



WHITE PAPER:

AI in the Boardroom: A Practical Guide for UK & Irish Company Secretaries

Executive summary

Company Secretaries are no longer administrators; instead, they have become strategic partners who can make significant material contributions to their organisations' success.

This white paper explores how the role has evolved, with particular emphasis on how Artificial Intelligence (AI) is impacting boards and board management. It is forward-looking and gives an overview of AI's regulatory, operational and technology-related opportunities and challenges. These include:

- The Company Secretary's role
- Regulatory context
- Where AI delivers immediate value
- Implementing AI safely
- Common AI concerns
- Measuring impact
- Positioning for the future
- Next steps

One of the biggest challenges facing CoSecs and their boards is unauthorised use of AI tools. As directors often handle sensitive information, it is imperative that boards adopt purpose-built AI tools that can create agendas, summarise notes, draft minutes, capture decisions and follow-ups, retrieve prior decisions, and generate insights by analysing board and committee activity.

OnBoard creates such tools, but they are not discussed in this document; it is system-agnostic and presents an objective overview of how CoSecs can successfully engage with AI to streamline their challenging jobs and provide better strategic and operational assistance to their boards and their organisations.

Table of contents

Executive summary	2
The Company Secretary's changing role	4
Expanding responsibilities	4
The governance capacity challenge	4
Regulatory context: what AI must respect	5
AI use cases	5
Approach AI with caution	
AI governance is the key	6
Where AI delivers immediate value for Company Secretaries	8
Board and committee meeting preparation	8
Minute-taking and meeting records	8
Compliance monitoring and filing preparation	9
Governance advice and board support	9
Step-by-Step: implementing AI safely in governance workflows	9
Identify suitable tasks: high-volume, low-judgement	10
Keep AI inside your governance system of record	10
Establish clear human oversight and assurance	10
Document AI use for audit and assurance	11
Addressing Company Secretaries' common AI concerns	11
Privacy and security	11
Skills and work processes	12
Accuracy and efficiency	12
Legal and regulatory	12
Measuring impact: what success looks like	13
Digital governance is the key to success	13
Before and after	13
Positioning for governance's AI-enhanced future	14
Foundational principles	14
Implementation benefits	14
Next steps	14
Building your AI governance framework	15
Getting ready for AI has never been easier	15
Reference materials	16
About OnBoard	16

The Company Secretary's changing role

The Company Secretary (CoSec) role has evolved far beyond taking notes, preparing board minutes and filing compliance documents. As governance becomes more important for managing organisations through turbulent times and changeable regulatory environments, CoSecs are playing strategic roles and advising their boards.

As the [Chartered Governance Institute UK & Ireland's](#) CEO noted in December 2025, “governance professionals are operating in an environment defined by rapid technological change, increasing scrutiny and growing organisational complexity”, and we now see CoSecs making significant strategic and operational contributions to their organisations.

Citing a 2025 Bridgehouse report finding that 82 per cent of UK companies now “view their company secretary as a strategic partner” in key initiatives, such as digital transformation and sustainability, [Sage Governance](#) (Sage) notes boards now view their CoSecs as “essential contributors to governance, culture, and corporate strategy”.

This expanded role makes the CoSec's task more complex, but it also provides more opportunities to contribute to the organisation, exercise strategic judgment and develop professional skills.

● Expanding responsibilities

This role shift – from administrative to strategic – means that many responsibilities land on the CoSec's desk. Sage notes that these include:

- Providing board governance support to ensure decisions are transparent and well-documented
- Guiding directors on regulatory compliance and governance requirements
- Embedding ethical leadership and sustainability principles into board discussions
- Facilitating communication between the board, management, and shareholders
- Managing executive governance support systems that streamline digital board operations.

Assigning these tasks and responsibilities to a single role makes good sense from an efficiency and skills perspective, making the role more challenging and more satisfying.

● The governance capacity challenge

Modern CoSecs require a range of skills and abilities, including governance and compliance, strategic thinking and decision-making, technology and data security, and high-level communications and personal relationships.

It's a demanding job profile, and one of the best ways to manage workloads and preserve operational efficiency is to ensure your organisation has the processes, protocols and tools to support their work.

It may fall to the CoSec to review work processes and help select and implement new tools, such as AI systems or other technical solutions for data privacy, secure messaging, document access control and more. You should embrace these opportunities, both to ensure you're well-equipped to do your job and to learn new skills and build new relationships.



Regulatory context: what AI must respect

Artificial Intelligence is here to stay. Yet the data shows that its adoption is running ahead of governance. While a [2025 Moneypenny survey](#) found that 39 per cent of businesses are already using AI and a further 31 per cent are considering it, a [2025 Microsoft survey](#) of UK workers found that 71 per cent already use 'shadow AI' tools at work.

This finding dovetails with [2025 Guardian research](#), which found that only 13 per cent of UK adults discuss their AI use with senior staff (and nearly half think of it as a tool to help people who aren't very good at their jobs).

Company Secretaries must play a role in ensuring that their organisations have appropriate AI policies, that AI tools are rolled out and unauthorised tools are not used, and that their boards are using purpose-built AI-powered governance tools.

● AI use cases

AI provides many tools and capabilities that can benefit workers and board members alike. Focusing on governance, King's College London Legal Tech Society's post [The Evolution of Artificial Intelligence within Corporate Governance – An Overview](#) notes that while "AI's role in governance includes exciting opportunities" for boards, including "unprecedented degrees of efficiency in compliance functions", it also "poses risk ... with new legislation being introduced across many jurisdictions". It discusses two use cases in particular:

- AI as a board member or observer: Combining predictive and generative AI to support board decision-making has great potential, with some businesses experiencing above-average growth through data-driven recommendations.
- AI in compliance monitoring: Monitoring internal systems to detect suspicious or non-compliant activity, automatically checking documents and other AI-driven tasks can make compliance checking significantly faster and more accurate.

In both cases, however, caution must be exercised, especially around potential litigation risks.

● Approach AI with caution

There are two reasons to exercise caution regarding AI adoption, whether at the board or operational level. First, AI systems are not infallible and can produce 'hallucinations', or output errors.

AI hallucination

[IBM explains](#) that "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 nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate."

Such outputs can create litigation risks in many areas, including misrepresentation, data protection breaches and defamation, "all of which can be amplified by AI-generated outputs such as hallucinations", according to the King's College note.

We recommend regarding all AI outputs as drafts that must be reviewed by an appropriately skilled human. King's College's note concurs, stressing that corporate AI governance frameworks "must emphasise a 'human-in-the-loop' approach so that litigation risk can be managed by trusted and experienced professionals".

Statutory obligations

The second reason to approach AI with caution is that board members and other senior company officers have statutory obligations that cannot be delegated to AI systems. These are general duties to act honestly, in good faith and for the benefit of the organisation.

Specifically, the [Institute of Chartered Accountants in England and Wales \(ICAEW\)](#) notes that the [UK Companies Act 2006](#) imposes general duties (ss. 170–181) on directors; in Ireland, the [Companies Act 2014](#) (s. 228) imposes fiduciary duties (see boxed text).

Failure to comply with these duties could expose your organisation to risks including shareholder and regulatory scrutiny, reputational harm and even legal liability. These risks make it clear that an effective AI governance framework should be a priority for any modern organisation.

AI governance is the key

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.

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 nonexistent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

Source: IBM, [What are AI hallucinations?](#)



Director's duties UK

- 1 Duty to act within powers
- 2 Duty to promote the success of the company for the benefit of its members (shareholders) as a whole
- 3 Duty to exercise independent judgment
- 4 Duty to exercise reasonable care, skill and diligence
- 5 Duty to avoid conflicts of interest
- 6 Duty not to accept benefits from third parties
- 7 Duty to declare interest in proposed transactions or arrangements

Source: *Company Act 2006* ss. 171-178



Director's duties Ireland

- a act in good faith in what the director considers to be the interests of the company
- b act honestly and responsibly in relation to the conduct of the affairs of the company
- c act in accordance with the company's constitution and exercise his or her powers only for the purposes allowed by law
- d not use the company's property, information or opportunities for his or her own or anyone else's benefit [with certain exceptions]
- e not agree to restrict the director's power to exercise an independent judgment [with certain exceptions]
- f avoid any conflict between the director's duties to the company and the director's other (including personal) interests [with certain exceptions]
- g exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person
- h in addition to the duty under section 224 (duty to have regard to the interests of its employees in general), have regard to the interests of its members.

Source: *Companies Act 2014*, s. 228

Where AI delivers immediate value for Company Secretaries

What are AI's best use cases for Company Secretaries and board members? Current uses focus mostly on improving meetings, decision-making and follow-up. These include board and committee meeting preparation, minute-taking and meeting records, compliance monitoring and filing preparation, and governance advice and board support.

We emphasise that in all cases, editorial and legal responsibility remain with the CoSec.

● Board and committee meeting preparation

Board papers can be sizeable and complex. Using AI tools to generate easy-to-access summaries and otherwise assist with meeting preparation is an obvious use case.

In the absence of an authorised AI solution, directors may upload their board papers to a chatbot and request a summary. We do not recommend this procedure, as the papers' contents may then be uploaded to the chatbot's LLM (large language model), thereby putting sensitive or confidential information at risk.

A better approach is to deploy a purpose-built AI suite – embedded in a secure governance platform and operating within the system of record – to generate summaries, which can be checked for accuracy (by the CoSec or a member of their team) before issuance.

AI tools can also help Directors to prepare for their meetings. They can quickly summarise research, generate questions to ask and assist when seeking general information, for example, with queries such as 'We'll be discussing AI and cybersecurity at our next board meeting. What are some concerns for directors?'

Regardless of the specific tools used, directors must exercise considerable caution when using publicly available chatbots to avoid inadvertently disclosing sensitive information.

Only a secure platform with appropriate access and governance tools can provide the privacy, confidentiality and auditability you require.

● Minute-taking and meeting records

AI tools can record, transcribe and summarise meetings. This is a convenient, time-saving function, but care must be exercised, especially when using AI-generated text for board minutes. The Harvard Law School Forum on Corporate Governance, in its 2025 note '[AI Can Draft Board Minutes—But Should It?](#)', notes several considerations:

- **Confidentiality and cybersecurity:**
Companies must ensure their AI tools do not share information and that their providers have robust security measures.
- **Notice and consents:**
Meeting participants should be notified that they're being recorded and be able to raise concerns.
- **Accuracy:**
All AI-produced material must be checked by the CoSec or a delegate for accuracy.
- **Privileged and confidential information:** Using AI tools may not be appropriate when discussing privileged or highly confidential information.
- **Circulation and retention:** AI-assisted minutes and summaries should be securely stored and regularly audited.

- **Litigation holds:**

AI-generated materials may contain information that is subject to litigation holds; if so, it must be reviewable and appropriately stored for discovery.

- **Information barriers:**

Ensure that AI meeting tools are consistent with existing information stores, permissions and processes.

● Compliance monitoring and filing preparation

Compliance is becoming more complex as businesses and their supply chains grow. Traditional approaches are time-consuming, and CoSecs are under significant pressure. AI tools can potentially relieve this pressure, strengthening auditability and consistency when appropriately governed.

In its 2025 document *How AI is poised to reshape compliance functions*, KPMG notes that “intelligent agents are beginning to enable companies to enable compliance systems to adapt to regulatory changes in real time. They monitor evolving legal requirements, flag areas of risk, and support timely implementation”.

Use cases include text generation and document support, legal content review and clause auditing, contract and guideline checks, whistleblowing case management, compliance monitoring and policy development.

KPMG notes that trust, governance and security concerns are currently barriers to adoption. It emphasises that “companies must navigate evolving regulatory guardrails” for AI use, as well as train staff and ensure their data is properly structured and of high quality.

Used in this way, the compliance function can move from being a gatekeeper to “a trusted enabler of intelligent, ethical growth”.

● Governance advice and board support

Boards must evolve to address AI and ensure their organisations take full advantage of its capabilities while managing and mitigating its risks. As noted above, using AI does not alter directors’ statutory responsibilities, and regulators are still refining their approaches.

With appropriate safeguards in place, directors can use AI systems to support their information-gathering and decision-making duties. They can also – while always exercising due caution, and without surrendering their judgment – use AI systems to provide governance advice, generate insights and improve internal systems.

Step-by-Step: implementing AI safely in governance workflows

In practical terms, how can Company Secretaries ensure AI is implemented safely in their governance workflows? Reference documents such as ISO 42001 – AI Management Systems, an AI systems management standard, which “sets out a structured way to manage risks and opportunities associated with AI, balancing innovation with governance”, will help you understand the task’s scope and requirements.

With such knowledge in mind, and absent any existing AI implementation methodology, we suggest a four-pronged approach:

- Identify suitable tasks: high-volume, low-judgement
- Keep AI inside your governance system of record
- Establish clear human oversight and assurance
- Document AI use for audit and assurance.

● Identify suitable tasks: high-volume, low-judgement

AI systems are fundamentally data analysis and pattern-matching tools. This makes them ideally suited for automating high-volume, low-judgement tasks. Automating such tasks is typically faster and more cost-effective than assigning them to team members, freeing them to focus on low-volume, high-judgement work.

Suitable tasks can be easily identified as repetitive, high-volume operations with clear judgment or decision criteria that do not involve creativity, empathy, or complex judgment, and that use structured or semi-structured data. The benefits of such automation can be immediate and include:

- **Cost reduction:** by automating manual tasks and processes
- **Efficiency:** by allowing workflows to run faster and without bottlenecks
- **Consistency:** by delivering uniform decisions across all data
- **Insight:** by delivering structured data that can drive analytics and discovery.

● Keep AI inside your governance system of record

If you are using AI for governance-related tasks, then your AI systems, processes and outputs must reside within your governance system of record – your single source of authoritative governance data. It's a software platform that contains meeting notes, board documents, skills matrices, workflow documentation, succession plans, financial information and other sensitive, auditable data.

Keeping any AI systems you use within your governance system of record strengthens auditability and consistency in two ways. First, it prevents potentially sensitive information from being sent (intentionally or otherwise) to an external system; and second, it ensures that all data, workflows, and outputs remain visible and fully accountable.

● Establish clear human oversight and assurance

It's critical to set clear guidelines around when and how humans should oversee and intervene in AI systems. As noted above, AI systems are best suited for high-volume, low-judgement tasks. When being used for more complex tasks, human oversight is required.

This oversight includes not only checking AI outputs for accuracy (for example, by reviewing AI-generated board minutes) but also establishing an AI assurance framework.

The Department for Science, Innovation & Technology's *Introduction to AI assurance* states that AI assurance is "a crucial component of wider organisational risk management frameworks for developing, procuring, and deploying AI systems ... it is more important than ever for organisations to start engaging".

It refers to the government's policy paper, *A pro-innovation approach to AI regulation*, which includes (at 3.2.3) the following five cross-sectoral principles for AI adoption:

- 1. Safety, Security and Robustness:** AI systems should operate in a robust, secure, and safe manner, and risks should be continually identified, assessed, and managed.
- 2. Appropriate Transparency and Explainability:** AI systems should be appropriately transparent and explainable.
- 3. Fairness:** AI systems should not undermine the legal rights of individuals or organisations, discriminate unfairly against individuals, or create unfair market outcomes.
- 4. Accountability and Governance:** Governance measures should be in place to ensure effective oversight of the supply of AI systems, with clear lines of accountability across the AI lifecycle.
- 5. Contestability and Redress:** Where appropriate, users, affected third parties and actors in the AI lifecycle should be able to contest an AI decision or outcome that is harmful or creates a material risk of harm.

Establishing oversight and assurance will protect your organisation from risks and contribute towards compliance with relevant laws and regulatory requirements.

● Document AI use for audit and assurance

Governance, audit and assurance all rely on accurate documentation and record-keeping. As AI systems become more widespread, their use must be carefully documented to avoid audit and assurance problems. PWC, in its note '[Responsible AI and internal audit: what you need to know](#)', notes three potential risks of unchecked AI use with an organisation:

- Making decisions that violate expectations or requirements around privacy, fairness and lack of bias
- Complicating audit by evading explainability
- Introducing security and IP risks through data leakage or using external systems.

The solution is to involve audit teams early in your AI adoption, so they can evaluate frameworks, assess risks and help build trust in your AI systems. Specifically, they should:

- Establish a line of sight across the AI landscape
- Audit AI governance structures
- Assess the adequacy of AI risk and control frameworks
- Embed internal audit into Responsible AI design
- Equip your teams with AI.

Adopting an audit-ready AI approach will help ensure your systems, however they are used, will remain low-risk, accurate and accountable.

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. Organizations use SORs to streamline core business functions and business decisions.

Source: IBM, [What is a system of record?](#)



Addressing Company Secretaries' common AI concerns

Many Company Secretaries are worried about AI's accuracy. The Chartered Governance Institute (CGI) of UK and Ireland, in a [2025 survey of more than 600 Company Secretaries](#), found that "74% of governance professionals are concerned about the accuracy of AI-generated content in corporate reporting". Further, "37% say the biggest challenge is board understanding of AI technology".

As with any technology, AI has potential downsides alongside its benefits. While it is set to improve and advance as it develops, it's important to keep its limitations and implications in mind. Some of these have already been laid out. For CoSecs, we can identify several key areas of concern: privacy and security, skills and work processes, accuracy and efficiency, and legal and regulatory.

● Privacy and security

Data security is of the utmost importance for all modern organisations. AI systems present unique challenges on this front, as they require access to large amounts of data, much of which is confidential and commercially sensitive.

Yet the keys to managing these concerns are simple in concept, if not in execution. Your AI systems should be part of your governance system of record. They should be fully vetted and risk-assessed by your audit and IT teams before deployment.

The Information Commissioner's Office's [*Guidance on AI and data protection*](#) provides useful guidance on key privacy and security matters, as does the National Cyber Security Centre's [*Guidelines for secure AI system development*](#).

As noted, using external systems puts sensitive data at risk, with potentially serious implications. Therefore, task your audit, IT and HR teams with developing an AI use policy. Ensure all users throughout your organisation are apprised of their responsibilities; provide training if necessary and ensure the policy is strictly enforced.

● Skills and work processes

Over-reliance on AI systems can potentially erode work skills, limit knowledge development and curtail critical thinking. Clearly define your systems' use cases and ensure appropriate user oversight is in place.

We recommend CoSecs continue taking an active role in checking and refining documents, especially those drafted by AI, as all your legal and regulatory responsibilities remain in place regardless of your organisation's technology stack.

Similarly, ensure AI-assisted work processes remain properly supervised, checked, and audited by you or knowledgeable team members, as appropriate.

● Accuracy and efficiency

AI systems are data-dependent, so it's vital to ensure that they're trained and making decisions on high-quality data. Data should be accurate, up-to-date and correctly formatted to prevent avoidable errors and avoid biases.

Similarly, AI systems require constant monitoring. This allows you to identify and correct any errors or biases. Task your IT team with keeping your systems updated and conduct regular audits of their outputs to optimise their accuracy, efficiency and return on investment.

● Legal and regulatory

CoSecs must be mindful of AI's legal and regulatory implications in three key areas: ethics, compliance and accountability:

- **Ethics:** Ensure your AI systems adhere to legal and ethical frameworks. This will help avoid biased decision-making and ethical dilemmas and ensure transparency.
- **Compliance:** Comply with all relevant data protection laws and regulations and handle personal data securely.
- **Accountability:** Establish clear protocols for AI decision-making and error handling.

Organisations such as Companies House (UK) and the Companies Registration Office (Ireland) provide further resources to help ensure your protocols and processes meet their legal and regulatory requirements.

There is little doubt that AI presents challenges as well as opportunities; CoSecs are uniquely placed to ensure their organisations mitigate the former as they embrace the latter.

Measuring impact: what success looks like

Successfully deploying an AI-enhanced corporate governance system is an important task for any modern business, and it will require significant cross-team coordination within your organisation.

The first step for any Company Secretary is to ensure their company has an AI governance framework that takes a values-led approach. The [OECD AI Principles](#) are one such example; they take a “human-centric approach” to promote AI use that is “innovative and trustworthy, and that respects human rights and democratic values”.

Your governance framework should specify where AI may be used, where it may not, and which data or information sources must be ‘locked down’ and made inaccessible to AI tools.

● Digital governance is the key to success

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, providing five insights:

- 1. Classifying digital risk:** Classifying your organisational digital risk environment remains a complex and ever-changing task.
- 2. Interconnected risks:** Interconnected risks are the ‘new normal’, whether they be new AI models, connected devices or emerging technologies.
- 3. Digital governance:** Digital governance approaches are forming to support innovations in technology and business processes.
- 4. Governance matters:** Good digital governance matters regardless of the external regulatory environment; as technology and regulations continue evolving, governance is your best ‘insurance policy’.
- 5. Digital governance can accelerate innovation:** An effective digital governance approach can help accelerate – not hinder – innovation, as good governance can streamline workflows and boost competitiveness.

Establishing a governance framework based on these insights will help ensure your organisation has the overall approach and the specific measures it needs for success.

● Before and after

Establishing governance metrics, KPIs, and other systems is essential to ensure your AI governance, and more broadly, your overall technology and business governance, is successful. In this sense, success looks like business as usual – assuming your organisation is already well-governed.

On a board level, for example, the ‘before and after’ view of good governance 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, governed by a coherent, values-led framework.

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

Positioning for governance's AI-enhanced future

There's never been a better time than now to start positioning your organisation for governance's AI-enhanced future. Adopting a carefully considered set of foundational principles and implementation practices will position your organisation to respond to new developments – in technology, regulation and your operational environment – as they arise.

Company Secretaries play a critical role here. The [UK Corporate Governance Code](#) and the [Irish Corporate Governance Code](#) both note that the CoSec should support its board to “ensure that it has the policies, processes, information, time and resources it needs in order to function effectively and efficiently”.

● Foundational principles

The first step is to set out your foundational principles for AI adoption. We reiterate that the government's five [cross-sectoral principles for AI adoption](#) – safety, transparency, fairness, accountability and contestability – can serve as foundational principles for your organisation's AI policies.

● Implementation benefits

Adopting a clear set of implementation guidelines helps organisations to maximise their gains and minimise their risks from AI. By preventing ad hoc, ‘under the table’ deployments, they ensure that your organisation's approach to AI is coherent, consistent and properly governed. Australia's National Artificial Intelligence Centre's 2025 [Guidance for AI Adoption: Implementation practices](#) suggests four key reasons to take a systematic approach:

- 1. Build trust with customers and stakeholders when using AI:** Customers and the community want to know that organisations are using AI ethically and responsibly. Implementing good governance practices can help to build trust with stakeholders.
- 2. Secure the intended benefits of AI while mitigating the risks:** Implementation practices help organisations focus on the purpose of AI adoption, align activities with strategic goals, and integrate responsible AI practices with existing governance mechanisms.
- 3. Build the confidence of decision makers and leaders to adopt AI at greater scale:** By establishing good governance foundations and practices, organisations adopting AI can more confidently experiment and take risks with new AI-powered initiatives.
- 4. Follow a roadmap that can help to navigate a complex governance landscape:** The implementation practices align with international standards and regulations, supporting organisations to adopt leading practices globally in responsible AI.



Next steps

This white paper's 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 with publicly available, consumer-grade tools on an ad hoc basis.

AI services company Insightful AI's note '[AI Policy in the UK: What Every Organisation Needs to Know](#)' suggests a logical, seven-step approach for building your governance framework, based on the UK government's principles, encompassing scope and risk assessment, roles and principles, and documentation and compliance.

● Building your AI governance framework

Below is Insightful AI's seven-step process for building your AI governance framework:

Scope and risk assessment

1. Define the scope: identify all AI systems your organisation uses or plans to implement, and create an AI inventory
2. Map risks and opportunities: assess potential impacts on individuals, communities and your organisation

Roles and principles

3. Assign roles: Establish clear accountability and oversight roles for AI governance
4. Align with five principles: structure your policy around safety, transparency, fairness, accountability and contestability

Documentation and compliance

5. Document procedures: create clear processes for AI system assessment and establish review cycles for performance, accuracy monitoring and policy updates
6. Review and update regularly: schedule quarterly reviews of system performance and annual policy updates
7. Check for dual compliance: if you serve UK and EU clients, map your processes to both territories' requirements.

● Getting ready for AI has never been easier

OnBoard AI is a practical, secure and compliance-focused governance platform. We believe in providing state-of-the-art governance using state-of-the-art tools. We understand, however, that the most powerful software platform in the world will be of little use if it's too difficult to deploy and use. That's why we offer ongoing support and risk-free evaluation services.

To start your AI journey, contact us today for a consultation or demonstration. We can map your current board information flows and identify any gaps, and suggest how an AI solution might help your business perform better. It's obligation-free, and we'd be delighted to meet you.

Reference materials

Below are several key references providing detailed information on governance, AI and risk management.

Corporate Governance Frameworks

- [UK Corporate Governance Code \(FRC\)](#)
- [Irish Corporate Governance Code 2024](#)

Company Law and Statutory Compliance

- [Companies Act 2006 \(UK\)](#)
- [Companies Act 2014 \(Ireland\)](#)
- [Companies \(Corporate Governance, Enforcement and Regulatory Provisions\) Act 2024](#)
- [Companies House UK](#)
- [Companies Registration Office \(CRO\) Ireland](#)

Professional Company Secretary Guidance

- [Chartered Governance Institute UK & Ireland \(CGI\)](#)
- [ICAEW governance and company secretarial guidance \(UK\)](#)

AI, Data Protection, and Regulated Use

- [ICO guidance on AI and data protection](#)
- [NCSC / UK Government AI security guidance](#)
- [ISO 42001 \(AI Management Systems\)](#)
- [OECD AI Principles](#)

About OnBoard

OnBoard is a board management platform built for how governance 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.

Explore how AI can support your board

[LEARN MORE](#)