THE MODERN COMPANY SECRETARY IN 2026

Navigating climate, AI and boardroom change in Australia and New Zealand

Table of Contents

Executive summary

The modern Company Secretary (CoSec) is busy. The role has evolved, from largely administrative – taking and distributing minutes, preparing board packs and scheduling meetings – to be far more strategic (and rewarding).

CoSecs now are responsible for guiding their organisations through pressing concerns relating to climate and sustainability, governance, cybersecurity and AI adoption.

In this paper, we have identified seven ‘themes’ that will be at the forefront of CoSecs’ minds through 2026. They are:

1. Climate and sustainability reporting
2. AI in the boardroom
3. Moving from PDFs to a digital system of record
4. Cyber, privacy and data retention
5. ESG, culture and director conduct
6. Structural complexity and NZ incorporated societies
7. Capacity, skills and role evolution

One of the key challenges facing many CoSecs is a lack of appropriate tools to manage their responsibilities. Too often, they are working with tools and workflows built for a different era, which can struggle to keep sensitive information private and secure.

We strongly advocate for adopting a purpose-built, secure and extensible board software platform to serve as a digital system of record and to provide further capabilities – including AI – as required.

Our recommended high-level action framework for CoSecs is:

Understand → **Prioritise** → **Modernise** → **Lead**

The 2026 governance landscape in Australia and New Zealand

Governance is always evolving. In recent years, we've seen considerable changes, especially around climate and sustainability, governance expectations, cybersecurity and data privacy. These forces intersect on the Company Secretary's (CoSec's) desk. With more information to manage, higher expectations and greater personal accountability, the stakes have never been higher, nor the consequences more dramatic.

This is to say that 'governance' is not an abstract or academic concern. Governance is not only critical to business performance, it's also critical to CoSecs' careers and reputations. Following are some of 2026's key governance concerns.

Climate and sustainability

In Australia, the Climate-Related Financial Disclosure (CRFD) regime took effect in 2024. Companies under its rubric must disclose climate-related risks and opportunities, including:

- Governance
- Risk management
- Emissions data
- Climate resilience.

The regime is aligned with Australian Standards, and large businesses began reporting in 2024; medium-sized companies will begin reporting in 2026. The CRFD recognises that climate change presents financial risk; savvy organisations recognise that integrating climate policies into financial plans and public disclosures is critical to achieving compliance and building public trust.

In New Zealand, the Financial Markets Authority (FMA) published its review of climate statements in December 2024. Its goal was to improve future disclosures and reporting, with key findings in six areas:

1. Compliance and quality
2. Challenges faced
3. Materiality and fair presentation
4. Methods and assumptions
5. Scenario analysis
6. Future monitoring.

Businesses of all sizes must understand their obligations under NZ's climate regime and ensure their processes and reporting will satisfy the government and the FMA.

Governance expectations

Our modern media environment makes it easier now than at any time in human history to access information. More voices can be heard, meaning that there are more demands on companies and their boards for ethical behaviour, and more pressure to maintain their 'social licenses' to operate.

This scrutiny brings environmental, social and governance (ESG) reporting, organisational culture, diversity debates and stakeholder engagement to the fore. From shareholder activism to consumer boycotts and other pressures, CoSecs must not only ensure their organisations are well-governed; they must also ensure they're publicly seen to be well-governed.

Cybersecurity and data privacy

We all know that cybersecurity is a constant and pressing concern for organisations of all types and sizes, from local sports clubs to the largest multinational corporations.

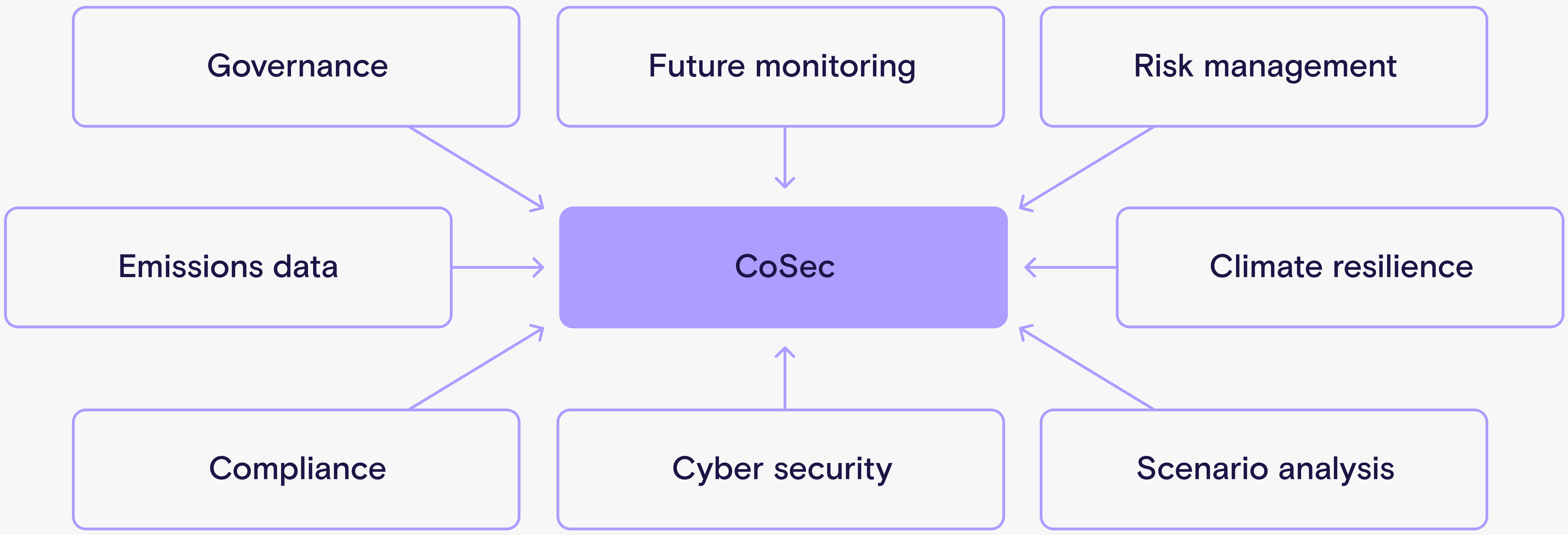
Compliance with privacy laws, both local and international, remains a key concern. CoSecs, directors and executives all must play their part in ensuring their organisations' policies and practices meet all legal and regulatory requirements, from data security to cyber resilience.

Seven themes for 2026

With the above in mind, we have identified seven key areas or themes for 2026:

1. Climate and sustainability reporting becomes real work
2. AI in the boardroom – use, risk and governance
3. Moving from PDFs to a digital system of record
4. Cyber, privacy and data retention – containing the blast radius
5. ESG, culture and director conduct
6. Structural complexity and the NZ incorporated societies crunch
7. Capacity, skills and role evolution

The remainder of this document explores these themes and their implications for CoSecs, and finishes with some practical suggestions and 'next steps'.



Climate and sustainability reporting becomes real work

Climate and sustainability reports are now board-level, director sign-off documents, not corporate social responsibility (CSR) side projects. Company Secretaries are responsible for orchestrating the process, including setting timelines, determining inputs, facilitating cross-functional approvals, and ensuring that board papers, minutes, and disclosures align.

Mandatory reporting from 2025

In Australia, the Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Bill came into effect on 1 January 2025. It requires organisations that meet certain criteria relating to their size (by revenue, assets, and employees), National Greenhouse Energy Reporting status (registered or not registered), and asset ownership (asset value and registration as a superannuation or corporate collective investment vehicle (CCIV)).

These criteria will identify organisations as belonging to Group 1, 2 or 3 for reporting purposes, which determines the start date for their mandatory reporting.

Similarly, environmental, social, and governance (ESG) reporting is mandatory for certain businesses. Companies must report on their ESG impacts in a structured and transparent manner. These reports will be scrutinised by regulators, investors and stakeholders alike.

In New Zealand, the existing mandatory reporting regime has undergone several significant changes. The Ministry of Business, Innovation and Employment (MBIE) announced in October 2025 three amendments to the country's climate reporting regime:

1. Changes to the climate-related disclosures (CRD) regime: raising the reporting threshold to NZD1 billion.
2. Removal of managed investment scheme (MIS) managers: removing the requirement for MIS managers to prepare annual climate statements.
3. Amendment of liability settings: reducing directors' and reporting companies' liability for climate reporting.

These changes will come into effect in 2026, as part of the Financial Markets Conduct Amendment Bill. A key impact will be the reduction in the number of reporting entities, from 164 to 76. They will remove 66 listed companies and 22 MIS managers from the regime.

Helpfully, the Financial Markets Authority (FMA), in its feedback on the first round of mandatory climate disclosures, noted that the reporting entities had put in an "enormous effort" and that overall, their disclosures "aligned with our expectations". It also noted how boards could improve on their efforts.

Benefits and challenges

Climate and ESG reporting help to ensure transparency, build investor confidence, maintain an organisation's social license and facilitate compliance with regulatory obligations. But producing these reports is not without challenges, including:

- Data collection and accuracy
- Compliance costs
- Changing regulations
- Integration with existing systems.

Ensuring that agendas, papers, and minutes are aligned and that climate governance is visible and defensible is a key outcome. From the CoSec's perspective, climate governance needs clear decision trails, historic access to papers, and reliable minutes.

THEME 2

AI in the boardroom – use, risk and governance

According to OnBoard's 2025 Board Effectiveness Survey, 69% of board directors are using AI today. The survey, conducted in partnership with the Governance Institute of Australia (GIA), found AI steadily making its way into board processes — from drafting minutes to summarising papers and preparing directors.

AI is steadily making its way into board processes, including drafting minutes, summarising long papers and preparing directors. Yet board processes – including, critically, security and other 'guardrails' – haven't kept pace. Uncertainty around confidentiality, access control and acceptable uses generates risks that may leave directors and other company officers liable.

AI use cases

With the above caveats in mind, AI has many promising use cases that could improve meetings, decision-making and follow-up. These include searching board materials, generating board minutes, tracking tasks and actions, identifying trends and risks, planning agendas and creating board books, and preparing directors.

Company Secretaries are typically asked to draft and summarise minutes, summarise lengthy board packs for time-poor directors, and draft agendas, resolutions and director communications. AI systems can assist with, or fully automate, these tasks, but caution is needed.

In the case of using AI to generate board minutes, for example, the AICD and GIA's 2025 joint statement Effective Board Minutes and the Use of AI notes that "AI should not be the sole tool relied on to prepare board minutes ... review and refinement of draft minutes will always be required by a governance professional ... to ensure that the minutes reflect board decisions accurately".

Approach AI with caution

The reasons for caution are twofold. First, AI systems pose unique risks that must be incorporated into company-wide risk assessments and data governance frameworks. AI systems are not infallible and can generate outputs with errors or even 'hallucinations'. IBM describes AI hallucinations as instances where the system "perceives patterns or objects that are non-existent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate".

Second, directors and company officers have statutory obligations to act with care and diligence, and in good faith, for the company's best interests, and not to use their position or information improperly. Accurate minutes are your board's best defence against any accusations of impropriety or misconduct. As noted above, while AI models can be useful for generating summaries, their outputs must be carefully reviewed by all interested parties before sign-off.

Further risks include sensitive information being pasted into unsecured public tools – such as commercially available large language models (LLMs) – and losing control of access privileges and compromising data retention regimes.

Embracing the benefits

The first step for any CoSec is to ensure their company has an AI governance framework for board-related tasks. This framework should specify where AI may be used, where it may not be used, and what data or information sources must be 'locked down' and made inaccessible to AI tools.

The UK Institute of Directors, in its paper AI in the Boardroom: The essential questions for your next board meeting, notes that "AI needs to be on the board agenda and considered seriously ... [it] should not be confined within the realms of IT, although the CIO may take responsibility". It further suggests 12 principles for ethical AI adoption:

1. Monitor the evolving regulatory environment.
2. Continually audit and measure what AI is in use and what they are doing.
3. Undertake impact assessments which consider the business and the wider stakeholder community.
4. Establish board accountability.
5. Set high level goals for the business aligned with its values.
6. Empowering a diverse, cross functional ethics committee that has the power to veto.
7. Document and secure data sources.
8. Train people to get the best out of AI and to interpret the results.
9. Comply with privacy requirements
10. Comply with secure by design requirements.
11. Test and remove from use if bias and other impacts are discovered.
12. Review regularly.

Locally, OnBoard's [Australia & New Zealand Artificial Intelligence Laws: Board of Directors' Guide] includes a useful overview of AI as it applies in the boardroom, covering legal oversights for both countries, notes on cross-border and international matters, lists of key steps and considerations CoSecs and boards should consider immediately, and more.

The goal is to ensure that companies can take advantage of AI's significant benefits by embedding it within a secure, properly governed board environment, rather than by individuals experimenting on an ad hoc basis with publicly available, consumer-grade tools.

What are AI hallucinations?

AI hallucination is a phenomenon where, in a large language model (LLM) often a generative AI chatbot or computer vision tool, perceives patterns or objects that are non-existent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

Source: IBM, *What are AI hallucinations?*

THEME 3

Moving from PDFs to a digital system of record

Information is more readily available than ever before. The ability to access data from a wide variety of sources is invaluable for board members, executives and Company Secretaries. Better information leads to better decisions, especially when it can be consumed in many different formats (including printed and digital documents, messages and emails, videos, podcasts and more) and in virtually any location (thanks to mobile devices and near-pervasive internet access).

There is a downside, however: information overload. The risk of being overwhelmed by emails, attachments, links to internal and external sources, and other ad-hoc tools and applications must be managed as carefully as any other risk.

Fragmented board information can take many forms, from conflicting document versions in various board members' inboxes to incomplete records when regulators or courts ask for a 'clean' history, and information over-sharing (with non-essential individuals able to access information) or under-sharing (with directors unable to access needed information).

As a result, CoSecs can find themselves spending significant time on document version control, making last-minute changes to board packs and managing information distribution lists. This is why for many organisations, deploying a digital system of record is a high priority. Providing a single, properly governed information hub for agendas, board packs, board minutes, policies, and decisions, these digital platforms enable them to manage information flows and establish trustworthy, secure systems of record.

A simple platform strategy

In its Organizational Digital Governance Report 2025, the International Association of Privacy Professionals (IAPP) surveyed its global membership base on "the extent to which organisations are defining, designing and deploying digital governance programs". More than 600 members from 45 nations and territories responded, and provided five "Key takeaways":

> **Classifying the organisational digital risk environment:**
> remains a complex and ever-changing task.

> **Interconnected risks are the new normal:**
> whether they be new AI models, connected devices or emerging technologies.

> **Digital governance approaches are forming:**
> to support innovations in technology and business processes.

> **Good digital governance matters regardless of the external regulatory environment:**
> as technology and regulators continue to evolve.

> **An effective digital governance approach may help accelerate – not hinder – innovation within an organisation:**
> as good governance can streamline innovation and boost competitiveness.

The 'before and after' view is striking: email chaos, version conflicts, security leaks, and constant messages and reminders across multiple document types and communication platforms, versus a single, secure online platform offering purpose-built tools and capabilities to manage messaging, voting, information sharing, discussions, minutes, and more.

There really is no comparison – and increasingly, no excuse not to modernise your governance procedures.

What is a system of record?

A system of record (SOR) is an authoritative source of business data. SORs can contain authoritative data on customers, employees, products, suppliers or other assets and entities related to everyday business processes. Organisations use SORs to streamline core business functions and business decisions.

Source: IBM, *What is a system of record?*

THEME 4

Cyber, privacy and data retention – containing the blast radius

Cyber incidents and privacy breaches increasingly involve board-level communications and materials. This means that Company Secretaries are often caught between transparency, legal risk and operational reality.

High-value, low-defence targets

Board communications are high-value targets, as they contain information that may be private, commercially sensitive or legally privileged – sometimes all three. Common weak spots include:

- Directors using personal email addresses and consumer messaging apps
- Board packs stored in ungoverned file shares
- No clear retention, archiving or legal hold processes.

In response, regulators are setting higher expectations around cybersecurity and digital resilience. How can busy CoSecs sift through the information overload and determine the key steps they should take to contain the 'blast radius' of a cyber attack or breach?

Best-practice guidance on cybersecurity and cyber governance abounds. We recommend relying on trusted sources, such as Cyber security priorities for boards in 2025-2026, a document jointly produced by the Australian Signals Directorate (ASD) and the AICD.

It addresses key questions including “Where should the focus be in 2025-26?” and includes notes on “What good cyber security governance look likes [sic] in 2025-26”. On a practical note, it suggests key questions CoSecs can ask of their governance, IT and risk teams, including:

- Does your organisation have event logging and threat detection?
- How does your organisation manage legacy information technology?
- How does your organisation manage its cyber supply chain risk?
- Does your organisation have a post-quantum cryptography transition plan?

Board information management

We recommend taking a three-pronged approach to shaping your organisation’s board information practices:

Least-privilege access and role-based permissions:
to ensure only the appropriate people have access to information.

Strong authentication for directors
to protect directors and provide them with secure access to their information.

Clear policies on what can and can’t leave the board platform:
to avoid misunderstandings, inadvertent sharing and other information leaks.

A simple framework: Prepare, protect, prove

With the above in mind, we recommend establishing a simple data security framework: prepare, protect and prove.

Prepare for incidents:
so that your organisation is never caught off-guard by an attack or a breach.

Protect board data:
so that it remains safe against inadvertent or accidental leaks, as well as against deliberate attacks.

Prove governance:
through audit-ready records, so you can demonstrate compliance and best practices.

THEME 5

ESG, culture and director conduct

Boards are scrutinised not just for their organisations' financial performance but also for how they address environmental, social and governance (ESG) matters, diversity, workforce culture and stakeholder trust.

These areas are harder to 'package' than financials. However, Company Secretaries still need to provide structure and evidence around reporting, to establish their organisations' credentials, not to mention compliance (where relevant).

The Harvard Law School Forum on Corporate Governance ('Harvard Forum'), in its note 'Integrating ESG Into Corporate Culture: Not Elsewhere, but Everywhere', states that while ESG is frequently discussed "in boardrooms, C-suites, investor meetings and regulators' remarks … [it] has yet to be mainstreamed, as it were, in internal corporate governance and operations".

Further, it states that "to be a meaningful factor in effectuating corporate purpose, ESG … must be integrated throughout corporate affairs".

ESG and culture issues can surface on board agendas for various reasons, including (but not limited to) whistleblower reports, media reports and stakeholder campaigns. CoSecs play a key role in protecting their organisations from 'blowback', typically by:

- Ensuring these issues are on the agenda early and not buried in 'other business'
- Curating the right information so directors can debate an issue's substance, rather than chasing data and sifting through news reports
- Recording how the board considered and responded to issues, so their deliberations and decisions are accessible whenever needed.

Directors under the spotlight

Our 2025 Board Effectiveness Survey Report included some alarming findings about 'people problems'. Specifically, respondents estimated that, on average, 36 per cent of board members are ineffective, while 87 per cent said that at least 10 per cent of their board wasn't pulling their weight.

It could be argued that to some extent, these responses reflect personal bias or difficult relationships – but the figures nevertheless point to the fact that not all members of all boards are as effective as they could be.

This is largely a cultural problem. If a board's culture is that some directors can 'get away' with not being fully across their duties, then it is inevitable that some will routinely fail to prepare adequately. This is one of the reasons why we regard culture governance as critical to any board's – and any organisation's– long-term success.

Establishing ESG and culture governance

Establishing ESG and culture governance as legitimate and important matters for the board's attention requires integrating them into the annual board calendar. This includes capturing enough detail in minutes and papers to demonstrate thoughtful oversight without over-exposing the organisation.

As the Harvard Forum notes, investors see value in ESG, integrating ESG is efficient and demonstrates commitment, and board oversight can forestall liability and reputational harm.

In its note 'A Board's Guide to Oversight of ESG', the Harvard Forum suggests a multi-part approach to helping Directors effectively govern ESG, and culture more broadly:

- Boards and management should identify which ESG elements are relevant and could rise to the level of "mission-critical" risk to the company.
- Boards should divide the various elements of ESG risk among their various committees or create a standalone ESG committee; even when so delegated, directors should regularly discuss ESG as a component of the company's long-term strategy and risk management.
- The board might consider amending its corporate governance guidelines to require best practices for benchmarking ESG practices, risk oversight and disclosure.
- The board should ensure that the division of responsibility for ESG matters, and the execution of those duties are documented appropriately through regular board agenda items and explicitly addressed.

A board's guide to ESG oversight

- **Identify** relevant ESG elements
- **Assign** ESG risks to relevant committees
- **Amend** corporate governance guidelines to require best practices
- **Include** ESG discussion on board agendas.

Source: Harvard Law School Forum on Corporate Governance, 'A Board's Guide to Oversight of ESG'

THEME 6

Structural complexity and the NZ incorporated societies crunch

Many Company Secretaries support multiple boards and entities, including parent organisations, subsidiaries, trusts, joint ventures and charitable arms. These roles require CoSecs to manage entity-level nuances across boards, committees, delegations, and documents, often with overlapping directors and executives. They must clearly understand these entities' structures, goals and activities, and maintain clear, correct distinctions and boundaries between them.

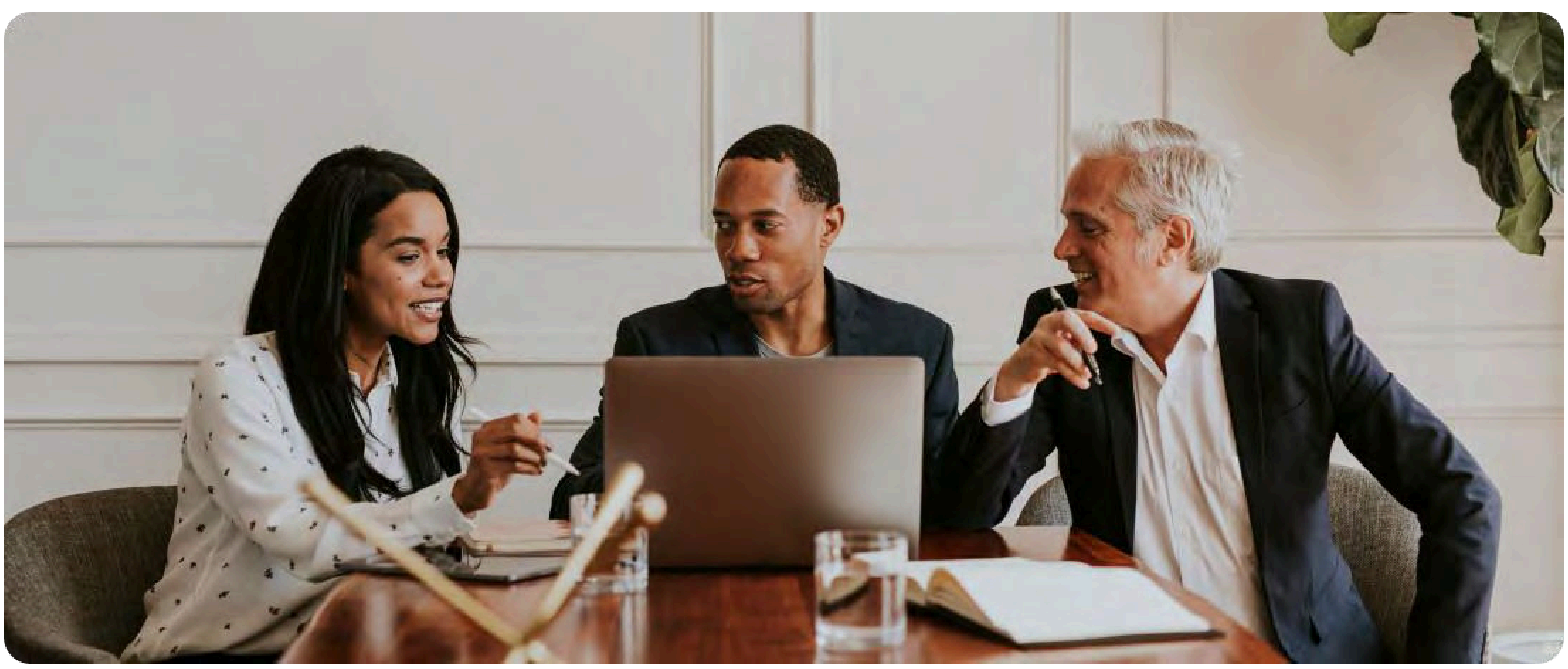
Changes for New Zealand's incorporated societies

In New Zealand, the Incorporated Societies Act 2022 "brings New Zealand's incorporated societies law into the modern era, with clearer governance, accountability and reporting requirements", according to Not-For-Profit Resource's note 'Incorporated Societies in New Zealand: Transitioning from the 1908 Act to the 2022 Act'.

The Act includes a hard deadline for re-registration: Inland Revenue (Te Tari Taake) notes that Incorporated Societies registered before 5 October 2023 must re-register by 5 April 2026 to retain their incorporated status.

Societies that don't re-register will need to apply for a new IRD number, as "when a society is deregistered, it loses its legal status as an incorporated body and will be treated as a new entity for tax purposes".

The change brings with it additional governance requirements and the opportunity for organisations to do more than the 'bare minimum' and ensure their governance is not merely compliant but rather is fully fit to provide effective oversight for years to come.



Multi-entity governance checklist

Supporting multiple boards and committees is a complex task. Below is a list of questions for CoSecs with such responsibilities: to help ensure you have the tools and capabilities you need.

- Do you understand your corporate structure, including all its groups and subsidiaries?
- Are any there cross-border governance concerns?
- Is your oversight model centralised, localised or a hybrid?
- Is there a group board in addition to individual organisation boards?
- Are there procedures in place for operational coordination and governance, including shared values and common goals?
- Are the group's ESG policies aligned across all entities?
- Do you have training in place to help directors and executives understand their multi-entity responsibilities?
- Do you have the technology platform you need to manage and maintain your responsibilities?
- For NZ incorporated societies, does your constitution include:
  - Your committee's powers and procedures
  - How the committee will be elected or appointed
  - How the contact person will be elected or appointed
  - How a person becomes a member of the society
  - Internal dispute resolution procedures
  - The name of a not-for-profit entity to which any assets will be distributed after you are wound up

THEME 7

Capacity, skills and role evolution

The AICD notes that a Company Secretary "is a governance specialist who provides advice to the board as well as fulfilling their legal responsibilities under the Corporations Act".

Yet the modern CoSec role is expanding faster than headcount or hours in the day. CoSecs must wear four 'hats' – administrator, board coach, governance architect, and risk guardian – and are expected to serve as governance strategists, educators, process designers, and technologists, in addition to managing their core workflows.

In particular, the shift from simply taking minutes and organising documents to a more strategic role – including shaping board agendas and organising forward plans, advising on board composition, evaluations and director development, and playing a key role in leading technological change in the boardroom – has added a significant burden.

This burden often requires CoSecs to educate themselves and gain new skills in areas such as technology, education, strategic planning and advocacy, among others. This load can lead to feeling constantly under pressure, feeling 'invisible' despite the heavy responsibility, and, in extreme cases, even burnout.

Making the CoSec role work

One relatively simple way for CoSecs to free up capacity is by automating low-value tasks, such as board pack compilation and distribution, and basic minute drafting. These automations allow CoSecs to spend more time on high-value governance leadership and other strategic tasks.

It's critical to have a good relationship with your Chair or CEO so you can discuss redefining your role and investing in better tools. If your organisation does not already have a digital governance platform in place, then now is a good time to discuss adopting one.

Not only will it enable you to optimise your job performance and better balance all your responsibilities, but it will also likely prove invaluable for simplifying, speeding up and securing all governance tasks. There are four key areas where a digital platform can assist you in your role:

Agenda and minutes precision:
create error-free agendas and minutes swiftly

Efficient meeting management:
refine meeting preparation and material handling

Superior stakeholder engagement:
boost satisfaction and streamline communication

Tailored board training:
benefit from personalised training and support tailored to your board's needs.

The 'four hats' every CoSec wears

What is a Company Secretary?

The company secretary in many organisations is a governance specialist who provides advice to the board as well as fulfilling their legal responsibilities under the Corporations Act.

Source: AICD, What is a Company Secretary?

Next steps and practical toolkit

Ready to take the next step? Two paths forward:

Join a conversation.
OnBoard hosts free webinars and roundtables on the evolving CoSec role, AI governance, cybersecurity and digital transformation. Visit our **Resource Centre** to see upcoming sessions.

See how your board information flows.
Book a consultation with our team. We'll map your current processes — from agenda creation to minute approval — and identify where time is lost, where risk lives, and where a governed platform could help.

2026 Company Secretary action plan

In the next 30 days: Understand

- Evaluate technology platforms
- Audit policies, protocols and workflows
- Clarify risk areas

In the next 90 days: Prioritise

- Select your technology platform
- Update policies, protocols and workflows
- Identify board skill and knowledge gaps

In the next 6 months: Modernise

- Implement your selected technology platform
- Publicise and operationalise updated policies, protocols and workflows
- Train directors

In the next 12 months: Lead

- Embed a modern meeting lifecycle
- Align climate, culture and ESG governance
- Clarify and refine the CoSec role

Is your governance future-ready?

Score yourself on the below six questions: one point per 'yes'.

1. Have we conducted an ESG audit? ____________
2. Are our data collection systems adequate to the task? ____________
3. Do our practices align with global standards? ____________
4. Have we engaged our stakeholders? ____________
5. Are we staying up to date on regulatory requirements? ____________
6. Do we have the expertise (internal or external) needed to meet our obligations? ____________

Evaluate your score:

0–2: Poor – your board information is potentially exposing you to unnecessary risk
3–5: Average – you have some effective procedures in place, but more can be done
6: Excellent – your board information is in very good shape and is well-managed

Regardless of your score, we recommend implementing a digital, AI-enabled board management platform to assist with all the checklist items (and more).

Answering these six questions will give you an immediate 'read' on your organisation's preparedness.

Checklist compilation

We have collected all the checklists presented in this document below.

Theme 2: AI in the boardroom – use, risk and governance

Principles for ethical AI adoption:

1. Monitor the evolving regulatory environment.
2. Continually audit and measure what AI is in use and what they are doing.
3. Undertake impact assessments which consider the business and the wider stakeholder community.
4. Establish board accountability.
5. Set high level goals for the business aligned with its values.
6. Empowering a diverse, cross functional ethics committee that has the power to veto.
7. Document and secure data sources.
8. Train people to get the best out of AI and to interpret the results.
9. Comply with privacy requirements
10. Comply with secure by design requirements.
11. Test and remove from use if bias and other impacts are discovered.
12. Review regularly.

Theme 4: Cyber, privacy and data retention

High-value, low-defence targets

- Does your organisation have event logging and threat detection?
- How does your organisation manage legacy information technology?
- How does your organisation manage its cyber supply chain risk?
- Does your organisation have a post-quantum cryptography transition plan?

Board information management

- **Least-privilege access and role-based permissions:** to ensure only the appropriate people have access to information.
- **Strong authentication for directors:** to protect directors and provide them with secure access to their information.
- **Clear policies on what can and can't leave the board platform:** to avoid misunderstandings, inadvertent sharing and other information leaks.

A simple framework: Prepare, protect, prove

- **Prepare for incidents:** so that your organisation is never caught off-guard by an attack or a breach
- **Protect board data:** so that it remains safe against inadvertent or accidental leaks, as well as against deliberate attacks
- **Prove governance:** through audit-ready records, so you can demonstrate compliance and best practices.

Theme 5: ESG, culture and director conduct

A board's guide to ESG oversight

- Identify relevant ESG elements
- Assign ESG risks to relevant committees
- Amend corporate governance guidelines to require best practices
- Include ESG discussion on board agendas

Theme 6: Structural complexity and the NZ incorporated societies crunch

Multi-entity governance checklist

- Do you understand your corporate structure, including all its groups and subsidiaries?
- Are any there cross-border governance concerns?
- Is your oversight model centralised, localised or a hybrid?
- Is there a group board in addition to individual organisation boards?
- Are there procedures in place for operational coordination and governance, including shared values and common goals?
- Are the group's ESG policies aligned across all entities?
- Do you have training in place to help directors and executives understand their multi-entity responsibilities?
- Do you have the technology platform you need to manage and maintain your responsibilities?
- For NZ incorporated societies, does your constitution include:
  - Your committee's powers and procedures
  - How the committee will be elected or appointed
  - How the contact person will be elected or appointed
  - How a person becomes a member of the society
  - Internal dispute resolution procedures
  - The name of a not-for-profit entity to which any assets will be distributed after you are wound up

About OnBoard

OnBoard is a board management platform built for the way governance actually works — the last-minute changes, the version control headaches, the security requirements that keep getting stricter.

More than 7,000 boards use OnBoard as their digital system of record: one secure place for agendas, board packs, minutes, policies, and decisions. AI capabilities help CoSecs draft minutes, summarise lengthy documents, and prepare directors — all within a governed environment where data never leaves the platform.

The themes in this paper — climate reporting, AI governance, cyber resilience, ESG oversight, and the expanding CoSec role — all require the same foundation: a single source of truth with clear audit trails, proper access controls, and tools that actually get used.

That's what OnBoard delivers.

Learn more: onboardmeetings.com