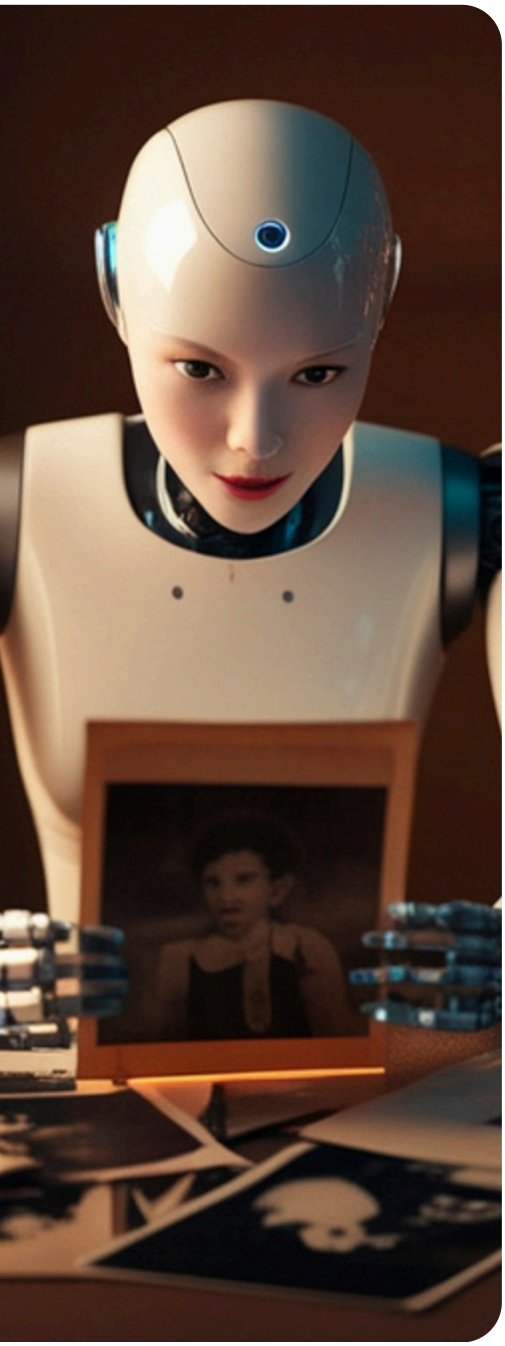
EXECUTIVE CYBER AND AI OBLIGATION CHECKLIST

Supporting Leadership Oversight Before and During AI Adoption



Artificial Intelligence is not solely a technology initiative. It is a governance, risk and accountability matter requiring oversight at board, executive and senior leadership level.

Directors, CEOs and senior executives share responsibility for ensuring that AI adoption aligns with the organisation's strategy, risk appetite, regulatory obligations and operational resilience.
Leadership duties in this context extend to:

- Exercising due care and diligence
- Acting in good faith and in the best interests of the organisation
- Maintaining effective risk oversight
- Meeting privacy, consumer protection and data obligations
- Ensuring cyber security and operational resilience

If AI is introduced without structured oversight, the resulting exposure may be commercial, regulatory, operational and reputational.

This checklist is designed to support executive-level review. It outlines:

- Leadership responsibilities in the context of AI adoption
- Practical questions senior leaders should be asking management and IT
- Common governance gaps that emerge during AI rollout
- The structures and reporting mechanisms that should be in place
- Early indicators that risk may be increasing

This resource is not technical. It is intended to assist decision-makers responsible for oversight, risk and accountability.

CorpIT

1. Leadership Oversight and Accountability

Senior leadership should be able to clearly articulate where AI governance sits within the organisation's structure and who holds responsibility for oversight. Practical questions to consider:

- Has AI been formally recognised as a governance and risk issue?
- Who is accountable at executive level for AI oversight and reporting?
- How is AI risk escalated to executive and board level?

Checklist:

- ☐ AI has been formally acknowledged as a governance matter
- ☐ Executive accountability for AI oversight is clearly defined
- ☐ Oversight responsibilities are embedded in governance or risk charters
- ☐ There is a documented escalation pathway for higher-risk AI use
- ☐ Leadership receives structured reporting on AI risks and opportunities

Common governance gap: AI adoption begins within operational teams before executive-level accountability is defined.

Risk if unchecked: Fragmented oversight and unclear responsibility increase exposure under leadership duties of care and diligence.

2. AI Visibility and Shadow Use

Effective oversight requires visibility across the organisation.

Practical questions to consider:

- Where is AI currently being used across departments?
- Is AI functionality embedded within existing SaaS or cloud platforms?
- Are employees using generative AI tools independently of formal approval?

Checklist:

- ☐ An AI inventory or register is maintained and regularly updated
- ☐ AI embedded in third-party systems is identified and understood
- ☐ There is a policy governing employee use of AI tools
- ☐ Shadow AI risks are actively monitored and managed

Common governance gap: No consolidated view of AI usage across the organisation.

Risk if unchecked: Leadership cannot manage risks that are not visible.

3. Strategic Alignment

AI adoption should be deliberate and aligned to organisational objectives.

Practical questions to consider:

- Is each AI initiative linked to documented business objectives?
- Has leadership reviewed the risk and value case for AI investment?
- Are there defined boundaries regarding where AI should not be used?

Checklist:

- ☐ AI initiatives are aligned to strategy
- ☐ Leadership has reviewed the associated risk and reward profile
- ☐ AI use reflects organisational values
- ☐ Clear limitations on AI use have been defined

Common governance gap: AI introduced for efficiency gains without structured strategic review.

Risk if unchecked: Strategic misalignment and reputational exposure.

4. Risk Management and Legal Exposure

AI-related risks must be integrated into the broader enterprise risk framework.

Practical questions to consider:

- Has each AI use case undergone formal risk and impact assessment?
- Are privacy, intellectual property and regulatory implications understood?
- How are third-party AI risks assessed and contractually managed?

Checklist:

- ☐ AI risks are integrated into the enterprise risk framework
- ☐ The organisation's risk appetite addresses AI use
- ☐ Impact assessments occur prior to deployment
- ☐ Supplier and vendor AI risks are contractually reviewed
- ☐ Legal and compliance implications are understood

Common governance gap: AI risk treated as a technical matter rather than an enterprise-wide governance issue.

Risk if unchecked: Regulatory breach, contractual disputes and reputational harm.

5. Data Governance and Cyber Security

AI materially changes how data is processed, accessed and exposed.

Practical questions to consider:

- What data feeds our AI systems?
- Could sensitive or confidential information be exposed through AI tools?
- Are cyber controls calibrated to AI-enabled threats?

Checklist:

- ☐ Data inputs to AI systems are identified and reviewed
- ☐ Data collection and use is lawful and documented
- ☐ Sensitive data exposure risks are understood
- ☐ Cyber controls account for AI-related attack surface expansion
- ☐ Data retention and deletion policies are enforced

Common governance gap: Existing data governance frameworks are not reviewed in light of AI expansion.

Risk if unchecked: Privacy breaches and cyber incidents.

6. Workforce and Culture Impact

AI adoption affects workforce capability, accountability and decision-making.

Practical questions to consider:

- How is AI changing roles and responsibilities?
- Are staff trained in responsible AI use?
- Is human judgement retained in material decisions?

Checklist:

- ☐ Leadership understands workforce impact
- ☐ Staff receive appropriate AI training
- ☐ Acceptable use guidelines are clearly defined
- ☐ Employees can raise concerns about AI system performance

Common governance gap: AI introduced without updating workforce policies or training frameworks.

Risk if unchecked: Operational disruption and internal control failures.

7. Stakeholder Impact and Transparency

AI-assisted decisions can materially affect customers, employees and stakeholders.

Practical questions to consider:

- How are AI-assisted decisions communicated to affected parties?
- Are there mechanisms for explanation, review or appeal where appropriate?

Checklist:

- ☐ AI decision impacts are assessed
- ☐ Transparency exists around AI-assisted decisions
- ☐ Mechanisms for explanation or review are available where required
- ☐ Vulnerable groups are considered in system design and deployment

Common governance gap: Automated decision-making implemented without transparency safeguards.

Risk if unchecked: Loss of trust and regulatory scrutiny.

8. Monitoring, Reporting and Early Risk Indicators

Oversight should be continuous rather than event based.

Practical questions to consider:

- How are AI systems monitored over time?
- What early warning indicators are escalated to leadership?

Checklist:

- ☐ Higher-risk AI systems are actively monitored
- ☐ KPIs exist for AI governance performance
- ☐ Internal or external assurance is considered
- ☐ AI governance is reviewed regularly at leadership level

Early indicators that risk may be increasing include:

- Rapid staff adoption of public AI tools without policy updates
- Unclear ownership of AI systems
- Sensitive data being entered into external platforms
- Vendor AI features introduced without executive review
- AI risk absent from executive reporting

Risk if unchecked: Governance becomes reactive rather than structured.

9. In the Event of a Cyber or AI-Related Breach

If a data breach or cyber incident involves AI, the organisation remains legally responsible for the data it controls. The use of AI does not transfer liability to the technology itself or automatically to a vendor.

In such circumstances, regulators and insurers are likely to assess whether leadership exercised reasonable oversight.

Senior leaders should be able to demonstrate that:

- ☐ AI use was formally recognised and recorded
- ☐ Privacy and cyber risks were assessed prior to deployment
- ☐ Clear accountability was assigned for AI systems
- ☐ Incident response plans contemplated AI-related scenarios
- ☐ Reporting obligations were met at executive and board level

The central question will be whether appropriate governance structures were established and actively maintained.

Executive Reflection

If your board, insurer or regulator asked:

“What structured governance did leadership put in place before and during AI adoption?”

Would your organisation be able to demonstrate:

- Clear accountability
- Documented oversight
- Integrated risk management
- Structured reporting and monitoring
- Defined escalation pathways

If there is uncertainty, it is worth reviewing your governance framework before AI adoption expands further.

If this checklist has identified uncertainty or structural gaps, contact Corp IT.

CorpIT