

Australian Institute of Company Directors

AICD PRACTICE STATEMENT:

Directors' oversight of company compliance obligations

November 2026

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 principles for effective monitoring and oversight in this practice statement will, however, have broad application for directors of organisations across all sectors.

This practice statement, originally published in 2024, has been updated in light of the Federal Court's decision in Australian Securities and Investments Commission v Bekier (Liability Judgment)[1] **(Bekier (Liability Judgment))**. It 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, directors must take reasonable steps to place themselves in a position to guide and monitor the management of the company. This includes taking a diligent and intelligent interest in the information available to them, seeking to understand that information, and applying an enquiring mind to their responsibilities.
- A director must understand the commercial fundamentals of the company's business and be aware of the key areas of material applicable regulation.
- This does not require directors to have detailed regulatory expertise or guarantee compliance with obligations, nor does a company's breach automatically place a director in breach of their duty of care and diligence.
- In some circumstances, relevant risks will require more intensive oversight by directors due to their significance for the organisation. Directors should oversee these risks with a level of rigour commensurate with their nature, scale and potential consequences.
- 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. What will be expected of a director will take into account the responsibilities of directorship and any additional roles or responsibilities that a director may hold on the board. There is a particular distinction between non-executive directors and executive directors.
- A director cannot be a 'passive recipient' of information, ignore red flags or close their eyes to corporate misconduct. If a director has a concern, they 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 on the advice of management and advisers, directors must critically assess such advice and bring their own independent judgement to bear.
- Board minutes should concisely demonstrate directors' active oversight of a company's regulatory compliance, including constructive challenge of management.

1 [2026] FCA 196 (Lee J).

1. Introduction

Australian organisations operate in a highly complex regulatory environment and are subject to a range of non-financial obligations, spanning areas such as workplace safety, employment, cyber security, privacy, anti-money laundering, anti-bribery and corruption, and sustainability-related matters including climate reporting, modern slavery, and the prevention of workplace sexual harassment.

Regardless of size or sector, a failure to comply in these areas can expose organisations to significant legal, financial and reputational consequences, including damaging relationships with customers, employees, shareholders, regulators and the broader community.

The board and directors individually play an important role in overseeing compliance with the organisation's obligations. This practice statement examines what the duty of care and diligence requires of directors in relation to an organisation's regulatory compliance.[2]

The Australian Securities and Investments Commission **(ASIC)** has in recent years focused on directors' oversight of non-financial risks, underscoring the importance of effective governance in this area.

To support directors in understanding their duty of care and diligence, in 2024 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. 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?

In 2026, the AICD commissioned Michael Hodge KC and Sonia Tame to update their opinion to reflect key legal principles confirmed and applied in Bekier (Liability Judgment) **(Hodge-Tame Opinion)**. While the case did not turn on any novel legal principles, it is a significant decision on the duty of care and diligence and involved ASIC taking a case against an entire board of an ASX-listed entity for alleged breaches of their directors' duties.

Informed by the views of the Hodge-Tame Opinion, this updated 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.

2 While not the focus of this practice statement, it should be noted that some regulatory obligations include specific personal obligations on directors (for example, 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. 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. See also Allens advice, commissioned by the AICD, on Criminal and Civil Frameworks for Imposing Liability on Directors.

2. Directors' standard of care

The duty of care and diligence requires directors to take reasonable steps to place themselves in a position to guide and monitor the management of the organisation. This includes taking a diligent and intelligent interest in the information available to them, understanding that information, and applying an enquiring mind to their responsibilities.

This requires awareness of the key areas of regulation that apply to the organisation, its operations and key risks but it does not demand omniscience. Nor does it impose a 'standard of perfection' on directors.[3]

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.

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 failed to take appropriate steps to prevent the breach or the risk of it occurring. 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, having regard to the magnitude of the risk, the probability of it occurring, any countervailing benefits to the company and the burden of taking steps to address it.

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

There is a distinction between non-executive directors and executive directors. Non-executive directors are not required to be involved in the affairs of the company at an operational level and are not expected to have the same knowledge of the company's operational activities as executive directors. Executive directors, on the other hand, bear responsibility for appropriately informing the board of matters material to its governance role, including serious legal, regulatory and reputational risks.

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

- a company breaches its regulatory 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 had material doubts about the company's compliance with this obligation and their ability to rely on management; 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, where appropriate, challenge assumptions or assurances;
- if appropriate, seek an external review after raising the matter with the chair or the board; and
- reach their own informed and independent view on the risk of non-compliance and actions in place to mitigate that risk.

3 Bekier (Liability Judgment) at [360] and [1953].

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.[4] 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.

To rely on the defence, a director must show that they made the business judgment in good faith for a proper purpose, did not have a material personal interest in its subject matter, informed themselves about the subject matter to the extent they reasonably believed to be appropriate, and rationally believed that the judgement was in the best interests of the company.

If directors, in the course of discussion at a board meeting, consciously turn their minds to a matter, and collectively reach a decision, such a conclusion, and the basis for it, should be recorded in the board minutes. The absence of contemporaneous records showing a judgement has been made could make it difficult to prove the defence.

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 others (including employees, management, professional advisers or experts, a board committee or other directors) in overseeing the organisation's obligations. Such advice cannot be blindly followed 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.[5] There must, however, be evidence that information or advice was, in fact, relied on. Equally, directors should not assume that the absence of reporting or silence from management or advisers on a matter means that there is no risk, particularly where there are red flags.

For the reliance to be reasonable, directors must critically consider the advice provided and whether it is appropriate to follow in the circumstances 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 appropriately qualified external advisers. Some information will also require greater scrutiny, particularly if a director possesses certain knowledge about the matter (for example, expertise in a matter via membership of a board committee) or an issue has been publicly reported on.

Delegation

Unless a company's constitution or specific regulatory requirements 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.[6] This cannot, however, be a 'set and forget' approach. In the context of the company's regulatory 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.

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

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

6 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.

3. Monitoring and oversight of corporate compliance

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 into, or oversight of, all compliance risks.

The level of board and/or risk committee oversight required of an organisation's compliance risks will be commensurate with the materiality of those risks and their likelihood of 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.

Some risks will be particularly significant to an organisation because of its operations, industry or regulatory environment. If not properly monitored or managed, these risks could result in significant harm to the organisation, including a serious threat to its continued existence. For example, the risk of food contamination for a food manufacturing business,[7] 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.

Further, some organisations will operate in high-risk contexts, such as sectors that are exposed to elevated legal, regulatory and reputation risk. This does not change the legal standard but does affect what is reasonably expected of the directors.

In these circumstances, directors are well advised to apply a laser focus to the relevant key risks on an ongoing basis, applying a proportionate level of vigilance, engagement and scrutiny. This may involve requiring regular reporting from management, ongoing director education, input from external advisers, 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:

- 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;
- information that does not align with a director's broader understanding of the business;
- signs of confirmation bias;
- 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.

> "Corporate governance failures seldom arise because information is entirely absent. More commonly, they arise because "the watchman sees the sword coming and does not blow the trumpet"; or because warning signs are insufficiently pursued; or because obvious questions are left unasked."
>
> **– Justice Lee, Bekier (Penalty Judgment)[8]**

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

8 ASIC v Bekier **(Penalty Judgment)** [2026] FCA 756 at [287].

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.[9] 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;
- a strong risk and compliance culture, including through modelling and supporting that culture and setting the company's risk appetite for legal and ethical non-compliance;
- the information that they receive in board packs, including setting expectations for reporting on material risks and requiring that they are provided with information in a form that is both comprehensive and capable of proper digestion; and
- how the company responds in the event of a compliance breach including what risk management improvements are made and remediation steps taken.

Board reporting

Board reporting is an essential enabling mechanism for directors to be able to discharge their duty of care and diligence.

Directors cannot rely on an inability to cope with voluminous board packs. The board can control the information it receives. The board should work with management to set the nature and volume of information it needs to fulfil its governance role.

The board's role includes:

- setting expectations, through the chair, in relation to board reporting, including the format, length and style of papers;
- requiring prompt escalation of material risks, including material compliance and regulatory risks;
- actively engaging with information provided, applying judgement, challenging management on the information received and seeking clarification or additional information where appropriate in the circumstances;
- regularly reviewing board reporting and whether it remains fit for purpose and aligned with the board's needs; and
- fostering a reporting culture that supports transparency, accountability and effective decision making.

Artificial intelligence **(AI)** may assist comprehension of papers, but its use should be controlled and formally governed by the board and it must not displace independent judgement and individual diligence. See AICD's AI use by directors and boards: Early insights for further discussion on how AI is being used within boardrooms and by directors.

Importantly, directors cannot be 'passive recipients' of information. A key aspect of their role is exercising active oversight. This includes bringing their experience, judgement and awareness of the external environment into the boardroom.

Where directors anticipate a significant risk to the interests of the organisation, the board should seek a plan from management (informed by outside experts where appropriate) for the risk to be addressed. The plan should cover required steps if the risk causes harm. 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.

If, following relevant enquiries, a director remains unsatisfied with responses or the way the issue is being dealt with by management, the director must decide what further action is appropriate. This would take into account the seriousness of the conduct or potential breach. While a director in these circumstances may feel it is prudent to resign to avoid personal liability in relation to the ongoing risk, they may also consider it is in the best interests of the organisation to stay on the board to continue to monitor the issue and press for appropriate action.

9 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.

Monitoring and oversight

Effective director oversight and monitoring practices may include:

- understanding accountabilities for key risks at management level, including risk management systems, policies and processes;
- allocating responsibilities for specific board committee oversight and understanding 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);[10]
- 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. 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, 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, 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.

Critically, however, this does not imply that directors should avoid seeking more information, making enquiries of management or external advisers, or taking on certain roles or board responsibilities.

These steps can place directors in a better position to identify emerging issues, oversee management's response and support active board oversight. A director cannot reduce their risk of personal liability by shielding themselves from relevant information. A director who chooses to 'put their head in the sand' exposes themselves to significant risk.

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.

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

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 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 advisers 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 usually place greater weight on contemporaneous evidence than an individual's recollection of events and discussions.

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 Effective board minutes and use of AI, minutes are not expected to be a transcript of the meeting or to record arguments for or against resolutions.

That said, questioning and challenge in board and committee minutes can assist in documenting that directors are exercising sustained scrutiny and insisting on explanation in circumstances where risks were obvious.

Board-approved minutes are the official record of the meeting, and directors should 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 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.

© 2026 Australian Institute of Company Directors Limited (AICD). Licensed under CC BY-NC-SA 4.0

For more information:

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

aicd.com.au