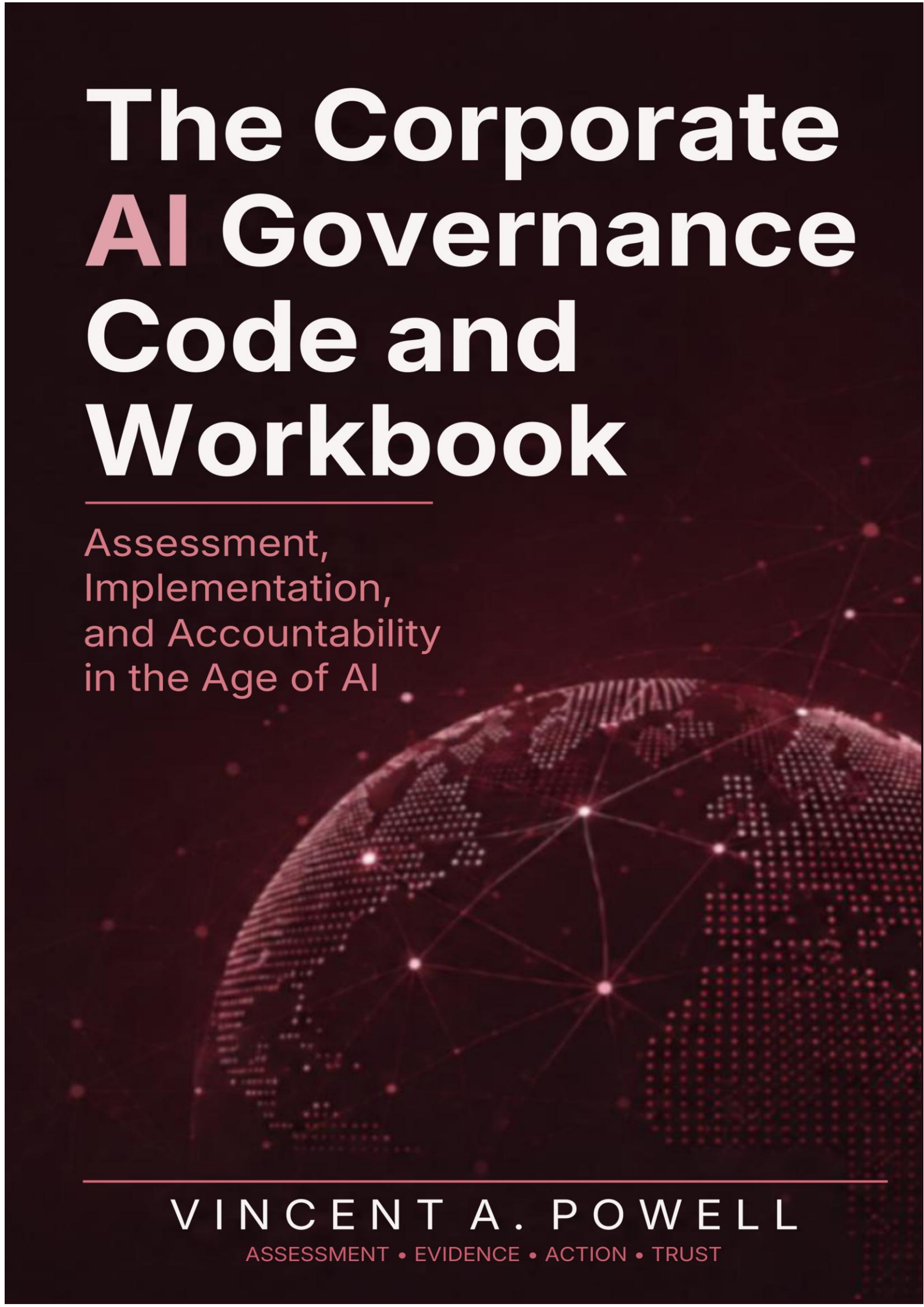
The Corporate AI Governance Code and Workbook

Assessment, Implementation, and Accountability in the Age of AI



VINCENT A. POWELL

ASSESSMENT • EVIDENCE • ACTION • TRUST

The Board's Guide to Corporate AI Governance Code and Workbook

Stewardship, Strategy, and Accountability in the Age of AI

Vincent A. Powell

The Board's Guide to Corporate AI Governance Workbook:

Stewardship, Strategy, and Accountability in the Age of AI

By Vincent A. Powell

ISBN TO BE ASSIGNED

This work was published by Oblongix Advisory Publishing.

DISCLAIMER AND LIMITATION OF LIABILITY

This book is provided for general informational and educational purposes only and does not constitute legal, financial, investment, accounting, technical, regulatory, privacy, data protection, or other professional advice. The content reflects the author's views as of May 2026 and may not be applicable to all organisations, industries, jurisdictions, or circumstances.

Readers must not rely on this book as a substitute for advice from qualified professionals. Decisions relating to legal compliance, financial investment, AI implementation, data governance, privacy, cybersecurity, or regulatory matters should be made only after consulting appropriate advisers familiar with the reader's specific situation.

This book discusses AI laws, standards, frameworks, and market developments for educational and strategic purposes only and does not constitute compliance advice for any jurisdiction or regulatory regime. Laws, regulations, standards, and industry practices are evolving rapidly, and readers are responsible for verifying current requirements.

All company names, product names, trademarks, and service marks are the property of their respective owners and are used solely for identification and educational purposes. Such references do not imply endorsement, affiliation, or sponsorship.

To the maximum extent permitted by law, the author and publisher disclaim all warranties and shall not be liable for any direct, indirect, incidental, consequential, or other damages arising from the use of this book or reliance on its content. Where limitations of liability are restricted by law, they apply to the fullest extent permitted.

Third-party materials are cited under applicable fair-use principles for commentary, criticism, analysis, and education. All interpretations and conclusions are the author's own. Full citations and connected sources are provided in Appendix 4.

Revision History

2026-05-05 First Edition

The Board's Guide to Corporate AI Governance Code and Workbook

Stewardship, Strategy, and Accountability in the Age of AI

Release 1.0

May 2026

This document sets out 'The Corporate AI Governance Code'. The Code is new and, at the date of publication, has no formal regulatory status; it is proposed as best practice for adoption by companies, and for consideration by regulators, governance bodies, and institutional investors as a framework for the oversight and standardised comparison of AI governance at board level.

Included in the 2nd half of the book is a full set of worksheets, consultation methodology and report descriptions which can be used by a Firm or another organisation to conduct and report on the status of compliance of the Firm to the code.

Preface

Artificial intelligence represents the most consequential general-purpose technology revolution deployed in business since the advent of the internet. It reshapes how organisations create value, make decisions, manage risk, and relate to their workforces and customers. It is not a discrete technology programme to be delegated to an individual function alone. It is a fundamental redesign of the enterprise.

Boards that govern AI well can create a durable competitive advantage, protect their stakeholders, and build the trust on which sustainable success depends.

This Code is proposed in recognition of three developments that now make specific AI governance guidance necessary:

- AI systems are increasingly making or materially influencing decisions that affect customers, employees, counterparties, and the public.
- The risks of ungoverned AI, including bias, opacity, dependency, and systemic failure, are now material in the financial and reputational sense.
- Existing corporate governance frameworks, while applicable, do not provide sufficient specificity to guide boards in discharging their AI-related duties.

This Code does not displace other codes or guidance, or the requirements of existing regulators. It supplements them, providing the AI-specific framework that boards, audit committees, remuneration committees, and their advisers require.

Table of Contents

AI Governance Code Scope and Application

This Code applies to any company, but it is particularly relevant to medium and large private companies. The Code applies on a proportionate basis. Companies should apply each Provision in a manner appropriate to the scale, complexity, and materiality of their AI activity, the size and resources of the organisation, and the sectors in which they operate.

The board's judgement on proportionality should itself be documented and, where material, disclosed. Proportionality is not a means of avoiding the discipline the Code requires; it is a means of applying that discipline in a form appropriate to the specific company.

The Code is intended to operate on a comply-or-explain basis. Companies are expected to comply with all provisions of the Code or explain in their annual report how alternative arrangements achieve equivalent outcomes and why those arrangements are appropriate for the company's circumstances.

Explanations should be specific and substantive. Generic explanations that do not enable shareholders to evaluate the board's approach will not satisfy this requirement.

Section A – Leadership and Purpose

A well-run company is one where the board sets clear direction, takes responsibility for outcomes, and ensures that AI serves the long-term interests of the company and its stakeholders. AI amplifies both the ambition and the risk of any organisation. The board must own both.

Principle A.1 – Board Ownership of AI Strategy

The board should ensure that AI is treated as a matter of strategic business importance and is not solely managed as a technology initiative.

Provisions

A.1.1 Strategic Integration. AI should be treated as part of corporate direction, not as an optional innovation track. The board should decide the role AI plays in long-term value creation and ensure that the company's posture on AI is aligned with purpose, strategy, culture, stakeholder expectations, and the economics of the business.

A.1.2 Executive Ownership. A named executive should carry enterprise-wide accountability for AI strategy and governance. This should not displace other leaders' responsibilities, but it should ensure there is a single point of executive answerability to the board.

A.1.3 AI as Business Redesign. The board should direct AI investment toward redesigning material processes and decisions, not toward a permanent state of pilots. AI should alter how the business works, not simply decorate the existing operating model.

Principle A.2 – Long-Term Agency and Technological Dependency

The board should actively manage the company's dependency on AI systems and external AI providers so as to preserve strategic control and operational resilience.

Provisions

A.2.1 Dependency Assessment. The company should know where its AI capability depends on external models, platforms, data sources, infrastructure, and specialist talent, and which of those dependencies are material.

A.2.2 Resilience and Control. Where the company depends materially on third-party AI, the board should ensure there are contractual, technical, and operational protections against loss of access, deterioration in service, or strategic disadvantage.

A.2.3 Strategic Optionality. The board should protect the company's ability to compete, adapt, and retain agency as AI markets evolve. That includes avoiding arrangements that quietly transfer proprietary know-how, data value, or workflow control to external providers.

Section B – Division of Responsibilities

There should be a clear division of responsibilities across the board and executive management for AI governance, with no individual exercising unfettered authority over AI strategy, deployment, or oversight.

Principle B.1 – Board Accountability for AI Governance

The board should establish clear lines of accountability for AI across the organisation and satisfy itself that these are operating effectively.

Provisions

B.1.1 Governance Structure. The board should decide how AI governance is distributed across the board and its committees, ensuring the arrangement is clear, coherent, and appropriate to the company's circumstances.

B.1.2 Management Accountability. Management responsibilities for AI strategy, delivery, risk, ethics, data, and oversight should be explicit and visible to the board.

B.1.3 Group and Cross-Border AI Governance. The board should ensure that AI governance standards operate coherently across the group, including subsidiaries, shared services, outsourced arrangements, and cross-border operations, and that local variation is controlled, justified, and visible.

Principle B.2 – Board Competence

The board should ensure it possesses sufficient knowledge and understanding of AI to discharge its governance responsibilities effectively.

Provisions

B.2.1 Expertise and Advice. The board should assess whether it has enough collective capability to oversee AI and should address gaps through development, appointments, or formal advice.

B.2.2 Board Briefings. The board should receive regular, structured information on the company's AI activity, external developments, regulatory change, and major incidents or risks.

B.2.3 Independent Scrutiny. Non-executives should be able to challenge AI-related proposals and should have access to independent expertise when needed.

B.2.4 Board and Director Use of AI. The board should govern its own use of AI and ensure that directors, board committees, and the board support process use AI tools in a manner consistent with confidentiality, privilege, recordkeeping, and sound judgement.

Section C – Decision-Making and Control

AI systems are increasingly embedded in the decisions that shape a company's strategy, its treatment of customers, and its relationship with employees. The board must ensure that decision rights are clearly defined, that human accountability is preserved, and that appropriate controls govern AI-influenced outcomes.

Principle C.1 – AI Decision Architecture

The board should ensure the company has a clear and documented framework governing how AI informs, supports, or makes decisions, with defined human accountability for all material outcomes.

Provisions

C.1.1 Decision Classification. Management should maintain a register of material decisions and classify the role of AI in each, distinguishing advisory, automated, and hybrid uses.

C.1.2 Human Accountability. Every material AI-assisted or AI-automated decision should have a named human accountable for outcomes.

C.1.3 Override and Escalation. Material AI systems should have functioning mechanisms for human override, escalation, and intervention, and those mechanisms should be tested.

C.1.4 High-Stakes Decisions. Where AI informs decisions with significant consequences for individuals, the company should provide documented human review processes and clear communication to affected parties.

C.1.5 Autonomous and Agentic Operations. Where AI systems can initiate, sequence, or execute actions with limited real-time human direction, the company should define and control the authority, boundaries, supervision, and intervention arrangements governing those operations.

Principle C.2 – AI Workflow Integration

The board should ensure that AI is embedded in the company's material business processes and that its value is measured against operational outcomes, not solely against capability metrics.

Provisions

C.2.1 Operational Deployment. Boards should expect AI investments to be integrated into real workflows with performance metrics that link AI use to business outcomes.

C.2.2 Portfolio Discipline. AI initiatives should be managed as a portfolio with clear priorities, deployment pathways, and decisions to scale, redirect, or stop work.

Section D – Risk, Assurance and Internal Control

AI introduces a distinct category of risk that does not map cleanly onto traditional enterprise risk frameworks. The board has primary responsibility for ensuring that AI risks are identified, assessed, and controlled appropriately throughout the technology lifecycle.

Principle D.1 – AI as Enterprise Risk

The board should ensure that AI risks are integrated within the company's enterprise risk management framework and that material AI risks are reported to the board on a regular basis.

Provisions

D.1.1 Risk Integration. AI risks should be assessed within the enterprise risk framework, with a taxonomy capable of capturing AI-specific characteristics.

D.1.2 Material Risk Disclosure. Where AI risks are material, they should appear in annual report risk disclosures and not remain hidden in internal technical reporting.

D.1.3 Risk Appetite. The board should articulate the kinds of AI use it is willing to tolerate and the degree of error, opacity, bias, and dependency acceptable in each context.

Principle D.2 – Internal Control and Assurance

The company should establish and maintain robust systems of internal control over AI systems and should provide the board with credible assurance that these controls are operating effectively.

Provisions

D.2.1 Lifecycle Controls. AI systems should be controlled across development, procurement, deployment, monitoring, change, and retirement.

D.2.2 Intervention Capabilities. The company should be able to suspend, override, or modify material AI systems when failures, unintended outputs, or changed conditions arise.

D.2.3 Incident Management. AI-related incidents should be identified, escalated, investigated, and remediated through a defined process, with significant matters reported promptly to the board.

D.2.4 Third-Party AI. Before using third-party AI, the company should perform due diligence and ensure ongoing monitoring obligations are built into contractual and operational arrangements.

D.2.5 AI Security, Red-Teaming and Abuse Resilience. The company should identify, test, and control the security and abuse risks specific to material AI systems, including adversarial manipulation, misuse, data leakage, unsafe tool access, and malicious or unintended system behaviour.

D.2.6 AI Governance in Transactions and Material Change Events. The board should ensure that material transactions and change events include explicit review of AI-related assets, liabilities, dependencies, and governance implications.

Principle D.3 – Data Governance

The board should ensure that data governance is treated as a business responsibility and is sufficient to support the safe, effective, and lawful use of AI.

Provisions

D.3.1 Data Ownership and Quality. Senior accountability for data used in material AI systems should be explicit, and the board should be satisfied that data quality is fit for purpose.

D.3.2 Lawful and Ethical Data Use. Data used in AI should be collected, processed, and retained lawfully and in ways consistent with reasonable stakeholder expectations.

D.3.3 Proprietary Data Assets. Boards should treat proprietary data as a strategic asset and set policies on how company data may be used by third-party models and whether rights to derived improvements are retained.

D.3.4 IP, Provenance and Recordkeeping. The board should ensure that the company can account for the provenance, rights position, and recordkeeping implications of data, models, prompts, outputs, and other artefacts used in or generated through material AI activity.

Section E – People, Culture and Remuneration

AI fundamentally alters the nature of work. A company that deploys AI without deliberate attention to its workforce (its skills, incentives, and trust) will fail to capture the technology's potential and will damage the organisational culture on which long-term success depends.

Principle E.1 – Workforce Impact and Transition

The board should oversee the impact of AI on the workforce and ensure that appropriate provision is made for skills development, redeployment, and workforce transition.

Provisions

E.1.1 Impact Assessment. Management should assess how AI changes roles, skills needs, and workforce composition and should report this as part of the company's people strategy.

E.1.2 Reskilling and Transition. Where AI materially changes role demand or skill requirements, the company should have credible, resourced plans for reskilling, redeployment, or workforce transition.

E.1.3 Workforce Disclosure. Annual reporting should explain how AI affects the workforce, including skills development, support for affected employees, and the company's approach to transition.

Principle E.2 – Remuneration and Incentives

Remuneration structures should support responsible AI adoption and should not create incentives for ungoverned, reckless, or unethical AI use.

Provisions

E.2.1 Outcome-Based Metrics. Where AI is material, incentive structures should measure outcomes enabled by AI rather than outdated activity measures that AI may make irrelevant.

E.2.2 Responsible Use Incentives. Incentive structures should reinforce responsible AI use and allow consequences where poor AI governance destroys value.

Principle E.3 – Culture and the Workforce Contract

The board should ensure that AI is deployed in a manner that preserves and strengthens the trust of the workforce and is consistent with the company's purpose and values.

Provisions

E.3.1 Workforce Engagement. Employees should be told clearly and honestly how AI is being used, how roles may change, and what the company's intentions are before material deployments occur.

E.3.2 Ethical Deployment. AI should not be used in employee surveillance, evaluation, or consequential decision-making in ways that are unexpected, disproportionate, or inconsistent with company values.

E.3.3 Shadow AI. The company should set clear, usable policies for employee use of AI tools, including consumer-grade and personal tools, and support responsible usage with guidance and training.

Section F – Transparency and Accountability

Transparency in AI governance builds the trust of investors, customers, regulators, and employees. Accountability ensures that when AI causes harm or fails to deliver value, there are credible mechanisms for redress. Both are essential to the social licence on which sustainable business depends.

Principle F.1 – AI Governance Disclosure

The board should ensure that the company reports clearly on its approach to AI governance, its material AI activities, and the manner in which AI risk is managed and overseen.

Provisions

F.1.1 Annual Report Disclosure. The annual report should describe board oversight of AI, executive accountability, AI risk management, and material AI risks or incidents.

F.1.2 Material AI Use. Where AI is material to stakeholders, the company should disclose the use in accessible terms and explain the governance arrangements around it.

F.1.3 Consistency with Regulatory Obligations. AI disclosures should be consistent with applicable regulator guidance and with international disclosure obligations where the company operates across borders.

F.1.4 Reliance on AI in Financial Reporting and Board Disclosures. Where AI materially supports financial reporting, management certification, forecasts, narrative reporting, or board-level disclosures, the board should ensure that reliance is controlled, reviewable, and consistent with the company's assurance obligations.

Principle F.2 – Accountability and Redress

The company should maintain credible mechanisms by which stakeholders can raise concerns about AI-driven decisions and seek appropriate redress.

Provisions

F.2.1 Redress Processes. Stakeholders affected by AI-influenced decisions should have accessible routes to raise concerns and seek timely, substantive review.

F.2.2 Explainability. Where AI materially influences consequential decisions affecting individuals, the company should be able to offer a meaningful explanation of the basis for that decision.

F.2.3 Regulatory Cooperation. The company should engage constructively and transparently with relevant regulators regarding AI governance and respond fully to inquiries.

Closing Statement

Good AI governance is not a compliance exercise. It is a discipline that must evolve as rapidly as the technology it governs. The companies that govern AI well will not merely satisfy regulators, they will earn the trust of the customers, employees, and investors on which long-term success depends.

This Code sets a minimum standard of board stewardship for AI. It is not a ceiling. Boards are encouraged to exceed its provisions where their circumstances, values, and ambitions demand it.

The ultimate purpose of AI governance is simply to ensure that organisations retain the capacity to act deliberately, control outcomes, and preserve their agency in a world increasingly shaped by AI.

Further Details

Further information including detailed questions and maturity assessment for Board Directors and Non-Executive Directors can be found in the book The Board's Guide to Corporate AI Governance - Stewardship, Strategy, and Accountability in the Age of AI written by Vincent A. Powell.

ISBN 978-1-9195185-5-8

https://www.theboardaiguide.com/

The Board's Guide to Corporate AI Governance

Assessment and Implementation Workbook

Vincent A. Powell

How to use this workbook

Use this workbook to assess current AI governance maturity, identify gaps, record evidence, assign actions, and track progress against each provision of the Corporate AI Governance Code.

Further instructions on recommended methodology can be found towards the end of the book after the worksheets.

Assessment Maturity Scale

Each provision contains the four maturity assessment questions from Appendix 1 of The Board's Guide to Corporate AI Governance. Questions retain their original numbering. Assessors should use evidence, interviews, and board or committee records to support each score.

Maturity scale

Score	Meaning
0 - Absent	No meaningful governance discipline is visible.
1 - Ad hoc	Practice exists in fragments or by exception, but is inconsistent and person-dependent.
2 - Defined	Policies, roles, or processes exist and are documented, but operation is not yet reliable or evidenced consistently.
3 - Operating	The discipline is functioning in practice and is visible in regular management and board activity.
4 - Assured	Operation is evidenced, tested, and subject to credible challenge, review, or assurance.
5 - Leading	The discipline is mature, adaptive, and demonstrably ahead of baseline practice.

Section A – Leadership and Purpose

A well-run company is one where the board sets clear direction, takes responsibility for outcomes, and ensures that AI serves the long-term interests of the company and its stakeholders. AI amplifies both the ambition and the risk of any organisation. The board must own both.

Risks and Issues

- ☐ AI treated as a technology project rather than a strategic business issue.
- ☐ No clear board-owned AI ambition, boundaries, or value thesis.
- ☐ Fragmented executive ownership.
- ☐ Permanent pilots with no business redesign or operational value.
- ☐ Hidden dependency on external AI providers, models, data, infrastructure, or talent.
- ☐ Weak resilience against provider failure, price changes, loss of access, or service degradation.
- ☐ Loss of strategic agency through vendor lock-in, data leakage, or transfer of know-how.

Principle A.1 – Board Ownership of AI Strategy

The board should ensure that AI is treated as a matter of strategic business importance and is not solely managed as a technology initiative.

Provision A.1.1 - Strategic Integration

A.1.1 Strategic Integration. AI should be treated as part of corporate direction, not as an optional innovation track. The board should decide the role AI plays in long-term value creation and ensure that the company's posture on AI is aligned with purpose, strategy, culture, stakeholder expectations, and the economics of the business.

Maturity assessment question	Response / notes
A.1.1.1 Has the board defined the role AI will play in the company's strategy?	
A.1.1.2 Can management explain how AI initiatives support long-term value rather than isolated experimentation?	
A.1.1.3 Is AI governance visibly connected to the company's purpose, culture, and stakeholder commitments?	
A.1.1.4 Do board papers discuss AI in business terms such as growth, productivity, resilience, quality, and trust?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
AI strategy paper	☐	☐
Board strategy papers and minutes	☐	☐
AI portfolio review pack	☐	☐
Business cases	☐	☐
Board calendar or agenda evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision A.1.2 - Executive Ownership

A.1.2 Executive Ownership. A named executive should carry enterprise-wide accountability for AI strategy and governance. This should not displace other leaders' responsibilities, but it should ensure there is a single point of executive answerability to the board.

Maturity assessment question	Response / notes
A.1.2.5 Is there one named executive the board can hold accountable for AI governance?	
A.1.2.6 Is the accountability enterprise-wide rather than confined to technology delivery?	
A.1.2.7 Is that accountability reflected in objectives and board reporting?	
A.1.2.8 Can the accountable executive demonstrate cross-functional authority and coordination?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
AI strategy paper	☐	☐
Board strategy papers and minutes	☐	☐
AI portfolio review pack	☐	☐
Business cases	☐	☐
Board calendar or agenda evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision A.1.3 - AI as Business Redesign

A.1.3 AI as Business Redesign. The board should direct AI investment toward redesigning material processes and decisions, not toward a permanent state of pilots. AI should alter how the business works, not simply decorate the existing operating model.

Maturity assessment question	Response / notes
A.1.3.9 Is each material AI initiative tied to a defined business process or decision domain?	
A.1.3.10 Are there explicit criteria for scaling, redirecting, or stopping AI initiatives?	
A.1.3.11 Does board reporting distinguish exploration from operational deployment?	
A.1.3.12 Can management show how AI has changed real workflows rather than only improved demonstrations?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
AI strategy paper	☐	☐
Board strategy papers and minutes	☐	☐
AI portfolio review pack	☐	☐
Business cases	☐	☐
Board calendar or agenda evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle A.2 – Long-Term Agency and Technological Dependency

The board should actively manage the company's dependency on AI systems and external AI providers so as to preserve strategic control and operational resilience.

Provision A.2.1 - Dependency Assessment

A.2.1 Dependency Assessment. The company should know where its AI capability depends on external models, platforms, data sources, infrastructure, and specialist talent, and which of those dependencies are material.

Maturity assessment question	Response / notes
A.2.1.13 Does the company have a current view of its material AI dependencies?	
A.2.1.14 Are dependencies classified by criticality and concentration?	
A.2.1.15 Has the board reviewed whether key providers are substitutable or strategically constraining?	
A.2.1.16 Do dependency assessments cover data, infrastructure, vendors, and model providers rather than only software contracts?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Dependency map or inventory	☐	☐
Vendor criticality assessment	☐	☐
Architecture diagrams	☐	☐
Contract summaries	☐	☐
Continuity or exit planning evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision A.2.2 - Resilience and Control

A.2.2 Resilience and Control. Where the company depends materially on third-party AI, the board should ensure there are contractual, technical, and operational protections against loss of access, deterioration in service, or strategic disadvantage.

Maturity assessment question	Response / notes
A.2.2.17 Are there contractual protections and oversight mechanisms for material AI providers?	
A.2.2.18 Has management tested how the company would respond to service disruption or provider exit?	
A.2.2.19 Can the company move key workflows, data, or configurations if required?	
A.2.2.20 Has the board decided which AI-related capabilities are too strategic to outsource completely?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Dependency map or inventory	☐	☐
Vendor criticality assessment	☐	☐
Architecture diagrams	☐	☐
Contract summaries	☐	☐
Continuity or exit planning evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision A.2.3 - Strategic Optionality

A.2.3 Strategic Optionality. The board should protect the company's ability to compete, adapt, and retain agency as AI markets evolve. That includes avoiding arrangements that quietly transfer proprietary know-how, data value, or workflow control to external providers.

Maturity assessment question	Response / notes
A.2.3.21 Has the board defined which capabilities or assets must remain strategically controlled?	
A.2.3.22 Do supplier arrangements protect proprietary data, knowledge, and process advantage?	
A.2.3.23 Are buy, build, and partner decisions evaluated partly on future optionality?	
A.2.3.24 Is the board discussing how AI changes the sources of competitive differentiation?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Dependency map or inventory	☐	☐
Vendor criticality assessment	☐	☐
Architecture diagrams	☐	☐
Contract summaries	☐	☐
Continuity or exit planning evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Section B – Division of Responsibilities

There should be a clear division of responsibilities across the board and executive management for AI governance, with no individual exercising unfettered authority over AI strategy, deployment, or oversight.

Risks and Issues

- Unclear allocation of AI oversight between board, committees, and management.
- Gaps or overlaps in accountability.
- AI governance inconsistency across subsidiaries, shared services, outsourcing, and jurisdictions.
- Insufficient board AI literacy or expertise.
- Board information that is irregular, unstructured, or too technical.
- Weak non-executive challenge or lack of independent expert advice.
- Unsafe board/director use of AI affecting confidentiality, privilege, records, or judgement.

Principle B.1 – Board Accountability for AI Governance

The board should establish clear lines of accountability for AI across the organisation and satisfy itself that these are operating effectively.

Provision B.1.1 - Governance Structure

B.1.1 Governance Structure. The board should decide how AI governance is distributed across the board and its committees, ensuring the arrangement is clear, coherent, and appropriate to the company's circumstances.

Maturity assessment question	Response / notes
B.1.1.25 Is there a clear and documented committee allocation for AI governance?	
B.1.1.26 Do committee remits reflect the actual AI issues facing the business?	
B.1.1.27 Can directors explain where AI risk, incentives, disclosure, and workforce matters are reviewed?	
B.1.1.28 Does the governance structure allow issues to move efficiently between committees and the board?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Governance map	☐	☐
Committee terms of reference	☐	☐
Delegations of authority	☐	☐
Responsibility matrix	☐	☐
Board and committee reporting	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision B.1.2 - Management Accountability

B.1.2 Management Accountability. Management responsibilities for AI strategy, delivery, risk, ethics, data, and oversight should be explicit and visible to the board.

Maturity assessment question	Response / notes
B.1.2.29 Are management accountabilities for AI documented and current ?	
B.1.2.30 Is the board receiving regular reporting against named responsibilities?	
B.1.2.31 Can management explain who owns strategy, delivery, risk, and ethics in practice?	
B.1.2.32 Have known gaps or overlaps in ownership been addressed?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Governance map	☐	☐
Committee terms of reference	☐	☐
Delegations of authority	☐	☐
Responsibility matrix	☐	☐
Board and committee reporting	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision B.1.3 - Group and Cross-Border AI Governance

B.1.3 Group and Cross-Border AI Governance. The board should ensure that AI governance standards operate coherently across the group, including subsidiaries, shared services, outsourced arrangements, and cross-border operations, and that local variation is controlled, justified, and visible.

Maturity assessment question	Response / notes
B.1.3.33 Has the board defined which AI governance standards must apply consistently across the group?	
B.1.3.34 Is there visibility over material AI activity in subsidiaries, shared services, outsourced arrangements, and overseas operations?	
B.1.3.35 Are local deviations from group standards documented, justified, and approved?	
B.1.3.36 Does board reporting surface cross-border regulatory, operational, and dependency issues in a coherent way?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Governance map	☐	☐
Committee terms of reference	☐	☐
Delegations of authority	☐	☐
Responsibility matrix	☐	☐
Board and committee reporting	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle B.2 – Board Competence

The board should ensure it possesses sufficient knowledge and understanding of AI to discharge its governance responsibilities effectively.

Provision B.2.1 - Expertise and Advice

B.2.1 Expertise and Advice. The board should assess whether it has enough collective capability to oversee AI and should address gaps through development, appointments, or formal advice.

Maturity assessment question	Response / notes
B.2.1.37 Has the board assessed its AI governance capability explicitly?	
B.2.1.38 Is there a plan to address capability gaps through development or advice?	
B.2.1.39 Do directors understand AI mainly as technology, or also as strategy, risk, workforce, and control?	
B.2.1.40 Is expertise available when difficult judgements or incidents arise?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Board skills assessment	☐	☐
Board briefing materials	☐	☐
External advice records	☐	☐
Non-executive challenge records	☐	☐
Board AI-use protocol	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision B.2.2 - Board Briefings

B.2.2 Board Briefings. The board should receive regular, structured information on the company's AI activity, external developments, regulatory change, and major incidents or risks.

Maturity assessment question	Response / notes
B.2.2.41 Does the board receive regular briefings on AI that are relevant to its responsibilities?	
B.2.2.42 Do those briefings cover internal activity, external change, regulation, and incidents?	
B.2.2.43 Are the briefings framed in business and governance terms?	
B.2.2.44 Does the board use the briefings to shape decisions rather than merely receive updates?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Board skills assessment	☐	☐
Board briefing materials	☐	☐
External advice records	☐	☐
Non-executive challenge records	☐	☐
Board AI-use protocol	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision B.2.3 - Independent Scrutiny

B.2.3 Independent Scrutiny. Non-executives should be able to challenge AI-related proposals and should have access to independent expertise when needed.

Maturity assessment question	Response / notes
B.2.3.45 Can non-executives obtain independent advice where the issue warrants it?	
B.2.3.46 Has independent scrutiny been used for major AI decisions or incidents?	
B.2.3.47 Do board papers support challenge rather than advocacy alone?	
B.2.3.48 Can the board demonstrate that executive proposals on AI are tested, not simply received?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Board skills assessment	☐	☐
Board briefing materials	☐	☐
External advice records	☐	☐
Non-executive challenge records	☐	☐
Board AI-use protocol	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision B.2.4 - Board and Director Use of AI

B.2.4 Board and Director Use of AI. The board should govern its own use of AI and ensure that directors, board committees, and the board support process use AI tools in a manner consistent with confidentiality, privilege, recordkeeping, and sound judgement.

Maturity assessment question	Response / notes
B.2.4.49 Has the board set explicit rules for its own use of AI?	
B.2.4.50 Do directors understand how confidentiality, privilege, and recordkeeping apply to AI-assisted work?	
B.2.4.51 Are AI-generated board summaries or drafts subject to verification and human judgement?	
B.2.4.52 Is the company secretariat equipped to support the board's use of AI safely and consistently?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Board skills assessment	☐	☐
Board briefing materials	☐	☐
External advice records	☐	☐
Non-executive challenge records	☐	☐
Board AI-use protocol	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Section C – Decision-Making and Control

AI systems are increasingly embedded in the decisions that shape a company's strategy, its treatment of customers, and its relationship with employees. The board must ensure that decision rights are clearly defined, that human accountability is preserved, and that appropriate controls govern AI-influenced outcomes.

Issues and Risks

- Unclear where AI influences material decisions.
- No named human accountable for AI-assisted or automated outcomes.
- Weak override, escalation, or intervention mechanisms.
- High-stakes decisions affecting individuals without proper human review.
- Autonomous or agentic AI acting beyond controlled authority.
- AI embedded into workflows without outcome-based performance measurement.
- AI portfolio sprawl without clear scale, stop, or redirect decisions.

Principle C.1 – AI Decision Architecture

The board should ensure the company has a clear and documented framework governing how AI informs, supports, or makes decisions, with defined human accountability for all material outcomes.

Provision C.1.1 - Decision Classification

C.1.1 Decision Classification. Management should maintain a register of material decisions and classify the role of AI in each, distinguishing advisory, automated, and hybrid uses.

Maturity assessment question	Response / notes
C.1.1.53 Does the company have a register of material AI-influenced decisions?	
C.1.1.54 Is the role of AI in each decision classified clearly?	
C.1.1.55 Is the register reviewed by the board or a committee?	
C.1.1.56 Does the classification drive governance consequences such as controls and human review?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Material AI decision register	☐	☐
Human accountability map	☐	☐
Override and escalation playbook	☐	☐
High-stakes review process	☐	☐
Action logs or audit trails	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision C.1.2 - Human Accountability

C.1.2 Human Accountability. Every material AI-assisted or AI-automated decision should have a named human accountable for outcomes.

Maturity assessment question	Response / notes
C.1.2.57 Does every material AI-assisted or AI-automated decision have a named human accountable for outcomes?	
C.1.2.58 Is accountability visible in role descriptions, decision rights, or governance records?	
C.1.2.59 Can management explain how accountable individuals exercise judgement over AI-influenced outcomes?	
C.1.2.60 Would the board be able to identify quickly who is answerable when a material AI decision goes wrong?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Material AI decision register	☐	☐
Human accountability map	☐	☐
Override and escalation playbook	☐	☐
High-stakes review process	☐	☐
Action logs or audit trails	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision C.1.3 - Override and Escalation

C.1.3 Override and Escalation. Material AI systems should have functioning mechanisms for human override, escalation, and intervention, and those mechanisms should be tested.

Maturity assessment question	Response / notes
C.1.3.61 Do material AI systems have functioning override, escalation, and intervention mechanisms?	
C.1.3.62 Are those mechanisms tested under realistic operating conditions?	
C.1.3.63 Do authorised staff know when and how to intervene?	
C.1.3.64 Can the company evidence that override rights are usable in practice rather than only in design?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Material AI decision register	☐	☐
Human accountability map	☐	☐
Override and escalation playbook	☐	☐
High-stakes review process	☐	☐
Action logs or audit trails	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision C.1.4 - High-Stakes Decisions

C.1.4 High-Stakes Decisions. Where AI informs decisions with significant consequences for individuals, the company should provide documented human review processes and clear communication to affected parties.

Maturity assessment question	Response / notes
C.1.4.65 Are high-stakes AI-influenced decisions identified and subject to documented human review?	
C.1.4.66 Are affected individuals told clearly that AI has materially informed the decision where appropriate?	
C.1.4.67 Do review processes have the authority to challenge, amend, or overturn AI-influenced outcomes?	
C.1.4.68 Could the company explain and defend its governance of high-stakes AI decisions to regulators and affected parties?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Material AI decision register	☐	☐
Human accountability map	☐	☐
Override and escalation playbook	☐	☐
High-stakes review process	☐	☐
Action logs or audit trails	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision C.1.5 - Autonomous and Agentic Operations

C.1.5 Autonomous and Agentic Operations. Where AI systems can initiate, sequence, or execute actions with limited real-time human direction, the company should define and control the authority, boundaries, supervision, and intervention arrangements governing those operations.

Maturity assessment question	Response / notes
C.1.5.69 Has the company identified where AI systems can take or sequence actions without case-by-case human approval?	
C.1.5.70 Are authority limits, reserved matters, and supervision arrangements defined for those operations?	
C.1.5.71 Can management evidence action logging, kill-switches, rollback, and environment segregation where relevant?	
C.1.5.72 Would the board be able to explain who authorised the autonomy, who is accountable for it, and how it would be stopped if behaviour became unsafe?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Material AI decision register	☐	☐
Human accountability map	☐	☐
Override and escalation playbook	☐	☐
High-stakes review process	☐	☐
Action logs or audit trails	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle C.2 – AI Workflow Integration

The board should ensure that AI is embedded in the company's material business processes and that its value is measured against operational outcomes, not solely against capability metrics.

Provision C.2.1 - Operational Deployment

C.2.1 Operational Deployment. Boards should expect AI investments to be integrated into real workflows with performance metrics that link AI use to business outcomes.

Maturity assessment question	Response / notes
C.2.1.73 Is AI operating in material revenue-generating or cost influencing workflows?	
C.2.1.74 Are outcome metrics defined and reviewed at board or committee level?	
C.2.1.75 Can management distinguish deployment from experimentation?	
C.2.1.76 Has the workflow itself changed, or has AI simply been added around the edges?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
AI portfolio review pack	☐	☐
Workflow redesign plan	☐	☐
Outcome metrics	☐	☐
Deployment pathway	☐	☐
Stop/scale/redirect decisions	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision C.2.2 - Portfolio Discipline

C.2.2 Portfolio Discipline. AI initiatives should be managed as a portfolio with clear priorities, deployment pathways, and decisions to scale, redirect, or stop work.

Maturity assessment question	Response / notes
C.2.2.77 Is the AI portfolio managed against clear priorities and deployment pathways?	
C.2.2.78 Are there explicit decisions to scale, redirect, or stop initiatives?	
C.2.2.79 Does reporting distinguish active experimentation from initiatives expected to deliver operational value?	
C.2.2.80 Can the board see how portfolio choices reflect strategy rather than accumulation of pilots?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
AI portfolio review pack	☐	☐
Workflow redesign plan	☐	☐
Outcome metrics	☐	☐
Deployment pathway	☐	☐
Stop/scale/redirect decisions	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Section D – Risk, Assurance and Internal Control

AI introduces a distinct category of risk that does not map cleanly onto traditional enterprise risk frameworks. The board has primary responsibility for ensuring that AI risks are identified, assessed, and controlled appropriately throughout the technology lifecycle.

Issues and Risks

- ☐ AI risks excluded from enterprise risk management.
- ☐ Material AI risks hidden in technical reporting rather than board or annual report disclosure.
- ☐ Undefined risk appetite for error, opacity, bias, autonomy, and dependency.
- ☐ Weak lifecycle controls from development/procurement through retirement.
- ☐ Poor incident detection, escalation, remediation, and board reporting.
- ☐ Third-party AI risks: diligence, monitoring, contracts, continuity, and assurance gaps.
- ☐ Data, security, provenance, IP, abuse, red-teaming, and transaction-related AI risks.

Principle D.1 – AI as Enterprise Risk

The board should ensure that AI risks are integrated within the company's enterprise risk management framework and that material AI risks are reported to the board on a regular basis.

Provision D.1.1 - Risk Integration

D.1.1 Risk Integration. AI risks should be assessed within the enterprise risk framework, with a taxonomy capable of capturing AI-specific characteristics.

Maturity assessment question	Response / notes
D.1.1.81 Are AI risks integrated into the enterprise risk framework rather than tracked separately as a technical issue?	
D.1.1.82 Does the risk taxonomy capture AI-specific characteristics such as bias, opacity, drift, concentration, and misuse?	
D.1.1.83 Are material AI risks reported regularly to the board or risk committee?	
D.1.1.84 Can management explain how AI risk reporting links to principal risks and risk ownership?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Enterprise risk register	☐	☐
AI risk taxonomy	☐	☐
Risk appetite statement	☐	☐
Board risk reporting	☐	☐
Annual report risk disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.1.2 - Material Risk Disclosure

D.1.2 Material Risk Disclosure. Where AI risks are material, they should appear in annual report risk disclosures and not remain hidden in internal technical reporting.

Maturity assessment question	Response / notes
D.1.2.85 Has the company assessed whether AI risk is a principal risk?	
D.1.2.86 Are material AI risks reflected in annual report disclosure where appropriate?	
D.1.2.87 Is external disclosure consistent with internal risk reporting?	
D.1.2.88 Would investors be able to understand the nature of the AI exposure from the annual report?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Enterprise risk register	☐	☐
AI risk taxonomy	☐	☐
Risk appetite statement	☐	☐
Board risk reporting	☐	☐
Annual report risk disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.1.3 - Risk Appetite

D.1.3 Risk Appetite. The board should articulate the kinds of AI use it is willing to tolerate and the degree of error, opacity, bias, and dependency acceptable in each context.

Maturity assessment question	Response / notes
D.1.3.89 Has the board defined an AI risk appetite in operationally useful terms?	
D.1.3.90 Does appetite differ by class of use or level of consequence?	
D.1.3.91 Are out-of-appetite uses escalated and visible?	
D.1.3.92 Is appetite reviewed as the company's AI use expands?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Enterprise risk register	☐	☐
AI risk taxonomy	☐	☐
Risk appetite statement	☐	☐
Board risk reporting	☐	☐
Annual report risk disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle D.2 – Internal Control and Assurance

The company should establish and maintain robust systems of internal control over AI systems and should provide the board with credible assurance that these controls are operating effectively.

Provision D.2.1 - Lifecycle Controls

D.2.1 Lifecycle Controls. AI systems should be controlled across development, procurement, deployment, monitoring, change, and retirement.

Maturity assessment question	Response / notes
D.2.1.93 Are controls defined across development, procurement, deployment, monitoring, change, and retirement for material AI systems?	
D.2.1.94 Do control owners, testing cycles, and approval points exist for each lifecycle stage?	
D.2.1.95 Can management show that controls remain current as systems and use cases change?	
D.2.1.96 Is lifecycle control evidence visible to the board or audit committee in a usable form?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.2.2 - Intervention Capabilities

D.2.2 Intervention Capabilities. The company should be able to suspend, override, or modify material AI systems when failures, unintended outputs, or changed conditions arise.

Maturity assessment question	Response / notes
D.2.2.97 Can the company suspend, override, or modify material AI systems when failures or changed conditions arise?	
D.2.2.98 Are intervention rights assigned clearly and tested periodically?	
D.2.2.99 Can interventions be executed promptly without creating wider operational confusion?	
D.2.2.100 Does the board receive assurance that intervention capability remains functional for critical systems?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.2.3 - Incident Management

D.2.3 Incident Management. AI-related incidents should be identified, escalated, investigated, and remediated through a defined process, with significant matters reported promptly to the board.

Maturity assessment question	Response / notes
D.2.3.101 Are AI-related incidents identified, escalated, investigated, and remediated through a defined process?	
D.2.3.102 Are significant incidents reported promptly to the board or relevant committee?	
D.2.3.103 Does incident reporting include root cause, consequence, remediation, and lessons learned?	
D.2.3.104 Is incident data used to improve controls, governance, and future deployment decisions?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.2.4 - Third-Party AI

D.2.4 Third-Party AI. Before using third-party AI, the company should perform due diligence and ensure ongoing monitoring obligations are built into contractual and operational arrangements.

Maturity assessment question	Response / notes
D.2.4.105 Does the company perform due diligence before using thirdparty AI in material contexts?	
D.2.4.106 Are ongoing monitoring obligations built into contractual and operational arrangements?	
D.2.4.107 Do due diligence and monitoring cover model provenance, performance, data use, resilience, and exit?	
D.2.4.108 Can the board explain how third-party AI exposure is governed after procurement, not only before it?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.2.5 - AI Security, Red-Teaming and Abuse Resilience

D.2.5 AI Security, Red-Teaming and Abuse Resilience. The company should identify, test, and control the security and abuse risks specific to material AI systems, including adversarial manipulation, misuse, data leakage, unsafe tool access, and malicious or unintended system behaviour.

Maturity assessment question	Response / notes
D.2.5.109 Has the company identified the security and abuse risks specific to its material AI systems?	
D.2.5.110 Are AI systems tested under adversarial as well as ordinary operating conditions?	
D.2.5.111 Can management contain or disable unsafe AI behaviour quickly when it emerges?	
D.2.5.112 Does board reporting distinguish AI-specific security risks from general cyber assurance?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.2.6 - AI Governance in Transactions and Material Change Events

D.2.6 AI Governance in Transactions and Material Change Events. The board should ensure that material transactions and change events include explicit review of AI-related assets, liabilities, dependencies, and governance implications.

Maturity assessment question	Response / notes
D.2.6.113 Do major transactions and change events include explicit review of AI-related assets, liabilities, and dependencies?	
D.2.6.114 Are inherited AI systems and vendors assessed before or during integration?	
D.2.6.115 Does the board see material AI findings in decision papers for acquisitions, outsourcing, and strategic partnerships?	
D.2.6.116 Are accountability, workforce, and regulatory consequences revisited when the operating model changes?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Control library	☐	☐
Lifecycle control evidence	☐	☐
Incident records	☐	☐
Third-party due diligence files	☐	☐
Security and red-team reports	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle D.3 – Data Governance

The board should ensure that data governance is treated as a business responsibility and is sufficient to support the safe, effective, and lawful use of AI.

Provision D.3.1 - Data Ownership and Quality

D.3.1 Data Ownership and Quality. Senior accountability for data used in material AI systems should be explicit, and the board should be satisfied that data quality is fit for purpose.

Maturity assessment question	Response / notes
D.3.1.117 Is senior accountability for data used in material AI systems explicit?	
D.3.1.118 Is data quality assessed against the requirements of the AI use case rather than assumed from legacy use?	
D.3.1.119 Can management explain how data quality issues are identified, escalated, and corrected?	
D.3.1.120 Does the board receive enough visibility to judge whether data is fit for purpose in material AI systems?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Data ownership map	☐	☐
Data quality dashboard	☐	☐
Data protection impact assessment	☐	☐
Data-use policy	☐	☐
IP/provenance/recordkeeping logs	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.3.2 - Lawful and Ethical Data Use

D.3.2 Lawful and Ethical Data Use. Data used in AI should be collected, processed, and retained lawfully and in ways consistent with reasonable stakeholder expectations.

Maturity assessment question	Response / notes
D.3.2.121 Has the company reviewed the lawfulness of data used in AI systems?	
D.3.2.122 Are material AI data uses consistent with stakeholder expectations and company values?	
D.3.2.123 Do retention and governance controls reflect AI usage?	
D.3.2.124 Are sensitive or novel uses escalated for review?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Data ownership map	☐	☐
Data quality dashboard	☐	☐
Data protection impact assessment	☐	☐
Data-use policy	☐	☐
IP/provenance/recordkeeping logs	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.3.3 - Proprietary Data Assets

D.3.3 Proprietary Data Assets. Boards should treat proprietary data as a strategic asset and set policies on how company data may be used by third-party models and whether rights to derived improvements are retained.

Maturity assessment question	Response / notes
D.3.3.125 Has the board identified the company's strategically important proprietary data assets?	
D.3.3.126 Are there policies controlling external use of that data for model training or improvement?	
D.3.3.127 Do commercial arrangements protect rights in data-derived improvements where relevant?	
D.3.3.128 Is data strategy discussed as a source of competitive advantage?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Data ownership map	☐	☐
Data quality dashboard	☐	☐
Data protection impact assessment	☐	☐
Data-use policy	☐	☐
IP/provenance/recordkeeping logs	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision D.3.4 - IP, Provenance and Recordkeeping

D.3.4 IP, Provenance and Recordkeeping. The board should ensure that the company can account for the provenance, rights position, and recordkeeping implications of data, models, prompts, outputs, and other artefacts used in or generated through material AI activity.

Maturity assessment question	Response / notes
D.3.4.129 Can the company explain the provenance and rights position of material AI inputs and outputs?	
D.3.4.130 Are recordkeeping expectations defined for consequential AI-assisted processes?	
D.3.4.131 Does management know where licensing, copyright, or provenance uncertainty remains?	
D.3.4.132 Are third-party terms reviewed for their effect on company data, prompts, outputs, and derived value?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Data ownership map	☐	☐
Data quality dashboard	☐	☐
Data protection impact assessment	☐	☐
Data-use policy	☐	☐
IP/provenance/recordkeeping logs	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Section E – People, Culture and Remuneration

AI fundamentally alters the nature of work. A company that deploys AI without deliberate attention to its workforce (its skills, incentives, and trust) will fail to capture the technology's potential and will damage the organisational culture on which long-term success depends.

Issues and Risks

- ☐ AI workforce impact not assessed before deployment.
- ☐ Skills gaps, role redesign, displacement, or redeployment handled reactively.
- ☐ Workforce transition underfunded or not credible.
- ☐ Poor disclosure of AI's workforce effects.
- ☐ Incentives rewarding speed, automation, or cost reduction without responsible governance.
- ☐ Employee distrust caused by unclear communication.
- ☐ Shadow AI, surveillance, opaque evaluation, or culturally inconsistent employee use.

Principle E.1 – Workforce Impact and Transition

The board should oversee the impact of AI on the workforce and ensure that appropriate provision is made for skills development, redeployment, and workforce transition.

Provision E.1.1 - Impact Assessment

E.1.1 Impact Assessment. Management should assess how AI changes roles, skills needs, and workforce composition and should report this as part of the company's people strategy.

Maturity assessment question	Response / notes
E.1.1.133 Has management assessed how material AI deployment affects roles and skills?	
E.1.1.134 Is workforce impact reported to the board as part of people strategy?	
E.1.1.135 Are assessments updated as the operating model changes?	
E.1.1.136 Does management distinguish between task change, role change, and workforce composition change?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce impact assessment	☐	☐
People strategy papers	☐	☐
Reskilling plan	☐	☐
Transition plan	☐	☐
Workforce disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision E.1.2 - Reskilling and Transition

E.1.2 Reskilling and Transition. Where AI materially changes role demand or skill requirements, the company should have credible, resourced plans for reskilling, redeployment, or workforce transition.

Maturity assessment question	Response / notes
E.1.2.137 Are reskilling and transition plans in place for materially affected roles?	
E.1.2.138 Are those plans funded and linked to future business needs?	
E.1.2.139 Can management explain redeployment or transition pathways?	
E.1.2.140 Has the board considered whether the transition is fair and	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce impact assessment	☐	☐
People strategy papers	☐	☐
Reskilling plan	☐	☐
Transition plan	☐	☐
Workforce disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision E.1.3 - Workforce Disclosure

E.1.3 Workforce Disclosure. Annual reporting should explain how AI affects the workforce, including skills development, support for affected employees, and the company's approach to transition.

Maturity assessment question	Response / notes
E.1.3.141 Does the annual report explain how AI is affecting the workforce where material?	
E.1.3.142 Is the disclosure specific about skills, support, and transition?	
E.1.3.143 Is disclosure consistent with internal workforce planning?	
E.1.3.144 Would an employee or investor find the description credible and informative?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce impact assessment	☐	☐
People strategy papers	☐	☐
Reskilling plan	☐	☐
Transition plan	☐	☐
Workforce disclosure draft	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle E.2 – Remuneration and Incentives

Remuneration structures should support responsible AI adoption and should not create incentives for ungoverned, reckless, or unethical AI use.

Provision E.2.1 - Outcome-Based Metrics

E.2.1 Outcome-Based Metrics. Where AI is material, incentive structures should measure outcomes enabled by AI rather than outdated activity measures that AI may make irrelevant.

Maturity assessment question	Response / notes
E.2.1.145 Has the remuneration committee reviewed whether legacy metrics remain appropriate in an AI-enabled model?	
E.2.1.146 Are outcome measures used where AI materially changes work?	
E.2.1.147 Do incentive measures balance value, control, and stakeholder outcomes?	
E.2.1.148 Is AI deployment itself distinguished from real performance improvement?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Remuneration committee papers	☐	☐
Incentive scorecards	☐	☐
Responsible-use metrics	☐	☐
Malus/clawback review	☐	☐
Performance management guidance	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision E.2.2 - Responsible Use Incentives

E.2.2 Responsible Use Incentives. Incentive structures should reinforce responsible AI use and allow consequences where poor AI governance destroys value.

Maturity assessment question	Response / notes
E.2.2.149 Could current incentives encourage ungoverned or reckless AI use?	
E.2.2.150 Have malus or clawback provisions been reviewed for AIrelated value destruction?	
E.2.2.151 Do leaders receive clear signals that responsible AI use matters to reward?	
E.2.2.152 Is governance failure treated as a performance issue, not just a technical incident?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Remuneration committee papers	☐	☐
Incentive scorecards	☐	☐
Responsible-use metrics	☐	☐
Malus/clawback review	☐	☐
Performance management guidance	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle E.3 – Culture and the Workforce Contract

The board should ensure that AI is deployed in a manner that preserves and strengthens the trust of the workforce and is consistent with the company's purpose and values.

Provision E.3.1 - Workforce Engagement

E.3.1 Workforce Engagement. Employees should be told clearly and honestly how AI is being used, how roles may change, and what the company's intentions are before material deployments occur.

Maturity assessment question	Response / notes
E.3.1.153 Does the company communicate with employees before material AI deployments?	
E.3.1.154 Is the communication honest about role impact and intent?	
E.3.1.155 Are employees told how to seek support or raise concerns?	
E.3.1.156 Does the board receive evidence about workforce sentiment and response?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce communications	☐	☐
Employee AI-use policy	☐	☐
Training records	☐	☐
Workforce sentiment evidence	☐	☐
Ethical deployment assessment	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision E.3.2 - Ethical Deployment

E.3.2 Ethical Deployment. AI should not be used in employee surveillance, evaluation, or consequential decision-making in ways that are unexpected, disproportionate, or inconsistent with company values.

Maturity assessment question	Response / notes
E.3.2.157 Are boundaries defined for AI use in employee surveillance or evaluation?	
E.3.2.158 Is proportionality assessed before deployment?	
E.3.2.159 Are sensitive employee-facing AI uses escalated appropriately?	
E.3.2.160 Could the company explain and defend the use to its workforce and regulators?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce communications	☐	☐
Employee AI-use policy	☐	☐
Training records	☐	☐
Workforce sentiment evidence	☐	☐
Ethical deployment assessment	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision E.3.3 - Shadow AI

E.3.3 Shadow AI. The company should set clear, usable policies for employee use of AI tools, including consumer-grade and personal tools, and support responsible usage with guidance and training.

Maturity assessment question	Response / notes
E.3.3.161 Does the company have a practical policy on employee AI tool use?	
E.3.3.162 Does that policy support responsible use rather than only prohibition?	
E.3.3.163 Have employees received training on safe and appropriate use?	
E.3.3.164 Does management understand the extent and nature of shadow AI in the business?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Workforce communications	☐	☐
Employee AI-use policy	☐	☐
Training records	☐	☐
Workforce sentiment evidence	☐	☐
Ethical deployment assessment	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Section F – Transparency and Accountability

Transparency in AI governance builds the trust of investors, customers, regulators, and employees. Accountability ensures that when AI causes harm or fails to deliver value, there are credible mechanisms for redress. Both are essential to the social licence on which sustainable business depends.

Issues and Risks

- ☐ Annual report disclosure too generic or unsupported by practice.
- ☐ Failure to explain material AI use to stakeholders in accessible terms.
- ☐ Inconsistent AI disclosure across regulators or jurisdictions.
- ☐ Uncontrolled reliance on AI in financial reporting, forecasting, certification, or board disclosures.
- ☐ No credible route for affected stakeholders to challenge AI-influenced decisions.
- ☐ Weak explainability for consequential decisions.
- ☐ Poor regulatory cooperation or inability to evidence governance during inquiry.

Principle F.1 – AI Governance Disclosure

The board should ensure that the company reports clearly on its approach to AI governance, its material AI activities, and the manner in which AI risk is managed and overseen.

Provision F.1.1 - Annual Report Disclosure

F.1.1 Annual Report Disclosure. The annual report should describe board oversight of AI, executive accountability, AI risk management, and material AI risks or incidents.

Maturity assessment question	Response / notes
F.1.1.165 Does the annual report explain board oversight and executive accountability for AI?	
F.1.1.166 Does it describe AI risk management with enough specificity to be useful?	
F.1.1.167 Are material AI risks or incidents disclosed where appropriate?	
F.1.1.168 Is the narrative consistent with internal governance and reporting?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Annual report disclosure draft	☐	☐
Disclosure committee papers	☐	☐
Material AI use register	☐	☐
Regulatory disclosure tracker	☐	☐
Audit committee review evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision F.1.2 - Material AI Use

F.1.2 Material AI Use. Where AI is material to stakeholders, the company should disclose the use in accessible terms and explain the governance arrangements around it.

Maturity assessment question	Response / notes
F.1.2.169 Has the company identified AI uses that are material to stakeholders?	
F.1.2.170 Are those uses disclosed in accessible language?	
F.1.2.171 Does disclosure explain the governance arrangements that apply?	
F.1.2.172 Would a reasonable stakeholder understand where AI materially affects them?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Annual report disclosure draft	☐	☐
Disclosure committee papers	☐	☐
Material AI use register	☐	☐
Regulatory disclosure tracker	☐	☐
Audit committee review evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision F.1.3 - Consistency with Regulatory Obligations

F.1.3 Consistency with Regulatory Obligations. AI disclosures should be consistent with applicable regulator guidance and with international disclosure obligations where the company operates across borders.

Maturity assessment question	Response / notes
F.1.3.173 Is the company tracking relevant AI-related disclosure guidance?	
F.1.3.174 Are AI disclosures consistent across regulatory and stakeholder contexts?	
F.1.3.175 Has cross-border exposure been considered where relevant?	
F.1.3.176 Is disclosure updated as guidance changes?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Annual report disclosure draft	☐	☐
Disclosure committee papers	☐	☐
Material AI use register	☐	☐
Regulatory disclosure tracker	☐	☐
Audit committee review evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision F.1.4 - Reliance on AI in Financial Reporting and Board Disclosures

F.1.4 Reliance on AI in Financial Reporting and Board Disclosures. Where AI materially supports financial reporting, management certification, forecasts, narrative reporting, or board-level disclosures, the board should ensure that reliance is controlled, reviewable, and consistent with the company's assurance obligations.

Maturity assessment question	Response / notes
F.1.4.177 Does the board know where AI materially affects financial reporting, forecasts, or disclosures?	
F.1.4.178 Are AI-assisted reporting outputs subject to documented review and evidential support?	
F.1.4.179 Has the audit committee considered the impact of AI on controls over reporting and assurance?	
F.1.4.180 Can management explain how board-approved disclosures remain reliable where AI has materially contributed?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Annual report disclosure draft	☐	☐
Disclosure committee papers	☐	☐
Material AI use register	☐	☐
Regulatory disclosure tracker	☐	☐
Audit committee review evidence	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Principle F.2 – Accountability and Redress

The company should maintain credible mechanisms by which stakeholders can raise concerns about AI-driven decisions and seek appropriate redress.

Provision F.2.1 - Redress Processes

F.2.1 Redress Processes. Stakeholders affected by AI-influenced decisions should have accessible routes to raise concerns and seek timely, substantive review.

Maturity assessment question	Response / notes
F.2.1.181 Can affected stakeholders easily raise concerns about AIdriven decisions?	
F.2.1.182 Are redress processes communicated clearly?	
F.2.1.183 Do cases receive timely and substantive responses?	
F.2.1.184 Is redress data used to improve systems and governance?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Redress process documentation	☐	☐
Complaint and appeals logs	☐	☐
Explainability standards	☐	☐
Regulatory engagement records	☐	☐
Governance improvement actions	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision F.2.2 - Explainability

F.2.2 Explainability. Where AI materially influences consequential decisions affecting individuals, the company should be able to offer a meaningful explanation of the basis for that decision.

Maturity assessment question	Response / notes
F.2.2.185 Can the company provide meaningful explanations for consequential AI-influenced decisions?	
F.2.2.186 Are standards for explanation defined and applied?	
F.2.2.187 Are systems without adequate explainability excluded from high-stakes use?	
F.2.2.188 Would a stakeholder be able to understand the basis of a decision and how to challenge it?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Redress process documentation	☐	☐
Complaint and appeals logs	☐	☐
Explainability standards	☐	☐
Regulatory engagement records	☐	☐
Governance improvement actions	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Provision F.2.3 - Regulatory Cooperation

F.2.3 Regulatory Cooperation. The company should engage constructively and transparently with relevant regulators regarding AI governance and respond fully to inquiries.

Maturity assessment question	Response / notes
F.2.3.189 Is there a clear process for managing AI-related regulatory engagement?	
F.2.3.190 Can the company assemble coherent evidence of governance quickly?	
F.2.3.191 Are responses to regulators prompt and transparent?	
F.2.3.192 Is regulatory feedback incorporated into governance improvement?	

Maturity assessment

0 - Absent	1 - Ad hoc	2 - Defined	3 - Operating	4 - Assured	5 - Leading
☐	☐	☐	☐	☐	☐

Comments

Evidence checklist

Evidence item	Exists	Adequate
Redress process documentation	☐	☐
Complaint and appeals logs	☐	☐
Explainability standards	☐	☐
Regulatory engagement records	☐	☐
Governance improvement actions	☐	☐
	☐	☐
	☐	☐
	☐	☐

Governance gaps

Recommended actions

Action	Owner	Priority	Target date

Project Setup and Stakeholder Engagement

Use this section to define the project scope, identify key stakeholders, plan interviews and workshops, and document governance observations.

Project Details

Project Name	
Client Organisation	
Primary Contact	
Project Sponsor	
Assessment Lead	
Project Objectives	
Scope of Assessment	
Business Units Included	
Countries / Jurisdictions	
Key AI Systems in Scope	
Target Completion Date	

Stakeholder Interview and Engagement Plan

Use this section to identify the roles and people who will be involved in the review process.

Role / Function	Suggested Interviewee	Group	Completed
Board Chair			☐
Chief Executive Officer			☐
Chief Technology Officer			☐
Chief Information Officer			☐
Chief Risk Officer			☐
General Counsel			☐
Chief Compliance Officer			☐
Head of Internal Audit			☐
Chief Human Resources Officer			☐
Chief Data Officer			☐
Cybersecurity Lead			☐
AI Product Owner			☐
Procurement Lead			☐
Privacy Officer / DPO			☐
Business Unit Leads			☐
Employee Representatives			☐

Assessment Methodology

Use this method to conduct the Corporate AI Governance assessment consistently, from project initiation through to sponsor sign-off. The method supports interview-based scoring, evidence validation, gap analysis, action planning, and final governance accountability.

Step	Assessment activity	Output
1	Establish the project, sponsor, and assessment governance. Agree the scope with the sponsor, including objectives, business units, jurisdictions, AI systems, exclusions, reporting route, review points, confidentiality expectations, and final sign-off process.	Approved project scope, named sponsor, agreed reporting route, review schedule, and sign-off expectations.
2	Identify board members and other people with governance, executive, operational, assurance, legal, risk, technology, data, workforce, procurement, or compliance responsibilities who should be interviewed. Decide on interviews individually or in groups	Stakeholder interview plan with names, roles, responsibilities, groups, interview priority, and completion status.
3	Interview each relevant participant or group using the full maturity questionnaire. Ask all 192 questions. Where a question is not applicable, mark it as N/A and record the reason. Allow each interviewee to give a maturity assessment for each Provision and record specific governance gaps and recommended actions.	Completed interview records, provision-level interview scores, N/A rationale, governance gaps, recommended actions, and notable differences in view.
4	Collect supporting evidence for each Principle. Evidence may include board papers, committee minutes, policies, risk registers, AI inventories, vendor records, assurance reports, incident logs, workforce communications, training records, and disclosure drafts.	Evidence register showing evidence requested, evidence received, owner, date, relevance, and adequacy.
5	Produce an average maturity score for each Principle from the interview maturity assessments. Record the range of scores where views differ materially between interviewees.	Principle score table showing average score, score range, number of respondents, and N/A count.
6	Correlate each maturity score with the supporting evidence. Identify where interview confidence is not supported by evidence, where evidence indicates stronger or weaker maturity, and where further validation is required.	Evidence-correlation notes showing supported scores, unsupported claims, maturity adjustments, and evidence gaps.
7	Summarise the governance gaps. Group gaps by Provision, Principle, Section, severity, materiality, accountable owner, and urgency.	Consolidated gap register with severity, materiality, owner, and priority.

Step	Assessment activity	Output
8	List the recommended actions. For each action, define the remediation activity, accountable owner, priority, target date, dependency, and expected governance outcome.	Action plan with accountable owners, priorities, due dates, dependencies, and status.
9	Summarise the whole report with the sponsor. Review findings, evidence, maturity scores, gaps, recommended actions, assumptions, limitations, and next steps. Obtain sponsor sign-off on the final report.	Sponsor-reviewed final report, agreed action plan, sign-off record, and review date.

The Final AI Governance Assessment Report

An AI governance assessment is only valuable if its conclusions can be understood, challenged, prioritised, and acted upon by the board and executive management. A poorly structured report creates the appearance of diligence while obscuring the issues that matter most. A well-constructed report does the opposite: it brings governance reality into view. It allows the board to understand where the organisation is genuinely in control, where governance exists only in form, and where strategic, operational, regulatory, or cultural weaknesses may expose the company to avoidable risk.

This chapter describes the recommended structure and contents of a comprehensive AI Governance Assessment Final Report. The report should not be treated as a compliance artefact alone. It is a board governance instrument. It supports oversight, internal audit review, remediation planning, investor engagement, regulatory readiness, and strategic decision-making.

A mature assessment report is evidence-led, operationally grounded, and strategically useful. It distinguishes clearly between observed strengths, material weaknesses, emerging risks, and management assertions that are not yet supported by evidence. It also creates a durable governance record: a document capable of demonstrating how the board understood and responded to AI governance issues at a particular point in time.

The structure described below is intended to support that objective.

Executive Summary

The Executive Summary is the most important section of the report because it is often the only section read in full by every board member. It should therefore be concise, commercially intelligible, and focused on matters requiring judgement rather than operational detail.

The purpose of the Executive Summary is not to restate the assessment process. It is to explain the organisation's AI governance position in practical terms. A strong summary allows the board to understand the organisation's maturity, principal exposures, and immediate priorities within a short period of reading.

The section should normally include:

- the overall maturity rating;
- key governance strengths;
- critical governance weaknesses;
- the most material enterprise risks;
- priority remediation actions;
- strategic observations; and
- an overall assurance opinion.

The maturity rating should not be presented as a numerical abstraction detached from operational reality. It should explain what the rating means in practice. A rating of "Defined", for example, may indicate that governance structures exist but are inconsistently implemented across business units. A rating of

"Operating" may indicate that governance processes are functioning consistently but remain insufficiently evidenced or independently assured.

Key strengths should identify the governance disciplines already operating effectively. Examples might include strong executive ownership, effective AI risk reporting, mature data governance, or well-developed third-party oversight.

Critical weaknesses should focus on issues capable of producing material operational, regulatory, financial, or reputational consequences. The report should resist the temptation to dilute serious weaknesses inside long lists of observations. Boards require clarity about what matters most.

The section should also identify the organisation's principal enterprise risks associated with AI use. These may include dependency concentration, lack of intervention capability, opaque decision-making, uncontrolled shadow AI, workforce trust deterioration, or weaknesses in incident response.

Priority remediation actions should distinguish between urgent stabilisation activity and longer-term governance enhancement. The board should be able to see immediately which actions require rapid executive attention and which represent broader maturity improvements.

Strategic observations are particularly important because AI governance is not solely a control exercise. The report should explain whether governance weaknesses are likely to impair strategic flexibility, resilience, competitive differentiation, or organisational trust over time.

Finally, the Executive Summary should conclude with an overall assurance opinion. This is not a legal opinion. It is a governance judgement about whether AI governance appears credible, partially effective, materially immature, or substantially deficient.

Assessment Scope and Methodology

The credibility of an assessment depends partly on the transparency of its methodology. A report that does not explain how conclusions were reached weakens confidence in the findings themselves.

This section should therefore describe the scope of the review and the methods used to perform it. The purpose is not procedural formality; it is governance defensibility.

The section should explain:

- the scope of the review;
- business units assessed;
- jurisdictions covered;
- documents reviewed;
- interviews and workshops performed;
- evidence standards applied;
- scoring methodology; and
- limitations and exclusions.

The scope statement should explain what parts of the organisation were included and excluded, and why. AI governance maturity can vary substantially across business units, legal entities, and geographies. Boards should therefore understand whether conclusions reflect enterprise-wide review or only selected operations.

The report should also identify the jurisdictions covered because legal and regulatory obligations may differ materially across territories. AI governance arrangements sufficient in one jurisdiction may be inadequate in another.

A mature methodology section also describes the evidence base used during the assessment. This includes policies, committee papers, architecture documentation, inventories, incident logs, vendor assessments, training records, and operational evidence demonstrating whether governance processes function in practice.

Interviews and workshops should also be described because governance maturity is often revealed through operational understanding rather than documentation alone. Interviews frequently expose gaps between formal policy and actual organisational behaviour.

The report should explain the maturity scoring model used, including how ratings were assigned and what thresholds distinguish one maturity level from another.

Finally, limitations and exclusions should be stated openly. A credible assessment acknowledges where evidence was incomplete, unavailable, or outside scope.

Overall Maturity Heatmap

The purpose of the maturity heatmap is to provide the board with a rapid visual understanding of where governance maturity is concentrated and where material weaknesses exist.

A heatmap should normally present maturity ratings across each major section of the governance framework. These may include leadership and purpose, division of responsibilities, decision-making and control, risk and assurance, workforce governance, and transparency and accountability.

Visual representation matters because governance weaknesses rarely exist in isolation. Patterns emerge more clearly when maturity is viewed comparatively across domains.

For example, a company may demonstrate strong strategic ambition while showing weak operational controls. Another may possess mature risk management disciplines but poor workforce governance. A heatmap allows these asymmetries to become visible quickly.

The section should also identify concentrations of governance weakness. Weaknesses that appear repeatedly across multiple principles often indicate deeper organisational issues such as fragmented accountability, weak governance culture, or poor operational integration.

Cross-functional governance observations should also be included. AI governance failures frequently occur at organisational boundaries rather than within individual functions. The report should therefore identify where coordination between technology, legal, operations, risk, human resources, procurement, and compliance appears weak or inconsistent.

The heatmap should support board judgement, not replace it. Visual scoring should always be accompanied by explanatory narrative.

Detailed Findings by Section and Principle

This section forms the operational core of the report. It explains how the organisation performed against each Principle and Provision within the assessment framework.

The purpose is not merely to record observations. It is to explain the governance consequences of what was found.

Each section should normally include:

- principle-level maturity assessment;
- positive observations;
- key weaknesses;
- risk implications;
- evidence reviewed;
- recommendations; and
- target maturity outcomes.

The maturity assessment should explain both the current state and the reasons supporting the rating. Boards should understand not only that governance is immature, but why.

Positive observations are important because they identify governance disciplines that should be preserved, reinforced, or replicated elsewhere in the organisation.

Key weaknesses should focus on operationally meaningful issues rather than stylistic deficiencies. The report should distinguish clearly between administrative imperfections and weaknesses capable of producing material governance failure.

Risk implications should connect governance deficiencies to enterprise consequences. This translation is essential because governance weaknesses become meaningful only when their operational impact is understood.

For example, the absence of tested intervention capability is not simply a process weakness. It may indicate inability to suspend harmful AI behaviour during operational failure. Similarly, poor workforce communication may indicate future trust deterioration and increased shadow AI adoption.

The section should also identify the evidence reviewed in support of conclusions. Governance findings should be traceable to observable evidence rather than impressionistic judgement alone.

Recommendations should be practical, prioritised, and proportionate to organisational maturity. Weak recommendations often fail because they describe abstract aspirations rather than operational actions.

Finally, target maturity outcomes should explain the governance state the organisation is expected to reach after remediation activity is completed.

Assessment Question Results

This section provides detailed traceability between the assessment framework and the report's conclusions. It converts high-level governance observations into auditable assessment outcomes.

The section should normally include:

- question-level scoring;
- supporting evidence;
- gap analysis;

- remediation recommendations; and
- traceability and auditability.

Each assessment question should be individually scored using the maturity framework adopted by the assessment.

Supporting evidence should identify the specific policies, reports, interviews, workflows, committee records, or operational artefacts supporting the rating assigned.

Gap analysis should explain what prevents the organisation from achieving the next maturity level. This distinction is important because governance maturity is rarely binary. Organisations often possess partial capability requiring refinement rather than wholesale redesign.

Remediation recommendations should therefore be directly connected to the identified gaps.

The traceability provided by this section is particularly important for internal audit, regulatory review, and future reassessment activity. It allows the organisation to demonstrate how conclusions were reached and how governance maturity evolved over time.

Risk Analysis

The Risk Analysis section translates governance observations into enterprise risk language understandable by boards, regulators, investors, and executive leadership.

The section should address:

- strategic risks;
- operational risks;
- regulatory and legal risks;
- financial risks;
- reputational risks; and
- workforce and cultural risks.

Strategic risks may include dependency concentration, loss of competitive differentiation, erosion of organisational agency, or excessive reliance on external providers.

Operational risks include model failure, workflow disruption, inaccurate outputs, poor intervention capability, weak monitoring, and insufficient incident management.

Regulatory and legal risks may include explainability failures, unlawful data use, inadequate disclosures, cross-border compliance conflicts, and sector-specific supervisory exposure.

Financial risks may include misallocated AI investment, liability exposure, operational losses arising from AI failure, and poor capital discipline associated with uncontrolled experimentation.

Reputational risks are increasingly significant because AI failures are highly visible and often interpreted as failures of governance rather than technology alone.

Workforce and cultural risks should also be analysed carefully. AI governance frequently fails where workforce trust deteriorates, communication becomes opaque, or shadow AI proliferates beyond formal oversight.

The report should not merely catalogue risks. It should identify which risks are material, which are emerging, and which appear insufficiently controlled.

Priority Recommendations

A mature assessment report distinguishes between observations and action. The Priority Recommendations section converts governance findings into a structured implementation agenda.

Recommendations should normally be grouped into:

- critical actions (0–90 days);
- high-priority actions (3–6 months);
- medium-term actions (6–12 months); and
- strategic long-term initiatives (12–24 months).

Critical actions should focus on issues capable of producing immediate material exposure. These may include absence of incident escalation capability, uncontrolled high-stakes AI use, missing governance ownership, or material regulatory exposure.

High-priority actions typically address structural governance weaknesses requiring organised remediation but not immediate emergency response.

Medium-term initiatives often involve governance integration, assurance enhancement, training, or workflow redesign.

Strategic long-term initiatives should address resilience, dependency reduction, advanced assurance capability, and strategic optimisation.

Recommendations should also identify accountable owners, dependencies, sequencing considerations, and expected governance outcomes. Recommendations without ownership rarely progress effectively.

The section should support implementation discipline rather than merely expressing aspiration.

Board-Level Decisions Required

One of the most important functions of the report is identifying issues requiring explicit board judgement. AI governance cannot be delegated entirely to management because many questions involve strategic trade-offs, risk tolerance, and organisational values.

This section should therefore isolate matters requiring direct board determination, including:

- AI risk appetite;
- acceptable autonomy thresholds;
- disclosure posture;
- strategic dependency tolerance;
- prohibited AI use cases; and
- workforce transition approach.

Risk appetite decisions are particularly important because AI governance often fails when organisations pursue automation without clearly defining acceptable levels of opacity, autonomy, bias, or dependency.

Boards should also determine where autonomous decision-making remains unacceptable regardless of operational efficiency.

Disclosure posture is another strategic governance decision. Boards must determine how transparent the organisation intends to be regarding material AI use, governance arrangements, and operational incidents.

Strategic dependency tolerance should also be discussed explicitly. Organisations increasingly rely on concentrated AI infrastructure providers. The board should determine what levels of dependency are acceptable and where resilience investment is required.

Similarly, prohibited AI use cases should be identified clearly. Mature governance frameworks define not only what AI may be used for, but what uses remain inconsistent with organisational values or risk tolerance.

Workforce transition decisions are equally important because AI adoption reshapes authority, pacing, and organisational trust. The board should determine the organisation's posture toward reskilling, redeployment, workforce support, and transparency.

This section ensures governance remains anchored in board stewardship rather than operational administration alone.

Evidence Appendix

The Evidence Appendix supports the integrity and defensibility of the assessment.

The appendix should identify the materials reviewed during the assessment, including:

- policies reviewed;
- committee papers;
- interview lists;
- incident logs;
- architecture diagrams;
- inventories;
- audit reports; and
- supporting evidence sources.

The purpose of the appendix is not documentary excess. It is evidential transparency.

Governance conclusions unsupported by evidence are difficult to defend during internal audit review, regulatory inquiry, litigation, or future reassessment activity.

The appendix should therefore provide sufficient traceability to demonstrate that findings were grounded in observable governance activity rather than unsupported assertion.

A mature appendix also helps the organisation maintain continuity between successive assessments. Over time, it becomes part of the institutional memory of how governance maturity evolved, what evidence was relied upon, and how remediation activity progressed.

Concluding Observation

A comprehensive AI governance assessment report should ultimately answer six board-level questions clearly and credibly:

1. What AI matters most to this organisation?
2. Where is the organisation materially exposed?
3. Who is accountable?
4. Which controls are genuinely operating?
5. Where are the most significant governance weaknesses?
6. What decisions must the board make next?

A report that cannot answer those questions may still create documentation, but it will not create governance clarity. The purpose of the assessment is not to demonstrate activity. It is to improve stewardship, strengthen organisational control, preserve strategic agency, and ensure that the company remains capable of governing AI deliberately rather than merely reacting to it.

Document updates and review log

Update the log to reflect changes made to this document.

Date	Name	Comments	Version

Integrity check: 48 provisions and 192 maturity questions included.

Sponsor Sign-Off

Sponsor name	Role	Signature	Date

Annual governance cycle

Month	Governance activity
January	Annual AI strategy review
March	Risk and control reassessment
May	AI incident simulation
July	Mid-year governance review
September	Regulatory horizon review
November	Governance maturity reassessment

Further Details

Further information including detailed questions and maturity assessment for Board Directors and Non-Executive Directors can be found in the book The Board's Guide to Corporate AI Governance - Stewardship, Strategy, and Accountability in the Age of AI written by Vincent A. Powell.

ISBN 978-1-9195185-5-8

https://www.theboardaiguide.com/

AI governance needs evidence and action.

This workbook turns board-level AI governance into a practical assessment discipline. It is designed for boards, NEDs, executives and advisers who need to test whether AI governance is operating, evidenced and improving.

It combines the Corporate AI Governance Code with structured worksheets, maturity scoring, evidence checklists, stakeholder engagement guidance and report templates—helping organisations assess compliance, identify gaps and prioritise action.

INSIDE YOU WILL DISCOVER:

Code Principles

Apply board-level AI governance principles across strategy, accountability, risk, people and disclosure.

Maturity Assessment

Score current governance from absent to leading using a clear six-point maturity scale.

Evidence and Controls

Capture evidence, gaps, owners and actions across each provision of the Code.

Workbook Templates

Use structured worksheets, assessment questions and practical evidence checklists.

Reporting Methodology

Turn findings into board-ready assessments and priority recommendations.

Annual Review Cycle

Track progress, sign-off and recurring governance improvement over time.

Written for board directors, NEDs, executives and advisers, this workbook provides a practical route from AI governance principles to evidence-based assessment, board challenge and accountable implementation.