's unique operating and contextual environment.

As the board and senior executives are responsible for setting the tone and ethical standards of the organisation and overseeing adherence to them, they must demonstrate that the agreed codes and standards are equally applicable to them and lead by example. Organisations that 'walk the talk' with regard to their code develop a reputation for honesty, integrity and principled business behaviour, which may form a key element of a company's brand and enhance its reputation.<sup>369</sup>

<sup>368</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Recommendation 3.2. 2019.

<sup>369</sup> 20 Questions directors Should Ask about Codes of Conduct, Gunns. M & Wexler, M. 2010.

The Governance Institute of Australia recommends that directors be required to commit to the code of conduct on appointment, regularly review the code of conduct, and seek assurance that relevant compliance systems are in place and are operating effectively.<sup>370</sup> When overseeing the implementation of the code, directors must ensure it is effectively communicated by management. The board should make certain that the code of conduct is taken seriously throughout the organisation, and breaches will give rise to disciplinary measures. Merely issuing a code, however, does not ensure it will be observed. To add value, the code must extend beyond a compliance focus and strive to cultivate and maintain an organisation-wide culture that focuses on encouraging positive moral behaviour while simultaneously striving to prevent ethical lapses.<sup>371</sup>

The code of conduct must continue to evolve with the changing environment. This includes laws and regulations, the operational environment, public opinion and the focus on acceptable business behaviour. Those developing or revising the code of conduct should consult frequently with specialists in areas addressed by the code.

## CULTURAL ISSUES

## Global operations

Companies with significant global operations face additional difficulties in evolving and implementing codes of ethics and conduct. In part, it is a matter of different cultural norms – what is generally acceptable in Australia might not be so acceptable in another country.

The board should be fully informed about conflicts between the company's values and business practices in various countries, as a lack of understanding of cultural differences may contribute to compliance breaches of international laws (e.g. bribery and facilitation, work health and safety practices), a lack of performance, loss of key employees and time consuming conflicts.

<sup>370</sup> Governance Institute of Australia, Good Governance Guide – Corporate Code of Conduct, 2011.

<sup>371</sup> K. M. Gilley, C. Robertson, T.C. Mazur, The bottom-line benefits of ethics code commitment, 2010.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Multinational companies are faced with several issues:

- how to foster a culture of ethical conduct in all countries of operation
- how to navigate cultural differences and norms
- how to ensure suppliers adhere to ethical codes of conduct
- how to engage a global workforce in understanding and adopting its corporate values
- how to meet all the legal and compliance obligations throughout all locations and
- language barriers between different global units.

When selecting leadership roles within a multinational company, cultural alignment may be a relevant consideration, in an attempt to promote consensus on a global, organisation-wide culture, particularly when appointing local leaders across international business units. Cultural alignment of potential candidates must therefore form part of any skills and attributes assessment, together with other criteria such as gender, age and ethnicity. When considering cultural alignment, best practice is to clearly define the organisation's culture (e.g. values, processes, expected behaviours, accountability processes and leadership style) and transparently measure candidates against this standard. It cannot be based on a gut feel.

However, you don't really need everyone to be the same in an organisation to foster an ethical culture. The key will be to keep ethics on the agenda and through regular communication, keep leaders accountable for ethical conduct to each other and to the board. A better selection tool would be a thorough background check for any history of ethical misconduct.

A failure to consider an organisation-wide code of conduct may lead to significant cultural differences in the executive levels of the company around the world, potentially fostering a lack of understanding and commonality of purpose that may lead to conflict and poorly executed decisions. Global principles, based on corporate values, should be promoted across the organisation, while still allowing for local cultural traditions within international business units.

**Mergers and acquisitions**

A 2012 review revealed that cultural fit can make or break the realisation of synergies between two strategically aligned companies that come together as the result of a merger or acquisition.<sup>372</sup> In other words, cultural differences are a major post-deal issue, and companies frequently associate integration issues with cultural variation and complexity. Organisations should pre-empt these issues, as opposed to blaming cultural differences for difficulties experienced during post deal integration.

Central considerations in managing the integration of company cultures include:

- assessing the differences in cultures from the outset
- defining a cultural end state and its implications for future ways of working
- engaging in deep cultural learning to move towards acculturation
- retention of rewards for key people and
- understanding what makes each and the combined business successful, and how this will be retained and built on.<sup>373</sup>

It should be considered whether the cultures of the two organisations are compatible, and if one will be dominant, how employees operating under the alternative culture will be embraced. If one culture is to prevail, retaining key leaders of that organisation to serve as role models is essential in order to promote the integrated culture. The key objective in some mergers or acquisitions is to incorporate the advantages of each organisation's culture, ultimately resulting in synergy. The possible end states for a merger or acquisition are found in Figure 1. A plan for the merging of cultures should be devised, depending on the defined cultural end state, incorporating educational efforts to assist employees to understand the corporate values they should adopt in the workplace.

<sup>372</sup> Dauber, D. (2012). Opposing positions in M&A research: culture, integration and performance. *Cross Cultural Management: An International Journal*, 19(3), 375-398.

<sup>373</sup> Marks, M. L., & Mirvis, P. H. (2011). A framework for the human resources role in managing culture in mergers and acquisitions. *Human Resource Management*, 50(6), 859-877.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

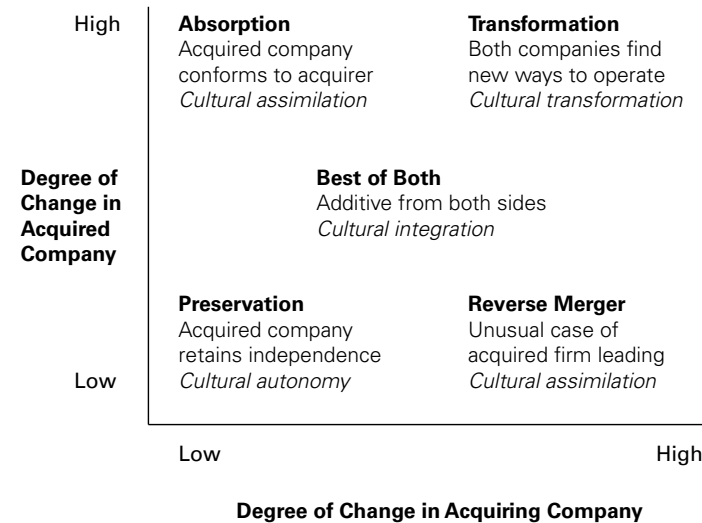
18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Possible cultural end states resulting from a merger or acquisition.



DEVELOPING A 'LEARNING CULTURE' WHERE 'BAD NEWS' IS COMMUNICATED

Recent corporate scandals highlight the importance of building a corporate culture that supports the giving and receiving of 'bad news' i.e. creating an environment of openness and honesty and the presentation of the hard truth.

A KPMG-sponsored survey found that only 55 percent of respondents believe that their organisation is effective at keeping the board aware of the key risk issues.<sup>374</sup> This is a cultural issue that the board must be cognisant of, ensuring that it builds an environment where "bad news" can be delivered without fear of retribution or personal repercussions. In practice, this requires boards to question

<sup>374</sup> KPMG, 2011, Enhancing Business Performance through Governance, Risk, and Compliance.

information provided by management and seek any additional information from the organisation that can assist in identifying and managing 'bad news', without creating an environment of 'punishment' of those who raise the issues.

An early warning system for problems can present the opportunity for timely and appropriate intervention, learning and continuous improvement and/or the redefining of strategy. A climate in which full disclosure is delivered in a timely manner should be fostered by senior management and endorsed by the board to encourage employees to immediately bring forth concerns. This relies on the implementation of processes to support accurate and timely reporting, as well as a culture of accountability, trust and openness which can only be built on individual and collective behaviours displayed and accepted by the board.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## WHISTLEBLOWER POLICY

The term 'whistleblower' refers to anyone who alerts superiors or the appropriate authorities to misconduct within an organisation (although we note that under the Corporations Act the term 'whistleblower' has a specific meaning and refers to individuals who make disclosures that are protected under the law). All employees and related individuals such as contractors and suppliers should be encouraged to raise genuine concerns about possible improprieties in the conduct of an organisation's business.

Employees may fear retribution or retaliation if they take their concerns to management or believe their allegations will not be taken seriously. They might not know who they should take the matter up with, and this becomes a more acute concern when the subject of the allegation is their manager or someone more senior.

Many companies use external reporting services to allow for anonymous reporting and eliminate the fear of retaliation. These services usually provide staff with a toll-free telephone number for reporting their concerns about fraudulent or improper conduct, in addition to other options such as web-based reports. All whistleblower reports should be assessed internally. If they appear to be genuine (i.e. not a vexatious, baseless or fraudulent report) they should be investigated, where possible, and reported to the audit committee. Some companies appoint an investigations officer for this purpose.

From 1 July 2019, the whistleblower protections of the Corporations Act were expanded to provide greater protection for 'eligible whistleblowers', which includes current and former officers, employees, contractors and suppliers of a company, as well as their spouses, immediate family and dependents, who report information that they have reasonable grounds to suspect indicates misconduct or an improper state of affairs in relation to the company.<sup>375</sup>

Further, Recommendation 3.3 of the ASX Principles and Recommendations provides that a whistleblower policy should identify the types of concerns that may be reported under the policy, explain how the confidentiality of the whistleblower will be

safeguarded and how they will be protected from victimisation, and provide training on employee rights and managerial responsibilities under the whistleblower policy.<sup>376</sup> A robust whistleblowing policy that is supported and implemented by an effective whistleblowing program will be particularly critical for companies given the changes to whistleblower protections laws passed by the Federal Parliament in February 2019 which expand the existing protections and remedies available to whistleblowers (refer to changes to whistleblower protection laws below).

## Changes to whistleblower protections laws

In February 2019 the Federal Government passed a Bill to strengthen Australia's whistleblower protection laws. The laws are the first major update of Australia's whistleblowing protections in nearly two decades, and impact almost every Australian business. The Bill has amended both the corporate and taxation laws to put in place a comprehensive series of safeguards for those individuals who disclose corporate or taxpayer misconduct. The new protections include:

- the ability for whistleblowers to make anonymous disclosures, and have their identity protected (including fines for revealing a whistleblower's identity without consent)
- an increased pool of potential whistleblowers will be eligible for protection (including former employees)
- a wide scope of disclosable matters, including information concerning "misconduct or an improper state of affairs"
- the ability for whistleblowers to disclose the information to a member of parliament or a journalist if no action is taken in response to a disclosure to a regulatory body and
- mandatory whistleblower policies for public companies, large proprietary companies and proprietary companies that are trustees of registrable superannuation entities.

<sup>375</sup> Corporations Act 2001, Part 9.4AAA.

<sup>376</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4rd edition, 2019, Box 3.3.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## BOARDROOM DYNAMICS

Board culture underpins board dynamics and has a decisive influence on performance. A well-functioning board generally displays coherence, trust and common values between members, encourages and has regard to differing viewpoints and opinions, and is able to reach a decision without animosity.<sup>377</sup> Healthy boardroom dynamics will encourage sound decision-making that delivers value to shareholders.

The working relationship between directors and management is one of the most influential factors in board effectiveness. Most productive relationships are built on mutual trust and respect, where both the board (and the chairman in particular) and the CEO work in partnership, each with an acute appreciation of the vital role played by each other in building shareholder value. Dysfunction can occur where either the chairman or the CEO is overly controlling and this behaviour goes unchecked.

## INFORMAL COMMUNICATIONS OUTSIDE BOARD MEETINGS

Informal communication is one of the most effective ways of sharing information, building knowledge and fostering constructive working relationships. For this reason, boards that communicate regularly, when necessary, with each other and management, are typically strong decision-makers.

## TRENDS

## Utilising independent measurement to understand culture

Internal audit and other external service providers also have a critical role to play in understanding and reporting on the human factors that impact on the processes, risks and controls in an organisation. As part of internal audits, organisations are now receiving reports on the cultural aspects of the internal audit engagements undertaken using a mixture of auditing techniques such as interviews, observations, surveys, data and documents analysis.

KPMG Internal Audit for example, can help to improve the internal audit quality by incorporating behavioural controls into a company's internal audit approach and reporting on behavioural controls findings and recommendations. We do this by using a mixture of auditing techniques noted above, as well as utilising a mixture of experts having a diverse educational background, for example psychology, sociology and business studies. Our internal audit reports are fact-based, specific and future oriented.

Learn more about KPMG's [model](#) for understanding cultural drivers or read our [Cultural drivers in Audit and Assurance factsheet](#).

## Incentive systems

Remuneration is also a key driver of culture, thus, having the right incentive systems is another important consideration for the board.<sup>378</sup> This includes the recruitment, performance management, remuneration and promotion systems that should not only reward good business performance but also take into account adherence (and non-adherence) to the company's culture and behavioural standards.

<sup>377</sup> Australian Government: Corporations and Markets Advisory Committee: Diversity on Boards of Directors, March 2009.

<sup>378</sup> Commissioner Hayne in the Interim Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry 28 September 2018, Volume 1, at page 5.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

This should avoid incentivising short-term business performance at the expense of the interests of stakeholders and the safety and soundness of the organisation. Companies should also establish clear and appropriate consequences, articulated and applied for staff found to be engaging in any undesirable or unacceptable behaviours.

Revised commentary in the ASX Principles and Recommendations makes clear that when determining appropriate remuneration structures, consideration should not only be given to incentivising executives and directors to pursue the growth and success of the organisation, but also to the need to ensure that incentives do not reward *“conduct that is contrary to the entity’s values or risk appetite”*.<sup>379</sup> In addition, consideration should be given to the implications of being perceived by the community to be paying excessively.<sup>380</sup>

## Useful references

- ASIC Regulatory Guide 73, Continuous Disclosure Obligations: Infringement Notices, Reissued 31 October 2017, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-73-continuous-disclosure-obligations-infringement-notice/>
- APRA Risk Culture Information Paper, October 2016, <https://www.apra.gov.au/sites/default/files/161018-information-paper-risk-culture1.pdf>
- Australian Prudential Regulation Authority, Prudential Inquiry into the Commonwealth Bank of Australia, 30 April 2018. Available at [https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry\\_Final-Report\\_30042018.pdf](https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf)
- ASX, ASX IR Intelligence, – [http://www.asx.com.au/documents/professionals/asx\\_ir\\_intelligence\\_brochure.pdf](http://www.asx.com.au/documents/professionals/asx_ir_intelligence_brochure.pdf)

<sup>379</sup> ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Recommendation 8.1. 2019.

<sup>380</sup> Ibid

- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.
- ASX Listing Rules, <http://www.asx.com.au/regulation/rules/asx-listing-rules.html>
- Australasian Investor Relations Association website, [www.aira.org.au](http://www.aira.org.au)
- Corporations Act 2001 (Cth).
- IIRC Discussion Paper, Towards Integrated Reporting – Communicating Value in the 21st Century, September 2011, [https://www.integratedreporting.org/wp-content/uploads/2011/09/IR-Discussion-Paper-2011\\_spreads.pdf](https://www.integratedreporting.org/wp-content/uploads/2011/09/IR-Discussion-Paper-2011_spreads.pdf)
- APRA Information Paper, Transforming governance, culture, remuneration and accountability: APRA’s approach – 19 November 2019
- Unlocking the upside of conduct risk, KPMG <https://home.kpmg/au/en/home/topics/conduct.html>

## For further information please contact:



**Alex Ong**

**Director, Compliance and Conduct**  
**ongalex@kpmg.com.au**



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 22. Cyber Security

Cyber security continues to be a strategic risk for all organisations and a topic for discussion at board-level with major incidents increasingly commonplace across a range of industries.

## In this chapter

- Introduction
- The rise of ransomware
- Regulatory changes in response to cyber security risks
- Cyber risk management
- What should a board consider?
- Cyber strategy aligns with business strategy
- Roles and responsibilities for cyber security have been defined and communicated
- The security model is comprehensive
- Security and privacy aligned
- Cyber security and data privacy in business continuity plans
- Critical success factors

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. How does the board maintain awareness of the cyber security threats and risks and how they affect the organisation?
2. Are the board aware of the organisation's critical processes and systems (assets)?
3. Does the organisation have a cyber security programme to meet the challenges of today's (and tomorrow's) cyber threat landscape?
4. Is cyber security discussed at board-level? If so, what key risk indicators are considered and how does the board support effective risk management in this area?
5. Has the board agreed their cyber risk appetite for the company? Does the board understand the key cyber security risks that have been accepted by the executives and whether this is within the board's stated cyber risk appetite?
6. Are cyber security aspects considered in major business decisions, such as mergers and acquisitions, partnerships, new product launches?
7. Is there an ongoing, organisation-wide awareness and training program established around cyber security?
8. Are the board confident that the organisation will know if it has been breached? What makes the board certain that it will find out in the right time frame?
9. How quickly can the organisation restore its critical processes and systems after they have been taken out in case of a large-scale cyber-attack? And how long can the company survive without its critical processes and systems?
10. Does the board have the right cyber expertise to fulfill its accountabilities?
11. Does management have a ransomware response plan? Do we have a board-approved policy on ransom payments?
12. Where are we in terms of our key regulatory obligations, related to cyber? Do we have a calendar of obligations? Do we have a defined process to report these, with adequate oversight and counterbalance?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Cyber security is not on the board or sub-committee agenda.
- Cyber risk is not specifically included in assessing business and operational risk.
- Cyber risk appetite has not been set and we do not understand how much we are spending on cyber security and whether this is enough.
- Specific accountability for cyber risk management / treatment, planning, and reporting is not defined.
- Organisational strategy and planning does not consider cyber security in the ever changing digital landscape.
- Cyber incident response simulations have not been conducted with executives, management and board members.
- Management has not tested in the last year whether critical processes and systems can be recovered in time after being taken out after a cyber incident.
- Our board has not set a cyber security strategy or approved any security policies.
- Our controls are not consistently applied across the on-premise and cloud environments and thus we may potentially be in breach of our key regulatory obligations.
- The board not being timely informed in case of material cyber security breaches.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## INTRODUCTION

Board level awareness of current and emerging cyber risks, and boards having a direct involvement in cyber security decision-making, is critical for the ongoing cyber resilience of an organisation. It is important that directors are proactive and focused on mitigating cyber risk. Boards have woken up to the call that they must address cyber security issues on their front lines, as it is not just an IT issue.

Cyber risks are an enterprise-wide risk management issue that could impact the entire business and indeed the extended ecosystem of suppliers, partners and customers. Senior leaders understand that getting cyber security right and managing the risk effectively can create a strategic advantage. However, to achieve long term success, strategic decision-making and the management of cyber risk must start in the boardroom.

Cyber criminals have become smarter, better organised, more resourceful and well-motivated. Since the pandemic, the increase in cyber security attacks have increased ten-fold as remote working has heightened the vulnerability of organisations to cyber threats. KPMG's 2020 Global CIO survey found 41% of surveyed organisations have experienced additional cyber security incidents, mainly from targeted spear phishing aimed at key personnel and large scale malware attacks since the pandemic began.<sup>381</sup> This has caused the demand for highly skilled cyber security experts to rise exponentially to address the growth in risk from cyber criminals.

As the graphic below illustrates, it is worth noting that not all cyber threats are external and the threat from insider action (human error) accounts for one third of all data breaches in Australia,<sup>382</sup> which can have a severe impact on reputation and service delivery.

For a number of years, boards have required cyber security to become a top investment priority. However, KPMG's experience is that although there is some fatigue around the issue, there is still a cyber security knowledge gap at many boards. Specifically, smaller and medium sized organisations typically still have a skills gap when compared with the major organisations.



<sup>381</sup> KPMG, 2021, Strengthening Australia's cyber security regulations and incentives, <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/australia-cyber-security-challenges-opportunities-kpmg-submission.pdf>

<sup>382</sup> Refer to Office of the Australian Information Commissioner, 2021, Notifiable Data Breaches Report: January – June 2021, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## THE RISE OF RANSOMWARE

There has never been a catalyst for technological and digital change like COVID-19. Since the start of the pandemic, cyber criminals around the world have capitalised on this disruption. They have further industrialised the scale at which they can launch attacks. At the top of the list, offering cyber criminals quick returns, is ransomware.

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. When ransomware attacks are successful, the costs can be substantial. Tangible costs include loss of revenue while systems are down, the cost of remediation and customer compensation or litigation. Intangible costs are harder to measure but may include diversion of staff resources and loss of reputation. In the worst cases, it could have even more impact long-term if trust is damaged.

The rising threat of ransomware is best dealt using a two-pronged approach; a pro-active approach to prepare defences for an attack and a re-active approach to respond quickly to an attack:

- **Pro-active methods** include assessing cyber-hygiene controls, ensuring backups and restoration controls are operating effectively, vulnerabilities are identified and remediated, training and awareness and developing a comprehensive incident response plan.
- **Re-active methods** include ensuring incident response is quick and adequate, communications and PR strategy is identified and quickly executed, forensic investigations, cyber-insurance and a clear legal advice.

Despite preparation, there could be situations where an organisation is faced with an existential question of whether to pay or not to pay a ransom. The Australian Cyber Security Centre (ACSC) strongly discourages paying a ransom to criminal actors, as does the UK and the US governments. Paying the ransom also does not guarantee that a victim's files will be recovered, or can be recovered in a timely manner.

While there are advantages and disadvantages of having a legislated ban on ransom payments and while the options are evaluated, the threat of ransomware still exists. Thus, it is critical for the Board and the industry/market in general to establish a viewpoint and adopt a position on the ransom payments.

## REGULATORY CHANGES IN RESPONSE TO CYBER SECURITY RISKS

Threats to the secure and effective performance of Australia's infrastructure are ever evolving – be it physical or logical. As we have seen above, cyber threats can surface internally, externally and emerge from aggressive or criminal activity, foreign powers, and terrorists amongst others.

The Australian Cyber Security Centre (ACSC) found that around one quarter of cyber security incidents reported in the 2020–21 financial year affected entities associated with Australia's critical infrastructure. The Australian Security Intelligence Organisation (ASIO), in its annual report 2020-21, has outlined that increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities which, if targeted, could result in significant consequences for our economy, security and sovereignty. In this ever-evolving cyber-threat landscape, the Australian government and regulators continue to encourage organisations to strengthen their defences.

For example, in 2018/2019, the Australian Prudential Regulation Authority (APRA) introduced the Consolidating Prudential Standard (CPS) 234 for APRA regulated entities (e.g. financial services organisations) focused on information security management, followed by announcing the requirements around independent reviews for CPS 234 in 2020.

Further, the Australian Government, in April 2022, amended the Security of Critical Infrastructure Act 2018 (SOCI Act), introducing a framework for Risk management programs; Systems of National Significance, including Enhanced Cyber Security Obligations. All of this emphasizes the need to manage risks associated with cyber security holistically and for improved governance throughout the ecosystem.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Both are covered below.

**APRA Prudential Standard (CPS) 234**

The introduction of APRA's CPS 234 in 2018, followed by its enforcement in 2019, has been a corner stone in the financial services cyber regulatory landscape. The standard outlines requirements across nine domains:

1. Roles/Responsibilities
2. Information Security Capability
3. Policy Framework
4. Information Asset Identification and Classification
5. Control Implementation
6. Control Effectiveness Testing
7. Internal Audit
8. Incident Management
9. APRA notification.

A Prudential Practice Guide (PPG) CPG 234 complements the standard.

The standards were further strengthened by a one-off tri-partite review announced in 2020, followed by pilot tri-partite reviews in 2021. APRA has specifically outlined that it *“expects boards to have the same level of confidence in reviewing and challenging information security issues as they do when governing other business issues.”*

APRA's CPS 234 applies to all 'APRA regulated entities' defined as:

- a. Authorised deposit-taking institutions (ADIs), including foreign ADIs, and non-operating holding organisations authorised under the Banking Act
- b. General insurers, non-operating holding organisations authorised under the Insurance Act

- c. Life organisations, including friendly societies, eligible foreign life insurance organisations (EFLICs) and non-operating holding organisations registered under the Life Insurance Act
- d. Private health insurers and
- e. Registerable superannuation entities (RSE) under the Superannuation Industry (Supervision) Act.

The key objective is to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. Further, to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.

**What does CPS 234 mean for directors?**

1. The Board is now accountable for information security and cyber incidents. Which means that, the Board must ensure that the security capability is appropriate for the organisation and its risks. If not, identify the gaps and develop and implement a remediation plan.
2. For information assets managed by a related party or third party, the APRA-regulated entity, must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.
3. All information assets must be classified by criticality and sensitivity including those managed by third parties.
4. Appoint subject matter experts as part of internal audit to provide information security specific assurance.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

5. Establish an appropriate, structured, and a comprehensive information security controls testing program to test the effectiveness. Further, report any gaps that cannot be remediated in a timely manner.
6. Notify APRA of information security incidents within 72 hours and material information security control weaknesses which cannot be remediated in a timely manner within 10 business days.

**Australia's Security of Critical Infrastructure Act**

The *Security of Critical Infrastructure Act 2018* (SOCI Act) seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in organisations that make up Australia's critical infrastructure.

The SOCI Act was first passed into law on 28 March 2018. Two bills have since been passed to amend the SOCI Act. The first Bill, *Security Legislation Amendment (Critical Infrastructure) Bill 2021* (SLACI Bill), is part of the Department of Home Affairs "Protecting Critical Infrastructure and Systems of National Significance" reforms and was passed into law on 2 December 2021. The second Bill, *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill) was passed into law on 31 March 2022.

The SOCI Act and its amendments apply to organisations operating in eleven broadly defined critical industries including: 1 - communications, 2 - data storage or processing, 3 - financial services, 4 - water and sewerage, 5 - energy, 6 - healthcare, 7 - higher education and research, 8 - food and grocery, 9 - transport, 10 - space technology, and 11 - defence sectors.

The SOCI Act is designed to progress Australia's critical infrastructure to be more resilient and secure, and to provide the government assurance of the resilience and security of Australia's critical infrastructure services management. The SOCI Act ensures the Government has access to information necessary to conduct risk assessments and the power to enforce mitigations if they are not implemented through collaboration. It is the Government's intention to continue to work with critical infrastructure owners and operators through a business-government partnership approach.

**What does the SOCI Act mean for directors?**

1. Boards should require executives to determine whether the organisation is in scope of SOCI Act. And if so, provide ownership and operational information to the register of critical assets operated by Department of Home Affairs
2. Boards needs to understand that mandatory reporting of cyber incidents is required to the Australian Signals Directorate's Australian Cyber Security Centre within applicable timeframes (either under 12 hours in case of cyber security incidents with significant impact, or under 72 hours for all other incidents).
3. In the event of a serious cyber security incident, the SOCI Act introduces extensive government powers in responding to cyber security incidents, ranging from information gathering, to directing actions and intervention requests.
4. Under the second Act, organisations are required to Develop a Risk Management Plan and:
  - Identify core organisational assets - information, personnel, physical facilities and critical suppliers
  - Develop context and risk identification processes
  - Identify hazards and risks applicable to your business assets
  - Clarify which risks are material risks, and their relevant impact on your organisation
5. Organisations are to comply with Sector-Specific Rules and boards should:
  - Understand requirements of the rules for their specific business
  - Identify activities required to comply with the rules (gap analysis) to mitigate risks
6. The board will be required to sign-off on the organisation's risk management program and compliance with the rules through an annual attestation within 30 days of EOFY. The Department of Home Affairs will be the regulator for most sectors and monitor compliance

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

## CYBER RISK MANAGEMENT

To effectively manage cyber security risks (as portrayed in the image below), an organisation's people, processes and technology must work in partnership towards the same objectives. Cyber risk management is a fundamental component of governance and must be integrated with supporting activities enterprise wide. This cannot be left solely to the technical specialists in IT and cannot be addressed in isolation. It is important that the Chief Information Security Officer (CISO), or equivalent, is an effective communicator to be able to work with the board to embed cyber security into an organisation's operating model.

It is critical that boards continue to drive a robust approach to managing cyber risk to reduce volatility and uncertainty. A robust cyber security assessment should focus on "cyber security leadership, governance, people risks, legal and regulatory compliance, business continuity plans, the organisation's operating model, technology and information risks". All organisations should periodically review their cyber security risk assessments to prevent, detect, contain and respond to threats to their critical processes and systems.



Source: KPMG



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## WHAT SHOULD A BOARD CONSIDER?

For many businesses, cyber security is an issue that is now regularly incorporated into board-level decision making. According to KPMG's 2021 Global CEO Outlook Pulse Survey, 59% of Australian CEOs plan to invest more in data security measures compared to a year ago. In addition, the top three risks to growth in the next three years were cyber (22%), regulatory (20%) and supply chain (12%).<sup>383</sup>

Boards are increasingly getting to grips with the risks that cyber threats pose to their business, both strategically and operationally. KPMG's experience is that boards frequently raise the need for more cyber security skills and experience in the boardroom. Despite this, we note that many boards do not have a clear understanding what their cyber risk appetite is and whether the company is spending enough money on cyber security and in the right areas.

Boards with the support of their sub-committees should continue to evaluate and coordinate the delegation of oversight for cyber security. KPMG's experience is that many audit committees continue to oversee cyber security and data privacy. However, as cyber risks becoming increasingly complex, it is important boards consider whether these risks require more attention at board-level or potentially in a sub-committee dedicated to IT, cyber and data governance. The addition of a sub-committee depends on the size and nature of the organisation as well as whether there is the right mix of skills and experience on the board, and sub-committees, to have robust conversations with management on cyber risks, and whether the organisation is doing enough.<sup>384</sup> This will improve reporting and discussions at board-level about cyber security.

<sup>383</sup> KPMG, 2021, Strengthening Australia's cyber security regulations and incentives, <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/australia-cyber-security-challenges-opportunities-kpmg-submission.pdf>

<sup>384</sup> KPMG, 2021, Oversight of cybersecurity and data governance, <https://assets.kpmg/content/dam/kpmg/uk/pdf/2021/07/oversight-of-cybersecurity-and-data-governance.pdf>

While board members are aware of the personal cyber risks they face alongside the corporate threat, it is important that they have a full understanding of the dangers as these evolve. Directors who have received no cyber risk training and participated in a cyber attack simulation over the past 12 months should be encouraged to sign up for support in the year ahead.

## CYBER STRATEGY ALIGNS WITH BUSINESS STRATEGY

Cyber security must be an enabler to the overarching business strategy and must consider what the business wants to achieve and by when. Security cannot be so restrictive that it hinders innovation and service delivery, and it must be proportionate to the risk(s) that the business faces. A good cyber security strategy will have clear linkages to an organisation's vision, objectives and innovation projects and businesses will have determined appropriate levels of acceptable risk.

Too often efforts to manage cyber related risks are not coherent with the overall business strategy. Many organisations fail to ask themselves "What are we trying to achieve as a business, and what are the cyber threats to those objectives that we need to counter?"

Cyber risk is an important strategic concern for boards of directors. Its true nature is dependent upon external threat factors, as well as the industry sector, business activities and corporate objectives.

A clear linkage between business objectives, the threats to those objectives, risk appetite and the enabling security capabilities to counter the threats, makes the investment decision easier and it becomes a more straightforward balance between Return on Investment (ROI) and residual risk.

Without a clear strategy and roadmap, people look for the latest, greatest thing being promoted in the market. Organisations end up focusing disproportionate resources into the implementation of expensive technology solutions – viewing them as some kind of universal panacea for any security fears – rather than emphasising skills and awareness or focusing on targeted security investments to enable business change.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## ROLES AND RESPONSIBILITIES FOR CYBER SECURITY HAVE BEEN DEFINED AND COMMUNICATED

Making it clear who is accountable for any type of risk or action is a crucial element of good governance. Organisations may assign senior responsibility for cyber risks to the Chief Financial Officer (CFO), the Chief Executive Officer (CEO), the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). Clear cut accountability is essential for effective cyber risk management but remember that final accountability always remains with the board.

People are crucial to the successful implementation of behaviours and controls that protect information and assets. A well thought-out, routine and up to date programme for training and awareness activities that covers employment from onboarding to termination is critical to preventing cyber-attacks and data breaches.

Reality shows that cyber security is very much driven by compliance. This is understandable, because many organisations have to accommodate a range of laws and legislation. However, it is counterproductive to view compliance as the ultimate goal of cyber security policy. Only an organisation that is capable of understanding external developments and incident trends, and using this insight to inform strategy and policy, will be successful in combating cyber-crime in the long term. Hence, it is important that all roles and responsibilities are communicated across the whole of the organisation and all employees receive regular cyber training. Regular training will allow all staff to understand and look out for the risks and threats that can impact their day-to-day activities.

## THE SECURITY MODEL IS COMPREHENSIVE

Controls and processes must cover all areas of cyber security and be designed and implemented to manage specific risks. There are various security models that organisations can use to align and map cyber practices against recognised industry standards. These

frameworks range from the Australian Cyber Security Centre's Essential Eight Maturity Model to comprehensive frameworks such as ISO/IEC 27001 Information Security Management and the United States National Institute of Science and Technology (NIST) Cyber security Framework.

The Australian Government's Australian Cyber Security Centre (ACSC) released the "Essential Eight" in 2017 and has been updating this regularly. It provides baseline mitigation strategies which are intended to make "it much harder for adversaries to compromise systems". These are as follows and a maturity model is available to understand the level of maturity against each strategy:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

The comprehensive NIST's Cyber Security Framework is shown below.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

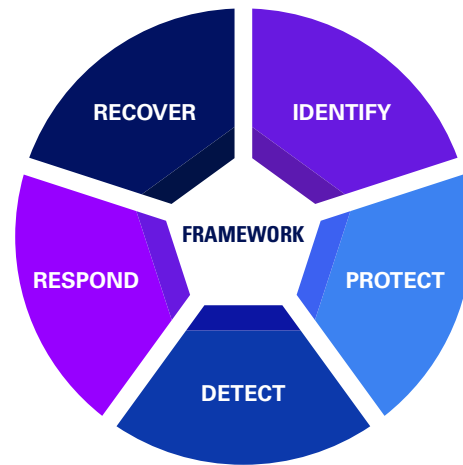
GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US



NIST Cyber Security Framework				
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Source: NIST Cyber security framework – Five key functions and 22 Categories of cyber controls

The framework enables organisations to plan, build, operate and maintain a model that is relevant and fit for purpose. The model must be built according to unique organisational needs, such as where an organisation operates, who its customers are, the threats it has for cyber security, as well as legal and regulatory requirements for security and data privacy.

SECURITY AND PRIVACY ALIGNED

The pandemic saw businesses pivot to alternative, digital strategies and supply chain adjustments to keep businesses continuing to operate without major disruption. Boards began to step up their oversight of cyber security and data privacy practices, which put both of these topics into the spotlight. Cyber security and data privacy were cited by directors as the most relevant governance issues to their corporate strategy in 2021. Data governance is often noted as overlapping with cyber security. However, data governance includes compliance with privacy legislation and regulation and how businesses legally process, store and use personal data. Wider stakeholders are paying greater attention to how their data is used, which can pose a significant reputational risk for an organisation. Hence, cyber security and privacy need to be handled carefully and in unison.

Boards should ensure an organisation has a robust data governance framework in place, as well as a cyber security framework to improve transparency on what data is being collected, stored and used. Through a board's sub-committee structure, data governance should be appropriately delegated to a committee, usually the Audit committee, to maintain effective oversight and identify critical risks and related controls to an organisation's data privacy, as well as cyber security.

Suspected Data Breach

Under the Notifiable Data Breach Scheme (NDB) any organisation or agency covered by the 1988 Privacy Act must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person

The notification to individuals must include recommendations about the steps an organisation should take in response to the data breach. NDBs and Privacy requirements more broadly are discussed in further detail in Chapter 23 Data Privacy and Personal Information.

## CYBER SECURITY AND DATA PRIVACY IN BUSINESS CONTINUITY PLANS

No two organisations are the same, therefore, there is no 'one-size-fits-all' business resiliency plan. Despite cyber incidents being complex and not always having the same attributes, incident management is a critical component of an overall cyber risk program and the effectiveness of an incident response plan. It is important to have a business continuity plan that tests cyber security and data privacy responses under different scenarios that are regularly reviewed, at least annually, to reflect changes in the external environment.

In addition, organisations should clarify which business leaders are accountable for business continuity and decision-making if an incident were to occur. This is particularly important if an incident involves third parties who have to be notified promptly.

## CRITICAL SUCCESS FACTORS

- The roles of directors and the board in overseeing cyber security and cyber incident responses are clearly defined and documented.
- Accountabilities and reporting lines for cyber security management are clearly defined and well understood.
- There is regular enterprise-wide cyber risk communication.
- There is a comprehensive awareness framework that focuses on effective communication throughout the organisation.
- The organisation is addressing the key issues and ensuring staff at all levels are receiving clear and relevant messages about cyber security and data privacy.
- The key issues and concerns around cyber security are clearly communicated in meetings and in communication from management.
- The board (and sub-committees) receive the right reports, such as a cyber security scorecard to effectively manage cyber security risks.
- An organisation is transparent in informing its stakeholders about cyber security risks and privacy concerns, including how data is used and stored.
- Cyber security and data privacy are included in business continuity plans and take into consideration security for the Cloud.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful References

- Federal Communications Commission (USA), Cyber Security Planning Guide <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- KPMG, Empowering Your business strategy with Cyber Security: <https://home.kpmg/gr/en/home/services/advisory/risk-consulting/it-advisory-services/cyber/empowering-business-strategy-with-cybersecurity.html>
- KPMG, Cyber security considerations 2022, <https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/11/cyber-security-considerations-2022.pdf>
- KPMG, 2019, Cyber Security in Telco, <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/global-perspectives-in-cyber-security-telco-au-march-2019.pdf>
- KPMG, 2018, Digital Supply Chain – the hype and the risks <https://assets.kpmg/content/dam/kpmg/au/pdf/2018/digital-supply-chain-hype-and-risks.pdf>
- KPMG, COVID-19: Restarting business – with security in mind <https://home.kpmg/xx/en/home/insights/2020/06/restarting-business-with-security-in-mind.html>
- KPMG, Critical Infrastructure reforms <https://home.kpmg/au/en/home/topics/critical-infrastructure-reforms.html>
- Cyber and Infrastructure Security Centre, <https://www.cisc.gov.au/resources-and-contact-information/resources>
- Australian Cyber Security Centre 2021, ACSC Annual Cyber Threat Report 1 July 2020 to 30 June 2021, p. 10.
- Australian Prudential Regulation Authority, <https://www.apra.gov.au/news-and-publications/improving-cyber-resilience-role-boards-have-to-play>
- Australian Prudential Regulation Authority, <https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services>
- Australian Prudential Regulation Authority, 2019, [https://www.apra.gov.au/sites/default/files/cps\\_234\\_july\\_2019\\_for\\_public\\_release.pdf](https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf)
- Australian Prudential Regulation Authority, 2019, [https://www.apra.gov.au/sites/default/files/cpg\\_234\\_information\\_security\\_june\\_2019\\_0.pdf](https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf)
- KPMG, 2021, The changing shape of ransomware, <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/the-changing-shape-of-ransomware-au.pdf>
- KPMG, 2021, Oversight of cybersecurity and data governance, <https://assets.kpmg/content/dam/kpmg/uk/pdf/2021/07/oversight-of-cybersecurity-and-data-governance.pdf>
- Harvard Law School Forum on Corporate Governance, April 2022, SEC Proposes Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Rules <https://corpgov.law.harvard.edu/2022/04/12/sec-proposes-cybersecurity-risk-management-strategy-governance-and-incident-disclosure-rules/#1>
- KPMG Board leadership Centre, 2021, Views from the boardroom: 2021 pulse survey, [https://boardleadership.kpmg.us/relevant-topics/articles/2021/view-from-the-boardroom-2021-pulse-survey.html?utm\\_source=tlpdf&utm\\_medium=referral&mid=m-00002771&utm\\_campaign=c-00105103&cid=c-00105103](https://boardleadership.kpmg.us/relevant-topics/articles/2021/view-from-the-boardroom-2021-pulse-survey.html?utm_source=tlpdf&utm_medium=referral&mid=m-00002771&utm_campaign=c-00105103&cid=c-00105103)
- Australian Cyber Security Centre, Essential Eight, <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>

## For further information please contact:



**Martijn Verbree**  
 Partner, Technology Risk  
 & Cyber Security  
 mverbree@kpmg.com.au

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 23. Data Privacy and Personal Information

Privacy legislation in Australia and around the world continues to evolve and strengthen, bringing data governance and the management of personal information to the forefront of many board agendas. The Australian privacy legislative environment is expected to further tighten, with the *Privacy Act 1988* (Cth) (the Privacy Act) currently undergoing significant reform in attempt to bring Australian more in line with overseas jurisdictions.

## In this chapter

- Privacy in Australia
- International Privacy regulation and the impact on Australian organisations
- How do organisations manage privacy risks?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. What privacy regulations are applicable to the organisation (important to check international jurisdictions and local state laws)?
2. What are the data privacy risks faced by the organisation?
3. Does management have a clear understanding of the information lifecycle, from collection, through to use, disclosure, retention and destruction?
4. Is the organisation adequately prepared to deal with a data breach involving personal information? Does it have the ability to quickly identify and manage data breaches?
5. What training and awareness activities are being undertaken to ensure staff throughout the organisation are aware of applicable privacy compliance obligations and risks?
6. Does the organisation have appropriate controls in place to help assess and manage privacy risks arising from organisational change or projects (e.g. conducting privacy impact assessments)?
7. Does the organisation understand and appropriately manage the privacy risks associated with engaging with third party vendors?
8. Does the board or relevant committee receive appropriate oversight on privacy / data governance, controls and incident/complaint reporting?
9. How is the organisation preparing for the upcoming Australian privacy regulatory reforms?
10. COVID-19 has led to an accelerated digitally connected economy – how is the organisation further prioritising privacy?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Privacy is not on the boardroom agenda.
- Privacy / data risk is not specifically included in assessing business and operational risk.
- Accountability for privacy or data governance is unclear and/or undefined.
- The organisation does not have a data breach response plan with clear actions and accountabilities.
- Projects involving the use of customer or other personal information are not considering privacy risks.
- The organisation does not adopt a 'privacy by design' approach within its operations.
- Personal information is not destroyed or disposed of when it is no longer needed for the purpose it was collected for, or it is not being retained in accordance with applicable retention laws.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## PRIVACY IN AUSTRALIA

Australia's privacy landscape includes a complex arrangement of Federal, State and Territory laws, with additional laws applying to some sectors, such as health and telecommunications. A Notifiable Data Breach (NDB) scheme requires reporting serious data breaches to Australian privacy regulator, the Office of the Australian Information Commissioner (OAIC).

The Privacy Act underwent major reform in 2014 (with the introduction of the Australian Privacy Principles (APPs) and the comprehensive credit reporting regime) and again in 2018 (with the introduction of the NDB scheme). Since then, the role of technology and data in the economy and the international flows of data in society have continued to change and accelerate.

The proposed changes to the Privacy Act are based on overseas regulations such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). While amending legislation is yet to be released, if the proposed changes are passed it will represent a significant reshaping of privacy laws in Australia.

### An overview of the Privacy Act

In Australia, the Privacy Act governs how applicable organisations must handle personal information. The Privacy Act applies to private sector organisations with a turnover of more than \$3 million, as well as most Commonwealth Government Agencies.

The Act includes a number of components, including the 13 Australian Privacy Principles (APPs) that are used to govern most organisations, as well as some specific regulations for organisations involved in credit reporting, health and medical research and the use of tax file numbers.

### The Australian Privacy Principles

The APPs are the heart of Australia's privacy regulatory framework and establish the governance standards, rights and obligations for APP entities relating to:

- collection, use and disclosure of personal information
- accountability and governance
- integrity of personal information
- right for individuals to access their personal information (which organisations must facilitate).

As principle-based legislation, the APPs incorporate little in the way of proscriptive regulatory requirements. APP entities are, therefore, left with a degree of flexibility in determining the best way to meet and uphold the requirements established by the 13 APPs.

The APPs are also technology neutral, meaning that the principles apply equally to information collected and stored on an organisation's Customer Relationship Management software, as information recorded as handwritten notes and stored in an employee's desk drawer.

### Mandatory Data Breach Notification Requirements

In addition to the APPs, Australian Privacy legislation also incorporates mandatory data breach notification obligations. This legislation is known as the NDB scheme and applies to all APP entities. The NDB scheme requires regulated entities to notify particular individuals and the OAIC of all eligible data breaches.

An eligible data breach is a breach that is likely to result in serious harm to any of the individuals to which the information in the data breach relates. This requires three criteria to be met:

1. Unauthorised access, disclosure or loss of personal information
2. That is likely to result in serious harm to one or more individuals and
3. Remedial action has not been able to prevent the likely risk of serious harm.

Accordingly, not all data breaches are notifiable. This highlights the importance for organisations to have clearly established mechanisms in place to quickly identify potentially notifiable data breaches.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

If organisations can quickly identify, assess and remediate data breaches, serious harm to individuals may be avoided, thereby removing the requirement to notify and be subject to the negative publicity and regulatory scrutiny that may follow.

**Insights from Notifiable Data Breach Reporting**

The OAIC releases regular statistics on the leading causes of notifiable data breaches. This information is a valuable resource for organisations as it highlights common issues or mistakes made by organisations, thereby providing insight into where organisations may require strengthening.

In the first year of the NDB Scheme, the OAIC received 964 notifications, which represented a 712 percent increase in notifications from prior to the introduction of the scheme.<sup>385</sup> While most data breaches were attributable to malicious or criminal attacks, data breaches arising from simple human error ranked alarmingly high (35 percent). These types of breaches were attributable to simple mistakes, such as the loss of unsecured storage devices or sending personal information via email to the wrong recipient.

This highlights the fact that good privacy management necessarily involves more than just cyber security, and the importance of preventative controls like the provision of training and awareness for all staff, particularly those in high-risk roles.

**Consumer Data Right**

The Australian Consumer Data Right (CDR) regime commenced in July 2020, with the aim providing consumers with greater access to and control over their data along with improving consumers' ability to compare and switch between products and services. The CDR enables more competition between service providers, leading not only to better prices for customers but also more innovative products and services.

<sup>385</sup> Refer to Office of the Australian Information Commissioner, 2019, Notifiable Data Breaches scheme 12-month insights report, <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/>

The CDR endeavours to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to access particular data in a usable form and to direct a business to securely transfer that data to an accredited data recipient.

Under the regime, "CDR consumers" (both individuals and businesses) are given a right to access, and direct accredited third parties (ADRs) to access and use, information held about that consumer by a data holder.

The security and integrity of the CDR regime is maintained by 13 privacy safeguards, contained in the *Competition and Consumer Act 2010* (Cth) and supplemented by the Consumer Data Rules. These privacy safeguards set out the privacy rights and obligations for users of the scheme, including the requirement for informed consent to collect, disclose, hold or use CDR data.

The CDR was rolled out across the banking sector in 2021, with energy and telecommunications to follow soon.

**INTERNATIONAL PRIVACY REGULATION AND THE IMPACT ON AUSTRALIAN ORGANISATIONS**

Privacy regulation in jurisdictions outside of Australia are constantly changing and evolving. Most notably, the arrival of the GDPR in early 2018 represents the most significant and far-reaching privacy legislation to date.

**The European General Data Protection Regulation**

The GDPR was introduced within the European Union to create a standard approach to data privacy across all member states and is widely regarded as the most stringent and comprehensive privacy legislative regime. While some elements of the GDPR overlap with the Privacy Act, there are several key differences, including:

- right for data subjects to revoke their consent to use their personal information at any time
- more stringent requirements relating to the provision of consent

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- notification of eligible data breaches within 72 hours (instead of the 30 days allowed under the Australian NDB Scheme)
- limitations on transferring personal information to locations outside of the EU
- much higher fines and regulatory enforcement powers, including up to €20 million or up to 4 percent global turnover (whichever is higher) in certain scenarios and
- application to organisations that operate in international jurisdictions.

**Applicability of the GDPR to Australian organisations**

The GDPR is notable for its extraterritorial applicability. The GDPR can have applicability to organisations that operate outside of the EU in two situations:

1. Where data processors or controllers have an establishment within the EU.<sup>386</sup> In this scenario the GDPR will apply regardless of whether personal data is actually processed in the EU or elsewhere.
2. Where data controllers or processors are located outside of the EU, but their processing activities relate to goods or services offered to individuals within the EU or monitor the behaviour of individuals within the EU.

**Other international privacy legislation**

While the GDPR is often referred to as the most significant piece of international privacy legislation for Australian organisations, other jurisdictions are quickly reviewing and updating their regulatory schemes.

In the United States, the CCPA is the first of its kind, introducing privacy regulation with an extraterritorial application. The CCPA applies to businesses that collect personal information relating to residents of California (regardless of where the business is located). Similar to the GDPR, the CCPA establishes certain rights for residents with respect to their personal information, along with obligations for organisations to handle personal information in certain ways. Other states are also due to introduce their own privacy legislation in coming years, each of which will vary in key ways.

Closer to home, the New Zealand Privacy Commissioner is positioning the country for privacy regulation reform with a Bill likely to be implemented in early 2020. The Bill calls for key reforms to New Zealand's existing privacy legislation, including:

- mandatory reporting of data breaches
- provide the Privacy Commissioner with the power to issue compliance notices to require or prevent organisations from doing something and
- introduction of new offences and increasing fines.

<sup>386</sup> Data controllers are parties that say how and why personal data is processed. Data processors are parties that act on behalf of a data controller.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

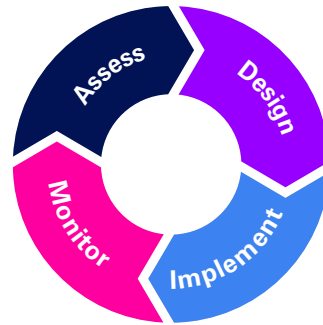
GLOSSARY

APPENDICES

CONTACT US

KPMG assists clients in complying with these complex privacy regulations through the four phases of the privacy management lifecycle: **Assess, Design, Implement, Monitor**

- Privacy maturity assessment
- Privacy audits
- Third party privacy assessments
- GDPR programme readiness
- CDR programme readiness
- Privacy management framework
- Privacy policies
- Data segregation
- Records management framework
- Privacy impact assessments



- Ongoing operations
- Privacy office support
- Incident management
- Data breach response and investigation
- Regulatory management
- Risk and obligations registers
- Data inventory
- Sensitive data finder
- Training and cultural change
- Data strategy, governance and technology innovation

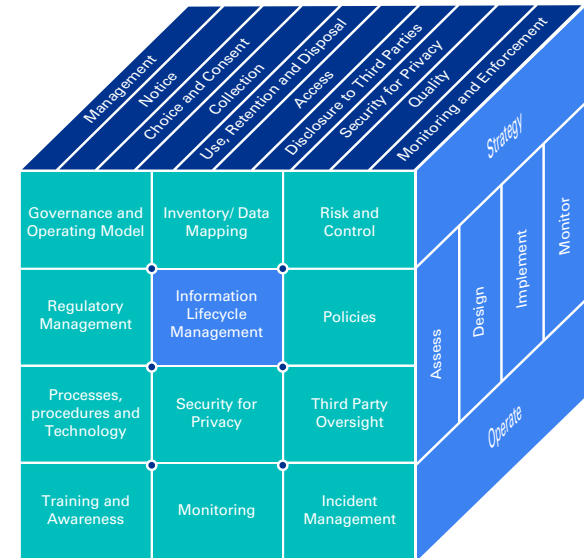
HOW DO ORGANISATIONS MANAGE PRIVACY RISKS?

Privacy risks are quickly becoming one of the most monitored risks for an organisation. Properly managing privacy risks requires a commitment and focus from staff throughout the organisation. This is due to the fact that privacy risks can surface not only from IT System failures or cyber security vulnerabilities, but also from a simple email being sent to an incorrect recipient.

KPMG Privacy Management Framework

The KPMG Privacy Management Framework is made up of 12 elements that align to the Generally Accepted Privacy Principles (GAPP) framework, which underpins most privacy legislation and regulation around the world. It offers a logical framework from which to identify, assess and manage privacy risks, and from which a range of privacy controls can be established to help manage privacy risks.

The KPMG Privacy Management Framework



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- KPMG Australia Privacy & Data Protection Services: <https://home.kpmg/au/en/home/services/advisory/risk-consulting/privacy.html>
- KPMG Data Protection Navigator: <https://home.kpmg/au/en/home/services/advisory/risk-consulting/privacy/data-protection-navigator.html>
- Global Comprehensive Privacy Law Mapping Chart: <https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/>
- OAIC Notifiable Data Breaches Report: January-June 2021: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021>
- OAIC guidance for Australian Organisations on the GDPR: <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/>
- OAIC guidance on how to respond to a data breach: <https://www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification/>

For further information please contact:



**Kelly Henney**

**Partner,  
Privacy and Data Protection  
Compliance and Conduct  
[khenney@kpmg.com.au](mailto:khenney@kpmg.com.au)**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 24. Human Rights and Modern Slavery

Human rights reporting requirements are growing around the world, and the global community of investors, governments, employees, and consumers increasingly expects enhanced human rights performance.

All organisations are exposed to human rights risks in their operations and supply chain. These are risks where people may experience or have experienced harm as a result of an organisation's decisions or practices.

Directors now have regulatory responsibilities for transparent mandatory reporting on modern slavery risks, and there is international acceptance that business has a responsibility to respect human rights.

## In this chapter

- The emergence of human rights as a business risk
- Legislation
- Challenging of managing modern slavery risks
- The role of the board
- Governance reporting and KPIs

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Is the company able to report at a group-level on behalf of all subsidiaries and across all geographies?
2. Does the board receive regular updates on changes to the structure, operations and supply chain of the company?
3. Has the board determined whether its approach to publicly releasing detailed information about its operations and supply chain is aligned with good practice?
4. Do board members understand what behaviours and practices constitute modern slavery and likely risk factors for the business and sector?
5. Has the board included modern slavery risks on its risk register?
6. Has the board established accountabilities for the identification of modern slavery risk through its committees or executive reports?
7. Has the board established KPIs for managing modern slavery risk?
8. Does the company express its commitment to protect human rights, including modern slavery, through a board approved public statement of policy?
9. Has the board introduced assurance measures for reporting on modern slavery due diligence?
10. Does the board monitor and review its human rights policies and their implementation?
11. Has the company benchmarked itself against good practices to determine its current maturity and future ambition?
12. Have the company's management systems and controls uncovered any instances of modern slavery and, if not, are they robust enough to do so?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- The company has no public commitment to respect human rights.
- There is no evidence of supply chain risk assessment or monitoring to identify human rights risks or impacts.
- There is no reporting to the board on the company's approach to responsible business.
- There are no accountabilities assigned for human rights or responsible business within the company.
- The company's risk management does not include human rights or modern slavery risk related considerations or screening criteria.
- The company has exposure to high-risk geographies, high-risk categories, risky business models or vulnerable populations.
- The company has been associated with human rights related abuses.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## THE EMERGENCE OF HUMAN RIGHTS AS A BUSINESS RISK

In 2011, the global community came together to develop the [United Nations Guiding Principles on Business and Human Rights](#), which explicitly recognise the responsibility of business to address and mitigate their human rights risks and impacts. Since the unanimous adoption of the Principles by the Human Rights Council, numerous countries around the world have enacted modern slavery reporting legislation requiring businesses to report publicly on their human rights due diligence in relation to modern slavery risk. In addition to modern slavery reporting requirements, countries have also started draft and enact mandatory human rights due diligence laws.

The global regulatory landscape now requires business to shift thinking from a traditional risk-to-business approach to an approach that puts risk-to-people at the centre of risk management efforts.

Most of the world's major businesses now have formal commitments and management approaches to respect human rights. Stakeholder expectations are elevated, with investors, shareholders, unions, regulators and civil society increasingly requiring visibility over a corporate social performance and how they are addressing the 'S' in ESG.

For example, the Corporate Human Rights Benchmark, which counts investors among its founders, rates 100 of some of the world's largest listed companies according to their publicly reported approach to human rights.

The retail and resources sectors led the corporate world's response to social risk, having been forced to respond earlier because of retail's reliance on base-skill labour and the significant impacts on communities from resource development and extraction. Now, human rights reporting requirements along with significantly increased expectations that boards will understand and manage non-financial risks is challenging other sectors to put respect for human rights on the agenda.

## LEGISLATION

In 2018, Australia introduced the *Modern Slavery Act 2018* (Cth), which requires reporting entities to publish an annual statement about what they are doing to manage the risk of modern slavery in their operations and supply chains. The Act follows the introduction of similar legislation in the UK and reflects Australia's commitment to develop regulatory frameworks to prevent the exploitation of workers globally. The Act requires entities with over \$100 million in consolidated revenue to publish an annual modern slavery statement. The board must approve the annual modern slavery statement, which is published on a central government register.

New South Wales (NSW) has also introduced modern slavery legislation, which takes effect on 1 January 2022. The NSW legislation was passed after two years of review and amendment to ensure it could effectively operate alongside the Commonwealth law. NSW Government agencies and private entities that deal with NSW Government agencies are captured by the legislation and are required to report on their actions to address modern slavery.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## A short history on business and human rights

Business impacts on human rights has been a subject of societal expectations as early as the 19<sup>th</sup> Century when the British public experienced an anti-slavery movement protesting the use of slaves in the Caribbean producing sugar for British consumption. The more recent focus on corporate accountability in this regard began in the mid-1990s, in response to significant human rights violations in the retail sector, including the use of 'sweatshop' labour and the more recent the Rana Plaza disaster in Dhaka, which led to the death of over one thousand people. In response, companies like Levi's, Nike, The Body Shop International and Ben & Jerry's established supplier codes of conduct and controls for testing conformance with those codes to mitigate labour-related risks. These global brands also started to commission supplier audits that looked at areas such as labour practices, environmental performance, and animal welfare.

As a result, there is today a body of over 30 years of work to address human rights risks and impacts in the supply chain. Despite this, and the growing responsible business expertise and services, many businesses are still immature in their management of these types of risk. For businesses more advanced in their journey, there is an increasing recognition of the need to go 'beyond compliance' to manage risks in a meaningful way that is focused on preventing harm to people. This includes adopting a collaborative approach to supplier engagement and innovative use of technology to secure and maintain trust in the supply chain.

## CHALLENGES OF MANAGING MODERN SLAVERY RISKS

In addition to driving improved business practice through transparent reporting, there is growing recognition that industry-wide and multi-stakeholder approaches are an important part of addressing the root causes of modern slavery. This is why there are a growing number of collaborative responses. Some sectors such as retail, property and mining have come together with shared responses to managing supplier platforms, and specific issues are targeted through multi-stakeholder initiatives.

Challenges that collaborative approaches seek to target:

- The complexity of global supply chains and the heavy reliance on agents makes it difficult for organisations to have clear oversight and influence over key areas of exposure.
- Traceability is challenging in the supply chain which diminishes accountability. There are more and more technology enabled traceability products and services being offered in the market to meet this challenge.
- Geo-political issues, such as mass migration, result in an increase in the supply of vulnerable low-skill labour.
- Historically there is weak understanding or engagement at senior executive and board level, due to labour practices and supply chain issues having a greater role in operational, rather than strategic, functions.
- The board has limited visibility over the entire supply chain. Additional resources and hence expenditure may be required to monitor this risk.
- Ability and time to respond to new legislation.
- Capacity and ability of staff to address impacts.
- Aligning human rights with values and culture.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Limitations of supply chain auditing

One control in managing supply chain risk is supply chain auditing. This involves setting company-specific standards or subscribing to industry or other multi-stakeholder established standards and auditing supplier performance against those standards. Suppliers and their workplaces are then subjected to a range of audits that can be conducted by the customer or by a third party. These audits typically look at the management approach to labour practices and should always involve worker interviews.

Audits can only ever be a diagnostic tool at a point in time. Successful risk management within the supply chain is not solely a point in time assessment, but rather, it ties together an organisation's human rights and supply chain touchpoints and, in the process, establishes an overall understanding of the nature of the supplier and the relationship with it. Achieving this can be a challenge when there are many tiers in the supply chain and the tendency has been to outsource supply chain risk.

Whilst the auditing of human rights practices is possible, there are high levels of audit fraud. For example, the stakes for failing an audit of human rights practices can be high, perversely creating a compelling reason to conduct audit fraud and facilitate auditor corruption. As a result, auditing should only be regarded as one potential component in a full program of human rights risk management. A meaningful response to human rights risk includes a collaborative approach to supplier engagement and capability building and is targeted to the areas of highest risk of harm to people.

## THE ROLE OF THE BOARD

The board has oversight of risk. A critical function of the board is to understand risk to people as part of non-financial risk management. Social media, increasing stakeholder and shareholder activism and scrutiny of the board's view of environmental, social and governance issues will continue to drive the need for directors to understand and take an active role in overseeing human rights risk management. Organisations are increasingly judged on their performance in non-financial risk management and performance, and it is up to directors to ensure they are proactively overseeing risk management and developing strategic responses in this context.

Specifically, with respect to modern slavery risk, the board should ensure that:

- There is a board approved human rights policy commitment.
- Behaviours and practices that constitute and facilitate modern slavery are understood across the business.
- Modern slavery risk is identified, assessed and mitigated.
- Modern slavery risk is included on the business risk register.
- Accountabilities for the identification and management of modern slavery risk through its committees or executive reports are established.
- The business is demonstrating progress in its reporting against the Australian mandatory reporting criteria.
- A risk management program is embedded within the company that:
  - addresses the areas of highest risk to people in the supply chain and operations of the business
  - details the expected values and behaviours of business personnel with respect to human rights issues
  - develops objectives and targets for improvements in risk management and its effectiveness, including relevant KPIs and metrics for reporting performance

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- creates clear standards that the company expects suppliers and business partners to meet and provides support for them to do so
- is regularly reviewed and tracked against good practice.
- Regular reports are provided to the board that monitor performance and highlight any emerging issues.
- Regular consultation with external stakeholders, included affected rights-holders, informs continuous improvement of risk management activity and business understanding of the experience and root cause of modern slavery.
- Human rights risk considerations are built into investment decision making processes.

### Presence of modern slavery in a supply chain can bring a company undone

By Richard Boele Partner, KPMG Banarra

#### Change is needed

Social compliance audits cannot be discussed without addressing the key question: what is their purpose? Are they about achieving better outcomes for workers, comfort to companies and their boards, or is it a more complex dynamic? How integrated are they in measuring company performance, both externally and internally? How many listed company directors know about their ethical sourcing programs, and the extent to which they deliver a positive social impact?

Much was said about changes to factories only coming when the focus was on what was done before and after an audit.

There are significant problems with the current situation with social compliance audits and with increasing worldwide digital connectivity – complacency is simply not an option.

During the 2019 SEDEX conference hosted by KPMG in Australia, there was a call for business to go 'beyond compliance' – a recognition that true impact will not come from audits alone.

#### What next?

It is clear that a significant section of the global ethical sourcing industry recognises that it is time to take stock. Put simply, the time has come to pause and question whether we are achieving the original intent of a social compliance audit. It may be necessary to think outside the audit box and develop new ways of thinking, with new tools and techniques. Technology has a key role to play.

The future of ethical sourcing is likely to contain audits for some time yet, however, the way audits are undertaken will need to change.

Regardless of how things change, change they must. Because without different responses to the most significant challenges in global supply chains, broader society will lose trust, and companies and their brands will be at greater risk.

## GOVERNANCE REPORTING AND KPIS

Reporting to the board on human rights and modern slavery risk in operations and the supply chain will continue to be accelerated by proliferating legislative reporting requirements.

**Meaningful reporting** will offer directors the necessary data to show that their business is appropriately identifying and managing modern slavery risks. Directors should proactively seek this information if they are not already receiving it. If they are provided with this information regularly, they should ensure that they understand the issues well enough to ask strategic questions that contribute to a cycle of continuous improvement and alignment with good practice in human rights due diligence.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

Meaningful board-level reporting on human rights, including modern slavery, includes:

- **A clear objective.** Focus on keeping the board informed risk and performance issues, and on building board capability to support strategic conversations. Regular reports should include performance measures, whilst capability building reports or sessions should be built into the board's agenda as part of the broader risk and strategy considerations.
- **Qualitative and quantitative metrics.** These include lead and lag metrics, as quantitative lag metrics alone limit the board to addressing minimum expectations only. Conversely, lead metrics can shift the board's focus to the development of broader, preventative measures. Data should measure performance, including effectiveness over time, and support strategic conversations towards continuous improvement.

Elements of good-practice board reporting include:

- a dashboard with key lead and lag indicators and exception reporting (e.g., number of critical non-conformances that are overdue for close-out)
- results of up-to-date salient issues processes to focus on those areas that strategically matter and where the risk to people is greatest
- key focus areas for improvement in the coming 12 months
- emerging human rights trends and developments relevant to the business.

For supply chain concerns, dashboard indicators could include:

- the number of new suppliers onboarded into the risk management program (this could be expressed as a percentage of the total number of new suppliers)
- the percentage of suppliers in the risk management program that have completed a self-assessment questionnaire

- the percentage of suppliers in the risk management program that have gone through a risk assessment to determine the level of human rights risk
- the percentage of suppliers in the risk management program that have a current, valid third-party ethical sourcing audit report
- the percentage of suppliers within the program that have open non-compliances waiting to be closed
- the percentage of those with open issues that are past their due date for closing non-compliances
- the number and type of supplier employee complaints or enquiries received via factory level help lines and grievance mechanisms, remembering that receiving no complaints is not usually an indicator of success
- the number, and brief description, of ethical sourcing related initiatives (involvement in industry working groups, developing tools to help suppliers deal with second tier suppliers, any country or product category with specific initiatives/partnerships).

In addition to the above quantitative indicators the report could also include:

- **Key focus areas for the next period** – a qualitative description of management responses to potential weaknesses (suggested by the dashboard report) or strategic responses to emerging trends.
- **Emerging Trends** – a description of emerging areas of relevance and challenge to business operations or supply chains.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.
- Australian Council of Superannuation Investors, 2019, Modern Slavery: Risks, Rights and Responsibilities – A Guide for Companies and Investors <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/modern-slavery-guide-for-companies-investors-feb-2019.pdf>
- Australian Institute of Company Directors, 2019, Modern Slavery Risk Oversight, <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/2019/pdf/modern-slavery/07236-5-modern-slavery-oct-19-a4-web.ashx>
- KPMG, 2019, Modern Slavery: Is Your Business Ready to Respond? <https://home.kpmg/au/en/home/insights/2018/09/modern-slavery-is-your-business-ready-to-respond.html>
- KPMG and the Australian Human Rights Commission, 2021, Financial services modern slavery guide <https://home.kpmg/au/en/home/insights/2021/02/financial-services-modern-slavery-practical-guide.html>
- KPMG and Australian Human Rights Commission, 2020, Property, Construction and Modern Slavery, <https://home.kpmg/au/en/home/insights/2020/08/property-construction-modern-slavery-practical-guide.html>
- KPMG and Australian Human Rights Commission, 2021, Health services sector modern slavery guide, <https://home.kpmg/au/en/home/insights/2021/11/health-services-modern-slavery-practical-guide.html>
- KPMG and Australian Human Rights Commission, 2021, Resources, energy and modern slavery, <https://home.kpmg/au/en/home/media/press-releases/2021/12/resources-energy-and-modern-slavery-16-december-2021.html>
- KPMG, 2020, COVID-19: Protecting vulnerable people, <https://home.kpmg/au/en/home/insights/2020/05/coronavirus-covid-19-protecting-vulnerable-people.html>
- Supplier Ethical Data Exchange (SEDEX) – [www.sedexglobal.com](http://www.sedexglobal.com)
- Business Social Compliance Initiative – <https://www.amfori.org/>

## For further information please contact:

**Tina Jelenic****KPMG Banarra****Director, Human Rights and Social Impact Services****[modernslavery@kpmg.com.au](mailto:modernslavery@kpmg.com.au)**

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# 25. Automation and AI

Automation and Artificial Intelligence (AI) will have a lasting impact for the future of organisations, the result will be far larger and will be deployed much faster than everyone anticipates. With digital business strategy moving to the heart of every business, organisations – public, private, government owned or not-for-profit – need to consider how they will engage with, and incorporate, automation and machine learning, or AI, into their thinking.

The pace of change, the change in the way in which customers behave and the ethical considerations for automation and AI, all require directors to have a strong understanding of this new risk profile, its impact on risk appetite and how these emerging technologies impact on their organisation's business model, culture and risk framework.

## In this chapter

- Evolution of the revolution
- Artificial intelligence versus machine learning
- Convergence of automation and AI
- Ethical considerations
- Algorithms
- Governance issues associated with automation, AI and machine learning
- Governance in regulatory uncertainty
- The role of the board

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. What is automation and AI, the scope of its impact on the organisation and industry, and the cost of missed opportunities?
2. How well does the board understand where automation and AI can deliver cost efficiencies?
3. Has the board considered the impacts (positive and negative) of automation and AI on the customer experience and on driving growth and customer loyalty?
4. Is the board challenging and rethinking existing ways of working or simply automating existing processes or approaches?
5. What do customers expect from the board and the firm? Are there better ways to meet their expectations using automation and AI?
6. Has the board considered the organisational and business model impacts from the disruption of increased automation and AI in society?
7. What are the ethical issues the board need to consider if directors are to adopt greater automation and AI into the business?
8. What are the potential regulatory impacts of a more automated economy, with respect to issues such as privacy, consumer protections, fraud, misconduct, cyber security etc.?
9. Has the board considered the wider "change management" aspects of the introduction of increased automation and AI?
10. Can executive leaders articulate the business impacts of automation and AI? What is the impact of a false positive vs negative? Is AI really the most suitable solution (could it be solved via more conventional means)? Should a human be in the loop? If so, when and in what capacity (oversight, arbiter or final decision maker)?
11. Should the firm safely follow or boldly lead? Is the firm partnering with innovative start ups and other third parties to accelerate its adoption of automation, AI and emerging technologies?
12. Does the firm have a robust risk management process and control framework to manage automation and AI?



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Automation and AI have not been discussed as part of risk and strategy discussions, or not discussed in a joint context of business and IT strategies.
- Automation and AI are deployed outside a structured automation strategy and operating model.
- No governance frameworks have been developed to monitor and/or provide assurance as to the quality, accuracy and/or rigour of the outcomes produced by automation and AI.
- Directors are reluctant to consider the emerging technologies because they fail to see the relevance to the business.
- The workforce implications of automation and AI innovations across the business are not understood.
- Executives cannot explain the potential or actual impact of automation and AI on the business – and which competitors are leading the space.
- Innovation is touted as important but is not supported, or invested in, by the business.
- Disruption is not on the strategic risk register.
- The appointment of a Chief Data Officer / Chief Analytics Officer to the executive team, or an individual whose responsible for automation and AI has not been considered, and the differences in these roles are not understood or discussed.
- There is no budget for innovation and investment in emerging technologies, such as AI, or that budget is not expressly linked to benefits realisations.
- The enterprise has struggled to get the basics right (e.g. poor data quality, very limited or poor quality descriptive and diagnostic BI) or has a history of issues with poor automation or AI outcomes.
- Automation and AI are proposed for operations in high risk, highly regulated, highly visible areas of the organization, or for operations in areas with direct impact on human safety.
- High turnover of technology staff and/or strategic consultants.
- Customer complaints/returns/credits are rising shortly after implementation.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## EVOLUTION OF THE REVOLUTION

We have entered the fourth industrial revolution. An age of automation, machine learning, AI, Internet of Things (IOT) connectivity, augmented and virtual reality and robotics. Industries, operating practices and careers will be replaced, recreated or made redundant. New careers and roles will be created that have never before been imagined. This revolution is leading many organisations to question what they stand for in the market, how their organisation operates and what this means for their traditional workforce model.

*Technology*

Despite the fact that technology – in the context of mechanising human activity – has been around for centuries, the technological age that we find ourselves in today has seen an unprecedented pace of change in the development and take up of digital devices designed to make our lives easier. Whether it is through automated manufacturing processes, bots that write news articles based on streams of internet information, or complex algorithms designed to predict our spending patterns – the opportunities, threats and the governance required to meet stakeholder expectations, is changing.

Technology is impacting business models in ways that would have been hard to predict a few years ago. Business models that have grown from 'garages' and do not own any real 'physical' assets, such as Uber, Airbnb and Facebook – have become the most valuable companies in the world. Things that may not have seemed possible a decade ago, are quickly evolving to become a reality. For example, who would have predicted wearable tech that captures biological statistics that can be downloaded into your (or an organisation's) cloud of data? Who expected Elon Musk to 'solve' South Australia's energy crisis or Twitter bots to influence an election campaign?

*Customer experience*

This digital revolution is driving change in the way customers interact with an organisation. It creates different expectations of service standards and delivery that go beyond the traditional definitions and measures of success. Machines are also now heavily involved in sales maximisation and demand creation, whether it's through click bait or the use of complex algorithms that monitor, track and pre-empt purchasing patterns of consumers (also known as personalised one-on-one marketing).

In 2014, global researcher, Gartner forecasted that by 2016, 89 percent of businesses would soon be competing primarily on customer experience and that by 2020, the customer will manage 85 percent of its relationships with enterprises without interacting with a human.<sup>387</sup> Most would agree that this prediction has become reality, and the COVID pandemic has increased the focus on virtual interactions in customer experiences.

Adding to this, not only are consumer behaviours expected to change, KPMG's Innovation team also predicts that technology faces the Trust Paradox as we proceed through the 2020s. Around the world, people are both increasingly dependent on, but distrustful of, how enterprises use digital technology. This will no doubt lead to greater regulatory scrutiny.

Consumer Data Rights (which started in the Banking industry and is now moving to the Energy sector and beyond) are transferring more power and ownership over personal data from the company to the consumer by enabling customers to freely exchange their data from one provider to another.

<sup>387</sup> Sorofman, J, 2014, Gartner surveys confirm customer experience is the new battlefield, <https://blogs.gartner.com/jake-sorofman/gartner-surveys-confirm-customer-experience-new-battlefield/>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

The broader role of public trust is also higher on the agenda for many organisations – whose 'bot' or algorithm do you trust? Who do you trust with your data? These are not subtle shifts. These are issues that will generate significant risks and opportunities for all types of businesses. Boards and directors need to understand what it means for their business – strategically and operationally. Every business must consider the impact of platforms, figure out how to leverage them or copy them.

## ARTIFICIAL INTELLIGENCE VERSUS MACHINE LEARNING

We use the term AI as an umbrella term to describe computer systems that are able to perform specific cognitive tasks typically requiring human intelligence. Machine learning is the way for AI to learn, and deep learning is a subset of that, using artificial neural networks to mimic brain activities using mathematical processes enabled by high powered computer processing hardware. The proliferation of AI has generally grown with the use of Big Data and leaps in computing power enabling increasingly sophisticated analytics, machine learning and deep learning algorithms.

Enterprises must actively seek to gain from advances in computer processing power, access to data and the ease of storage that are driving the developments in AI. Directors and Executives will need to have a clear vision and organisations must have a strong culture in order to effectively plan and manage this shift to machine driven intelligent enterprise.

## CONVERGENCE OF AUTOMATION AND AI

Automation and AI can be considered, and deployed, separately. However, they are increasingly convergent technologies and are often deployed together to streamline and scale decision-making across organisations.

Automation (sometimes known as 'Robotic Process Automation', or RPA) typically replaces human action on a computer system by:

- following a set of pre-programmed steps (think of an ATM's computer determining whether to dispensing cash or not); and/or
- using a trained AI model to determine the next step (think of a marketing system learning customer preferences and sending tailored offers to them).

The benefit and risk of such a system varies greatly and is generally dependent on the level of autonomy, human programming and the nature of the process or decision being automated.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

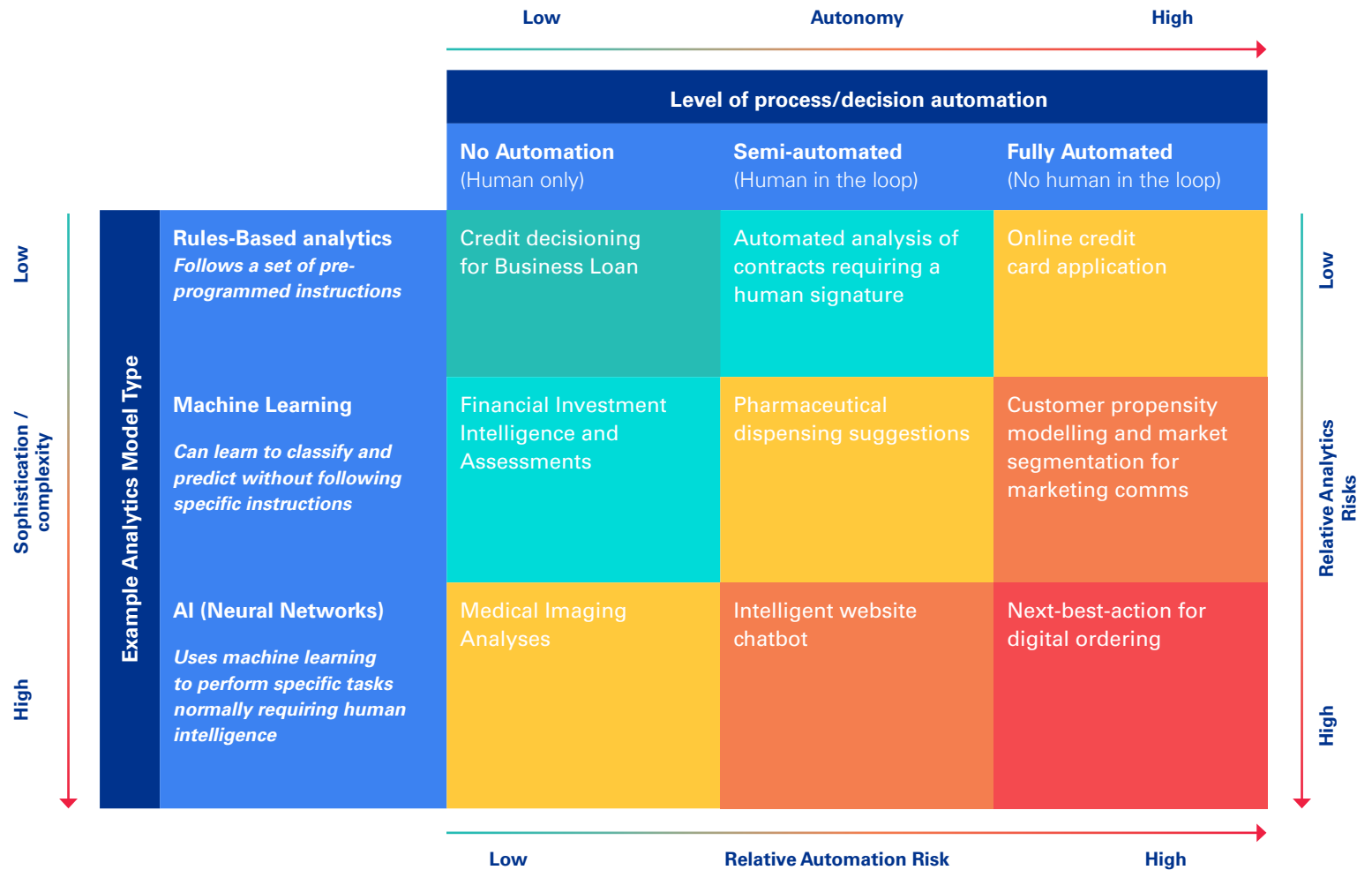
18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

GLOSSARY

APPENDICES

CONTACT US

RELATIVE RISK OF A SYSTEM BASED ON ITS ANALYTICS SOPHISTICATION AND AUTONOMY



Rules-based analytics are certainly not free of risk as human error in their development and execution can lead to major issues, however they are generally more transparent and thus easier to audit, control and manage compared to Neural Networks. The nature resultant impact of a poor decision or automation is not depicted here, but will also have a significant influence on the overall risk (for example, an incorrect credit decision for business loan may have a higher overall impact than an incorrect intelligent chat-bot suggestion).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## ETHICAL CONSIDERATIONS

The rise of automation and AI can raise significant ethical issues for the enterprise and the community, which are being felt in board rooms across the globe. The World Economic Forum (WEF) has highlighted several ethical considerations associated with the increase in sophistication and adoption levels of AI.<sup>388</sup> These are:

- unemployment
- inequality of wealth distribution
- social impacts and lack of human connectedness
- artificial 'stupidity' and poor machine 'learning'
- bias in AI analysis and outcomes
- security against adversaries
- protecting against unintended consequence
- singularity and staying in control of AI
- robot rights – reward and incentives for AI.

From a director's perspective, these issues can raise several governance issues. Most obvious, at present, are those associated with workforce changes, security and social implications.

**Workforce changes**

As more and more processes, and even entire job roles, become automated the current roles that we know today will continue to change. They will be replaced by new roles and through organic growth. Ethically, this can cause issues for some organisations who have established themselves as employers of choice but are now faced with significant changes to their workforce in terms of FTEs, skills and more 'agile' or flexible work arrangements. But as some roles are disappearing, brand new job roles are already starting to emerge such as *Metaverse Engineer and Blockchain Architect*.

<sup>388</sup> Bossmann, J., 2016, Top 9 ethical issues in artificial intelligence, <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/>

Directors, as leaders of culture within an organisation, need to be asking management:

- What are the potential impacts of automation and AI on our people?
- How do we balance customer experience, employee experience, profitability and workforce changes in the context of greater automation, cost pressures and social responsibility?
- How do we deal with cultural change and the human impact?
- What do we offer in terms of training and re-training?
- What will our stakeholders think – is cost a bigger driver of consumer spending than organisational behaviour and ethics?

It may come down to how transitions are handled, rather than the extent of the transition itself.

**Security**

Automation and AI can be deployed to enhance security activities. Data security is already a hot topic under the banner of 'cyber risk', and machine learning algorithms are being used extensively in cybersecurity to sift through millions of transactions and volumes of network traffic to detect threats. As automation and AI evolve and we see further advances in what machines are capable of, we must also consider physical security. Drones, for example, are being used for deliveries of goods, driverless cars are being touted as a future delivery service as well – but what does this mean for the physical safety of our customers and citizens – be it from hackers, or privacy issues associated with information (text, pictures, personal details, personal preferences etc.)? Regulatory change is likely to evolve further in these areas, particularly in the context of geo-politics and national security.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

**Social Impact**

Despite the increased demand from consumers for greater digital connectivity and 'smart' devices to simplify or streamline our lives, the social impacts of losing human connection are already being felt in many parts of the community. Organisations may be asked – by stakeholders or regulators – about how they are addressing some of these broader community issues. Reporting frameworks, such as the Global Reporting Initiative (GRI), and social indices such as 'FTSE 4 Good' are becoming more mainstream, as stakeholders demand greater transparency on an organisation's social impacts. Often these issues are beyond the organisation's direct control but still require oversight and influence in the eyes of the community.

The organisation 'Partnership on AI'<sup>389</sup> has been established to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to serve as an open platform for discussion and engagement about AI and its influences on people and society.

**ALGORITHMS**

Algorithms in their simplest form, are a set of instructions to solve a problem or complete a task. They form the basis of most of the AI we see in everyday platforms such as Facebook and Netflix. Data is collected and sorted, decisions are then made by the algorithms, through an iterative process of validation and verification from internal and external sources. The outcomes of these complex algorithms inform decision making in the organisation or buyers of the information.

One example is IBM 'Watson' – a learning platform using many algorithms and processes that takes in various forms of public and private information, arriving at outputs that help inform decision-making. The outputs generated by Watson are calculated using a set of instructions and behavioural parameters, including psychological and mood reading information, based on specific words or sentence structures used.

<sup>389</sup> For further information go to [www.partnershiponai.org](http://www.partnershiponai.org)

**GOVERNANCE ISSUES ASSOCIATED WITH AUTOMATION AND AI**

We are in an environment where directors must now govern for constant change, rather than for managing change from one fixed state to another. With **foresight, insight and oversight** the keystones of governance, directors must apply these lenses to all aspects of their organisation in the context of automation and AI.

**Foresight** must include consideration of automation and AI, and the different risks and opportunities they present to their organisation. Anticipating the required changes within your organisation is critical. It may be as simple as knowing who can advise on the impact of technology disruption, or as complex as considering how to re-define the very industry your company operates in. Bringing new technology and consumer scenarios – disrupting old thought patterns and ways of doing things – is imperative to testing the sustainability of the existing business model. The past is no longer always a good predictor of the future. As AI is adopted within the business world and in our private lives, successful organisations will be those who are open-minded and committed to staying ahead of – or at least at pace with – the pack, and who maintain public trust.

**Insight** takes the form of truly understanding the wide range of risks and opportunities specific to your industry and your organisation. What value can you bring to the discussion about the impacts of these changes for you and your customers? Directors need to inform themselves, and provide relevant challenge and feedback to management, when it comes to developing and embedding

***As a board member, consider the following examples. What are some of the challenging questions that you would ask to determine the risks, opportunities and strategies for your organisation?***

- Example 1 – the CEO of your organisation comes to your board with a proposal for a new form of technology that would allow you to collect personal data from your customers (through wearable clothes that gather physiological data) and use automation and AI to conduct processing and analyses.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- *What are the risks associated with this from a privacy perspective? What are your responsibilities with the data? How could you use the information to better service your customers? How could you use the information to generate additional forms of revenue? Are there any ethical issues with (for example, selling this data to health insurers), which may impact individual customer health insurance premiums? What if the data is inaccurate? Who is liable?*
- *Example 2 – Your CEO comes to the board with a proposal to introduce AI that can analyse data on your truck drivers. Heart rates, driving styles, rest breaks and other data could help to improve the safety of your workers and the efficiency of your deliveries, perhaps even shape incentive and accountability frameworks. How might this impact on employee relations? How could this data reduce or improve profitability (e.g. reducing insurance premiums for trucks), or reshape your business model entirely? What are the privacy and health obligations regarding the drivers' data that you would hold?*

Broadly, directors need to consider what information they need in order to be able to constructively challenge and test management's assumptions. In this context, directors need to seek a level of tension in the business that pushes the organisation into more innovative and lateral thinking. If you are not generating a little tension you may not be getting close enough to the value creation needed to be successful in a new operating environment.

The **oversight** role with respect to automation and AI is largely the same as for any other area of governance. Just as the board needs to develop relevant KPIs for performance (for example, with respect to financial oversight), the board also needs to develop relevant KPIs that will enable oversight of the success of innovation and technology adoption. The board should consider any risk thresholds that might apply to innovation and 'planned' disruption to its business. These thresholds include having clarity over when to 'walk away' from an automation or AI project that is not performing as planned.

Oversight from external bodies may also increase in areas of automation and AI. Governments will be increasingly expected to consider regulation of AI usage based on ethical concerns (such as systemic biases, fairness or privacy issues) or to incentivise the decommissioning of redundant ways of doing business due to community demands for change.

Amongst all this change, there is also a role for **AI to assist the board** in their oversight role. It will not be long until 'Siri' (or similar) is available to answer questions and you can ask "Siri, have we complied with our reporting obligations this quarter?"

AI systems are fallible as they are built and run by humans. It is likely they will continue to make mistakes and directors will need to ensure that the organisation considers the risks and appropriate safeguards. Further, directors must ensure they remain properly informed of the financial position of the company (beyond merely asking a 'bot') to ensure they comply with their legal duties (see [Chapter 1 Directors' Legal Duties](#)).

In some cases it may not be very important to know how and why an AI system made a decision, whilst in other cases it may be critical, for example, deciding what medications should be provided to a patient or what custodial sentence should be imposed for a conviction. Automation and AI should be fully understood, regularly re-trained and tested and continually updated and managed. To achieve this, some leading global organisations have even included bots in their organisational charts, effectively giving business line-managers responsibility for their oversight and performance management just as they would their human direct reports (although they're less likely to get a year-end bonus).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## GOVERNANCE IN REGULATORY UNCERTAINTY

Regulation in a changing environment presents as a challenge for businesses. Often businesses like certainty in order to predict and control risk, and a stable regulatory environment can be beneficial. However, with ongoing rapid advancements in automation and AI, regulation can lag significantly behind 'cutting edge' use cases.

Often, we see that existing regulation is updated to try to keep pace with changes in the community. Regulatory change can be in response to specific events, to lobbying designed to incentivise investment, to deter misconduct, or to protect rights that reflect community standards and expectations. The pace of change in technology far exceeds the pace of change in any regulatory and governance frameworks. In addition, the global nature of the digital economy during this fourth industrial revolution means that reaching consensus or consistency in regulations can take even longer.

So how do directors govern in the face of (i) uncertainty over the pace and extent of future regulation (ii) multiple jurisdictions and cross-border differences in regulation and (iii) inadequate regulation or regulatory protections that do not keep pace with the technological issues?

In the absence of up-to-date regulation, a more agile and proactive approach to governance is required – and is likely to become more and more essential. Anticipating technology changes, anticipating regulation, anticipating (or leading) sector and industry Codes of Conduct – and changing strategies in response – may be required to maintain a competitive edge.

## THE ROLE OF THE BOARD

The board has responsibility for creating a vision of the organisation's future based on foresight that considers a range of scenarios. In the context of a more automated and artificially intelligent world of customer interactions, manufacturing processes and data analytics, directors need to:

- be curious and informed – constantly ask, what is the new tech trend?
- understand how automation and AI technologies – no matter how far-fetched it may seem in today's terms – will impact the business in the short, medium and longer term?
- put existing and future strategies into context – i.e. what could the world look like? Whilst change is difficult or may not seem necessary in today's terms, what are the risks of **not** adapting to these changes?
- expect the unexpected – even the most unlikely scenarios can come to fruition – who would've thought that driverless cars would be possible so soon?
- encourage innovation and be prepared to fail at times (within defined risk thresholds)
- look holistically at the organisation's strategic assets, recognising that they may no longer be physical assets but focused more on customer experience
- proactively recruit board members who can constructively question and challenge the organisation's strategies.



## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Useful references

- Partnership on AI – [www.partnershiponai.org](http://www.partnershiponai.org).
- Gartner research – [www.gartner.com](http://www.gartner.com)
- KPMG, Data and automation in contract management <https://home.kpmg/au/en/home/insights/2021/06/data-and-automation-in-vendor-contract-management.html>
- KPMG and the University of Queensland, Trust in Artificial Intelligence: A five country study, <https://home.kpmg/au/en/home/insights/2021/03/artificial-intelligence-five-country-study.html>
- KPMG, Artificial intelligence (AI) and the great privacy challenge, <https://home.kpmg/au/en/home/insights/2019/02/artificial-intelligence-great-privacy-challenge.html>
- Australian Human Rights Report on risks posed by AI and Emerging tech - <https://tech.humanrights.gov.au/>

## For further information please contact:

**Paul Hyland**

**Lead for Data and AI Ethics,  
Audit, Assurance &  
Risk Consulting**  
[phyland@kpmg.com.au](mailto:phyland@kpmg.com.au)

**Mark Geels**

**Director, Data and Analytics  
Audit, Assurance &  
Risk Consulting**  
[mgeels@kpmg.com.au](mailto:mgeels@kpmg.com.au)

# 26. Social Media

In this hyper-connected world, the explosion in social media use has resulted in an empowered consumer. This empowered consumer, along with the convergence of social and traditional media, has introduced contemporary risks that many 'heritage' risk management frameworks are not equipped to deal with.

## In this chapter

- Rethinking social media and risk
- Unpacking social licence to operate
- Truth, opinion and business outcomes
- The marketing trap
- Aversion to action
- Tokenism as a response
- ESG and Business
- Finding solutions
- There is an upside to embrace

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Questions that company directors should ask

1. Has a review been done to identify and understand potential social media risks facing the organisation?
2. Does the organisation have a documented framework for identifying, mitigating and managing social media risk?
3. Has the organisation identified the possible exposures that it may face from social media?
4. Has a review of the possible impacts of social media on the supply chain been undertaken?
5. What social media regulations are in place for our industry and have they been considered?
6. Is there a single point of accountability for social media risk?
7. How is social media risk reported to the board?
8. How literate is the board with respect to the use of social media?
9. Is there a social media plan in place?
10. Has an analysis been undertaken to identify key influencers and stakeholders for the business in the social media landscape? What proactive engagement strategies are in place to manage these stakeholders?

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Red flags

- Lack of recognition that social media is a risk.
- Little understanding of the underlying risks stemming from social media beyond reputational risk.
- No formalised social media monitoring or reporting in place that extends beyond the 'Marketing Department'.
- Limited social media governance frameworks.
- Frequent social media mishaps or gaffes occurring.
- The organisation does not embrace the many benefits of social media.
- No expansion of customer service, investor relations or public affairs into the social media operating framework.
- Lack of innovation to see social media as more than a 'campaign' tool.
- Reporting is limited to 'vanity metrics' such as the number of Twitter followers or Facebook Page 'Likes'.
- Social media is not used at all, or is not used effectively, to influence and gauge customer and stakeholder sentiment.
- The organisation has no understanding of how key competitors are using social media.
- There is no social media monitoring to determine what is being said about the organisation.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## RETHINKING SOCIAL MEDIA AND RISK

Senior leaders have contended with social media and risk; they understand that it exists, and that social media is as much a risk medium as it is an opportunity for marketing, to service customers and facilitate sales.

For some organisations, social media has not been thought of as a cause of risk, which often positions social media as something to suppress, avoid and to apply a series of risk controls to. It follows a 'gaffe' view of social media and risk, where we think of social media and risk as something that we do to ourselves, a self-inflicted wound. While this was true in the early 2010's, this was simply a minor growing pain in the development of social media as a business consideration, like a toddler slipping on their toy as they learn to move amongst the environment. The business community fixed this in a few years, but the scars remained, and we think of remaining below the parapet for as long as we can, as the best we can hope to do. We have put in place controls, however, across the industry these are relatively simple, and include training, passwords, senior approval of content etc. – these are important, but these are just hygiene measures.

We need to re-think social media and risk – changing our perception to consider it a channel where stakeholder communication and customer interactions takes place and replaced older forms of communication that were slower moving and more costly. Social media is a technology and a medium, it is not a risk class.

Aon's 2021 Global Risk Management Survey recorded the #2 risk felt by Australian C-Suites as 'Damage to reputation/brand', and the #6 risk as 'Regulatory/legislative changes'. We contend two things in relation to these findings:

1. Social media is the platform where these risks gather momentum and become visible; and
2. Regulatory/Legislative changes are driven often by damaged industry reputations, especially amongst business-to-business operators.

These risks are classified in the Top 10 because social media exists, and because the general public uses social media more dynamically than businesses.

## UNPACKING SOCIAL LICENCE TO OPERATE

Social licence is an important lens to frame trust. It acknowledges people and communities play a role in granting approval of how companies, and in some cases an entire industry, conduct their business and how governments form policy. We need to be mindful that social media helps facilitate a narrative, it can streamline anger into something measurable, and has transferred power from institutions to communities.

Because of this, people have become empowered to approach businesses and Government through social media channels. People can communicate with politicians and businesses online, but more often, they will engage in a conversation online aware that CEOs and politicians, special interest groups, and businesses are becoming more likely to consume the message.

Businesses and Government can spend too much time asking "how does this impact our business or policy" when they should be asking "how does our business or policy impact on people?", and should focus more on the most vulnerable people and communicating and engaging with stakeholders openly.

## TRUTH, OPINION AND BUSINESS OUTCOMES

Some have said we are living in a 'post-truth' society. This is probably untrue, but society is struggling to maintain its natural scepticism and objectivity. A 2020 research piece "COVID-19: Australian news and misinformation" from the University of Canberra "found that nearly two-thirds (66 percent) of people say they have encountered misinformation about COVID-19 on social media.

This has only been exacerbated during COVID-19 and the online 'infodemic', which, according to the 2021 Edelman Trust Barometer has led to trust from all sources of information (search engines, traditional media, owned media, and social media) at record lows.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

- **GOVERNANCE OVERSIGHT**

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

For businesses who otherwise enjoy a healthy community perception, correcting misinformation swiftly and directly is key. For those involved in contested-spaces, it can be more effective to garner tangible advocacy from supporters than to attempt to sway ideological opponents to your business.

**THE MARKETING TRAP**

Original business perceptions of social media saw marketing become the predominant owners of the channel. Social media carries implications across a business, most commonly including marketing & brand, communications, Government affairs and customer; but also risk, IT, investor relations, procurement and human resources. The best approaches acknowledge that social media touches all of these points and gives an independent and expert view of the priorities and uses for the social media data programs and content strategies.

When businesses leave social media to any particular division, businesses close-off potential uses of the medium and the data within it.

**AVERSION TO ACTION**

The business community is not used to acting on issues through social media on a day-to-day basis, and so teams are ill-prepared to use social media to address issues. Often, teams will choose to wait and see if an issue becomes significant before acting, and this will lead to either a missed opportunity to assert the truth and develop credibility for the social media program, or an issue that requires a response that we are late to engage with. This can occur over periods as short as a single day, or can last for months or years.

There are cultures where communication teams are hesitant to engage in topics where they do not feel they have support from senior leadership support, and so businesses often forego the chance to positively shape their reputation unless there is a major issue present.

Because of this paralysis, businesses lag over the course of days, months (or years), to address risks outside of their complete control.

**TOKENISM AS A RESPONSE**

Some businesses operate on a generally mistaken approach that they will be forgiven for their stance or actions in one area if they adopt a principled stance or action in another. This is especially ineffective where the criticism relates to core business function. This is called 'tokenism', and follows a general belief that a business can meaningfully shift the dial on its reputation by setting its own agenda.

This is not the case. Businesses need to tackle the potential issue head on, addressing the concerns of people so they can shift the dial.

**ESG AND BUSINESS**

The world has changed. Consumers and employees have increasingly different expectations, both from businesses they buy from, and work for. Leaders are under pressure from regulators and the market to prove they are acting responsibly and acting sustainably.

Now, more than ever, it is important to embed ESG into business strategy, with social media playing a pivotal role in the execution of any communications strategy. Businesses need to tell the story behind ESG actions, utilising authentic employee advocacy video campaigns to showcase honest and transparent stories about the evolution of the business.

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## • GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## FINDING SOLUTIONS

Senior leaders have acknowledged the need for action, however, have been generally unable to develop risk controls. There exists a suite of leading-practice approaches to managing external risk through social media, as follows:

1. **Social Media Risk Diagnostic** – take a risk view of the social media conversations taking place around your brand, products, issues and industry to look at risk through the lenses of the customer, public and employees.
2. **Social Media Governance Review** – receive an independent audit of the social media team, into how well it is resourced, how it seeks to use social media, its access to decision makers and its processes. Enact changes that better position the team to manage external risk holistically.
3. **Social Media Strategy Development** – Develop a social media strategy or refine an existing one so that it is approaching risk and the competing broader business objectives in a way that is endorsed by an independent view, and facilitated by best-practice and evidence-based methods.
4. **Social Media Intelligence Monitoring** – Implement daily monitoring for social and digital media, which comes to decision-makers in a filtered way, with analysis, insight and recommendations. Develop a workplace culture that acts on issues.
5. **Customer Service Review** – Analyse the approach and strategy your business or organisation takes to using social media as a customer service channel, and provide recommendations.

## THERE IS UPSIDE TO EMBRACE

Social media has allowed businesses to have increased access to people, and an ongoing data source around the businesses' reputation, regulatory affairs, customer satisfaction and investor perspective. It has allowed a direct means of communications to 'narrowcast', as opposed to 'broadcast'. These are all positive changes for business, and there is no longer an excuse that a groundswell movement could emerge to which the business was not aware.

Social media is a business' opportunity to manage external risk.

## Useful references

- Task Force on Climate-related Financial Disclosures (TCFD) Knowledge Hub, <https://www.tcfhub.org/>

## For further information please contact:



## Louise Pogmore

Partner, Customer Intelligence,  
Customer Brand and Marketing Advisory  
[lpogmore@kpmg.com.au](mailto:lpogmore@kpmg.com.au)

# Glossary

<b>AASB</b>	Australian Accounting Standards Board	<b>CCPA</b>	California Consumer Privacy Act
<b>ACCC</b>	Australian Competition and Consumer Commission	<b>CDR</b>	Consumer Data Right
<b>ACNC</b>	Australian Charities and Not For Profits Commission	<b>CEO</b>	Chief Executive Officer
<b>ACSC</b>	Australian Cyber Security Centre	<b>CFO</b>	Chief Financial Officer
<b>ACSI</b>	Australian Council of Superannuation Investors	<b>CIO</b>	Chief Information Officer
<b>ADI</b>	Authorised Deposit-Taking Institutions	<b>CISO</b>	Chief Information Security Officer
<b>AFS</b>	Australian Financial Services	<b>CPS</b>	Consolidating Prudential Standards
<b>AGM</b>	Annual General Meeting	<b>COP</b>	Conference of Parties
<b>AI</b>	Artificial Intelligence	<b>CPA</b>	Certified Public Accountant
<b>AIATSIS</b>	Australian Institute of Aboriginal and Torres Strait Islander Studies	<b>CRO</b>	Chief Risk Officer
<b>AIC</b>	Australian Investment Council	<b>CR</b>	Corporate Responsibility
<b>AICD</b>	Australian Institute of Company Directors	<b>CSF</b>	Crowd-Sourced Funding
<b>APP</b>	Australian Privacy Principles	<b>D&amp;O</b>	Directors and Officers
<b>APRA</b>	Australian Prudential Regulation Authority	<b>DoA</b>	Delegation of Authority
<b>ASIC</b>	Australian Securities and Investment Commission	<b>EER</b>	Extended External Reporting
<b>ASIO</b>	Australian Security Intelligence Organisation	<b>EFLIC</b>	Eligible foreign life insurance organisations
<b>ASX</b>	Australian Securities Exchange	<b>ERM</b>	Enterprise Risk Management
<b>ATO</b>	Australian Taxation Office	<b>ESG</b>	Environmental, Social and Governance
<b>AUASB</b>	Auditing and Assurance Standards Board	<b>FRC</b>	Financial Reporting Council
<b>BRC</b>	Board Risk Committee	<b>FTE</b>	Full Time Equivalent
<b>CA ANZ</b>	Chartered Accountants Australia and New Zealand	<b>GAAP</b>	Generally Accepted Accounting Principles
<b>CaIPERS</b>	California Public Employees Retirement System	<b>GAPP</b>	Generally Accepted Privacy Principles
<b>CAMAC</b>	Corporations and Markets Advisory Committee	<b>GIA</b>	Governance Institute of Australia
<b>CATSI Act</b>	The Corporations (Aboriginal and Torres Strait Islander) Act 2006	<b>GDPR</b>	General Data Protection Regulation

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US



## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

### APPENDICES

### CONTACT US

<b>GFC</b>	Global Financial Crisis	<b>PE</b>	Private Equity
<b>GPFS</b>	General Purpose Financial Statements	<b>PEC</b>	Private Equity Committee
<b>GRC</b>	Governance, Risk and Compliance	<b>PPG</b>	Prudential Practice Guide
<b>GRI</b>	Global Reporting Initiative	<b>PRI</b>	Principles for Responsible Investment
<b>GST</b>	Goods and Services Tax	<b>RAPs</b>	Reconciliation Action Plans
<b>HSEC</b>	Health, Safety, Environment and Community Committee	<b>RBA</b>	Reserve Bank of Australia
<b>HSR</b>	Health and Safety Representative	<b>ROI</b>	Return on Investment
<b>IASB</b>	International Accounting Standards Board	<b>RPA</b>	Robotic Process Automation
<b>ICGN</b>	International Corporate Governance Network's	<b>RSE</b>	Registerable Superannuation Entities
<b>IFRS</b>	International Financial Reporting Standards	<b>SASB</b>	Sustainability Accounting Standards Board
<b>IIA</b>	Institute of Internal Auditors	<b>SEC</b>	US Securities and Exchange Commission
<b>IMF</b>	International Monetary Fund	<b>SGC</b>	Super Guarantee Charge
<b>IOT</b>	Internet of Things	<b>SLACI Bill</b>	Security Legislation Amendment (Critical Infrastructure) Bill 2021
<b>ISO</b>	International Organization for Standardisation	<b>SLACIP Bill</b>	Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022
<b>KMP</b>	Key Management Personnel	<b>SMSF</b>	Self-Managed Superannuation Fund
<b>KPI</b>	Key Performance Indicators	<b>SOCI</b>	Security of Critical Infrastructure Act
<b>LIT</b>	Lost Injury Time	<b>SOX</b>	Sarbanes-Oxley Act
<b>LPI</b>	Leading Performance Indicator	<b>SPFS</b>	Special Purpose Financial Statements
<b>M&amp;As</b>	Memorandum and Articles of Association	<b>TCFD</b>	Task Force on Climate-related Financial Disclosures
<b>MD</b>	Managing Director	<b>TNFD</b>	Task Force on Nature-related Financial Disclosures
<b>NDB</b>	Notifiable Data Breach	<b>TP</b>	Transfer Pricing
<b>NIST</b>	National Institute of Science and Technology	<b>TrueTCO</b>	True Total Cost of Ownership
<b>NFP</b>	Not for Profit	<b>TTC</b>	Tax Transparency Code
<b>OAIC</b>	Office of the Australian Information Commissioner	<b>UN-FCCC</b>	United Nations Framework Convention on Climate Change
<b>OECD</b>	Organisation for Economic Cooperation and Development	<b>WEF</b>	World Economic Forum
<b>ORIC</b>	Office of the Registrar of Indigenous Corporations	<b>WHS</b>	Workplace Health and Safety
<b>PAYG</b>	Pay as You Go		
<b>PCBU</b>	Person Conducting a Business or Undertaking		

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

# Appendix 1: Board Charter

The purpose of a board charter is to describe the board's terms of reference and outline the board's approach to important governance practices.

Research into board charters of Australia's top 50 listed companies indicates that charters can cover a broad range of matters, including those in the box below:

## Matters which may be found in a board charter

- Board role descriptions
- Role of chairman
- Role of the committee chairmen
- Role of the company secretary
- Role of managing director/CEO
- Director letter of appointment
- Directors' induction and education
- Tenure
- Board committees
- Conflicts of interest
- Indemnities and insurance
- Deed of indemnity, insurance and access
- Directors' and officers' insurance
- Access to board papers
- Access to independent professional advice
- Strategic direction and oversight
- Access to management
- Code of conduct
- Corporate social responsibility/sustainability
- Political donations
- Compliance system
- Policies and procedures
- Board's role in crisis management
- Integrity of financial reporting
- CEO and CFO assurance
- Annual report to shareholders
- Reporting to stakeholders
- Annual general meeting
- Board and individual directors' performance assessment
- Review of CEO performance
- Director remuneration
- Quorum

- FOREWORD

- THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
    - 2. Governance Roles
    - 3. Government
    - 4. Not-For-Profit Organisations
    - 5. Proprietary Limited Companies
    - 6. Indigenous Culture

- GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
    - 8. Stakeholder Engagement

- GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
    - 10. Company Leadership
    - 11. Board Committees
    - 12. Investment Management
    - 13. Productive Meetings
    - 14. Strategy and Planning
    - 15. Receiving Assurance
    - 16. Tax Governance & Transparency
    - 17. Risk Management

- GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
    - 19. Private Equity
    - 20. Health, Safety and Wellbeing
    - 21. Culture and Conduct
    - 22. Cyber Security
    - 23. Data Privacy and Personal Information
    - 24. Human Rights and Modern Slavery
    - 25. Automation and AI
    - 26. Social Media

- GLOSSARY

- APPENDICES

- CONTACT US

# Appendix 2: Annual Agenda

The board and annual agenda should be designed as a practical work plan where the board's staple business items are allocated to a particular meeting. The example annual agenda attached is one approach to the categorisation of business items and their allocation to specific meetings. In this example, it is assumed there will be 12 meetings of the board including an annual strategy day. An underlying objective of the annual agenda is to achieve balance in the board's workload through the year and ensure all board responsibilities are attended to.

The items of business have been categorised as follows:

- matters that the board has resolved for its decision (reserved authorities)
- matters which have been delegated (e.g. to the CEO or a board committee) (delegated authorities)
- matters that are purely for information and do not require a board decision (reporting)
- procedural matters that may arise at any or every board meeting (matters that may be applicable to all meetings).

The matters listed in the annual agenda and the scheduling of such matters will vary from company to company. Each board should identify the core matters for inclusion in the annual agenda. As well as the anticipated board business, there will be other matters which arise that require the board's attention such as a merger or acquisition or major capital expenditure. An annual agenda may be set out in many different ways. A different format is provided in [Appendix 5 Audit committee and annual agenda](#).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

	Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 1	<ul style="list-style-type: none"> <li>- Board charter</li> <li>- Annual agenda</li> <li>- Retained authorities</li> <li>- Delegated authorities</li> <li>- Chairman, individual director and committee roles</li> <li>- Company secretary's role</li> <li>- Advisory boards</li> <li>- Full-year or interim financial reporting</li> <li>- CEO's position description and goal setting</li> </ul>	<ul style="list-style-type: none"> <li>- Investor relations strategy</li> <li>- Management delegations, accountability and approval levels</li> <li>- Board and management information system</li> <li>- Strategic plan (actions and accountabilities)</li> </ul>	<ul style="list-style-type: none"> <li>- Regulatory and compliance report</li> <li>- CEO/CFO report</li> </ul>	<ul style="list-style-type: none"> <li>- Conflict and disclosure of interests</li> <li>- Litigation and non-compliance issues</li> <li>- Insider trading</li> <li>- Share trading</li> <li>- Continuous disclosure</li> <li>- Access to company records</li> <li>- Meeting agenda/ papers/ preparation/procedures/ decision-making processes</li> <li>- Independent professional advice</li> </ul>

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

	Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 2	<ul style="list-style-type: none"> <li>– Board and committee succession planning</li> <li>– Risk appetite and risk management policy</li> </ul>	<ul style="list-style-type: none"> <li>– Risk management strategy</li> <li>– Risk profile and assessment</li> <li>– Management accountability for risk</li> <li>– Internal control environment</li> </ul>	<ul style="list-style-type: none"> <li>– Audit committee report</li> <li>– CEO/CFO report</li> <li>– Major project reports</li> <li>– Risk management report</li> </ul>	<ul style="list-style-type: none"> <li>– Protocols for board/ management interaction between board/ committee meetings</li> <li>– Decision-making outside the boardroom (circular resolutions)</li> <li>– Board minutes</li> <li>– In-camera minutes</li> <li>– Board member induction and education</li> </ul>
Meeting 3	<ul style="list-style-type: none"> <li>– CEO succession planning</li> <li>– Board training plan</li> <li>– Corporate planning and budgeting</li> </ul>	<ul style="list-style-type: none"> <li>– Reporting and communications strategy</li> <li>– Review of key policies and procedures</li> </ul>	<ul style="list-style-type: none"> <li>– Investor relations report</li> <li>– Remuneration committee report</li> <li>– CEO/CFO report</li> </ul>	
Meeting 4	<ul style="list-style-type: none"> <li>– Director appointments/ re- election</li> <li>– Director remuneration policy</li> <li>– Non-executive director remuneration</li> <li>– Director independence</li> <li>– Review of constitution</li> </ul>	<ul style="list-style-type: none"> <li>– Code of conduct</li> <li>– OH&amp;S plan</li> <li>– Corporate budgeting and planning</li> </ul>	<ul style="list-style-type: none"> <li>– Regulatory and compliance report</li> <li>– CEO/CFO report</li> </ul>	
Meeting 5	<ul style="list-style-type: none"> <li>– Directors' and officers' indemnity and insurance</li> <li>– Internal audit plan</li> <li>– External audit plan</li> </ul>	<ul style="list-style-type: none"> <li>– Whistleblower policy</li> <li>– IS strategy/policy</li> <li>– Director induction program</li> </ul>	<ul style="list-style-type: none"> <li>– Audit committee report</li> <li>– CEO/CFO report</li> <li>– Major project reports</li> <li>– Risk management report</li> <li>– Analyst and institutional presentations</li> </ul>	

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## • APPENDICES

## CONTACT US

	Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 6	<ul style="list-style-type: none"> <li>– Assurance map</li> <li>– Half-year strategy review</li> </ul>	<ul style="list-style-type: none"> <li>– Crisis management and continuity plan</li> <li>– CSR strategy</li> </ul>	<ul style="list-style-type: none"> <li>– Investor relations report</li> <li>– Nominations committee report</li> <li>– CEO/CFO report</li> </ul>	
Meeting 7	<ul style="list-style-type: none"> <li>– Related party transactions</li> <li>– CEO/CFO attestations</li> </ul>	<ul style="list-style-type: none"> <li>– Management attestations</li> </ul>	<ul style="list-style-type: none"> <li>– Regulatory and compliance report</li> <li>– Audit committee report</li> <li>– CEO/CFO report</li> </ul>	
Meeting 8	<ul style="list-style-type: none"> <li>– Director retirement/ removal</li> <li>– Statutory reporting</li> <li>– In-camera meeting with external auditor</li> </ul>	<ul style="list-style-type: none"> <li>– Capital management strategy</li> </ul>	<ul style="list-style-type: none"> <li>– Remuneration committee report</li> <li>– Whistleblower report</li> <li>– CEO/CFO report</li> <li>– Major project reports</li> <li>– Risk management report</li> <li>– External audit report</li> </ul>	
Meeting 9	<ul style="list-style-type: none"> <li>– CEO appraisal</li> <li>– Executive remuneration</li> <li>– CEO and senior executive service agreements</li> <li>– Annual report and accounts, including directors' report, solvency declaration and corporate governance statement</li> </ul>	<ul style="list-style-type: none"> <li>– Management and staff remuneration and HR policy</li> </ul>	<ul style="list-style-type: none"> <li>– Investor relations report</li> <li>– Audit committee report</li> <li>– CEO/CFO report</li> </ul>	<ul style="list-style-type: none"> <li>– Protocols for board/ management interaction between board/ committee meetings</li> <li>– Decision-making outside the boardroom (circular resolutions)</li> <li>– Board minutes</li> <li>– In-camera minutes</li> <li>– Board member induction and education</li> </ul>

• FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

• APPENDICES

CONTACT US

	Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 10	<ul style="list-style-type: none"> <li>– Dividend policy</li> <li>– AGM documentation</li> <li>– Shareholder profiling</li> <li>– External audit independence, appraisal, retention, appointment and remuneration</li> </ul>	<ul style="list-style-type: none"> <li>– Compliance program</li> </ul>	<ul style="list-style-type: none"> <li>– CEO/CFO report</li> </ul>	
Meeting 11	<ul style="list-style-type: none"> <li>– Board and individual director evaluation</li> <li>– Committee evaluation</li> </ul>	<ul style="list-style-type: none"> <li>– Tax strategy</li> </ul>	<ul style="list-style-type: none"> <li>– Regulatory and compliance report</li> <li>– Audit committee report</li> <li>– CEO/CFO report</li> <li>– Major project reports</li> <li>– Risk management report</li> <li>– Analyst and institutional presentations</li> </ul>	

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## • APPENDICES

## CONTACT US

# Appendix 3: Audit Committee Charter

## PURPOSE

The audit committee (the committee), appointed by the board of directors (the board), assists the board to fulfil its oversight responsibilities relating to:

- the preparation and integrity of the company's financial accounts and statements
- internal controls, policies and procedures that the company uses to identify and manage business risks
- qualifications, independence, engagement, fees and performance of the external auditor
- the external auditor's annual audit of the financial statements
- the resources, performance and scope of work of the internal audit function
- company compliance with legal, regulatory requirements and compliance policies.

Effective corporate governance depends on the active and collaborative participation of the committee, board of directors, external auditors, internal auditors, other assurance providers and management. Ensuring that this collaboration occurs effectively and efficiently is fundamental to the committee's success.

The existence of the committee does not diminish the board's responsibility to ensure the integrity of the financial reporting.

## AUTHORITY

The board has authorised the committee, within the scope of its duties and responsibilities set out in this charter, to:

- perform the activities required to address its responsibilities and make recommendations to the board
- resolve any disagreement between management and the external auditor, with areas of significant disagreement being advised to the board
- select, engage and approve the fees (within operational limits) for professional advisers that the committee may require to carry out its duties
- subject to the agreed protocol:
  - require the attendance of any company manager or staff member at meetings, as appropriate
  - have unrestricted access to management, employees and information it considers relevant to its responsibilities under this charter.

## MEMBERSHIP

The board chairman is responsible for nominating committee members for approval by the board.

The committee will comprise at least [insert number] members, all of whom should be independent (as defined in the board charter) non-executive directors.

The committee members must be 'financially literate' (i.e. able to read and understand financial statements and challenge information presented in committee meetings).



## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

At least one committee member must have 'accounting or related financial expertise' and at least one member must have relevant industry experience.

Committee member appointments are for an initial term of [insert number] years and the appointment is reviewed annually, or earlier, if circumstances dictate.

Committee member rotation is encouraged. Wherever possible, the board also ensures that changes in committee membership are staggered to maintain continuity.

The company secretary or their designate is the committee secretary.

## CHAIR

The board chair is responsible for nominating the committee chair for approval by the board.

The committee chair must be an independent, non-executive director and not the chair of the board.

Should the committee chair be absent from a meeting, the committee members present must appoint a chair for that particular meeting, who should not be the chair of the board.

## EDUCATION

The company will assist the committee in maintaining appropriate financial literacy, the company is responsible for providing new members with an appropriate induction program and educational opportunities, and the full committee with educational resources relating to accounting principles and procedures, current accounting topics pertinent to the company, and other resources, as reasonable requested by the committee.

## MEETINGS

The committee must meet at least [insert number] times per year. If a member is unable to be physically present, they may participate by video or tele-conference.

A notice of each meeting, with relevant supporting agenda papers, confirming the date, time and venue is to be forwarded to each committee member (with a copy to all directors) at least 5 working days before each meeting.

The committee chair, the board chair or any other committee member may call a meeting of the committee. The external auditor or internal auditor may request the committee chair or a committee member to call a meeting. The committee chair may waive the 5 working days notice period if agreed by all members.

The committee chair may invite any person or persons (other than duly appointed members) to attend meetings of the committee, but not necessarily for the full duration of the meeting, a standing invitation shall be issued to:

- other directors
- the CEO
- the CFO
- the internal and external auditors
- the compliance manager and other relevant members of management.

[Insert number] members will constitute a quorum.

The committee chair is not entitled to a second or casting vote.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## MINUTES

The committee secretary or delegate must prepare the minutes of the committee meeting within 7 working days. After the committee chair has given preliminary approval, the draft minutes are circulated to all committee members and the other board directors.

The minutes of the meetings must be confirmed and signed at the next committee meeting.

## COMMUNICATION

The committee is expected to maintain free and open communication with the external auditor, the internal auditor and management.

## DUTIES AND RESPONSIBILITIES

In assisting the board to fulfil its responsibilities, the duties of the committee are as follows.

### *Assessment of financial information*

Review any significant accounting and reporting issues, including professional and regulatory announcements, and understand their effect on the company's financial statements.

Review all published half-year and annual financial statements of the company, which require the approval of the board, based on the recommendation of the committee, and hold discussions regarding the financial statements with the external auditor and management before submission to the board.

The committee will pay specific attention to:

- the consistency of accounting policies and appropriate adoption of any new accounting standards
- considering the need for, appropriateness of and correct disclosure of, any changes made to the company's accounting policies
- the treatment and disclosure of complex or unusual transactions, including off-balance sheet structures

- significant judgements made by management in preparing the financial statements, including any signification accounting estimates
- the going-concern assumptions
- review, at least annually, the written attestations provided by the CEO and CFO for Australian reporting purposes that:
  - the company's financial records have been properly maintained
  - the company's financial statements and notes present a true and fair view, in all material respects, of the company's financial condition, and are in accordance with relevant accounting standards
  - the financial statements are founded on a sound system of risk management and internal compliance and control, and that the system is operating effectively in all material respects in relation to financial reporting risk
  - the company's risk management and internal control and compliance systems are operating efficiently and effectively in respect to its material business risks.

### *External auditors*

Recommend to the board the appointment, evaluation and removal of the external auditors.

Review and approve the external auditors' proposed audit plan and audit approach, including materiality levels.

Review and agree on the terms of engagement and the audit fees for the external auditors prior to the commencement of each audit.

Review the independence and objectivity of the external auditors and their compliance with all relevant independence requirements including:

- financial interests in clients and other business relationships
- employment and other personal relationships
- the level of non-audit services provided

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

- the rotation of audit partners
- limitations on external audit partner providing services other than audit, review or attestation.

Understand any material alternative treatment of financial information that has been discussed with management, including their ramifications, together with the treatment preferred by the external auditor.

Discuss the appropriateness of accounting policies, estimates and judgements.

Review the external auditor's summary management report, detailing the results and significant findings from the audit and management responses.

Meet regularly with the external auditor, without management present.

Resolve any disagreements between management and external auditors in the financial reporting and advise any significant issue to the board.

Review and approve the external auditor's process for the rotation and succession of audit and review partners, including their approach to managing the transition.

Obtain from the external auditors and review the independence declaration required under the Corporations Act.

### *Internal auditors (if any)*

Approve the appointment, remuneration and removal of the head of internal audit.

Review the internal audit charter to ensure the appropriate organisational structure, authority, access and reporting arrangements are in place. Ensure appropriate resourcing of the internal audit function.

Approve and review progress against the internal audit work plan:

review the internal audit coverage and annual work plan, and monitor progress of the work plan

- advise the board on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- oversee the co-ordination of audit programs conducted by internal and external audit respectively
- review significant internal audit reports and findings.

Review progress on management actions. Monitor progress against the annual work plan, including any significant changes to it, any difficulties or restrictions on the scope of activities and any significant disagreements with management.

Discuss issues with internal audit in the absence of management.

Consider the major findings of the internal audit reports and review management's response in terms of content and timeliness. Monitor management's implementation of internal audit recommendations. Periodically review the performance of internal audit.

### *Risk management and internal controls*

Approve the company's risk management policy and oversee the risk management system, including the risk management function and its resourcing.

Approve and monitor the company's risk profile developed by management, covering the principal enterprise-wide risks, including strategic, operational, legal and financial.

Review the operational effectiveness of the policies and procedures relating to risk and the company's internal control environment.

Review management evaluation of the effectiveness of internal controls.

Review the effectiveness of the company's insurance activities.

Ensure executive remuneration risk and controls are linked to the overall risk profile.

## FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## APPENDICES

## CONTACT US

## Compliance

Review the effectiveness of the company's approach to achieving compliance with laws, regulations, industry codes and company policies.

Review compliance with the company's values and related behaviours and the code of conduct. Review and monitor the effectiveness of policies, procedures and processes for complying with continuous disclosure requirements.

Obtain regular updates from management, legal counsel and the company secretary regarding compliance matters that may have a material impact on the company's activities. Review any correspondence from regulatory bodies regarding significant issues.

## Other responsibilities

Ensure that there is a process in place for the board chair and committee chair to be immediately informed of any issue of significant non-compliance or litigation. Oversee the process for the receipt, retention and treatment of information received from the internal whistleblower policy and procedures, and also from external complainants regarding matters relating to audit, the financial statements, internal controls or possible fraud.

Review any fraud reports. Review and discuss any reports concern any breach of fiduciary duty. Hold regular executive sessions with the CEO, CFO and other senior management to discuss private matters with the committee.

Act as a forum for communication between the board and senior management and internal and external audit. Review the effectiveness and level of cooperation between management, the internal auditor (if any), the risk management function (if any) and the external auditors. Review reports to the shareholders on the role and responsibilities of the committee. Conduct special investigations (if required). Perform any other duty of undertaking that the board may request from time to time.

Review, for potential conflict of interest situations, and pre-approve related party transactions on an ongoing basis.

## REPORTING

In addition to providing the board with a copy of the agenda, committee papers and minutes of its meetings, the committee will ensure that:

- the committee chair reports to the board on committee meetings, regarding all relevant matters and appropriate recommendations, in a written report (with supporting material) for noting or approval by the board
- the committee addresses any other reporting responsibilities.

## REVIEWS

To ensure that the committee is fulfilling its stewardship duties to the board, the committee will:

- review, at least annually, the committee charter and recommend to the board any appropriate amendments for approval
- review the annual agenda incorporating any changes in the charter
- conduct an annual assessment of its performance against its charter duties and responsibilities and provide a report of the findings to the board
- conduct an annual assessment of each committee member (the committee chair should provide a report of the findings to the board chair).

## FOREWORD

## THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

## GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

## GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

## GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## • APPENDICES

## CONTACT US

# Appendix 4: Audit Committee Induction Framework

Over the last few years the responsibilities of audit committees have increased significantly. It is no longer sufficient for audit committee members to have only a rudimentary knowledge of financial and regulatory matters. Committees cannot provide meaningful protection for shareholders unless their committee members are in a position to challenge management. To do this effectively, they must have the skills, knowledge and expertise, and be supported by access to independent advisors.

A formal induction program for new committee members is essential. A comprehensive committee induction program could include an information package, training sessions and meetings with key executive. The following outlines suggested inclusions in an induction framework.

## INFORMATION PACKAGE

An information package could include:

- committee charter
- committee annual agenda
- committee papers and minutes for the previous 12 months
- outline of the resources used by the committee to undertake its duties
- external auditor relationship
- accounting policies and approved practices
- regulatory and compliance framework for the company's business
- risk management policies
- risk management and control framework
- internal auditor's work plan
- details of the compliance framework, together with background on the key compliance obligations, both internal and external
- last annual report to the board on how the committee has discharged its duties.

## • FOREWORD

### THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

### GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

### GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance & Transparency
17. Risk Management

### GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Private Equity
20. Health, Safety and Wellbeing
21. Culture and Conduct
22. Cyber Security
23. Data Privacy and Personal Information
24. Human Rights and Modern Slavery
25. Automation and AI
26. Social Media

## GLOSSARY

## • APPENDICES

### CONTACT US

## TRAINING SESSIONS

Training sessions could be facilitated to guide audit committee members on:

- protocols
- effective meetings
- roles and accountabilities
- conflict of interest
- financial report review
- internal audit planning
- risk reporting review and attestation
- internal audit report review
- compliance reporting review
- external audit reporting.

## MEETINGS

Meetings to discuss the committee charter, how the committee operates, the main business and financial dynamics and other matters of significant could be held with the:

- committee chair
- CEO
- CFO
- internal auditor
- compliance officer
- company secretary and general counsel
- external auditor.

In addition, it may be useful to schedule discussions with other senior management regarding key operations and hold a follow-up meeting with the committee chair to discuss any issues arising from the induction program.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

# Appendix 5: Audit Committee Annual Agenda

This example annual agenda is linked to the example audit committee charter. In this example there are five scheduled committee meetings planned for the year.

Scheduled meetings					
	Dec	Feb	Mar	Jul	Sept
Foundation					
Review audit committee charter and annual agenda	Recommended timing				
Assess committee's independence, financial literacy, skills and experience				Recommended timing	
Determine number of meetings for forthcoming financial year			Recommended timing		
Committee chairman to determine meeting agenda and required attendees, including management and assurance providers	Recommended timing	Recommended timing	Recommended timing	Recommended timing	Recommended timing
Enhance financial literacy – update on current financial events	As required	As required	As required	As required	As required
Review of ongoing audit committee member education plans	As required	As required	As required	As required	As required
Conduct an assessment of the committee's performance against its charter and provide a report to the board					As required
Conduct an assessment of the individual member's performance					Recommended timing
Consider committee member rotation and succession planning					Recommended timing

Recommended timing       As required

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT

- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Assessment of financial information					
Review significant accounting and reporting issues					
Review financial matter affecting the half year					
Review and approve half year financial statements					
Review financial matters affecting the year end					
Review and approve annual financial statements					
Review attestations of the CEO and CFO for Australian reporting					
Review with management its evaluation of internal control structure and procedures for financial reporting, including any significant deficiencies or material weaknesses					
Scheduled meetings					
	Dec	Feb	Mar	Jul	Sept
Annually review and discuss with management and the external auditors, management's assessment of the effectiveness of internal control structure and procedures for financial reporting					
Review and discuss any reports concerning evidence of material violation or breaches of fiduciary duty					
Review and discuss any reports submitted by the external auditor detailing any instances of fraud or possible illegal acts on the part of senior management					
Review process, policies and procedures for continuous disclosure obligations					
Review conflicts of interest and related party transactions					
External auditors					
Recommend appointment, evaluation and removal of the external auditors					
Review audit plan and scope of audit work and any changes thereto					
Recommend terms of engagement and audit fees					
Consider policy in relation to non-audit services					

Recommended timing       As required



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT



- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Review and pre-approve non-audit services	As required
Consider objectivity/independence and obtain independence declaration from external auditor	Recommended timing
Review external auditors' report and findings and progress on management actions	Recommended timing
Discuss implications of any significant changes in accounting standards	As required
Discuss appropriateness of accounting policies, estimates and judgements	As required
Discuss external auditors' view on control environment, including fraud and risk management	As required
Resolve any disagreement between management and the external auditor in the financial reporting and report any significant issues to the board	As required
Discuss issues with auditor in the absence of management	Recommended timing
Ongoing communication (written/oral) between the external auditor with the committee	As required
Review report from external auditor on quality control procedures	Recommended timing
Review the external auditors process for rotation and approach for managing transition	Recommended timing
<b>Internal auditors</b>	
Approve appointment and review performance	Recommended timing
Review internal audit charter	Recommended timing
Review internal audit plan and any changes required to the plan including any resource issues	Recommended timing
Review progress against the audit plan	Recommended timing
Review significant internal audit reports and findings	Recommended timing
Review progress on management actions	Recommended timing
Discuss issues with the internal auditor in the absence of management	Recommended timing
Review the performance of internal audit <sup>390</sup> , including organisational structure, qualifications and independence.	Recommended timing

 Recommended timing       As required

390 Undertaken by an external party periodically, e.g. every 2 to 3 years.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

- 1. Directors' Legal Duties
- 2. Governance Roles
- 3. Government
- 4. Not-For-Profit Organisations
- 5. Proprietary Limited Companies
- 6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

- 7. Accountability to Shareholders
- 8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

- 9. Structuring an Effective Board
- 10. Company Leadership
- 11. Board Committees
- 12. Investment Management
- 13. Productive Meetings
- 14. Strategy and Planning
- 15. Receiving Assurance
- 16. Tax Governance & Transparency
- 17. Risk Management

GOVERNANCE OVERSIGHT



- 18. Environmental, Social and Governance (ESG)
- 19. Private Equity
- 20. Health, Safety and Wellbeing
- 21. Culture and Conduct
- 22. Cyber Security
- 23. Data Privacy and Personal Information
- 24. Human Rights and Modern Slavery
- 25. Automation and AI
- 26. Social Media

GLOSSARY

APPENDICES

CONTACT US

Risk management and internal controls			
Review risk management policy and risk management system	Recommended timing	As required	As required
Review risk profile	Recommended timing	As required	As required
Review internal controls and report to the board	Recommended timing	As required	As required
Review operational effectiveness of risk policies and procedures and internal control environment	As required	Recommended timing	As required
Review the effectiveness of the company's insurance activities	Recommended timing	As required	As required
Ensure effective remuneration risk and controls are linked to the overall risk profile	Recommended timing	As required	As required
Compliance			
Review legal and regulatory matters that may have a material impact on the company	As required	As required	As required
Review compliance report from management, and correspondence (if any) from regulatory bodies	Recommended timing	As required	As required
Review any correspondence from regulatory bodies	As required	As required	As required
Review compliance with company values and related behaviours, and the code of conduct	As required	As required	As required
Review compliance with continuous disclosure requirements	As required	As required	As required
Other responsibilities			
Review whistleblowing arrangements and reports	Recommended timing	As required	As required
Review fraud report	Recommended timing	As required	As required
Hold regular executive sessions with senior management	As required	As required	As required
Review level of cooperation between management, internal auditor and external auditor	As required	As required	As required
Review report to the shareholders on the role and responsibility of the committee	As required	As required	Recommended timing
Conduct special investigations and perform other activities, as appropriate	As required	As required	As required
Reporting			
Maintain minutes and report to the board	Recommended timing	As required	As required

 Recommended timing       As required



## Contact us

### Adelaide

**Justin Jamieson**  
**Partner**

**T:** +61 8 8236 3191

**E:** [jjamieson@kpmg.com.au](mailto:jjamieson@kpmg.com.au)

### Brisbane

**Rowena Craze**  
**Partner**

**T:** +61 7 3233 9682

**E:** [rowenacraze@kpmg.com.au](mailto:rowenacraze@kpmg.com.au)

### Perth

**Caron Sugars**  
**Partner**

**T:** +61 8 9263 4850

**E:** [ccobargsugar@kpmg.com.au](mailto:ccobargsugar@kpmg.com.au)

### Melbourne

**Richard Jamieson**  
**Partner**

**T:** +61 3 9288 6005

**E:** [jamiesonr@kpmg.com.au](mailto:jamiesonr@kpmg.com.au)

### Sydney

**Jeff O'Sullivan**  
**Partner**

**T:** +61 2 9335 8336

**E:** [josullivan1@kpmg.com.au](mailto:josullivan1@kpmg.com.au)

### Canberra

**Phillip Sands**  
**Partner**

**T:** +61 2 6248 1390

**E:** [pjsands@kpmg.com.au](mailto:pjsands@kpmg.com.au)

**[KPMG.com.au](https://www.kpmg.com.au)**

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2022 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

April 2022. 825963209AARC.