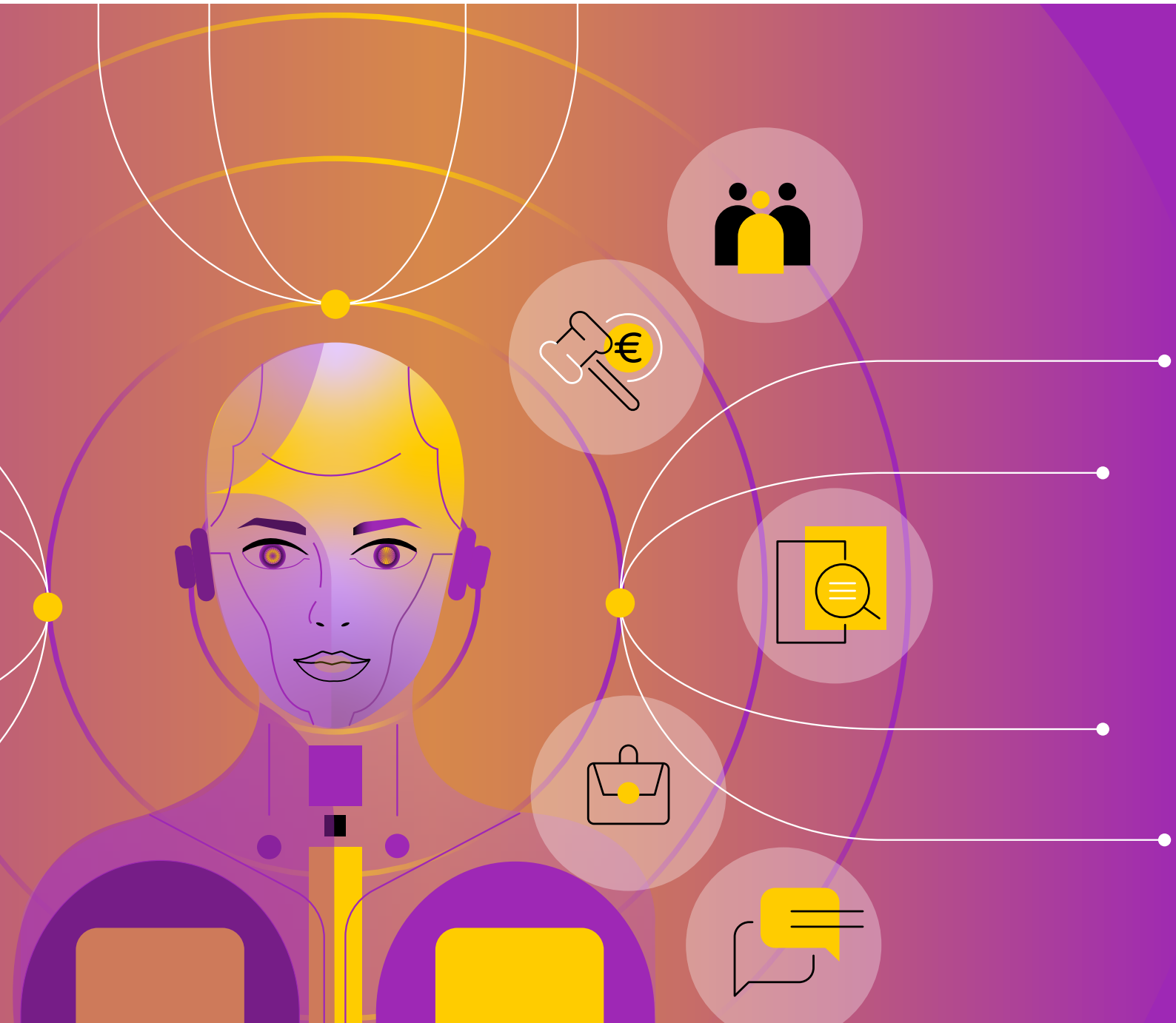
ACCOUNTANCY EUROPE.

ecoDa The European Voice of Directors

AI GOVERNANCE

TEN PRINCIPLES FOR EFFECTIVE BOARD OVERSIGHT

BRIEFING PAPER / OCTOBER 2026



CONTENTS

WHY GOOD CORPORATE GOVERNANCE MATTERS FOR AI ADOPTION 4

01 STRATEGY AND VALUE CREATION

PRINCIPLE 1: TREAT AI AS A CORE STRATEGIC ISSUE FOR BOARDS 6

PRINCIPLE 2: FOCUS ON VALUE CREATION, NOT JUST TECHNOLOGY ADOPTION 8

02 GOVERNANCE AND ACCOUNTABILITY

PRINCIPLE 3: ESTABLISH CLEAR GOVERNANCE AND ACCOUNTABILITY 10

PRINCIPLE 4: BUILD ORGANISATIONAL READINESS 13

PRINCIPLE 5: OVERSEE WORKFORCE AND OPERATING MODEL TRANSFORMATION 15

03 RISK OVERSIGHT AND INTERNAL ASSURANCE

PRINCIPLE 6: PRIORITISE OVERSIGHT ACCORDING TO RISK AND IMPACT 17

PRINCIPLE 7: ENSURE RESPONSIBLE AND TRUSTED AI USE 20

PRINCIPLE 8: SEEK EVIDENCE, INTERNAL ASSURANCE AND TRANSPARENCY 22

04 BOARD CAPABILITY AND EFFECTIVENESS

PRINCIPLE 9: STRENGTHEN BOARD AI CAPABILITY 25

PRINCIPLE 10: EMBRACE AI IN YOUR OWN WORK 27

WHERE ARE WE ON OUR AI GOVERNANCE JOURNEY? 30

ANNEX 1: PRACTICAL TOOLS 31

ANNEX 2: RESOURCES 32

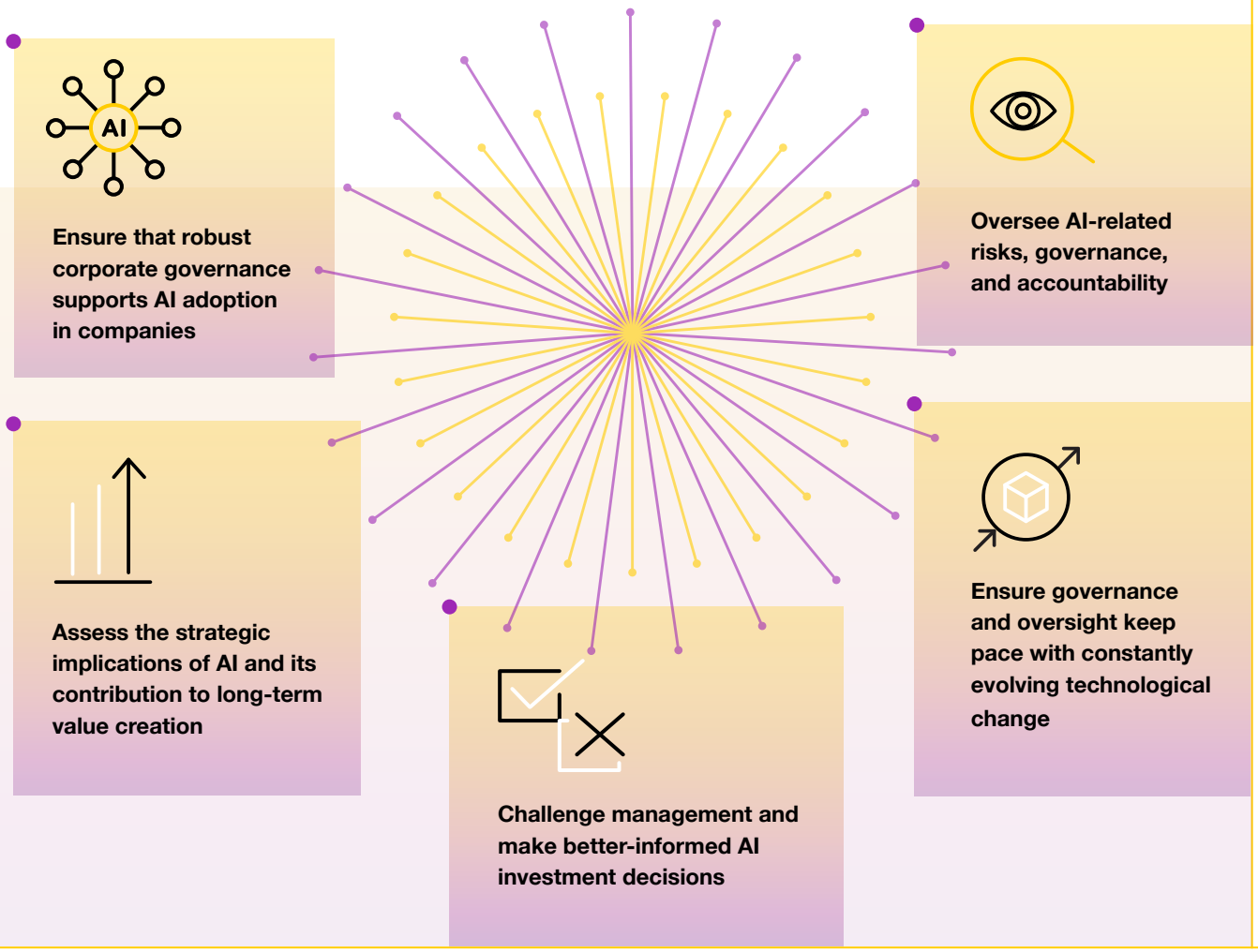
HIGHLIGHTS

Artificial Intelligence (AI) is reshaping how companies create value, compete, manage risks, and operate. This creates new challenges and opportunities for company leadership and boards. This paper aims to support them in ensuring that robust corporate governance and board oversight underpin AI adoption in companies.

Company boards are responsible for setting companies' strategic direction, overseeing long-term value creation and managing risk. Therefore, effective AI oversight is firmly a board-level responsibility.

This joint Accountancy Europe-ecoDa paper provides practical, principles-based guidance to help boards oversee AI adoption in their organisations through effective governance. It also highlights the key questions boards should ask from management to support informed oversight and decision-making.

By reading this paper, board members should be better equipped to:



WHY GOOD CORPORATE GOVERNANCE MATTERS FOR AI ADOPTION

Artificial Intelligence (AI) is transforming industries and economies, disrupting markets, reshaping competitive dynamics, and creating new strategic opportunities. Its impact extends far beyond mere productivity gains, as it is also influencing strategic choices, business models, operating structures, organisational capability, decision-making processes, and long-term value creation.

AI presents both a strategic opportunity and a governance challenge for companies and organisations. While it can accelerate innovation, enhance performance and help organisations reimagine how they create value, it may also introduce new operational, regulatory, legal, ethical, and reputational risks.

Navigating these opportunities and risks requires robust corporate governance and board leadership, which this joint Accountancy Europe-ecoDa paper aims to support. It builds on our previous collaboration to promote strong corporate governance, including our joint work on ESG governance.

Realising AI's potential requires a corporate governance system that balances innovation with accountability and effective risk management. It also depends on strong organisational foundations, including high-quality data, appropriate technology infrastructure, robust processes and controls, a skilled workforce, and a culture that supports the responsible adoption of AI at scale.

Crucially, AI cannot be a substitute for good corporate governance. AI can amplify existing organisational strengths and weaknesses, meaning that poor governance with AI is often simply poor governance at scale. Effective boards remain responsible for judgement, challenge, oversight, and decision-making. AI can support these activities, but it cannot replace them. Supporting the setup of such robust governance processes is the core objective of this paper.

AI oversight is not about boards becoming technologists. It is about ensuring that AI is used deliberately, safely and in ways that support strategy, create value, maintain trust and preserve accountability. The board's role is to set the boundaries, test the value case, oversee material risks, require evidence, and ensure that management has the capability and discipline to execute.

AI increasingly encompasses not only systems that generate predictions, recommendations or content, but also systems capable of taking actions, interacting with other systems and executing tasks with varying degrees of autonomy. As AI evolves from decision support towards increasingly autonomous capabilities, boards should ensure that governance, oversight, and accountability arrangements keep pace.

WHAT IS AI?

- **An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.**[1]

ARE BOARDS PREPARED FOR AI?

To inform this paper, Accountancy Europe and ecoDa conducted a qualitative, small-scale online survey of

87 EUROPEAN COMPANY DIRECTORS ACROSS DIFFERENT INDUSTRY SECTORS

to assess organisational AI readiness and board preparedness for AI governance and oversight. A detailed analysis of the survey results is available here.

Overall, the findings point to two broad conclusions: AI has become a strategic board issue, yet many organisations are still developing the governance and organisational capabilities needed to realise its full potential.

OBJECTIVE

This paper provides boards with practical, principles-based guidance on the governance of AI and its implications for strategy, accountability, risk management, and long-term value creation.

The paper sets out ten principles that:

- clarify the board's role in overseeing AI-driven business strategy
- highlight key areas for board attention, and
- propose a set of questions boards should ask management to support effective oversight.

The paper is designed to strengthen boards' ability to assess management assumptions critically and challenge decisions where needed. It aims to support boards in navigating AI in a fast-moving business and technological environment.

1 See Explanatory memorandum on the updated OECD definition of an AI system (2024), OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris.

01 STRATEGY AND VALUE CREATION

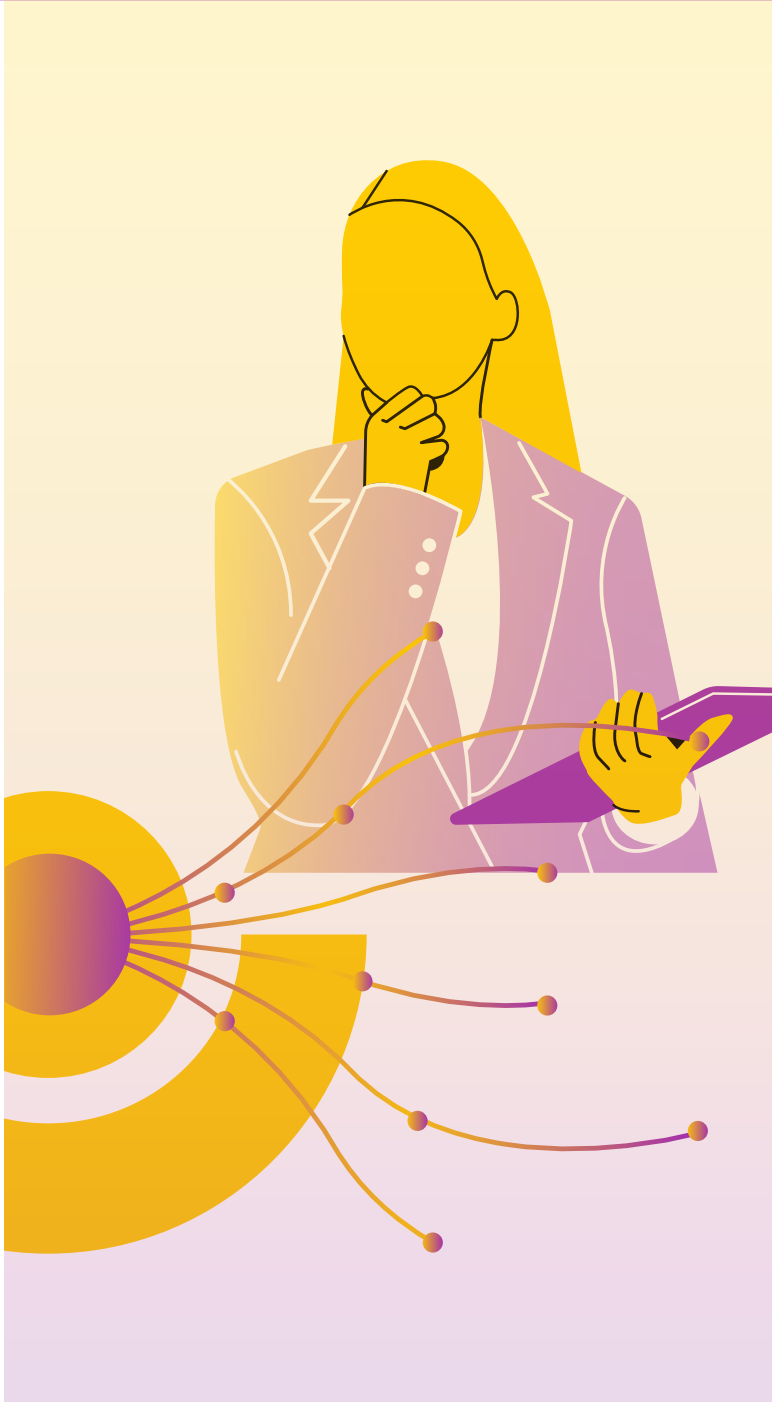
PRINCIPLE 1

TREAT AI AS A CORE STRATEGIC ISSUE FOR BOARDS

AI should be assessed not only for its efficiency gains, but also for its potential to transform business models, strengthen competitive advantage and create long-term value. A key strategic question is whether AI is being used to optimise the current business model, or to fundamentally redefine how the organisation creates and delivers value. This distinction should be explicit and deliberate.

AI is also increasing the strategic importance of assets such as proprietary data, customer insights, intellectual property, platforms and operational capabilities. Sustaining competitive advantage will depend not only on adopting AI technologies but also on how these assets are developed, protected and leveraged.

In parallel, investor expectations, regulatory developments such as the EU AI Act, and growing demands for transparency and accountability are raising expectations for AI governance. Governance over AI should therefore be treated as a core element of corporate governance and the strategic responsibility of the board, rather than a standalone technology issue.



BOARD INSIGHT

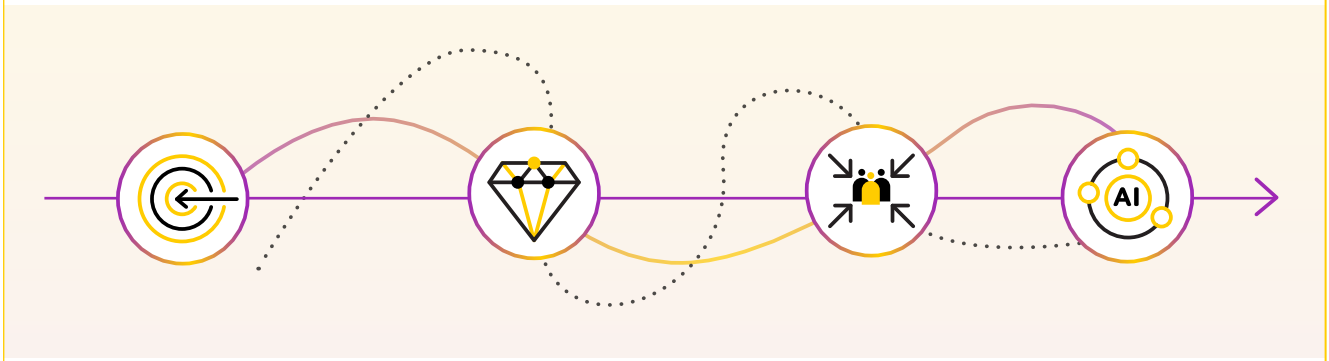
DON'T CHASE AI, LEAD IT STRATEGICALLY

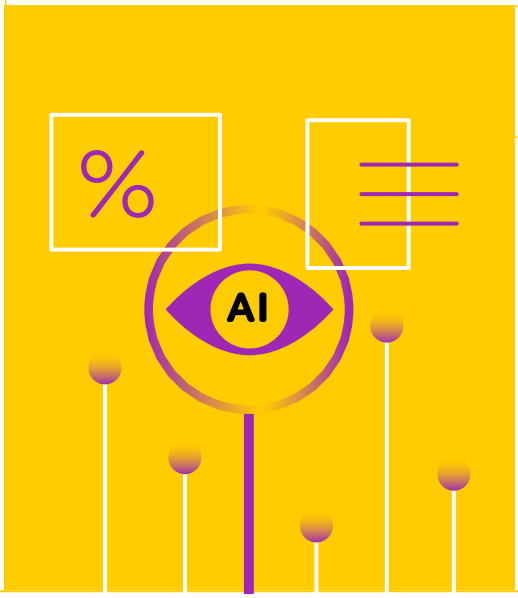
- **Boards should be cautious about being drawn into an AI "arms race"**, reacting to competitor announcements that are often overstated or driven by hype rather than genuine capability. They must remain vigilant in distinguishing noise from signal, ensuring that real competitive threats are identified and addressed before they erode the organisation's strategic position.

- **Boards' focus should be on prioritising meaningful AI-driven value creation**, moving beyond disconnected tools, pilots, or initiatives. The key is disciplined discernment: neither complacency nor reactivity, but a clear-eyed assessment of value creation opportunities and the capabilities required to deliver them across the organisation.

- **AI adoption should be driven by business strategy, business and stakeholder needs.** It should focus on where AI can strengthen the organisation's value proposition, improve customer experience, increase speed, reduce cost, or enhance internal processes.

- **Boards should recognise that the greatest value from AI may not come from simply automating existing activities,** but from redesigning processes and operating models around AI capabilities. This may require rethinking workflows, decision-making processes, and organisational structures – rather than layering AI onto outdated ways of working. Strong ownership by top management is essential.





KEY QUESTIONS FOR BOARDS

STRATEGIC AI OVERSIGHT

1. How could AI reshape our strategy, business model, competitive position, and long-term prospects?

2. How can we use AI to drive system-wide value creation rather than simply improving efficiency?

3. Where can AI deliver genuine competitive advantage for us, and how are competitors already using it to disrupt the market?

PRINCIPLE 2

FOCUS ON VALUE CREATION, NOT JUST TECHNOLOGY ADOPTION

Deploying AI is not an objective in itself. AI initiatives should have clearly defined objectives and credible pathways to delivering value. Boards should evaluate AI initiatives based on their ability to deliver measurable and sustainable outcomes that advance the organisation's objectives, relative to their costs, risks and expected benefits.

This includes assessing where AI creates strategic advantage, where it supports operational improvement, and whether the expected value is likely to be realised by the organisation rather than primarily captured by vendors, platforms, customers or other stakeholders.

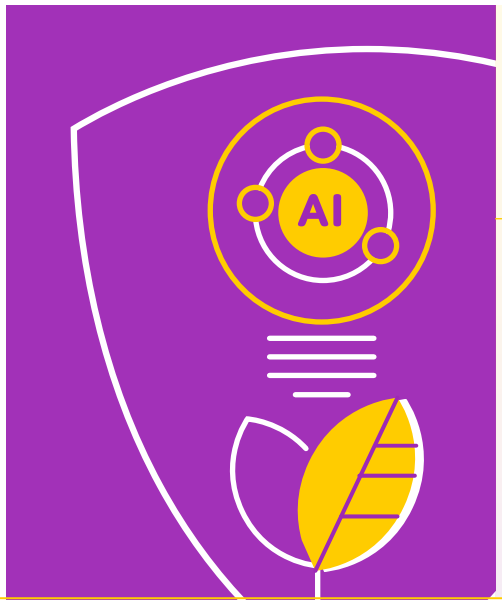
CONSIDERATIONS FOR AI INVESTMENTS

AI investments should be subject to the same discipline as other major capital allocation decisions, including an upfront assessment of their expected value, risk profile and governance requirements, together with clear investment objectives, expected returns, defined success metrics, structured review points and explicit accountability for delivery.

CONSIDERATIONS FOR AI INITIATIVES

AI initiatives should be assessed based on demonstrated outcomes rather than activity-based metrics such as the number of pilots, models or deployments. This means challenging whether expected benefits are real, measurable, durable and scalable, rather than assumed on the basis of technological promise or vendor claims.

Organisations should establish clear decision criteria for AI initiatives, including predefined conditions for approving, pausing, redesigning or terminating projects where expected value is not being realised or risks become unacceptable.



BOARD INSIGHT

RISKS OF AI ADOPTION AND NON-ADOPTION

Failing to adopt AI may result in strategic stagnation and erosion of competitive position. Overly cautious approaches may lead to missed opportunities for growth and innovation. Equally, rushing into AI adoption without appropriate governance may create unnecessary costs or risks that outweigh the expected benefits. Boards should therefore assess both adoption and non-adoption scenarios to achieve an appropriate balance between innovation, resilience and risk.

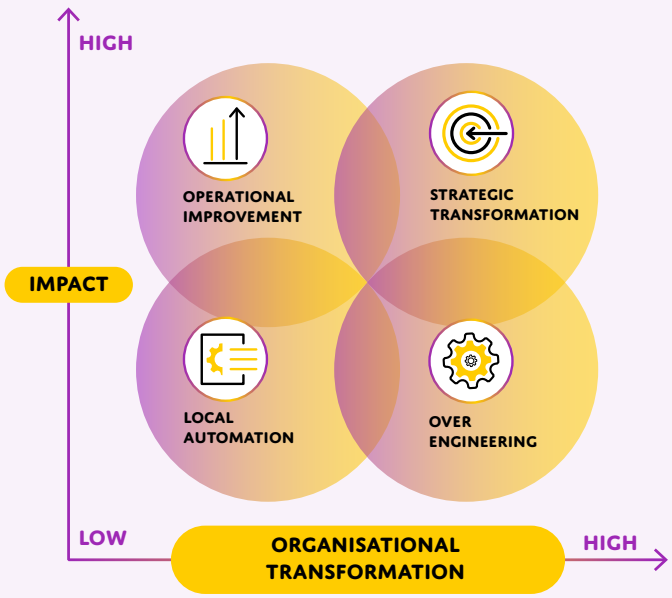
BOARD INSIGHT

BALANCE TRANSFORMATION AND VALUE CREATION

AI initiatives differ not only in their potential impact but also in the degree of organisational change they require. Boards should challenge whether anticipated benefits are realistic, scalable and capable of being captured by the organisation, taking into account implementation costs, enterprise-wide investment requirements, and the likelihood that competitors may have access to similar technologies. They should also distinguish between local productivity gains and enterprise-wide value creation. Significant transformation efforts are justified only where they support clear strategic objectives and measurable business outcomes.

Fig.1 illustrates how boards can assess AI initiatives according to both their potential impact and the degree of organisational transformation they require.

FIG.1 AI INITIATIVE PORTFOLIO



KEY QUESTIONS FOR BOARDS

INVESTMENT DISCIPLINE AND VALUE REALISATION

1. What business outcomes are expected from major AI initiatives, and how will they be measured?
2. What evidence gives us confidence that the expected benefits are real, scalable and capable of being realised across the organisation?
3. Does management understand how AI may reshape our business model, functions, competitive positioning and value creation opportunities to make informed investment and transformation decisions?
4. How will return on investment and value realisation from AI be tracked over time?
5. At what point will AI initiatives be paused, redesigned, or stopped if they fail to deliver the expected value? How do we determine when that should be the case?
6. Who is ultimately accountable if AI initiatives fail to deliver expected business value?
7. How is our investment in AI aligned with our risk appetite?
8. What are we explicitly choosing not to do with AI, and is this boundary clearly understood and enforced at executive level?

02 GOVERNANCE AND ACCOUNTABILITY

PRINCIPLE 3

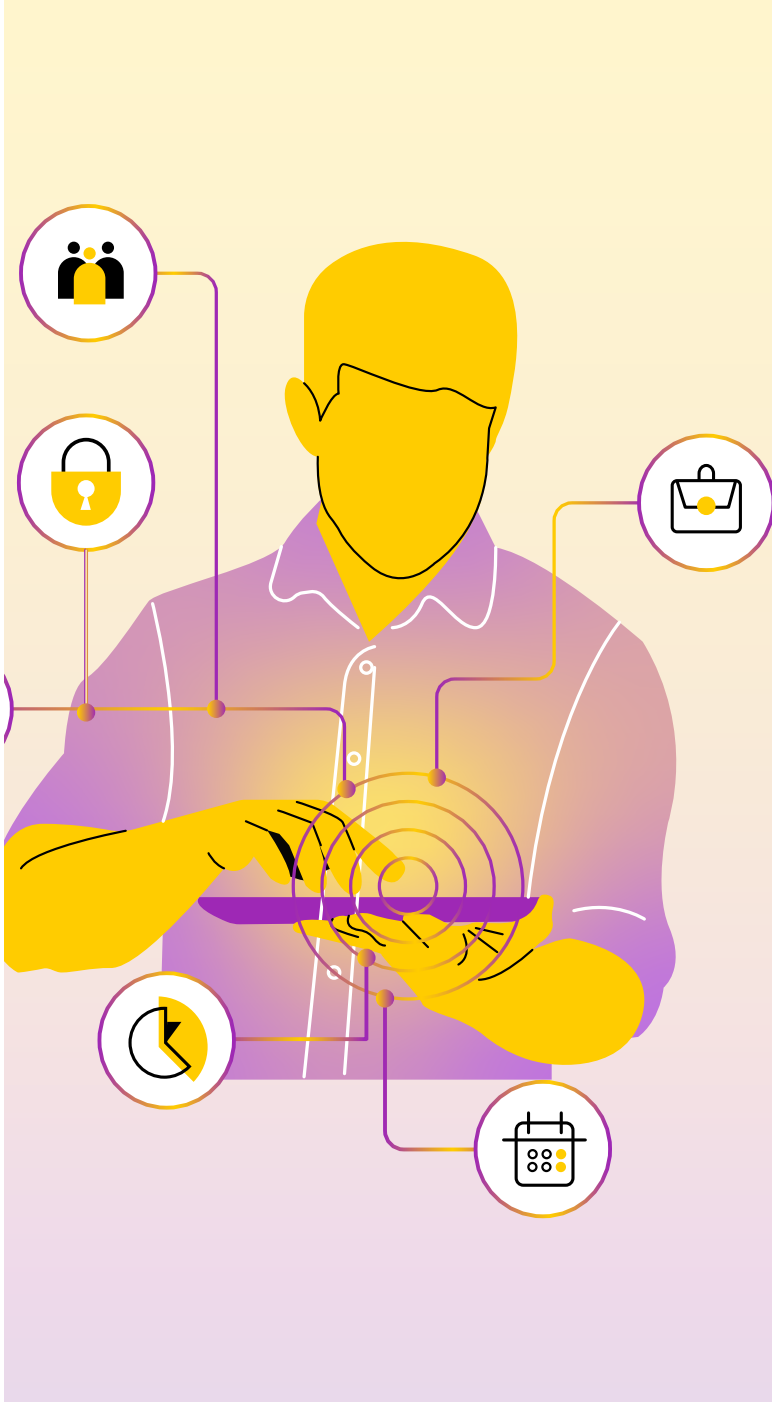
ESTABLISH CLEAR GOVERNANCE AND ACCOUNTABILITY

Governance over AI should be embedded within existing enterprise governance, supported by AI-specific capabilities, controls, skills and escalation mechanisms. There is no need for a complete re-design or reinventing the wheel on governance systems unless explicitly deemed necessary.

In practice, this involves integrating AI risks, controls, and decision-making into existing business processes, operational workflows, reporting frameworks, and internal assurance mechanisms, while adapting controls where AI-specific safeguards are required.

AI governance entails establishing clear accountability for outcomes and decisions, including where decisions are automated, the required extent and form of human oversight, and how failures, unintended consequences, or control breakdowns are identified and escalated.

Accountability for AI outcomes cannot be delegated to technology. Responsibility remains with business and functional management and, ultimately, with the board, regardless of the degree of automation. Responsibilities for decision-making, oversight and escalation should therefore remain clearly assigned.



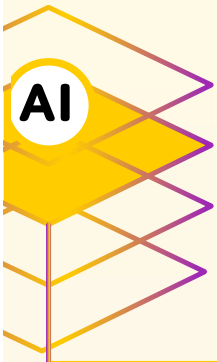
Boards should ensure that AI responsibilities are appropriately coordinated across board and committee structures, including audit, risk, technology, and other relevant committees. Audit and risk committees should integrate AI into existing oversight processes, supported by clear accountability, reporting, and escalation arrangements.

Audit and risk committee members, in particular, should assess whether internal controls have been meaningfully adapted to address AI-related risks or simply repackaged from pre-AI frameworks.

KEY QUESTIONS FOR BOARDS

GOVERNANCE AND ACCOUNTABILITY

1. How have AI-specific capabilities, controls, skills and escalation mechanisms been integrated into our enterprise risk management systems?
2. How is accountability for AI governance allocated across business, risk, legal, compliance, technology, and other relevant functions?
3. How should AI oversight be integrated into our existing committee structures, or should it be supported by a dedicated digital and technology committee?
4. Do our governance structures provide sufficient challenge and escalation for high-risk AI decisions?
5. Does internal audit review AI systems as part of its audit plan?
6. How have we assessed our potential liability exposure where AI outputs contribute to decisions affecting customers, employees, or other stakeholders?



HOW TO EMBED AI INTO GOVERNANCE, RISK & CONTROL SYSTEMS?

- **Build on existing** governance and enterprise risk management frameworks
- **Embed AI risks** into internal controls, reporting, and internal assurance processes
- **Adapt existing controls** or introduce AI-specific safeguards where necessary
- **Assess AI impacts** on business processes, control environments, and reporting reliability
- **Regularly review** and update controls as AI capabilities and risks evolve

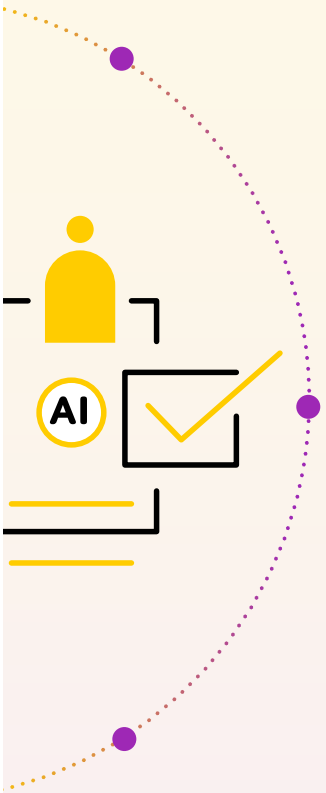
Dedicated committees may provide deeper expertise, while integration into existing committees may support more holistic oversight and reduce silo risk. Many organisations expand audit/risk committee mandates while keeping strategic AI discussions at full-board level.

INTERNAL ASSURANCE AND THE THREE LINES OF DEFENCE

AI oversight should follow the three lines of defence model, clearly defining responsibilities for management, risk, compliance, and internal assurance functions. This approach strengthens accountability and ensures effective challenge and assurance across the organisation.

RETAIL BANK AI-SUPPORTED CREDIT APPROVAL PROCESS – APPLYING THE THREE LINES OF DEFENCE

The following example is illustrative and simplified to demonstrate governance responsibilities rather than the detailed operation of a credit approval process.



01. FIRST LINE OF DEFENCE
BUSINESS AND TECHNOLOGY

The retail lending and data science teams design and operate AI models that support the broader credit assessment process. These models may assist in assessing borrower characteristics, risk factors, and other relevant information, while operating within approved lending policies and remaining subject to appropriate human review. The teams monitor model performance, bias indicators, and customer complaints, remediating issues as they arise.

02. SECOND LINE OF DEFENCE
RISK, COMPLIANCE AND AI GOVERNANCE

Risk and compliance functions define the conditions under which AI can be used in credit decisions, including governance requirements, validation standards, and appropriate human oversight. They set fairness and explainability standards, require approval for high-risk models, and independently review model design, testing, validation, and ongoing performance. They challenge assumptions and can require changes or block deployment where risks exceed the organisation's risk appetite.

03. THIRD LINE OF DEFENCE
INTERNAL AUDIT

Internal audit periodically assesses whether the AI-supported credit decision process is governed and controlled in line with internal policies and regulatory expectations. It tests whether governance arrangements, model controls including data confidentiality, human oversight, and monitoring processes are operating effectively in practice, and reports findings to the audit and risk committees and the board.

MANAGEMENT OWNERSHIP AND ACCOUNTABILITY

Management oversight of AI should operate through clearly defined roles across business, technology, risk, compliance, legal, reputational, security, and assurance functions, supported by effective reporting, challenge, and escalation mechanisms.

MANAGEMENT RESPONSIBILITIES FOR AI

- Integrating AI investment and deployment into strategy and operating model transformation
- Developing AI related workforce skills, training, and awareness
- Developing governance frameworks, policies, and user guidance
- Continuous review of policies, controls, and capabilities as the environment evolves

PRINCIPLE 4

BUILD ORGANISATIONAL READINESS

ORGANISATIONAL READINESS

Effective AI adoption requires clear business ownership and organisational readiness across data, technology, people, governance, and culture. High-quality data, robust infrastructure, workforce capability, leadership commitment, and targeted upskilling, including recruitment of expertise where necessary, are essential foundations.

Boards should oversee the organisation's capability to learn and adapt as AI evolves. This includes AI literacy, controlled experimentation, rapid learning cycles, and the ability to scale or discontinue initiatives based on evidence and changing conditions.

KEY QUESTIONS FOR BOARDS

GETTING READY FOR AI

Boards should challenge management on whether readiness is real or assumed:

1. Do we have sufficient internal capability, data quality, and infrastructure to support safe and compliant AI deployment, or are we relying on external vendors and assumptions of readiness?
2. Where is AI adoption most likely to fail in practice, e.g. in skills, culture, data, or process integration, and what evidence supports that view?

DATA AS THE FOUNDATION FOR AI

Boards should ensure that AI-related data governance explicitly addresses confidentiality risks, including the use of external or cloud-based AI systems. This includes understanding how data is stored, processed, reused, or exposed, and ensuring that sensitive or regulated data is not inadvertently shared through AI tools.

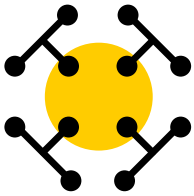
Importantly, AI-related data governance extends beyond confidentiality and privacy to address data quality, provenance, ownership, and ongoing stewardship. Many AI failures originate in poor data rather than model design. Boards should therefore be satisfied that the organisation understands the data which AI systems rely on, and has appropriate governance over its quality, provenance, use, lifecycle, and any mechanisms through which AI-generated outputs are incorporated into organisational knowledge or used to inform decision-making.

KEY QUESTIONS FOR BOARDS

DATA GOVERNANCE

1. Do we understand what data our AI systems rely on, and do we have the right to use it?
2. Who is accountable for data quality, and who is responsible for remediating data-related issues?
3. How do we ensure confidentiality of proprietary or non-public information is maintained?
4. Can the provenance and use of AI-related data be traced where necessary?

OPERATIONAL RESILIENCE AND EXTERNAL DEPENDENCIES



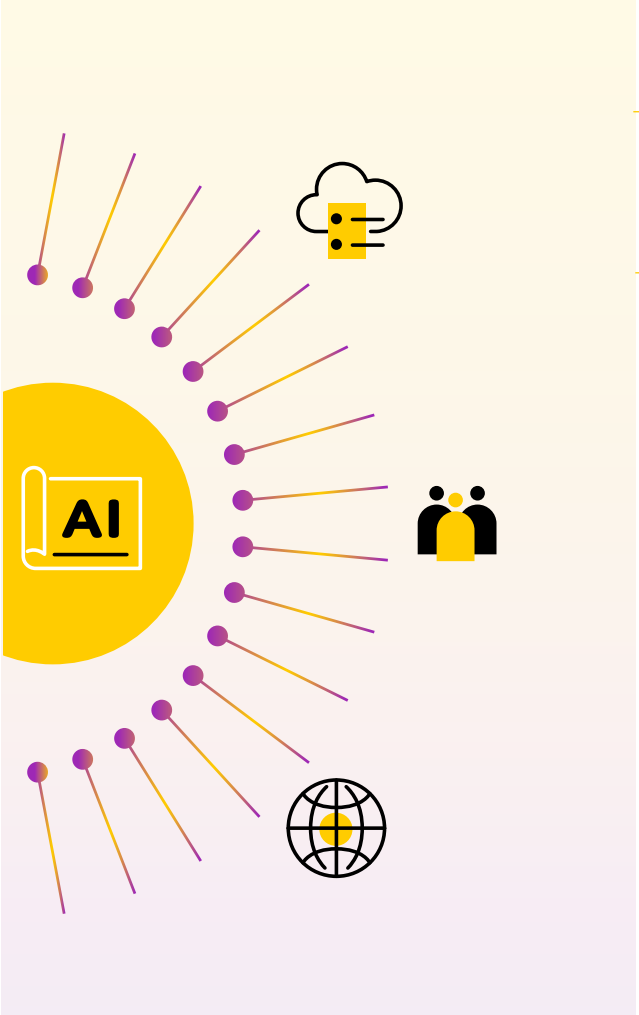
Organisational readiness requires understanding the strategic dependencies created by AI adoption.

As organisations increasingly rely on a relatively small number of cloud providers, AI model developers, technology platforms and other specialist suppliers, boards should assess how these dependencies could affect resilience, operational continuity, regulatory exposure, strategic autonomy, and long-term strategic flexibility.

Boards should consider how changes in regulation, geopolitics, market concentration, or supplier resilience could affect the organisation's ability to execute its AI strategy, maintain operational resilience, and retain sufficient control over critical technologies, data, and AI capabilities.

Readiness assessments should identify capability gaps, prioritise investment, and ensure implementation roadmaps reflect regulatory, operational, privacy, and legacy system constraints. They should also assess the extent to which data, infrastructure, cybersecurity, and resilience capabilities are sufficient to support AI adoption at scale.

AI changes the organisation's cybersecurity risk profile by introducing new attack vectors, increasing dependence on third-party platforms, and creating additional risks relating to confidential data, model integrity, and AI-enabled cyber threats. Boards should therefore consider whether existing cybersecurity and resilience arrangements adequately address these AI-related risks.



KEY QUESTIONS FOR BOARDS

OPERATIONAL RESILIENCE AND EXTERNAL DEPENDENCIES

1. Which dependencies on suppliers, platforms, jurisdictions, skills, or regulatory frameworks could materially limit or disrupt execution of our AI strategy?
2. Have we adequately assessed the data sovereignty, GDPR, operational resilience, and strategic dependency implications of relying on third country cloud or AI infrastructure for critical processes?
3. Are disaster recovery and business continuity arrangements tested for AI-related disruption scenarios?
4. Have we assessed how AI changes our cyber risk profile, and are our cyber resilience and incident response arrangements evolving accordingly?

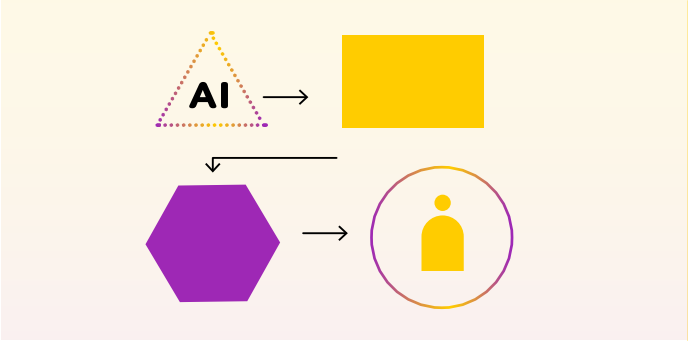
PRINCIPLE 5

OVERSEE WORKFORCE AND OPERATING MODEL TRANSFORMATION

AI workforce oversight is not solely an HR issue. It is a strategic, operational, and reputational issue that affects organisational resilience, future leadership capability, and long-term competitiveness.

Boards should oversee how AI reshapes workforce structure, work redesign, decision-making, management roles and responsibilities, talent pipelines, skills requirements, and organisational culture. This includes ensuring appropriate investment in workforce planning, reskilling, upskilling, leadership development, and effective change management.

The pace of AI-driven change requires continuous adaptation of workforce capabilities, governance approaches, and operating models. Management should prepare the organisation through workforce planning, work redesign, and targeted capability development. Poorly managed workforce impacts may weaken organisational culture, reduce trust, create capability gaps, concentrate decision-making, and increase overdependence on AI. This could ultimately undermine organisational resilience and long-term performance.



Replacing entry-level roles with AI may remove the apprenticeship pathways through which future managers, specialists, and leaders develop operational judgement and institutional knowledge. Over time, this can weaken internal talent pipelines and increase dependence on external hires, vendors, or AI systems themselves.

BOARD RESPONSIBILITIES FOR WORKFORCE OVERSIGHT

- Monitor the impact of AI on talent pipelines, succession planning, and future leadership capability
- Align workforce planning, work redesign, reskilling, upskilling, and staff and leadership development with AI strategy and future capability needs
- Ensure change management supports adoption, trust, and effective use of AI across the organisation
- Consider ethical and societal implications of workforce transformation
- Monitor transparency and communication regarding AI systems affecting employees

KEY QUESTIONS FOR BOARDS

WORKFORCE TRANSFORMATION

1. Are we using AI primarily to replace labour, augment human capability, or redesign work, and are the implications of this choice understood?
2. Could AI adoption unintentionally weaken future leadership or specialist talent pipelines?
3. What workforce transition and reskilling programmes are in place, how do we assess their effectiveness, and how are employees being supported through AI-driven change?
4. How is AI changing the way people work across the organisation, and are we managing that transformation effectively?
5. Are there significant differences in AI adoption, capability or readiness across business functions or geographies that could create operational or governance risks?
6. Do we have the right AI skills and capabilities at executive and board level and, if not, how will any gaps be addressed?
7. Are employees provided with clear policies and appropriate training on the responsible use of AI, including the use of enterprise and personal AI tools and the protection of confidential information?
8. How are we building trust in AI while maintaining appropriate human judgement, governance, and accountability?
9. What evidence gives us confidence that our workforce is ready to adopt AI safely, effectively, and at scale?

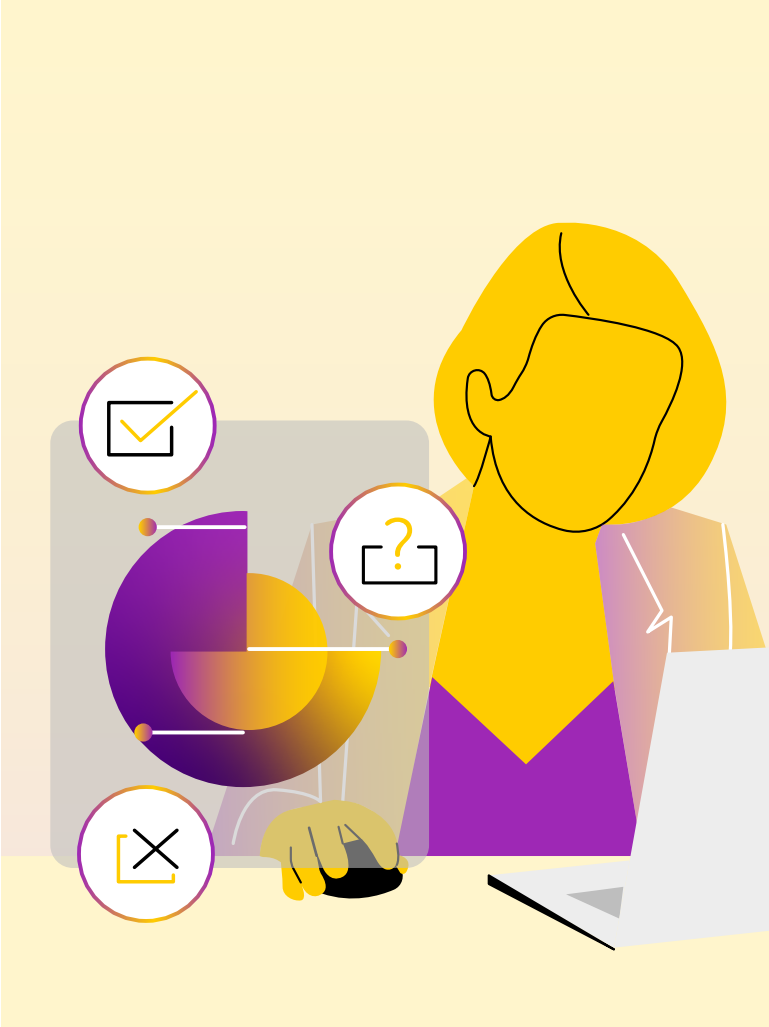
03 RISK OVERSIGHT AND INTERNAL ASSURANCE

PRINCIPLE 6

PRIORITISE OVERSIGHT ACCORDING TO RISK AND IMPACT

AI can create competitive advantage through speed, scale, automation, and enhanced decision-making, but it also introduces strategic, operational, regulatory, legal, reputational, ethical and resilience risks that must be understood and balanced against its potential benefits. When not properly governed, AI can amplify errors, bias, control failures, and poor decisions.

Boards should define and oversee the organisation's AI risk appetite across strategic, operational, financial, legal, and reputational dimensions. This should include defining acceptable levels of AI-related risk, clear red lines and uses that should be prohibited or restricted.



Effective board oversight also requires recognising behavioural risks, including automation bias – the tendency to place undue reliance on AI-generated outputs because they appear authoritative or data-driven. Governance and control frameworks should encourage independent review, effective challenge, and clear accountability.

Not all AI applications require the same level of oversight. Governance, controls, reporting, internal assurance, and board oversight should be proportionate to the significance, purpose, and risk profile of each AI application. Different governance

considerations may arise depending on whether AI is used to support internal productivity, interact with customers, inform or automate decisions, operate autonomously, or perform regulated or business-critical activities.

Boards should ensure management applies a structured and consistent approach to classifying material AI applications and potential risks. Classification should consider factors such as impact, autonomy, regulatory obligations, explainability, organisational dependency, and other relevant risk characteristics. The board should oversee these material AI classifications and challenge those that appear inconsistent with the organisation's risk appetite, regulatory obligations, or potential impact.

Risk classifications should not create a false sense of assurance. Boards should remain alert to hidden risks also in seemingly low-risk AI applications where scale, automation, dependencies, or limited transparency may create significant cumulative operational, governance, or reputational consequences over time.

DIFFERENT AI APPLICATIONS RAISE DIFFERENT GOVERNANCE QUESTIONS

Examples include:

- Predictive and analytical AI
- Generative AI
- Decision-support AI
- Customer-facing AI
- Automated decision-making
- Agentic or autonomous AI
- AI embedded in third-party software
- AI used in regulated or business-critical functions
- AI used by employees outside approved organisational systems (shadow AI)*

** Shadow AI refers to the use of AI tools or systems for work-related activities without organisational approval, oversight, or governance.*

HIDDEN RISKS IN "LOW-RISK" AI

- AI-generated code introducing untraceable or non-maintainable logic
- Model drift in lower-priority systems going undetected
- Automation failures creating cascading operational errors
- Vendor models limiting explainability, traceability, or provenance

BOARD INSIGHT

AI RISK RADAR

LOW	MODERATE	HIGH/ CRITICAL	UNACCEPTABLE
Example AI use / Limited-impact internal productivity tools	**Example AI use /** Analytics and decision-support tools	**Example AI use /** Customer-facing or automated decision-making systems	**Example AI use /**Applications that exceed the organisation's risk appetite, are deemed unlawful under applicable legislation or create unacceptable ethical, legal, or reputational consequences
Governance Response / Proportionate oversight and monitoring	**Governance Response** / Standard controls and performance monitoring	**Governance Response** / Enhanced governance, internal assurance, and board oversight	**Governance Response /** Prohibited

KEY QUESTIONS FOR BOARDS

RISK-BASED OVERSIGHT

Understanding the organisation's AI risk exposure

1. Which AI applications could cause the greatest physical, operational, financial, regulatory, or reputational harm if they failed?
2. What is the worst-case scenario from our use of AI, and are we realistically prepared to manage it?
3. Where could AI create irreversible damage to trust, compliance, or licence to operate?

Risk classification and proportional oversight

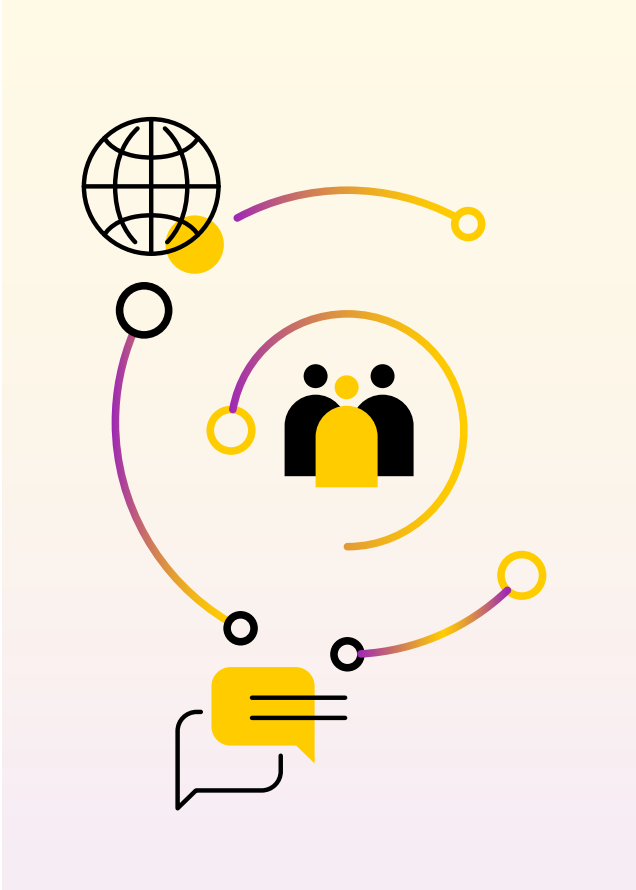
1. Do we maintain an up-to-date inventory of AI systems, use cases, and associated risk classifications?
2. How has the organisation identified AI systems that are high-risk, including where relevant under applicable regulation (e.g. the EU AI Act)?
3. Are governance, oversight, and internal assurance arrangements proportionate to the significance and risk profile of our AI applications?

PRINCIPLE 7

ENSURE RESPONSIBLE AND TRUSTED AI USE

Responsible AI extends beyond legal compliance. AI governance should be grounded in organisational values, legal obligations, ethical considerations and the broader public interest. Key considerations include fairness, non-discrimination, confidentiality, transparency, explainability, and appropriate human oversight.

Boards should be prepared to navigate difficult trade-offs where commercial objectives, stakeholder expectations, individual rights, and societal impacts may not always align. Boards should therefore consider whether AI use would withstand scrutiny from regulators, stakeholders, and the wider public, particularly where decisions affect individuals, markets, or society.



Mechanisms should exist for individuals affected by AI-driven decisions to challenge outcomes where appropriate. Under the EU AI Act, transparency and human oversight are legally enforceable requirements for certain high-risk AI systems.

Boards should understand how human oversight is applied in practice, including whether individuals are directly involved in decisions (human-in-the-loop), monitoring outcomes (human-on-the-loop), or providing strategic oversight (human-in-command).[2]

Boards should also ensure that oversight extends to third-party AI providers and services, including whether external systems align with the organisation's ethical standards, transparency expectations, responsible data sourcing, fairness, and accountability.

Boards should also consider the broader consequences of AI adoption, including workforce impacts, environmental considerations, and unintended long-term effects that may not be captured through traditional risk and compliance processes. These can significantly influence stakeholder trust, organisational reputation, and long-term value creation.

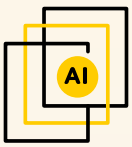
2 See Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment (July 2020), European Commission.

KEY QUESTIONS FOR BOARDS

RESPONSIBLE AND TRUSTED AI USE

JUDGEMENT AND ACCOUNTABILITY

1. If a material AI failure occurred within our organisation today, could we clearly explain who is accountable, how it happened, and why controls did not prevent or detect it earlier?
2. Are we making deliberate decisions where commercial benefits may conflict with stakeholder expectations, organisational values, or broader societal impacts?
3. Are there AI applications that are lawful but could nevertheless undermine trust, fairness, or our reputation?



TRANSPARENCY AND GOVERNANCE

1. Could we clearly explain to customers, regulators, employees, investors, and the public how our most significant AI systems influence decisions and outcomes?
2. Is AI genuinely governed through existing risk and control frameworks, or is there de facto “shadow governance” driven by IT, vendors, or individual business units?
3. How are we detecting, monitoring, and managing “shadow AI” use across the organisation, including employee use of external AI tools and platforms?
4. Are policies governing employee use of AI, including generative AI and “shadow AI”, clearly defined and kept up to date?

TRUST AND STAKEHOLDER EXPECTATIONS

1. Which of our AI use cases could create the greatest risk to stakeholder trust if they failed or attracted public scrutiny?
2. Are there AI uses that stakeholders would reasonably expect us to disclose, even where there is no legal obligation to do so?
3. Are we proactively building stakeholder trust in our AI use, or reacting only when scrutiny arises?

PRINCIPLE 8

SEEK EVIDENCE, INTERNAL ASSURANCE AND TRANSPARENCY

ASSURANCE AND OVERSIGHT

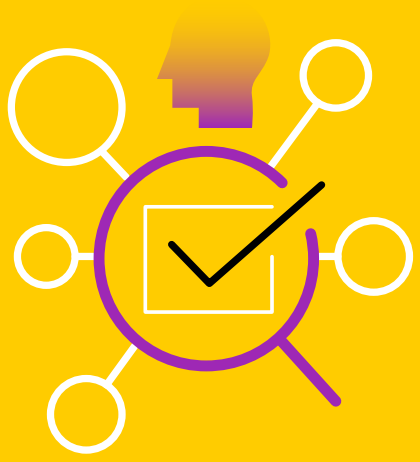
Effective AI oversight requires evidence, internal assurance, ongoing monitoring, and transparent reporting. However, in most companies and organisations, internal assurance over AI is still evolving and remains immature, uneven, and sometimes technically challenging.

Organisations may have limited visibility into how AI risk management, controls, and outputs perform in practice. Boards need to understand what can and cannot be assured; the capabilities and limitations of existing assurance functions; whether assurance covers governance, system design, operation, model performance or outcomes; and the limitations of current internal assurance approaches.

Boards should ensure that internal assurance frameworks provide independent and reliable evidence regarding AI governance, reliability, legal and regulatory compliance, confidentiality, resilience, operational performance, and the effectiveness of key controls.

Internal assurance structures should include capable and independent internal audit, risk, compliance, and technology assurance functions. Clear escalation mechanisms should be in place, together with appropriate authority to intervene or halt AI systems where necessary.

Boards and audit committees should also understand how AI is used within the external audit process and how this may affect audit quality, assurance, and oversight.



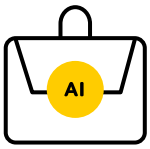
KEY QUESTIONS FOR BOARDS

INTERNAL ASSURANCE AND OVERSIGHT

1. What evidence gives us confidence that AI controls and governance arrangements are operating as intended?
2. Can AI decisions and outputs be traced, explained, and evidenced where required?
3. Do internal audit, risk, compliance, and technology assurance functions have sufficient capability, methodology, and technical expertise to assess AI risks and controls effectively?
4. Which AI use cases and related business or governance processes warrant independent external assurance?

KEY QUESTIONS FOR BOARDS

AI USE IN EXTERNAL AUDIT



As part of the development of the recommendation for the appointment of a statutory auditor or audit firm:

1. Where and how do the candidate-external auditors plan to use AI within the audit process?

As part of the annual external audit process:

1. Where and how has the external auditor used AI within the audit process?
2. Whether and how has the external auditor used AI within quality management?
3. Whether and how has the external auditor used AI to determine his or her independence of the audited entity?

MONITORING, REPORTING AND TRANSPARENCY

Internal assurance is strengthened when boards have visibility into how AI performs in practice; how incidents are managed; how decisions are challenged; and how outcomes are documented and reported.

Management reporting should provide clear visibility of AI use and its impact on business model, key business processes and outcomes, as well as associated risks, incidents, dependencies, and controls. It should distinguish experimentation from proven value creation and provide visibility of material failures, limitations, implementation challenges, and lessons learned.

AI incidents, control failures, and operational disruptions should be managed through clearly defined responsibilities, escalation thresholds, response procedures, and resilience testing. Boards should ensure appropriate mechanisms exist to identify, investigate, and address control failures.

Appropriate transparency should also be maintained for regulators, investors, customers, employees, and other stakeholders. This includes clear communication of how AI supports strategy; how risks are managed; and how the organisation is ensuring responsible and trustworthy AI use.

KEY QUESTIONS FOR BOARDS

MONITORING, REPORTING AND TRANSPARENCY

1. Do we have sufficient visibility into how AI is affecting our business model, key business processes and organisational performance?
2. Are our incident management and intervention mechanisms sufficiently robust?
3. Are disaster recovery and business continuity arrangements tested for AI-related disruption scenarios?
4. Where and how is AI influencing our financial or non-financial reporting processes?
5. What level of visibility do we want to provide into AI risks, dependencies, incidents, and outcomes?
6. What should be disclosed publicly, to whom, and when?

HUMAN JUDGEMENT AND ACCOUNTABILITY

Strong governance over the use of AI-generated outputs requires clear documentation and an appropriate audit trail of how AI systems influence decisions, including the nature of inputs, the design of algorithms, the role of AI-generated outputs, validation and review activities, decisions taken, and the professional judgement applied.

This supports auditability, regulatory compliance, transparency, and accountability in the event of challenge or failure.

KEY QUESTIONS FOR BOARDS

HUMAN JUDGEMENT AND ACCOUNTABILITY

1. Can AI decisions and outputs be traced, explained, and evidenced where required?
2. How are AI outputs validated, challenged, and monitored for bias, hallucinations, drift, or loss of traceability?
3. How are management and employees prevented from over-relying on AI outputs, particularly in high-impact decisions?

04 BOARD CAPABILITY AND EFFECTIVENESS

PRINCIPLE 9

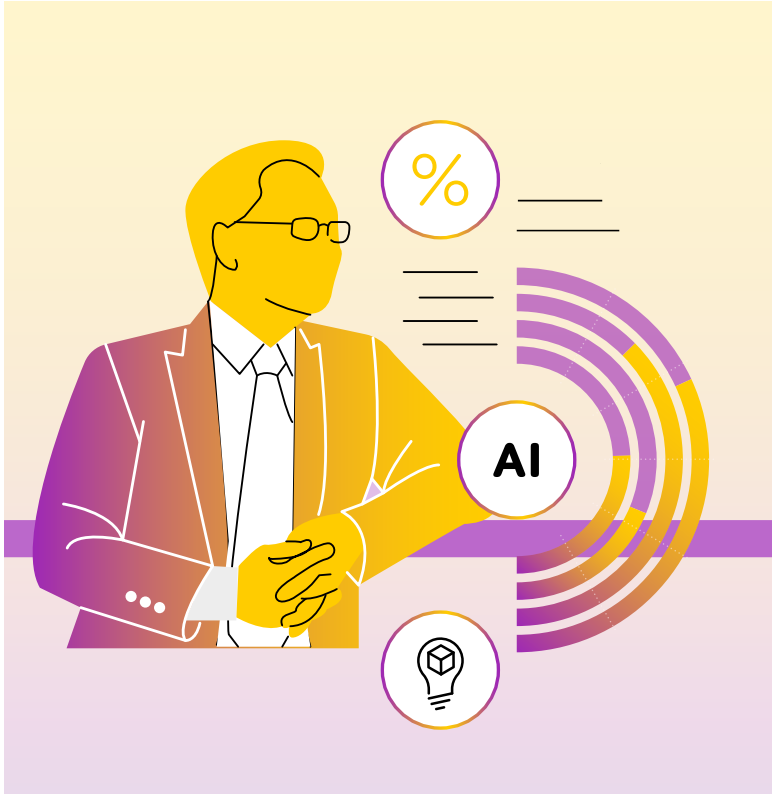
STRENGTHEN BOARD AI CAPABILITY

AI literacy underpins effective board oversight in an AI-enabled organisation. Directors are not expected to be technical experts, but they must have sufficient understanding of AI systems to challenge management, assess strategic choices, and evaluate risks.

The focus should be on decision-relevant understanding, rather than technical detail, with depth varying according to the organisation's sector, risk exposure, and use of AI.

Board learning should prioritise the business and governance implications of AI, including strategic options, investment decisions, operational impact, risk exposure, and regulatory responsibilities. Broader digital competence should also encompass awareness of cybersecurity and other emerging technologies that interact with AI systems.

When internal expertise is limited, boards should bring in external specialists to strengthen internal assurance, provide independent challenge, and support informed decision-making on complex or high-risk AI issues.



Governance structures, committee mandates, reporting lines, and agenda allocation should be reviewed periodically to ensure they remain appropriate as AI adoption increases. This includes ensuring oversight responsibilities are clearly defined, technology and risk receive sufficient attention, and oversight cadence[3] reflects the speed and materiality of AI-related developments.

3 See Annex 1 - Board agenda and oversight cadence

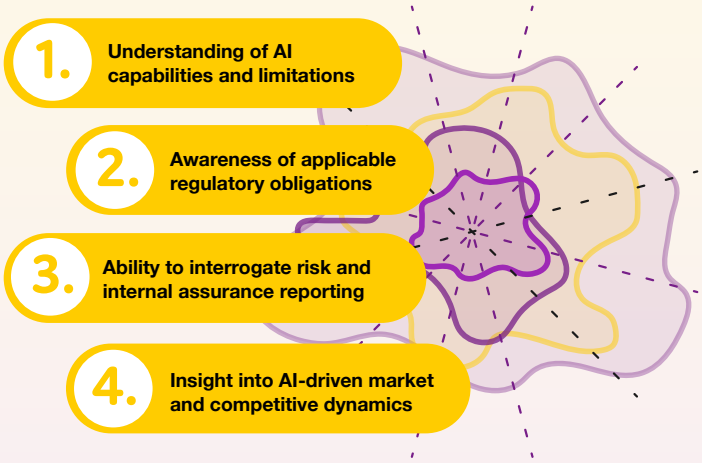
BOARD INSIGHT

AI COMPETENCY BASELINE FOR DIRECTORS

Directors need sufficient understanding to distinguish between narrow AI systems trained for specific tasks and general-purpose models capable of generating novel outputs across domains.

This includes understanding what the AI system's training data is and how its provenance, quality, and bias profile directly affect the reliability of outputs. Directors should also be able to critically assess management presentations where AI-related claims are not supported by sufficient evidence or transparency.

Beyond this baseline, boards should undertake periodic self-assessment against a defined AI competency framework covering four areas:



BOARD INSIGHT

AI, CYBERSECURITY AND DIRECTOR LIABILITY

In Europe, the EU AI Act and NIS2 Directive together reinforce a governance model in which boards are expected to oversee AI-related risks, controls, and cybersecurity measures. Under NIS2, management bodies may face personal liability for failures in cybersecurity oversight, while the AI Act increases expectations regarding risk management, governance, and accountability for AI systems.

The direction of travel is clear: regulatory scrutiny in Europe but potentially also beyond is increasingly focused not only on organisational failures, but also on the adequacy of board oversight.

KEY QUESTIONS FOR BOARDS

BOARD AI LITERACY

1. Does the board have the knowledge and capability to oversee AI strategically, including its opportunities, risks, regulatory developments, workforce implications, and governance requirements?
2. How is the board ensuring ongoing AI literacy and capability development, including through external expertise, briefings, or structured training where appropriate?
3. What balance of capability best supports effective oversight: specialist expertise within the board, broader full-board literacy, or a hybrid approach?
4. How is the board ensuring its understanding remains current as AI capabilities evolve rapidly, including generative AI, systems capable of autonomous actions, and other emerging developments?

PRINCIPLE 10

SEEK EVIDENCE, INTERNAL ASSURANCE AND TRANSPARENCY

USE AI TO IMPROVE BOARD AND COMMITTEE EFFECTIVENESS

AI can support board governance, oversight, and decision-making processes, ranging from very basic support functions such as note taking for minutes and summarising information, to more elaborate purposes. When used appropriately, it can save time and enhance analysis, reporting, challenge, and committee effectiveness.

Boards should consider the various AI use cases available to the board, individual directors, and board committees. AI-driven analytics can help generate insights, questions, and alternative perspectives across many aspects of board work.

Board agendas may be analysed over time to assess consistency with strategic priorities, identify recurring themes, highlight gaps in oversight, and reveal patterns or issues that may not be apparent from individual meetings.

Board materials and shared information may be analysed, challenged, and explored using AI tools to sharpen key messages, test assumptions, and identify additional insights. Such tools should serve as a complement to, rather than a substitute for, director review and judgement.

AI may also be used to simulate the perspectives of stakeholders, customers, employees, regulators, competitors, or investors, helping boards explore alternative viewpoints and strengthen challenge and discussion.

The board's approach to AI use should accommodate differing levels of AI literacy, individual use of AI tools, and the use of assistive technologies where appropriate.

BOARD INSIGHT

USE AI TO ENHANCE CHALLENGE, NOT REPLACE JUDGEMENT

Boards should treat AI as an input to challenge thinking, not as a source of answers or questions to ask at the board or board committee meeting.

Used well, AI systems can improve board effectiveness, e.g. faster and deeper analysis, quality of challenge, surface blind spots and alternative perspectives, and enhance board discussions.

Used poorly, AI systems can disrupt board meetings diverting valuable time and attention from informed strategic decision-making towards debunking false claims or challenging flawed AI-generated recommendations.

Different board committees may adopt AI differently depending on their responsibilities:

- Audit and Risk Committees may use AI-enabled analysis to identify patterns or anomalies in data or information.
- Remuneration Committees may use AI-supported analysis for compensation benchmarking, workforce analysis, or long-term incentive plan scenario modelling.

- Nomination and Governance Committees may use AI to support succession planning, governance reviews, scenario analysis, or assessment of market developments and stakeholder expectations.

Where AI materially supports board or board committee work, its use should be transparent and documented.

GOVERN THE BOARD'S AND COMMITTEES' OWN USE OF AI

Boards and committees should approach the use of AI in their own work with the same discipline they expect from management. Board use of AI should be governed, transparent, secure, and designed to enhance, rather than substitute for, informed human judgement.

Boards should define clear principles for their own use of AI, aligned with the organisation's broader AI governance framework and AI use policies. This may include defining acceptable and prohibited use cases, restrictions on unauthorised AI tools and systems, confidentiality requirements, and expectations regarding transparency of use.

For example, boards may permit the use of AI for brainstorming, research, or analysis, while prohibiting the upload of board papers or sensitive organisational information into unauthorised systems.

Protecting confidentiality should be a central consideration in all board AI use cases. Confidential board information should not be entered into unauthorised, non-secure, or public AI tools.

Boards should ensure that approved tools provide appropriate confidentiality, security, and data protection safeguards and are subject to appropriate legal and data governance approval.

MAINTAIN SCEPTICISM, TRANSPARENCY & ACCOUNTABILITY

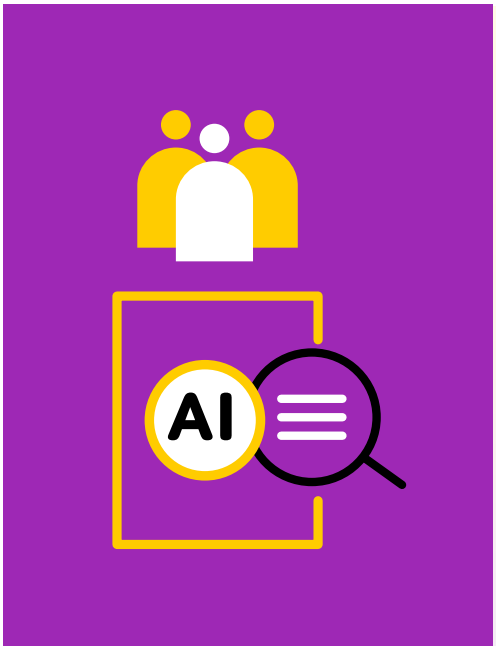
Reviewing materials prepared using AI systems requires heightened professional judgement. The use of AI in preparing board papers, analysis, or recommendations can improve efficiency and insight, but may also introduce risks such as bias, hallucinations, or over-simplification.

Where AI has been used in preparing board papers, analysis, or recommendations, its use should be transparent. Boards should understand the relevant data sources, assumptions, the degree of automation involved, and any validation or review processes applied to assess whether outputs are reliable, explainable, and appropriate to the decision context.

This requires board members to exercise increased scepticism, challenge underlying assumptions, and seek clarity on how AI has been used in generating the information they receive, rather than assuming outputs are robust, objective, or neutral. As AI becomes more capable, the quality of board challenge becomes more, not less, important.

Professional judgement also requires board members to challenge whether AI-supported analysis enhances or undermines decision quality. This includes considering the limitations of AI, including bias, hallucinations, incomplete information, and lack of explainability, and ensuring that AI outputs are used proportionately to their reliability and the significance of the decision.

Accountability remains a core AI governance principle. Boards should ensure that accountability for AI-generated outputs is clear, including how those outputs have been validated and what review, challenge, or internal assurance processes have been applied before information is relied upon in decision-making.



KEY QUESTIONS FOR BOARDS

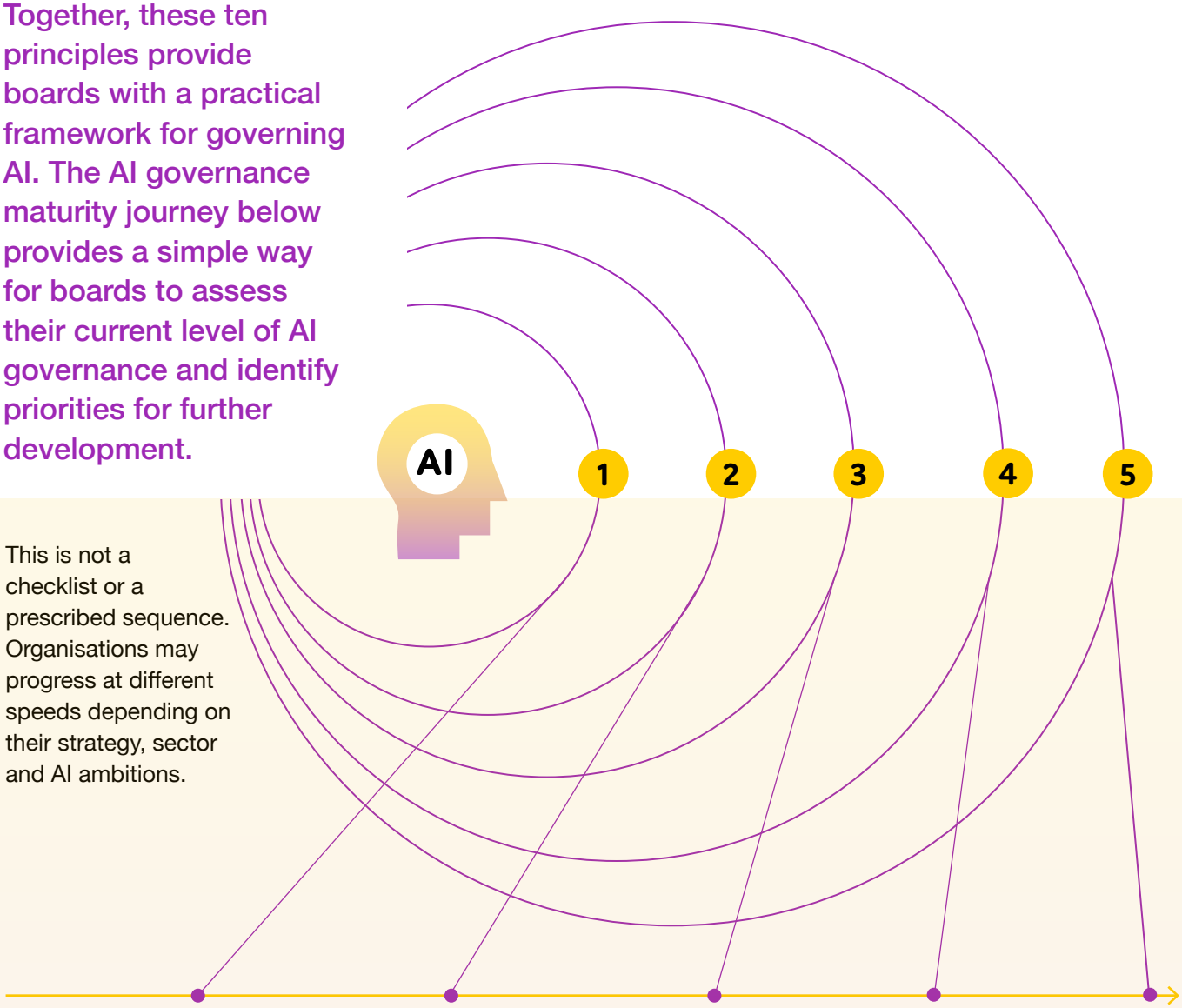
BOARD USE OF AI

1. Are we applying to our own use of AI the same governance standards we expect from management?
2. Are we appropriately informed when AI has materially contributed to board papers, analysis, or recommendations?
3. Is AI strengthening the quality of board judgement and challenge, or making us more reliant on AI-generated outputs?

WHERE ARE WE ON OUR AI GOVERNANCE JOURNEY?

Together, these ten principles provide boards with a practical framework for governing AI. The AI governance maturity journey below provides a simple way for boards to assess their current level of AI governance and identify priorities for further development.

This is not a checklist or a prescribed sequence. Organisations may progress at different speeds depending on their strategy, sector and AI ambitions.



AWARE

Board recognises AI as strategically important, but has limited visibility of AI applications, inventory, ownership or reporting.

MAPPED

The organisation maintains an inventory of material AI applications, with clear ownership and risk classification.

CONTROLLED

Policies, controls, reporting, internal assurance and escalation arrangements are operating effectively.

STRATEGIC

AI investments and applications are aligned with business strategy, value creation and operating model transformation.

ADAPTIVE

Continuous monitoring, learning, internal assurance and board capability are embedded, enabling governance to evolve alongside AI.

ANNEX 1: PRACTICAL TOOLS

BOARD AGENDA AND OVERSIGHT CADENCE

Boards should consider integrating oversight of AI into regular board and committee agendas through a combination of strategic reviews, periodic monitoring, and event-driven escalation.

ANNUAL OR STRATEGIC-CYCLE DISCUSSIONS

- Review AI-driven business strategy, risk appetite, and acceptable use boundaries
- Assess AI impact on business model, competitiveness, and workforce strategy
- Review governance maturity, ethics, explainability, and human oversight
- Assess major AI investments and transformation initiatives
- Review regulatory developments and assurance requirements

PERIODIC OVERSIGHT AND MONITORING

- Oversee whether AI initiatives are delivering measurable business value
- Ensure that AI risks remain within the board's agreed risk appetite
- Assess whether the organisation has the capabilities to use AI responsibly and effectively
- Hold management accountable for effective AI governance in daily operations
- Review vendor dependencies and resilience risks

EVENT-DRIVEN ESCALATION TRIGGERS

- Major AI failures or harmful outcomes
- Deployment of significant new AI capabilities or high-risk systems
- Regulatory breaches, investigations, or litigation
- Failure of critical AI systems, vendors, or control mechanisms
- Breakdown of safeguards or loss of effective human oversight

ANNEX 2: RESOURCES

AI PRINCIPLES, REGULATION AND GUIDANCE

- OECD AI Principles (2019, updated 2024), OECD
- OECD Framework for the Classification of AI Systems (February 2022), OECD
- OECD Due Diligence Guidance for Responsible AI (February 2026), OECD
- Artificial Intelligence Act (June 2024), European Union
- Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment (July 2020), European Commission
- Draft Commission guidelines on the classification of high-risk AI systems (May 2026), European Commission
- Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector (June 2021), EIOPA
- General principles for the use of Artificial Intelligence in the financial sector (July 2019), De Nederlandsche Bank
- Guidelines for the Responsible Use of AI in the Public Service (May 2025), Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation
- Encyclical Letter Magnifica Humanitas of His Holiness Pope Leo XIV on Safeguarding the Human Person in the Time of Artificial Intelligence (May 2026), The Holy See

BOARD-FOCUSED AI GOVERNANCE RESOURCES

- AI Governance Principles for Boards: Supporting responsible AI oversight at board level (April 2026), INSEAD and KPMG
- Boards at the Frontier - AI, Governance, and the Case for Board Leadership (July 2026), Gernandt & Danielsson
- Empowering AI Leadership: An Oversight Toolkit for Boards of Directors (2019), World Economic Forum
- Key questions to start your corporate AI journey (2026), GUBERNA
- Navigating the AI Frontier: Key Questions for Boardroom Oversight (2026), GUBERNA
- AI Governance Playbook for Boards (January 2026), EqualAI
- Director Essentials: Implementing AI Governance (September 2025), National Association of Corporate Directors

- A Director's Guide to AI Board Governance (July 2024), Institute of Directors New Zealand
- AI in the boardroom: A guide for directors (March 2026), Institute of Directors New Zealand
- The AI reckoning: How boards can evolve (December 2025), McKinsey
- AI governance: What it is, why it matters and how to implement it (June 2026), Diligent
- The Role of Investors in AI Governance (April 2026), Oxford Martin AI Governance Initiative
- Rethinking Board Insight: Why AI is becoming a governance essential – Global Board Director Survey Report (February 2026), Financial Times
- Board Oversight of AI (September 2024), Harvard Law School Forum on Corporate Governance
- AI Safety: The Role of the Board in Assessing and Managing AI Risk (Summer 2024), Skadden, The Informed Board
- Strategic governance of AI: A roadmap for the future (April 2025), Deloitte

AI RISK MANAGEMENT, CONTROLS AND MANAGEMENT SYSTEMS

- Realize the Full Potential of Artificial Intelligence (September 2021), COSO
- Achieving Effective Internal Control Over Generative AI (2026), COSO
- Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023), NIST, US Department of Commerce
- Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024), NIST, US Department of Commerce
- ISO/IEC 42001:2023 – Information technology — Artificial intelligence — Management system (December 2023), ISO

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 49 professional organisations from 35 countries that represent close to 1 million professional accountants, auditors and advisors. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18).

ABOUT ECODA

ecoDa is an independent and unique umbrella organization representing the main national institutes of directors across Europe. Our member institutes collectively encompass around 55,000 individual board members from 26 countries, serving on the boards of companies of all sizes and sectors.

Our main focus is corporate governance. All our member institutes are each recognised as the leading institute for directors and governance in their respective country.

ecoDa is in the EU Transparency Register (No 37854527418-86).

ACCOUNTANCY EUROPE

Avenue des Arts 46
1000 Brussels, Belgium
+32 (0) 2 893 33 60

info@accountancyeurope.eu

www.accountancyeurope.eu

https://www.linkedin.com/company/accountancyeurope

https://www.youtube.com/@accountancyeurope

ECODA

Avenue des Arts 6-9
1210 Brussels, Belgium
+32 4 985 02 68 7

contact@ecoda.eu

www.ecoda.eu

https://www.linkedin.com/company/ecoda-asbl

https://www.youtube.com/@ecodatheeuropeanvoiceofdir1304