Australian Institute of Company Directors

OCTOBER 2024

AICD PRACTICE STATEMENT:

Directors' oversight of company compliance obligations

This AICD Practice Statement focuses on a director's duty of care and diligence under the Corporations Act as it applies to the oversight of a company's regulatory compliance obligations.

The AICD's Director Tool: General Duties of Directors provides a broader overview of the suite of fiduciary, statutory and common law duties in Australia.

This Practice Statement provides practical guidance and suggested steps for non-executive directors to discharge their duty, as well as 'red flags' to look out for. It does not constitute legal advice.

Executive summary

- A director must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise in that position and in the company's circumstances.
- To discharge that duty, a director must understand not only the commercial fundamentals of the company's business but also have awareness of the key areas of applicable regulation.
- This does not mean that a director must have detailed knowledge of the relevant regulation, guarantee compliance with obligations or eliminate all of the company's compliance risks.
- Nor does it mean that a company's breach of its regulatory compliance obligation automatically puts its directors in breach of their duty of care and diligence.
- There may be certain existential risks specific to the company that will require more intensive oversight by directors due to their significance.
- While decisions are made collectively by the board, a director's duty of care is owed individually.
- All directors must act with a reasonable degree of care and diligence, however what will be expected of a director will take into account the inherent responsibilities of directorship and any additional roles or responsibilities that a director may hold on the board.
- A director cannot ignore red flags or close their eyes to corporate misconduct. In these circumstances, a director should promptly raise the concern with the chair and/or board, make further enquiries of management, and if deemed necessary, seek external advice.
- While directors are entitled to rely upon the advice of management and advisers, directors must critically assess such advice and bring their own independent judgment to bear.
- Board minutes should concisely demonstrate directors' active oversight of a company's regulatory compliance, including constructive challenge of management.

1. INTRODUCTION

Australian companies are subject to a range of non-financial regulatory obligations - from work, health and safety, employee entitlements, cyber security and data protection, to anti-money laundering and anti-bribery and corruption laws. In many cases, they also may need to comply with sustainability related requirements, such as reporting on climate risks and emissions profiles, modern slavery risks in the supply chain, gender pay gap and the prevention of workplace sexual harassment.

This practice statement focuses on the duty of care and diligence of directors relating to their companies' regulatory obligations, but it should be noted that some regulatory obligations include specific personal obligations on directors (for example, work health and safety laws). It is also not uncommon for laws to impose accessorial liability on individuals on the basis of their involvement in contravening conduct by a company or another person. At the Commonwealth level, such liability can be criminal or civil.[1]

Regardless of sector or size, a company's obligations can be complex - presenting operational, compliance and conduct risks, while requiring ongoing monitoring by directors. A failure to comply can carry serious legal, financial and reputational consequences for organisations, including damaging relationships with customers, employees, shareholders and regulators.

ASIC has in recent years commenced proceedings focused on alleged breaches of a director's statutory duty of care and diligence[2] in relation to a company's breach of its non-financial regulatory compliance obligations. ASIC has also been clear that it expects directors to focus on, and manage effectively, the specific non-financial risks their organisations face as well as broader, more common risks (e.g. cyber security threats).

Against the backdrop of a growing focus on sustainability, increasing regulation and governance requirements in Australia, there is a question of what is required of directors in overseeing their company's compliance with these obligations.

The AICD's mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. To support directors in understanding their duty of care and diligence, the AICD commissioned barristers, Michael Hodge KC and Sonia Tame, to examine the application of directors' duty of care and diligence to a company's legal and regulatory compliance obligations (**Hodge-Tame Opinion**). Key questions to Counsel included:

- When does a breach of a company's regulatory obligation give rise to a breach of directors' duty of care and diligence?
- When are individual directors in breach of their duty versus the whole board?
- To what extent can directors delegate responsibilities or rely on the advice of others in overseeing a company's regulatory compliance?

Informed by the views of the Hodge-Tame Opinion, this AICD Practice Statement provides guidance on the steps that directors can take to effectively discharge their duty of care and diligence in overseeing their companies' compliance obligations.

1 For example, under the *Corporations Act 2001*(Cth) (where an individual can be deemed as involved in a contravention, even where they lack knowledge that there is a breach of the law by the relevant individual or company), or the Criminal Code Act 1995 (Cth) (which requires the individual to intend to assist the commission of the offence). See also Allens Linklaters advice, commissioned by the AICD, on **Criminal and Civil Frameworks for Imposing Liability on Directors**.

2 Section 180 of the *Corporations Act 2001* (Cth).

2. DIRECTORS' STANDARD OF CARE

A company's breach of its legal or regulatory compliance obligation does not necessarily mean that a director has breached their duty of care and diligence. Equally, it is not necessary for a company to actually breach its compliance obligation for a director to be found in breach of their duty of care and diligence.

It is also important to distinguish between director accountability for governance and individual wrongdoing. ASIC Chair, Joe Longo, has clarified that:

> "Not all poor company behaviour or even contraventions of the law by a company can be said to be failures of governance. There may well be an individual who can be identified as responsible for the wrongdoing and the issue may not be one of directors' duties."
>
> — ASIC Chair, Joe Longo,
> AICD's Annual Governance Summit 2023

What matters in determining whether a director has breached their duty of care and diligence is whether a director's conduct has caused or permitted, or they have failed to take appropriate steps to prevent, the company's breach (or the risk of a breach) of its regulatory obligation. The courts will take into account whether:

- there was a foreseeable risk of harm to the company's interests at the time of the relevant conduct; and
- a reasonable director would have been alert to this risk and taken appropriate action to mitigate that risk.

Directors must take reasonable steps to place themselves in a position to guide and monitor the management of the company. The duty of care and diligence requires directors to be aware of the key areas of regulation that apply to the company, its operations and key risks. Of course, directors should bear in mind that there are additional statutory duties that impose a set of obligations on directors in specific areas, for example under work health and safety laws or the Financial Accountability Regime (FAR) for financial services entities. These duties operate in parallel with a director's general duty of care and diligence, but are not the focus of this practice statement.

Directors must identify and act in the company's best interests (which is not limited to short term financial or commercial interests), and to actively safeguard those interests. The **Walker-Ng legal opinion** and **AICD's Practice Statement** make clear that directors' duty to act in good faith in the best interests of the corporation provides directors with considerable discretion to determine and act on what they consider to be in the best interests of the company, including by taking into account potential reputational impact. In doing so, the AICD encourages directors to take a long-term view of where the company's interests lie, and not to take an approach that risks significant reputational or stakeholder harm by maximising short-term profits.

Importantly, there is 'no one size fits all' for directors in satisfying the duty of care and diligence. The courts will take an objective view of what a 'reasonable director' would do depending on the circumstances. Relevant factors will include the type of company, its nature, resources and size, the regulatory environment, the particular roles and responsibilities of the director, what they knew, or should have realised had they made appropriate enquiries when put on notice, as well as what they did or did not do in performing their role.

It is conceivable that a director may breach their duty of care and diligence where, for example:

- a company breaches their regulatory compliance obligation (although this alone is insufficient);
- the director knew, or should have known, that there was a risk of harm to the company if this obligation was breached (for example, by causing significant financial and/or reputational harm);
- the director had reason to question or material doubts about the company's compliance with this obligation; and
- the director relied on the advice and assurances of management and did not make further enquiries about the company's compliance when a reasonable director in their position would have done so.

Conversely, a diligent director in these circumstances would:

- be aware of the key areas of regulation applicable to the company;
- be alert to 'red flags' indicating a risk of breaching this obligation and the harm that would flow from doing so;
- make enquiries of management and/or, if appropriate, seek an external review after raising the matter with the chair or the board; and
- reach their own informed but independent view on the risk of non-compliance and actions in place to mitigate that risk.

While the board should require management to have a system in place for compliance with all regulatory obligations, this does not mean that the board will have detailed insight or oversight of all compliance risks. The level of board and/or risk committee oversight required of entity's individual compliance risks will be commensurate with the materiality of those risks and the likelihood of those risks materialising. In other words, not all compliance risks can or should be treated equally. The board risk committee, where it exists, can play an important role in triaging and prioritising what matters require escalation to the full board.

There may be major risks that will have particular significance for an organisation. If not properly monitored or managed, these risks could result in significant harm to the company, including a serious threat to its continued existence. For example, the risk of food contamination for a food manufacturing business[3], the risk of foreign bribery by a natural resources company operating in a country with opaque approvals processes and acknowledged corruption problems, or airline safety risks for an aviation company. Directors are well advised to apply a laser focus to these existential risks, including requiring regular reporting from management, ongoing director education, input from external advisors, and verification or assurance of management's risk management approaches as appropriate.

RED FLAGS

Directors must remain alert to 'red flags' that require further enquiry. These may include, for example:

- Lack of, or gaps in, reporting or lack of candour from management to the board on key compliance matters;
- Critical reports or feedback from regulators suggesting poor risk management;
- Persistent lack of investment in key systems and risk areas;
- Frequent or increasing policy and protocol exceptions;
- A risk category that is rated as high and/or increasing;
- Unresolved or repeat internal control deficiencies relating to compliance matters;
- Lack of communication or information sharing across functional and business lines;
- Lack of evidence or documented diligence to support management assurances;
- High management confidence that risk controls are effective without regular review or verification;
- Increased customer/supplier complaints; and
- Significant outsourcing of services with limited management oversight or control.

3 Marchand v. Barnhill, No. 533, 2018 (Del. June 19, 2019) (Blue Bell Creameries USA Inc.).

3. MONITORING AND OVERSIGHT OF CORPORATE COMPLIANCE

Of course, it is not possible to eliminate all risk of exposure to a potential breach of a director's duty, just as it is not possible to eliminate all risks for a company.[4] It will often be impossible for directors to have a line of sight on the risk of breach of every regulatory obligation, particularly in large, complex entities.

What directors can influence is:

- a considered and system-based approach to monitoring a company's compliance risks;
- modelling and supporting a strong risk and compliance culture, including setting the company's risk appetite for legal and ethical non-compliance; and
- how the company responds in the event of a compliance breach including what risk management improvements are made and remediation steps taken.

Where directors anticipate a significant risk to the interests of the company, directors should seek a plan from management (informed by outside experts where appropriate) for the risk to be addressed, and if the risk eventuates into an actual harm, how it will be dealt with. Directors should critically assess whether the plan is adequate and hold management accountable for implementing, and revising, the plan as necessary. While this does not require a detailed inspection of day-to-day activities, directors should regularly monitor and seek updates from management at board or committee meetings or, if urgent, by ad hoc meetings or communications outside of board meetings.

MONITORING AND OVERSIGHT

Effective director oversight and monitoring practices may include, for example:

- Understanding accountabilities and ownership of key risks at management level, including risk management systems, policies and processes;
- Allocating responsibilities for specific board committee oversight and understanding if and how responsibilities are shared between multiple committees;
- Clearly defining the categories and levels of risk to be escalated to the board or board committee for detailed consideration;
- Setting expectations for regular reporting on:
  - new or emerging risks, or changes in existing risks, and what controls have or will be established;
  - non-compliance, incidents or "near misses";
  - internal and external audit reviews of compliance and independent risk assessments;
  - indicators of the risk and compliance culture within the organisation;
- Active engagement on management reports, including constructive challenge of management assumptions and assurances (that is, a "don't tell me, show me" approach);[5]
- Understanding findings and/or recommendations of independent expert reports, including having a reasonable basis for a decision to take or not take follow up action;
- Regular scanning of the external environment (for example, compliance matters receiving regulatory or media attention, particularly of industry peers); and
- Receiving briefings from management and/or external experts on current and emerging risk areas.

4 In monitoring a company's regulatory compliance, a director may also be under a mistaken belief about certain facts. In respect of certain claims by ASIC, a court will not make a declaration that a director has contravened their duty of care and diligence where the director has actively turned their mind to consider whether or not the facts existed and their mistaken belief about those facts is reasonable. Section 1317QC of the Corporations Act (the 'mistake of fact' defence) may be available in respect of an action brought by ASIC for a declaration of contravention, pecuniary penalty order or compensation order.

5 Prudential Inquiry into the Commonwealth Bank of Australia (CBA), Final Report, 30 April 2018 (available here).

4. INDIVIDUAL DIRECTOR VERSUS WHOLE-OF-BOARD ACCOUNTABILITY

The board as a whole has responsibility for the management of the company and directors generally make decisions collectively. However, a director's duty of care and diligence is owed by, and liability for a breach will attach to, each director individually.

Where a collective decision, or omission, of the board is made that results in the company breaching its regulatory compliance obligation, it is possible that every board member may have been in breach of their duty of care and diligence. However, liability is likely to depend on the particular roles, responsibilities and knowledge that each director had.

In some circumstances, more may be expected of directors who hold certain roles or positions (for example, the board chair, or chair or members of the board risk committee), as well as directors who have access to information about risks or potential harms that other directors do not.

The board chair has a key role to play in minimising the risk of information asymmetries across the board, particularly those resulting from the closer relationship between the chair and CEO, and should seek to ensure that information is appropriately shared with the board where it is relevant to their responsibilities and decisions to be made. At the same time, the chair of the risk committee should require that matters involving significant potential risk and harm to the company are escalated to the whole board as appropriate.

Critically, however, this should not imply that directors are better off to avoid seeking more information, making enquiries of management or external advisors, or taking on certain roles or board responsibilities. Directors should not ignore red flags or close their eyes to corporate misconduct. If facts come to a director's attention which raise questions or trigger doubt, they have a duty to make the appropriate further enquiries. This includes where directors are put on notice of risks, outside of formal board interactions, in the company's external environment. For example, if a director reads a media report that modern slavery practices have been detected at one of the company's key existing suppliers, when they know the company's modern slavery statement reports limited supply chain risks.

If, following relevant enquiries, a director remains unsatisfied with responses or the way the issue is being dealt with by management, there will be an individual decision to be made as to the appropriate course of action, taking into account the seriousness of the potential breach of a compliance obligation. While a director in these circumstances may feel it is prudent to resign to avoid personal risks in relation to the ongoing risk, they may also consider it is in the best interests of the company to stay on the board to continue to monitor the issue and press for the company to take appropriate action.

Much will however depend on a close analysis of the particular factual circumstances that arise when a breach is alleged, including the magnitude of the risk of harm and the probability of its occurrence, along with the expense, difficulty and inconvenience of taking alleviating action and any other competing responsibilities.

5. THE ROLE OF BOARD MINUTES

In determining whether a director has breached their duty of care and diligence in circumstances where the company has breached its regulatory compliance obligation, the court will have regard to what a reasonable director would have done in relation to the risk of that breach in all relevant circumstances. One of the key challenges for directors if their conduct is later called into question is that:

- risks tend to look more likely in hindsight to the court after they have manifested; and
- a director's consideration of those risks may look as if they lack the level of concern warranted once the risk has eventuated.

It is important that board meeting minutes concisely record directors' engagement on key risks, and that they sought further information from management and/or external advisors where they considered it necessary. The absence of any record showing directors' active oversight and monitoring will be unlikely to assist directors in defending an allegation that they breached their duty of care and diligence. The court will invariably place greater weight on contemporaneous evidence than an individual's recollection of events and discussions.

Individual directors can also record their own notes of matters considered, clarified or questions asked to show their active oversight subject to any board policy. However, directors should bear in mind that individual notes are discoverable and admissible in court as evidence. Board approved minutes are the official record of the meeting, and directors should therefore be mindful that notes taken individually could create a risk of ambiguous, inconsistent or incomplete records when viewed together with the formal board minutes. A clear and consistent approach should be agreed by the board and documented. This may include agreed protocols for individual note-taking that does not inhibit a full and frank discussion around the board table and the retention or deletion of annotations and notes recorded electronically or physically on board papers.

It is not necessary for board minutes to record every question asked, answer given or view expressed. As noted in the AICD and Governance Institute of Australia's **joint statement on board minutes**, minutes are not expected to be a transcript of the meeting or to record arguments for or against resolutions.

That said, a reference in the minutes to the board having "noted" a particular agenda item in the board pack relating to a risk is unlikely to persuade the court that the directors have substantively and appropriately engaged with the relevant issues. Rather, more compelling evidence of directors' active oversight would include references in the minutes to the time taken by the board to discuss the issue and constructively challenge management about the risks identified and actions being taken to manage them, particularly if steps are taken to follow up and address those items at or before subsequent board meetings.

BUSINESS JUDGMENTS

The 'business judgment rule' defence to an allegation of breach of the duty of care and diligence applies where directors make a decision 'to take or not take action' in respect of a matter relevant to the business operations of a corporation.[6] It does not apply where directors do not turn their mind to a matter.

The 'business judgment rule' defence is relatively restricted in the case of directors' 'oversight' of compliance risks and monitoring duties, and existing case law suggests that it is likely to be of limited utility in the context of a company's breach of regulatory compliance obligations.

That said, there may be some decisions involving compliance which could be characterised as relating to a company's business operations. For example:

- a budgeting decision made by the board to provide or not provide funds for the company to address particular compliance risks; or
- a decision by a director to seek or not seek further information or advice in relation to a matter concerning business operations.

RELIANCE ON INFORMATION OR ADVICE PROVIDED BY OTHERS

It is likely to be both appropriate and necessary for directors to rely on information or advice from certain others (including employees, management, professional advisers or experts, a board committee or other directors) in overseeing a company's regulatory compliance. Such advice cannot be blindly followed, however, and the director must believe on reasonable grounds that the person being relied on is reliable and competent.

Reliance on the advice of others may be an available defence for directors responding to an alleged breach of the duty of care and diligence, provided the reliance was made in good faith and after having made an independent assessment of the information or advice.[7] There must however be evidence that information or advice was, in fact, relied upon. Equally, directors cannot rely on the omission of information or silence from management or advisers on a matter.

For reliance to be reasonable, directors must critically consider the advice provided and whether it is appropriate to follow in the circumstances and/or whether further enquiry is required. Directors must make their own independent assessment of key compliance risks, informed by, but constructively challenging, management advice.

Depending on the circumstances, it may not be enough for directors to accept the assurances of management about the company's regulatory compliance. Certain matters may require independent review or investigation by competent external advisers. Some information or advice will also require greater scrutiny, particularly if a director possesses certain knowledge about the matter at hand (for example, relevant expertise and/or experience or involvement with a matter via a board committee role) or an issue has been publicly reported on.

DELEGATION

Unless a company's constitution provides otherwise, directors may delegate any of their powers to a director, a board committee, an employee or others who they reasonably believe are reliable and competent in relation to the power delegated.[8] This cannot however be a 'set and forget' approach.

In the context of the company's regulatory compliance obligations, a director's oversight responsibilities will remain irrespective of delegation. A director is permitted to delegate their powers, but not their duty of care and diligence. It may require directors to obtain ongoing reporting from their delegate and to respond appropriately to changing circumstances, particularly if they become aware of an increase in risk that poses a serious threat of harm to the company.

6 Section 180(2) and (3), *Corporations Act 2001* (Cth).

7 Section 189 of the Corporations Act. Section 189 is not available for executive officers of a company who are not directors of the board.

8 Section 198D of the Corporations Act. Section 198D is not available to executive officers, such as a Chief Financial Officer (CFO) delegating any of their executive powers to other corporate officers.

Australian Institute of Company Directors

ABOUT THE AICD

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

DISCLAIMER

This document is guidance prepared by the Australian Institute of Company Directors. It has been designed to provide general information and as a starting point for undertaking a board-related activity. The material in this document does not constitute legal, accounting or other professional advice. While reasonable care has been taken in its preparation, the Australian Institute of Company Directors does not make any express or implied representations or warranties as to the completeness, currency, reliability or accuracy of the material in this document. This document should not be used or relied upon as a substitute for professional advice. To the extent permitted by law, the Australian Institute of Company Directors excludes all liability for any loss or damage arising out of the use of the material in this document. The opinions of those quoted do not necessarily represent the view of the Australian Institute of Company Directors.

For more information

T: 1300 739 119
E: policy@aicd.com.au

JOIN OUR SOCIAL COMMUNITY

aicd.com.au

CCT1168_24