winmark

AI Governance

Frameworks, Best Practices and Policies in 2024

Foreword

In 2024, artificial intelligence (AI) has reached a pivotal moment of widespread adoption and capability. While AI offers immense potential for productivity gains, operational efficiencies, and new revenue opportunities, it also brings significant challenges around governance, ethics, and implications in the workforce.

Leaders feel pressured to invest and innovate rapidly in AI, often with a ‘fear of missing out’ (FOMO) driving decision-making over prudent long-term planning. There is a fundamental tension between the urgency to capitalise on AI's benefits and the critical need for appropriate governance and strict human control. The urgency to establish proper guidelines is not just a technocratic necessity, but a societal imperative, ensuring that these powerful tools are used in a responsible manner.

Ultimately, success will hinge on organisations striking the right balance – harnessing AI's potential while implementing the necessary guardrails to mitigate risks and hazards.

This guide aims to help in that goal by compiling insights from members of Winmark’s C-Suite networks who have shared their governance practices for responsibly deploying AI.

winmark

Contents

Acknowledgments

We would like to thank all of the Winmark members who shared their valuable insights and experiences during the development of this guide.

How to use this guide

Our insights and recommendations are positioned to impel individuals and organisations to develop and action ethical and effective AI policies and procedures, aligned to wider regulatory frameworks

winmark

01

Key Considerations and **Frameworks**

Align
Develop a clear code of ethics and principles for the responsible use of AI within the organisation

Core values and principles

(shared by Winmark's members for individuals, businesses, organisations and governments)

Safety	Security	Transparency	Accountability
Accuracy	Education	Engagement	Adaptability

02

Implementing
AI Governance

Implement
Design, align and implement AI policies and procedures across operational scenarios and assess its potential risk

Winmark's AI Governance Implementation Cycle

1. Map → 2. Frame → 3. Defend → 4. Train → 5. Communicate → 6. Evolve → 7. Assess

03

AI Governance:
Member examples

Inspire
Dive into a collation of checklists, use cases, and best practices, shared by Winmark members

Winmark's member examples

BBC · Rolls-Royce · LexMundi · WCLO · WCHRO · WCOO · WCIO

01 Key Considerations and Frameworks

winmark

Core values and principles for AI Governance (1/2)

When implementing your AI governance program, leveraging established frameworks can provide valuable structure and guidance and help ensure you are adopting recognised, public standards. It also underpins transparency and consistency across your organisation when it comes to auditing AI tools and evaluating AI systems.

The following key values and principles to guide ethical AI implementation are shared by Winmark members.

Principles	Key considerations shared by Winmark's members
Safety Security	✓ Establish risk mitigation strategies, including rigorous testing, human oversight, and controlled piloting of AI use cases before full deployment. ✓ Implement robust risk assessment processes to identify potential risks associated with AI systems, such as bias, security vulnerabilities, IP infringement, and environmental impacts. Analyse potential misuses and harmful capabilities proactively.
Transparency Accountability Accuracy	✓ Assign clear roles and responsibilities for AI governance, such as data stewards or AI ethics officers. ✓ Establish multiple lines of defence, involving developers, risk evaluators, and independent auditors, to ensure accountability. ✓ Integrate AI governance into existing compliance frameworks, policies (e.g., data ethics, vendor assessment), and operating models. ✓ Implement appropriate oversight models based on the required level of human involvement: human-in-the-loop, human-on-the-loop, or human-out-of-the-loop. ✓ Balance the need for innovation with the importance of regulation and human oversight. ✓ Implement measures to identify AI-generated content (e.g., watermarking) and promote transparency in AI use. ✓ Establish a clear IP framework for AI-generated content. ✓ Use open source AI responsibly, establishing intended uses and guardrails.

winmark

Core values and principles for AI Governance (2/2)

By addressing the following key considerations in this section, C-Suite leaders can establish comprehensive and robust AI governance policies that prioritise ethical practices, risk management, accountability, and transparency. Further, it reinforces the commitment to the responsible development and deployment of AI technologies within their organisations.

*For more information about how Winmark can construct your AI advisory board by bringing industry expertise, government stakeholders, global AI institutions and academia to your doorstep, please contact john.jeffcock@winmarkglobal.com

Principles	Key considerations shared by Winmark's members
Education	✓ Promote AI literacy across the organisation through comprehensive training programs tailored to different roles and responsibilities. ✓ Upskill or reskill employees to work effectively with AI systems and address potential job displacement or role changes. ✓ Foster a culture of responsible AI development and deployment through education and alignment with organisational values. ✓ Establish mechanisms for transparent communication about the organisation's AI practices, decision-making processes, and potential impacts.
Engagement	✓ Actively participate in industry collaborations, global forums, and multistakeholder dialogues to stay informed about best practices and contribute expertise.* ✓ Foster partnerships with academic institutions and contribute resources to nurture local AI talent and inclusive access.*
Adaptability	✓ Design AI governance policies and programs to be adaptable and responsive to the rapidly evolving AI landscape and regulatory environment. ✓ Incorporate change management protocols and regularly review and update governance measures based on emerging best practices and stakeholder feedback. ✓ Adopt a mindset of continuous learning and improvement, staying informed about global AI developments and contributing to the advancement of AI safety research.

02 Implementing AI Governance

Winmark's AI Governance Implementation Cycle

Stage 1: Plan

Map

2.1 Mapping AI Principles to Written Policies and Procedures

Using key AI principles and ethics as a guide, **create new procedures** (or amend current) that address specific AI scenarios and usage across the organisation

Frame

2.2 Utilising comprehensive frameworks

Cross-reference planned AI principles, ethics and procedures against existing regulatory frameworks

Stage 2: Act

Defend

2.3 Establishing multiple lines of defence

Establish roles and responsibilities for AI developers, risk evaluators and independent auditors, thus forming a robust, three-tiered defence mechanism

Stage 3: Manage

Train

2.4 Promoting AI literacy through organisation-wide training

Develop a tiered training curriculum to meet the various educational needs of technical and non-technical roles

Communicate

2.5 Driving a responsible AI culture aligned with organisational values

Integrate multiple communication channels and measures to further engagement and alignment with organisational values

Stage 4: Reflect

Evolve

2.6 Designing an adaptable programme to keep up with evolving regulations

Build a wider ecosystem of stakeholders to ensure AI procedures are developing at pace and in line with regulation

Assess

2.7 Addressing specific AI risks and opportunities

Conduct a risk assessment and mitigation strategy, and implement regular review cycles

winmark

2.1 Mapping AI Principles to Written Policies and Procedures

Translate abstract ethical principles and guidelines into specific, **actionable policies** and procedures that cover all aspects of AI development and deployment within the organisation.

For example, if one of the principles is **"fairness,"** create detailed procedures on how to **identify** and **mitigate** algorithmic bias, conduct fairness testing, and ensure equitable outcomes.

Assign **responsibilities** and **accountability** for adhering to these procedures across relevant teams and functions.

Implementation

01 **Identify** and list your organisation's core AI principles and ethical guidelines.

02 For each principle, **brainstorm** specific scenarios and use cases relevant to your organisation.

03 **Develop** detailed procedures for each scenario, addressing how to apply the principle in practice.

04 **Create** a cross-functional team to review and refine these procedures.

05 **Document** the policies and procedures in a clear, accessible format.

06 **Establish** a review cycle to regularly update these documents as AI technologies and use cases evolve.

winmark

2.2 Utilising comprehensive frameworks

Adopt and **align** with existing regulatory frameworks (sources below) as models for responsible AI development, such as:

- The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems
- The European Union's Ethics Guidelines for Trustworthy AI (base for the EU AI Act)
- The Montreal Declaration for Responsible AI
- The AIGA AI Governance Framework
- NIST Artificial Intelligence Risk Management Framework
- MIT's AI Governance Framework
- The U.S. AI Bill of Rights
- Canada's Artificial Intelligence and Data Act,.

You should also consider participating in or supporting **self-regulatory organisations** for **AI industry oversight** and/or consider participating in **regulatory sandboxes** to test AI applications in a controlled environment. This will demonstrate both your **credibility** and **commitment** to **responsible AI practices** and allows you to contribute to industry-wide standards.

Implementation

Review and **align** your governance policies with chosen frameworks.

Create a **cross-functional team** to oversee the implementation of the framework.

Develop an audit schedule and process for your AI systems based on the framework's guidelines.

Establish channels for collaboration with industry peers and regulatory bodies to stay updated on best practices.

winmark

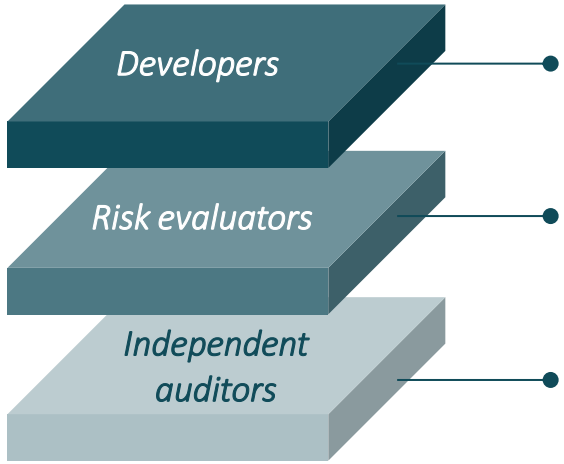
2.3 Establishing multiple lines of defence

Human oversight and supervision mechanisms are crucial components of a balanced approach to AI implementation.

AI systems, particularly in **high-stakes** or **critical decision-making scenarios,** should not operate autonomously without human involvement.

By incorporating human supervision, organisations can **monitor the AI's behaviour**, intervene when necessary, and make informed adjustments to **mitigate risks** and ensure alignment with **ethical principles** and performance expectations.

Consider implementing a three-tiered approach to manage AI-related risks and ensure accountability:



The first line of defence involves the developers and subject matter experts who design and build the AI systems, following established protocols and embedding responsible practices.

The second line comprises risk evaluators or compliance teams who independently assess and monitor AI systems for potential risks, such as bias, security vulnerabilities, or ethical concerns.

The third line consists of independent auditors who periodically review and evaluate the effectiveness of the AI governance program, providing objective assurance and recommendations for improvement.

Implementation

1. **Define** the three lines of defence: developers, risk evaluators, and independent auditors.
2. **Clearly outline** roles, responsibilities, and reporting structures for each line.
3. **Develop** specific protocols and checklists for each line of defence to follow.
4. **Implement** a system for tracking and documenting the activities of each line of defence.
5. **Establish** communication channels between the lines to ensure smooth information flow.
6. **Create** a schedule for regular meetings between representatives of each line to discuss emerging issues and improvements.

winmark

2.4 Promoting AI literacy through organisation-wide training

Develop comprehensive training programs tailored to different roles and levels within the organisation to enhance understanding of responsible AI development and deployment.

For technical teams (data scientists, developers, etc.), **provide in-depth training** on ethical AI principles, bias mitigation techniques, privacy-preserving methods, and relevant regulations.

For non-technical roles (leadership, marketing, customer support), offer training on the **fundamentals of AI,** its potential impact, and the organisation's AI governance policies and practices.

Implementation

1. **Assess** current AI literacy levels across different departments and roles.
2. **Develop** a tiered training curriculum, catering to technical and non-technical roles.
3. **Create** or **source** training materials (e.g., online courses, workshops, webinars).
4. **Implement** a learning management system to track training progress.
5. **Schedule** regular training sessions and set completion deadlines.
6. **Develop** a mechanism for employees to provide feedback on the training and suggest improvements.
7. **Establish** a system to recognise and reward completion of AI literacy programs.

winmark

2.5 Driving a responsible AI culture aligned with organisational values

Implementation

Ensure that the organisation's AI governance policies and practices are **deeply rooted** in and aligned with its core values and ethical principles.

Leadership should consistently communicate and exemplify the importance of ethical AI practices, creating an environment that encourages **open dialogue, accountability,** and **continuous improvement.**

Clearly articulate how AI governance aligns with your organisation's core values.

Establish an AI governance champion network across departments.

Integrate AI ethics and governance into performance evaluations and job descriptions.

Develop an internal communication strategy to regularly highlight responsible AI practices.

Create channels for employees to raise concerns or suggest improvements related to AI use.

.

Implement an AI ethics award or recognition program to incentivise responsible practices.

Organise regular events (e.g., hackathons, seminars) focused on ethical AI development.

winmark

2.6 Designing an adaptable program to keep up with evolving regulations

Build flexibility and adaptability

Build flexibility and **adaptability** into the AI governance program from the outset, allowing for regular reviews and updates to policies, procedures, and controls.

Implement robust change management

Implement robust change management protocols to ensure that any updates or modifications to the governance program are properly communicated, implemented, and monitored across the organisation.

Stay informed on regulation

Stay informed about emerging regulatory developments, industry standards, and best practices, and be prepared to adjust the governance program accordingly.

Engage with diverse stakeholders

Establish channels for ongoing dialogue and engagement with a diverse range of stakeholders, including employees, customers, industry peers, academic institutions, civil society organisations, and regulatory bodies.

Seek feedback and insights from these stakeholders on the organisation's AI governance policies, practices, and potential impacts, using this input to refine and enhance the governance framework continually.

Implementation

1. **Assign a team or individual** responsible for monitoring AI regulatory developments.
2. **Establish relationships** with legal experts specialising in AI and data protection laws.
3. **Create a system** for regular review and update of AI governance policies (e.g., quarterly or bi-annually).
4. **Develop a change management protocol** for implementing updates to the governance program.
5. **Establish a stakeholder feedback mechanism**, including customers, employees, and partners.
6. **Create a risk assessment process** to evaluate the impact of potential regulatory changes.
7. **Participate** in industry forums and regulatory discussions to stay informed and contribute to policy development.

winmark

2.7 Addressing specific AI risks and opportunities

By addressing both **AI risks and opportunities** systematically, you can create a balanced AI governance program that **protects** against potential harms while **fostering innovation** and **positive impact**:

Managing AI Risks

Deepfakes and Misinformation	**Implement** detection tools and policies to mitigate the spread of AI-generated false content.
Malware and Security Threats	**Enhance** cybersecurity measures to protect against AI-powered attacks. This may include AI-based threat detection systems.
Bias and Fairness	**Regularly audit** AI systems for biases and implement fairness-aware machine learning techniques.
Privacy Concerns	**Ensure robust** data protection measures and compliance with privacy regulations in AI systems.

Encouraging AI opportunities

Promote research	**Allocate resources** to research AI's potential societal benefits. This could involve partnerships with academic institutions or internal R&D initiatives.
Innovation Support	**Create an environment** that encourages responsible AI innovation within your organisation. This might include innovation challenges or dedicated time for AI-related projects.
Positive Use Cases	**Identify and prioritise** AI applications that can have significant positive impacts on your business, customers, or society at large.

Implementation

1. **Conduct a comprehensive risk assessment** of your AI systems and potential use cases.
2. **Develop a risk mitigation strategy** for each identified risk, assigning responsible teams and timelines.
3. **Create an opportunities roadmap**, outlining potential beneficial AI applications
4. **Establish an AI ethics committee** to oversee both risk mitigation and opportunity exploration.
5. **Implement regular review cycles** to reassess risks and opportunities as AI technologies evolve.

Not every AI use case requires designated frameworks, extensive processes and top-down intervention. Framing Winmark's AI Governance Implementation Cycle (AGIC) against common industry use cases / applications and risk categorisation can steer organisational stakeholders towards executing a rational policy that delivers on the hygiene factors for effective AI governance

Winmark's AI Governance Implementation Cycle	High risk	Medium-risk	Low-risk
2.1 Mapping AI Principles to Written Policies and Procedures	✓	✓	
2.2 Utilising comprehensive frameworks	✓	✓	✓
2.3 Establishing multiple lines of defence	✓	✓	
2.4 Promoting AI literacy through organisation-wide training	✓	✓	
2.5 Driving a responsible AI culture aligned with organisational values	✓	✓	✓
2.6 Designing an adaptable programme to keep up with evolving regulations	✓	✓	
2.7 Addressing specific AI risks and opportunities	✓	✓	✓

Level of Risk[1]	Common examples of AI use cases by industry / applications	Hygiene factors for effective AI Governance
High-risk *Applications have significant implications for safety, fundamental rights, and societal well-being*	• Healthcare *e.g., medical diagnostics, treatment recommendations, robotic surgery* • Employment *e.g., recruitment processes, performance evaluation, employee monitoring* • Legal *e.g., predictive policing, facial recognition, biometric identification* • Critical Infrastructure *e.g., managing electricity grids, water supply, and transportation networks.* • Financial Services *e.g., credit scoring, fraud detection, algorithmic trading*	1. Full application of Winmark's AI Governance Implementation Cycle (AGIC) and compliance with regulatory frameworks. 2. Consider undertaking risk, conformity or compliance assessments conducted by a reputable third-party before go-to-market 3. Strengthen stages 2.5, 2.6 and 2.7 of the AGIC to continuously monitor the AI system's performance.
Medium-risk *Applications can influence decisions and actions but do not pose significant risks to safety or fundamental rights.*	• Customer Service *e.g., AI chatbots, virtual assistants* • Marketing *e.g., targeted advertising, customer segmentation, personalised content / campaigns.* • Education *e.g., personalised learning tools, administration* • Retail *e.g., inventory management, personalised shopping experiences, customer behavior analysis*	1. Ensure high-quality, accurate, and representative data is used to train and operate the AI system. 2. Ensure necessary human oversight and intervention mechanisms in the AI system's operations. 3. Maintaining detailed documentation and records of the AI system's development, deployment, and performance
Low-risk *Applications have minimal impact on individuals' rights, safety or wellbeing.*	• Basic automation *e.g., sorting emails, managing calendars* • Virtual assistants for personal use *e.g., scheduling, reminders* • Content recommendations for personal use *e.g., music or video streaming*	1. Ensure user awareness when interacting with an AI system, especially in specific contexts like generative AI or deepfakes. 2. Disclose AI-Generated content for generative AI systems by marking output as artificially generated or manipulated e.g., creating synthetic audio, images, or text

[1] Source: EU AI Act

Glossary of Terms to distinguish the nuances in governing the use of AI tools

winmark

Term	Definition	Additional considerations
Narrow AI *Other nomenclatures: Weak AI, Artificial Narrow Intelligence (ANI)*	AI systems designed to perform a specific task or a set of closely related procedures. It is considered limited in scope and operates under a pre-defined set of rules. Common examples include conducting administrative tasks (voice assistants) and detecting trends and patterns (personalisation, optimisation)	• Methodologies behind constructing rule-based / decision-making actions should be publicly available to ensure Transparency and Fairness to clients, customers and end users
Generative AI	AI systems that can create new content, such as text, images, music, or code, by learning from existing data. Common examples are ChatGPT (text), DALL-E (images), and general Adversarial Networks (GAN)	• Authenticate generated content and traceability • Robust risk management structure to resolve misinformation and deepfakes • Privacy and fraud e.g., mimicking real individuals and identities, misuse of personal data in generated outputs
Ethics	Principles and values that guide individual and organisational behavior.	• Used to build a foundation of trust with users and stakeholders • Commitment to Ethics can enhance brand reputation and ensure the sustainable use of AI in the long-term
Regulation	Rules or directives made and maintained by an authority, such as a government or regulatory body.	Use of AI tools are governed and may target specific actions, processes and behaviours within an organisation to ensure the maintenance of Ethics
Compliance	Adherence to mandatory AI regulations, frameworks and internal policies through a prescriptive and/or formalised process.	Ensures the organisation meets all areas of regulation. Some organisations may align with regulatory frameworks but are not compliant in its implementation if they do not address every aspect

02 Implementing AI Governance

Remember that AI governance policies should be designed with a long-term view, allowing for maturation and adaptation to rapidly advancing technology. Begin discussions on AI governance early to address IP, data protection, and liability issues, and view AI governance as an opportunity for innovation while maintaining trust and confidence among stakeholders.

By implementing thoughtful, comprehensive, and forward-looking AI governance policies, organisations can balance technological advancement with ethical considerations and long-term interests.

winmark

03 AI Governance: Member examples

winmark

3.1 Phases of AI Development

Winmark's AI Advisory board met to discuss how C-Suite leaders take advantage of the opportunity that AI presents, whilst mitigating its risks.

Following the discussion, Winmark created a table that summarises organisations' process implementing AI and helps organisations decide where to focus their resources on.

Innovation / Inflated Expectations → Tough reality / Early Productivity Gains → The New Norm →

	Phase 1: Personal Adoption	Phase 2: Process Evaluation	Phase 3: Product development		Phase 4: Business transformation
Purpose	Cultural AI Change: One Person at a Time	Replacing simple processes and tasks to free time	Material Process Interventions (internal)	New Product and Service Development (external)	End to End Business Transformation
Focus	Personal Competencies, Performance and Productivity	Function Back Office (Low Risk)	Complex Technical Interventions (low / zero risk tolerance)	Data Based Product / Service Development	Client Acquisition to Fulfillment
Example	Summary Meeting Actions (MS CoPilot)	Contract Management	Compliance Reporting	Online recruitment tool	Marcoms -> Order -> Payment -> Fulfilment
Benefit	Time Saved, Ease of Usage & Productivity	Speed of Turnaround, Accuracy & Consistency	Speed, Accuracy and Cost Reduction	Speed, Revenue and Client Satisfaction	Sustainable and Effective Business Model

3.2 BBC's AI Principles

The BBC's AI Guidance (source) outlines its core principles in how AI should be used, including that its usage should:

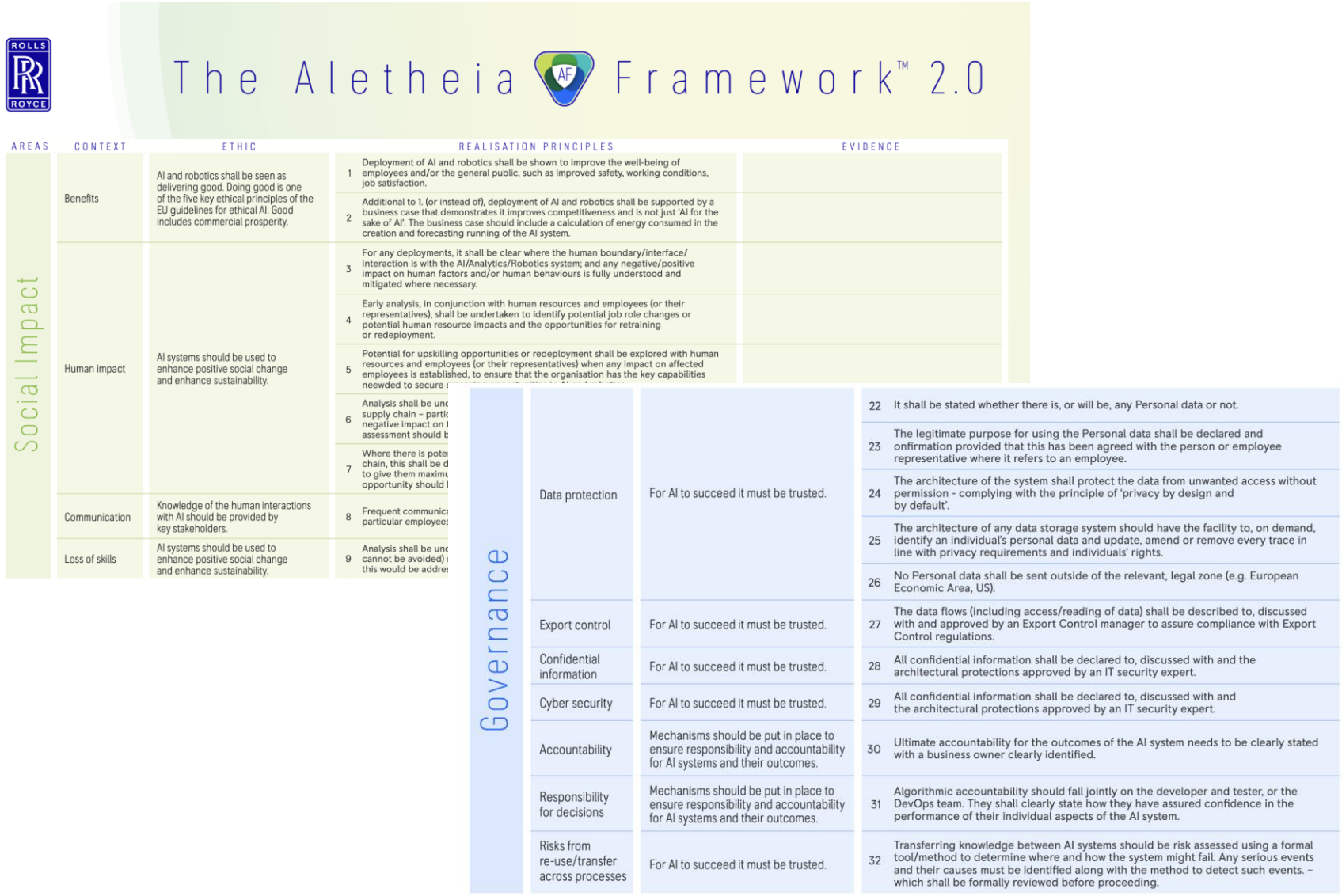
- Comply with editorial values
- Be transparent to audiences and have effective human oversight
- Not undermine audience trust
- Not be used to directly create news, current affairs, or factual journalism content
- Support editorial production or research, but with careful human oversight and monitoring

Principles	Key considerations
Act in the public's best interests	✓ Align AI use with BBC's public service mission and values ✓ Comply with BBC's editorial values, guidance, and guidelines ✓ Ensure fairness, equity, and inclusivity for audiences and staff ✓ Implement secure, robust, and safe AI systems
Prioritising talent and creativity	✓ Respect rights of creators, contributors, and rights holders ✓ Consider data protection and privacy rights ✓ Use AI to support and enhance human insight and creativity
Being open and transparent	✓ Clearly communicate AI use and data collection to audiences and staff ✓ Explain the reasons for AI use, its functioning, and its impact ✓ Ensure proper supervision and accountability for AI use ✓ Maintain effective and informed human oversight over AI systems

3.3 Rolls Royce: Alethia Framework

The Rolls Royce Aletheia Framework (source) is a toolkit for promoting ethics and trustworthiness in AI. The framework emphasises the importance of ethical considerations and public trust in realising the full potential of AI, and is freely available to all organisations. It helps ensure:

- Ethical implications of AI are fully considered
- AI systems are as fair as possible
- AI makes trustworthy decisions



AREAS	CONTEXT	ETHIC		REALISATION PRINCIPLES	EVIDENCE
Social Impact	Benefits	AI and robotics shall be seen as delivering good. Doing good is one of the five key ethical principles of the EU guidelines for ethical AI. Good includes commercial prosperity.	1	Deployment of AI and robotics shall be shown to improve the well-being of employees and/or the general public, such as improved safety, working conditions, job satisfaction.	
			2	Additional to 1. (or instead of), deployment of AI and robotics shall be supported by a business case that demonstrates it improves competitiveness and is not just 'AI for the sake of AI'. The business case should include a calculation of energy consumed in the creation and forecasting running of the AI system.	
	Human impact	AI systems should be used to enhance positive social change and enhance sustainability.	3	For any deployments, it shall be clear where the human boundary/interface/ interaction is with the AI/Analytics/Robotics system; and any negative/positive impact on human factors and/or human behaviours is fully understood and mitigated where necessary.	
			4	Early analysis, in conjunction with human resources and employees (or their representatives), shall be undertaken to identify potential job role changes or potential human resource impacts and the opportunities for retraining or redeployment.	
			5	Potential for upskilling opportunities or redeployment shall be explored with human resources and employees (or their representatives) when any impact on affected employees is established, to ensure that the organisation has the key capabilities neewded to secure	
			6	Analysis shall be unc supply chain – partic negative impact on assessment should b	
			7	Where there is pote chain, this shall be d to give them maximu opportunity should	
	Communication	Knowledge of the human interactions with AI should be provided by key stakeholders.	8	Frequent communica particular employees	
	Loss of skills	AI systems should be used to enhance positive social change and enhance sustainability.	9	Analysis shall be unc cannot be avoided) this would be addres	
Governance	Data protection	For AI to succeed it must be trusted.	22	It shall be stated whether there is, or will be, any Personal data or not.	
			23	The legitimate purpose for using the Personal data shall be declared and onfirmation provided that this has been agreed with the person or employee representative where it refers to an employee.	
			24	The architecture of the system shall protect the data from unwanted access without permission - complying with the principle of 'privacy by design and by default'.	
			25	The architecture of any data storage system should have the facility to, on demand, identify an individual's personal data and update, amend or remove every trace in line with privacy requirements and individuals' rights.	
			26	No Personal data shall be sent outside of the relevant, legal zone (e.g. European Economic Area, US).	
	Export control	For AI to succeed it must be trusted.	27	The data flows (including access/reading of data) shall be described to, discussed with and approved by an Export Control manager to assure compliance with Export Control regulations.	
	Confidential information	For AI to succeed it must be trusted.	28	All confidential information shall be declared to, discussed with and the architectural protections approved by an IT security expert.	
	Cyber security	For AI to succeed it must be trusted.	29	All confidential information shall be declared to, discussed with and the architectural protections approved by an IT security expert.	
	Accountability	Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.	30	Ultimate accountability for the outcomes of the AI system needs to be clearly stated with a business owner clearly identified.	
	Responsibility for decisions	Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.	31	Algorithmic accountability should fall jointly on the developer and tester, or the DevOps team. They shall clearly state how they have assured confidence in the performance of their individual aspects of the AI system.	
	Risks from re-use/transfer across processes	For AI to succeed it must be trusted.	32	Transferring knowledge between AI systems should be risk assessed using a formal tool/method to determine where and how the system might fail. Any serious events and their causes must be identified along with the method to detect such events. – which shall be formally reviewed before proceeding.	

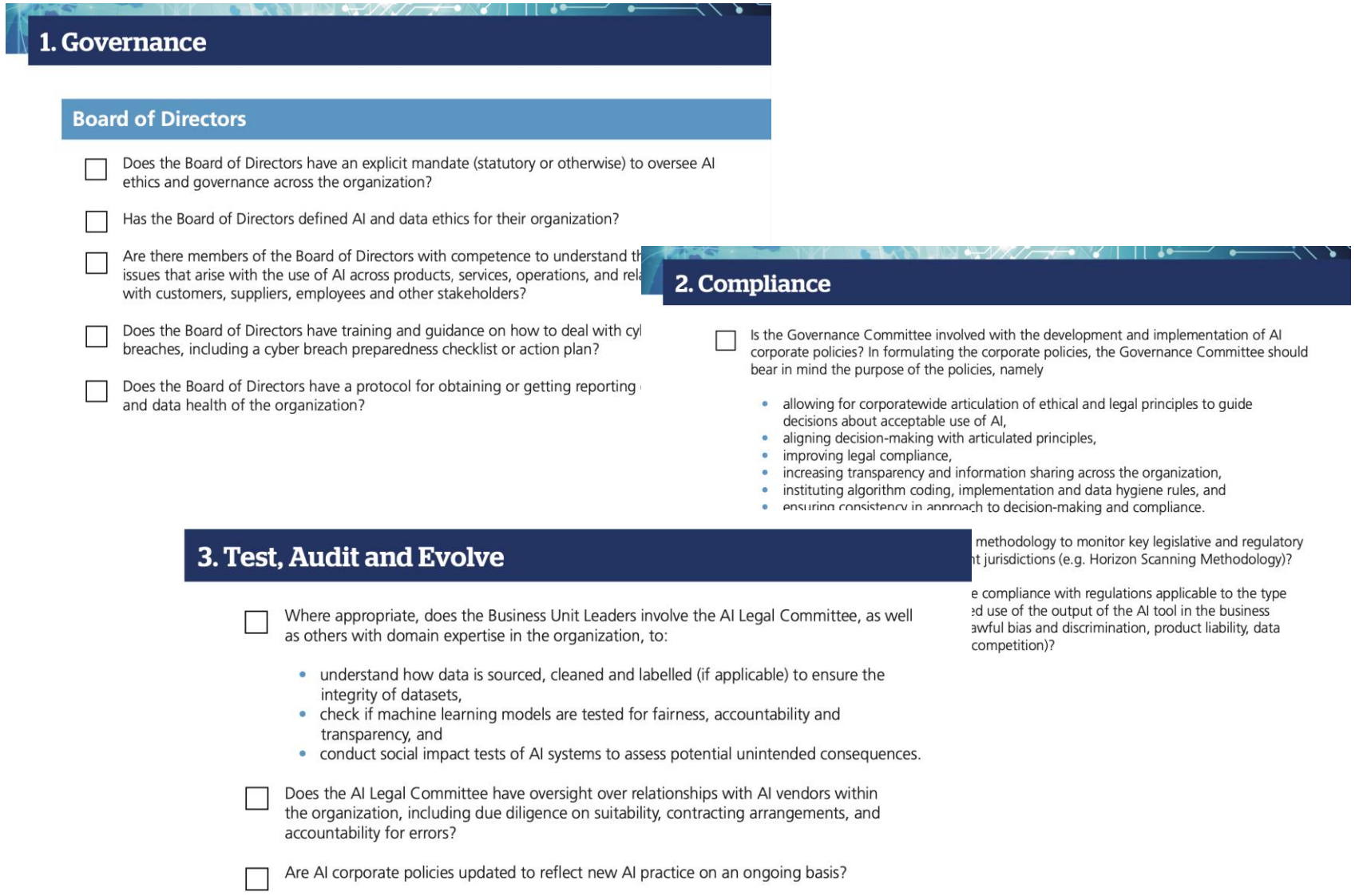
winmark

3.4 Lex Mundi: AI Readiness Checklist for Corporate Legal Functions

LexMundi

This AI Readiness Checklist for Corporate Legal Functions (source) was developed by Lex Mundi to help General Counsel navigate AI in their businesses and the regulatory environment.

The checklist was created in response to the increasing demand on corporate legal functions to guide various stakeholders through AI-related ethical and legal risks. It was informed by consultations with General Counsel and is intended as a starting point to identify key issues.



1. Governance

Board of Directors

- ☐ Does the Board of Directors have an explicit mandate (statutory or otherwise) to oversee AI ethics and governance across the organization?
- ☐ Has the Board of Directors defined AI and data ethics for their organization?
- ☐ Are there members of the Board of Directors with competence to understand th issues that arise with the use of AI across products, services, operations, and rel with customers, suppliers, employees and other stakeholders?
- ☐ Does the Board of Directors have training and guidance on how to deal with cy breaches, including a cyber breach preparedness checklist or action plan?
- ☐ Does the Board of Directors have a protocol for obtaining or getting reporting and data health of the organization?

2. Compliance

- ☐ Is the Governance Committee involved with the development and implementation of AI corporate policies? In formulating the corporate policies, the Governance Committee should bear in mind the purpose of the policies, namely
  - allowing for corporatewide articulation of ethical and legal principles to guide decisions about acceptable use of AI,
  - aligning decision-making with articulated principles,
  - improving legal compliance,
  - increasing transparency and information sharing across the organization,
  - instituting algorithm coding, implementation and data hygiene rules, and
  - ensuring consistency in approach to decision-making and compliance.

3. Test, Audit and Evolve

- ☐ Where appropriate, does the Business Unit Leaders involve the AI Legal Committee, as well as others with domain expertise in the organization, to:
  - understand how data is sourced, cleaned and labelled (if applicable) to ensure the integrity of datasets,
  - check if machine learning models are tested for fairness, accountability and transparency, and
  - conduct social impact tests of AI systems to assess potential unintended consequences.
- ☐ Does the AI Legal Committee have oversight over relationships with AI vendors within the organization, including due diligence on suitability, contracting arrangements, and accountability for errors?
- ☐ Are AI corporate policies updated to reflect new AI practice on an ongoing basis?

methodology to monitor key legislative and regulatory
t jurisdictions (e.g. Horizon Scanning Methodology)?

e compliance with regulations applicable to the type
d use of the output of the AI tool in the business
awful bias and discrimination, product liability, data
competition)?

winmark

This Guidance (source) was provided by a Finance sector firm who are approaching AI with a structured and cautious strategy. The firm has established a dedicated AI Task Force (AITF) to oversee AI initiatives and deliver expected outcomes, while an AI Governance Board (AIGB) manages digital risks associated with AI.

They have conducted an AI usage survey to understand current attitudes and practices, and are developing internal guidelines, including an AI Prompt Guide for effective use of AI tools.

Member example:
3.5 Guidance for Artificial Intelligence Approach

They have conducted an AI usage survey to understand current attitudes and practices, and are developing internal guidelines, including an AI Prompt Guide for effective use of AI tools. The company maintains strict control over AI tool usage, with only approved tools from their AI Inventory permitted for work. Currently, they have approved Copilot, Adobe Firefly, and Teams Premium, while popular tools like ChatGPT and Google Bard are not approved.

Policy and process:
All AI tools used for work need to have been approved.
The AI Governance Board meets weekly to review requests for new tools. Once we're confident the tool meets our standards of quality, security and data protection, we will approve it for use.
If you've found a new AI tool you'd like to use, you can submit a Request a new AI or ML tool.
Please only use the following AI tools for inputting our data and work:

- Copilot (chat, notebook and compose) A multifunctional AI tool based on OpenAI's GPT4.0 generates text and images, available to all staff by default. Please be cautious in the way you use images and note:
- You can use the images for idea generation and internal presentations (make sure you clearly label the image as made by Dall-E).
- You can't use the images for public facing or project use.
- Adobe Firefly A licensed AI tool used for image generation, available subject to approval, license chargeable to your cost centre.
- Teams Premium an enhanced version of Teams, AI generated minutes etc, available to all staff on request, license chargeable to your cost centre.

Please don't use AI tools that have not been approved.

No other AI tools are currently approved for use at [Company name], including ChatGPT, Google Bard, and MidJourney.

winmark

Member example:
3.6 AI Usage Policy & Best Practices

WCLO

This AI Usage Policy & Best Practices (source) example was provided by a CLO in the technology sector. It provides guidelines for risk management, and maintaining ethical standards.

Summary of Best Practices:

- ✓ Emphasises the importance of safeguarding intellectual property rights when deploying AI tools and create contractual safeguards to ensure organisations retain ownership of input data and AI-generated outputs.
- ✓ Outlines measures to maintain confidentiality and secure information, including data encryption, access control, regular auditing, and secure data transmission.
- ✓ Details the responsibilities of employees in handling inputs, verifying AI outputs, and ensuring non-harmful and non-discriminatory content.
- ✓ Provides a structured decision-making process to ensure compliance and prevent misuse when using Large Language Models (LLMs).
- ✓ Recommends actions and checks to ensure compliance with legal and corporate standards when using generative AI tools in scenarios such as data input verification, output assessment, intellectual property protection, and ethical content creation.
- ✓ Discusses methods to enhance the reliability of AI tools and promote in-context learning strategies to improve AI performance.
- ✓ Mitigates ethical challenges such as biased content generation, reliance on expansive web-scraped data, and technical challenges such as usage limits.

winmark

Member example: 3.7 Guidelines on using AI in legal proceedings

WCLO

These Guidelines on using AI in legal proceedings (Dubai) (source) advise on the use of large language models and generative AI in proceedings before the DIFC (Dubai International Financial Centre Courts); and apply to parties in proceedings who are considering the use of Large Language Models (LLMs) and Generative Content Generators (GCGs).

The principles include transparency, accuracy and reliability, and the best practices include verifying the accuracy and reliability of AI-generated content, early disclosure of the use of AI, educating clients, and protecting client confidentiality and complying with legal obligations.

1. Transparency and Disclosure
   - ✓ Parties must disclose the use of AI systems, the source of AI-generated content, and any potential limitations or biases.
   - ✓ Transparency is crucial in documents such as pleadings, witness statements, affidavits, and skeleton arguments.
2. Verification of AI-Generated Content
   - ✓ AI-generated content must be verified for accuracy and reliability.
   - ✓ Practitioners should evaluate the reliability of AI-generated evidence, considering the AI's training data, algorithms, and potential biases.
3. Compliance with Legal and Ethical Standards
   - ✓ Practitioners must comply with the Mandatory Code of Conduct for Legal Practitioners and relevant laws, including Data Protection Law and Intellectual Property Law.
   - ✓ The Courts have the authority to reject AI-generated content that does not meet these standards.
4. Best Practices for Using AI in Legal Proceedings
   - ✓ Ensure AI-generated content is up-to-date, relevant, and based on accurate data.
   - ✓ Avoid over-reliance on AI technologies and maintain professional judgment.

04 Additional Frameworks and Useful Sources

4.1 UK's AI Ethics and Principles Framework

In March 2023, the UK Government published its AI Regulation White Paper (source) setting out its pro-innovation and pro-safety approach to AI regulation. Issued by the Department of Science, Innovation and Technology, the report shares values, principles and key considerations on developing tools and guidance for implementing the use of AI:

Safety, security, robustness:

- ✓ Understand and communicate the level of safety related risk in their regulatory remit
- ✓ Stress the importance of AI developers and deployers (within regulators' remits) undertaking safety risk assessments and implementing appropriate mitigations to identified risks
- ✓ Consider how AI developers and deployers should mitigate and build resilience to cybersecurity related risks throughout the AI life cycle

Appropriate transparency and explainability:

- ✓ Explain that appropriate levels of transparency and explainability help to foster trust in AI and increase AI use
- ✓ Encourage AI developers and deployers to implement appropriate transparency and explainability measures
- ✓ Understand that this principle is necessary for the proper implementation of the other four principles

Fairness:

- ✓ Continue to develop, publish descriptions or signpost to existing descriptions of fairness that apply to AI systems' outcomes within their regulatory remit
- ✓ Consider how AI systems that are used in their regulatory remit are designed, developed, deployed and used considering this description of fairness
- ✓ Note that aligning descriptions of fairness and developing joint tools and guidance is particularly important in cross-cutting regulatory remits

Accountability and governance:

- ✓ Place clear expectations for compliance and good practice on appropriate actors in the AI supply chain (within regulators' remits), including expectations for what appropriate internal accountability and governance frameworks might look like
- ✓ Consider whether existing powers that place accountability on decision makers are applicable in the context of AI and to AI developers and AI deployers
- ✓ Seek to foster accountability through promoting appropriate transparency and explainability

Contestability and redress:

- ✓ Where appropriate, encourage AI developers and AI deployers (within regulators' remits) to provide clarity to users on which routes they can use to contest AI outcomes or decisions
- ✓ Highlight that appropriate transparency and explainability is key to ensuring that AI deployers or end users can contest outcomes and are aware of routes to redress

4.2 Updated UK Government response to AI Regulation (1/2)

Department for Science, Innovation, & Technology

In February 2024, the government announced a range of measures (source) to guide businesses and individuals in actively regulating the use of AI. The approach builds upon many of the principles in the AI Regulation Whitepaper 2023 and outlines an AI governance ecosystem to demonstrate the interconnected relationships between government, regulators and industry.

1. Strategic Approach and Principles

Balanced and Adaptive Governance

- ✓ Recognise both potential benefits and challenges of AI
- ✓ Adopt a flexible, non-statutory approach to AI governance
- ✓ Implement cross-sectoral principles adaptable to specific contexts
- ✓ Ensure continuous monitoring and adaptation of governance policies

Innovation and Safety Balance

- ✓ Promote innovation while ensuring strong safety measures
- ✓ Implement AI assurance techniques and technical standards
- ✓ Consider developing an internal "AI Safety Institute"

2. Risk Management and Compliance

Comprehensive Risk Assessment

- ✓ Develop a cross-economy AI risk register
- ✓ Conduct ongoing analysis of potential regulatory gaps
- ✓ Establish a dedicated team for cross-sectoral risk monitoring

Specific Risk Mitigation

- ✓ Focus on societal harms, misuse risks, and autonomy risks
- ✓ Address emerging risks like electoral interference, discrimination, and IP issues

Compliance Framework

- ✓ Develop clear guidelines for AI project teams
- ✓ Implement an Algorithmic Transparency Recording Standard (ATRS)
- ✓ Create an "AI Management Essentials" scheme for minimum standards

3. Technical and Operational Considerations

Data Management

- ✓ Ensure high-quality input data for AI models
- ✓ Manage various data types: organisational, reporting, testing, operational, user feedback, and financial

Model Testing and Verification

- ✓ Implement robust, independent testing of AI models before deployment
- ✓ Establish a comprehensive, ongoing testing process
- ✓ Ensure outputs are within expected bounds

Bias and Fairness

- ✓ Report on steps taken to account for bias in datasets
- ✓ Disclose levels of bias in AI outputs

Transparency and Explainability

- ✓ Prioritise testing and verifying AI outputs
- ✓ Attempt to establish how outputs are arrived at

Compute Resources

- ✓ Plan for access to necessary computational resources
- ✓ Monitor government initiatives for AI research resources

4.2 Updated UK Government response to AI Regulation (2/2)

Department for Science, Innovation, & Technology

4. Legal and Ethical Implications

Copyright and Intellectual Property
- ✓ Prepare for potential changes in copyright framework for AI training
- ✓ Consider licensing agreements and financial settlements

Liability and Responsibility
- ✓ Understand liability for AI-related harms
- ✓ Expect more regulatory guidance on this issue

Ethical Considerations
- ✓ Prioritise transparency in AI systems and decision-making
- ✓ Consider ethical implications, especially in areas like HR and recruitment

5. Organisational Capabilities and Structure

Capability Building
- ✓ Invest in workforce upskilling and internal AI expertise development
- ✓ Consider partnerships with academic institutions or research organisations

Cross-departmental Collaboration
- ✓ Establish cross-departmental collaboration on AI governance
- ✓ Create a steering committee for coherent approaches across business units

6. Market and Workforce Impact

Market Competition Awareness
- ✓ Be aware of potential market dominance by leading AI developers
- ✓ Consider both proprietary and open-source options in AI strategy

Workforce Adaptation
- ✓ Prepare for AI-driven changes in the nature of work
- ✓ Equip workforce with skills to effectively utilise AI

7. Public-Private Collaboration and External Engagement

Public Sector Engagement
- ✓ Look for collaboration opportunities with public sector AI initiatives
- ✓ Engage with industry peers and international partners for knowledge sharing

International Considerations
- ✓ Stay informed about international dialogues and best practices
- ✓ Monitor global AI governance initiatives

8. Continuous Improvement and Future-proofing

Regular Policy Reviews
- ✓ Implement regular reviews of AI governance policies
- ✓ Develop a monitoring and evaluation plan for the governance framework

Anticipating Future Regulations
- ✓ Prepare for potential mandatory measures for highly capable AI systems
- ✓ Develop internal processes for testing and benchmarking powerful AI systems

4.3 Principles for the responsible use of AI in government

Central Digital & Data Office

Summary of principles to guide the safe, responsible and effective use of generative AI in government organisations (source), prepared by the Chief Technology Officer for Government:

Principle 1: You know what generative AI is and what its limitations are: Understand generative AI's core concepts and limitations. Recognise that it can produce unreliable results and should not be trusted without validation.

Principle 2: You use generative AI lawfully, ethically and responsibly: Implement input evaluation and content filtering to ensure responsible and ethical use, avoiding inappropriate, toxic, or biased outputs.

Principle 3: You know how to keep generative AI tools secure: Prioritise data security by protecting sensitive information, using privacy-enhancing technologies, and maintaining comprehensive logs for auditing.

Principle 4: You have meaningful human control at the right stage: Incorporate human oversight in development and operation, including review of input data, model performance assessment, and output evaluation.

Principle 5: You understand how to manage the full generative AI lifecycle: Establish continuous monitoring and evaluation processes, collecting and analysing performance metrics throughout the AI system's lifecycle.

Principle 6: You use the right tool for the job: Select models and deployment approaches based on specific use case requirements, considering factors such as capability, availability, and cost-effectiveness.

Principle 7: You are open and collaborative: Foster collaboration by learning from other government organisations' experiences and engaging with suppliers to understand their services.

Principle 8: You work with commercial colleagues from the start: Consider cost factors and engage with cloud service providers from the project's inception.

Principle 9: You have the skills and expertise needed to build and use generative AI: Invest in skill development, particularly in areas such as prompt engineering and understanding AI frameworks.

Principle 10: You use these principles alongside your organisation’s policies and have the right assurance in place: Align AI implementation with organisational policies and conduct regular architectural reviews to ensure compliance and effectiveness.

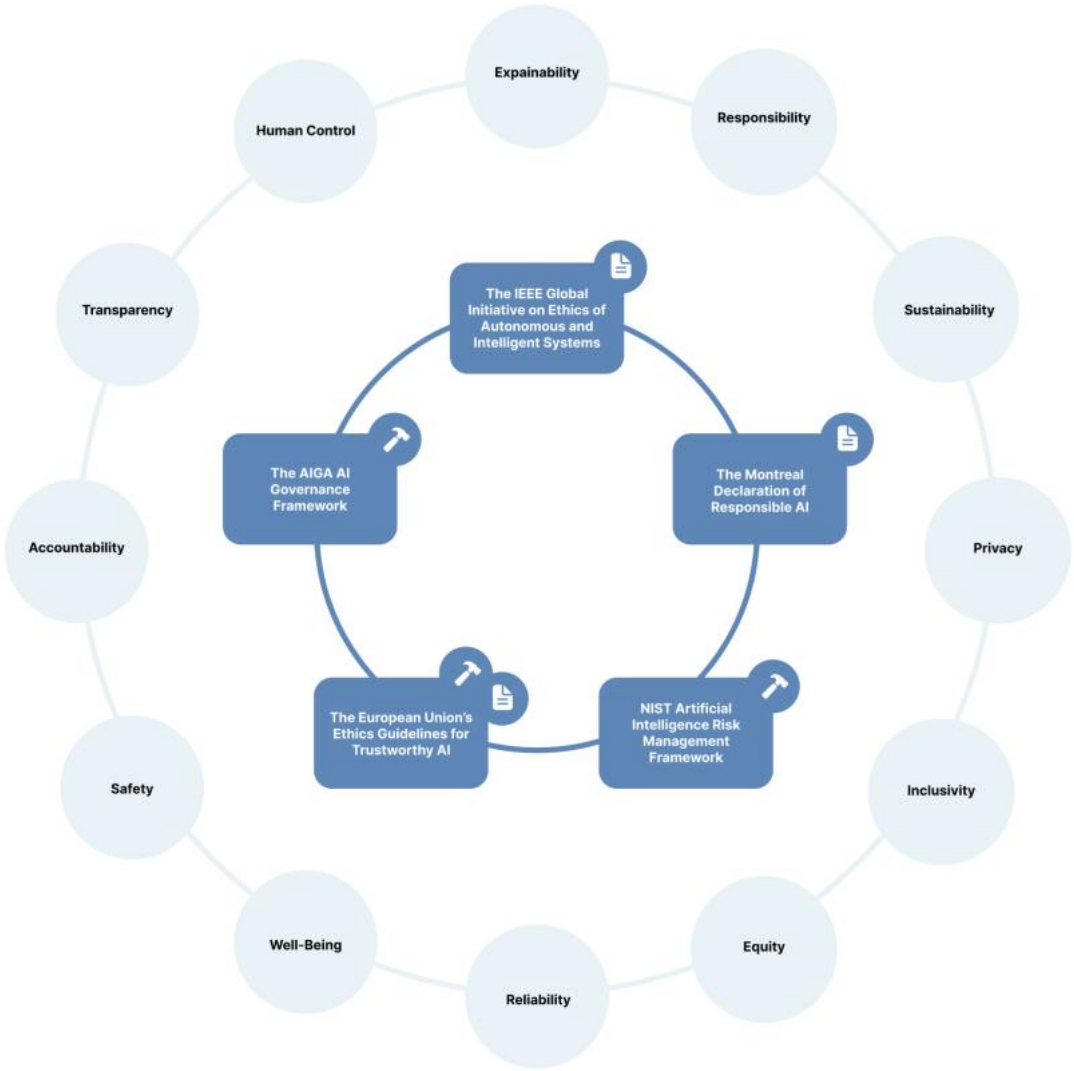
4.4 European AI Alliance

The European AI Alliance Implementing AI Governance Guide (source) provides guidance on navigating existing frameworks and advises on how to get started in AI governance.

The framework is underpinned by 12 principles and aims to address challenges related to safety, bias and privacy.

It introduces a process with actionable steps for implementing AI governance and some guidance on how to put AI governance principles into practice within an organisation, for example:

1. Familiarise yourself with AI governance frameworks and understand core principles such as transparency, accountability, safety, and privacy.
2. Assess your organisation's specific context, including its size, industry, and existing AI practices and identify areas where AI governance is most relevant and needed.
3. Coordinate cross-departmental implementation and involve stakeholders from legal, technical, and business teams manage risk and execution
4. Develop a roadmap that outlines the sequence of actions and prioritise these based on urgency and impact.
5. Continuously monitor AI systems' performance and adherence to governance principles and be prepared to iterate and adapt as needed.



4.5 European Union's AI Act

The EU AI Act is a risk-based approach (source) to assess AI systems according to 4 risk levels (unacceptable risk: prohibited; high risk: strictly regulated; limited risk: transparency requirements; minimal or no risk: unregulated).

Key recommendations (source) are to implement a similar risk-based approach to categorise AI projects in organisations which can help prioritise resources and attention. Additionally, to develop a clear framework for assessing the risk level of each AI initiative, considering factors such as potential impact on individuals, scale of deployment, and areas of application.

Obligations for high-risk systems include:

- ✓ Adequate risk assessment and mitigation
- ✓ High-quality datasets to minimise risks and discriminatory outcomes
- ✓ Logging of activity for traceability
- ✓ Detailed documentation
- ✓ Clear information provision to deployers
- ✓ Human oversight measures
- ✓ Robustness, security, and accuracy requirements

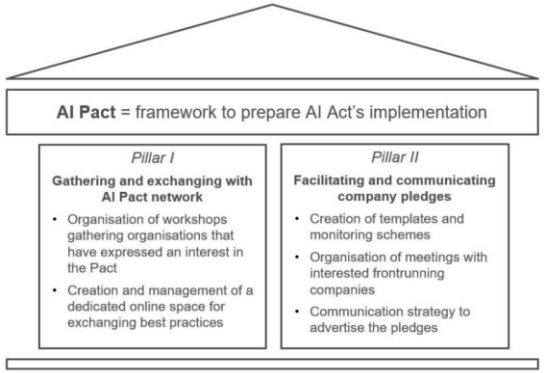
It emphasises the need for thorough documentation of AI systems, including their purpose, training data, and potential risks to support both compliance and internal governance. It recommends that organisations implement systems for the ongoing monitoring of AI performance, with processes for continuous improvement and human oversight mechanisms. Finally, organisations should develop clear communication strategies about AI use, both internally and for customers or end-users.

Then, the European Commission launched the AI Pact initiative (source) to encourage early adoption of the AI Act's key principles and requirements. It's designed to support organisations in preparing for the implementation of the AI Act ahead of its legal deadlines. Key features of the AI Pact are structured across two pillars:

Pillar I: Acts as a gateway to engage the AI Pact network, encouraging the exchange of best practices and providing practical information on the AI Act implementation process.

Pillar II: Encourages AI system providers and deployers to prepare early and take actions towards compliance with requirements and obligations set out in the legislation.
It helps organisations to:

- ✓ Understand and prepare for the AI Act's requirements ahead of time
- ✓ Facilitate knowledge sharing and best practice development among participants
- ✓ Provide a framework for organisations to demonstrate their commitment to responsible AI development and use
- ✓ Potentially influence the practical implementation of the AI Act through feedback from early adopters
- ✓ Build trust in AI technologies by showcasing proactive compliance efforts



4.6 AIGA AI Governance Framework

The AIGA AI Governance Framework (source), developed within the AIGA (AI governance and Auditing) research project (source) and financially supported by the AI Business Program of Business Finland to:

- ✓ Provide a practice-oriented framework for implementing responsible AI.
- ✓ Supports compliance with the upcoming European AI regulation (the AI Act, under preparation).
- ✓ Provides a template for decision-makers to address the key questions on the use of AI.
- ✓ Is value-agnostic.
- ✓ The Hourglass Model of Organisational AI Governance (source) presents the overall structure of the AIGA AI Governance Framework.
- ✓ The AI Governance Lifecycle (source) maps AI governance tasks to the OECD's AI system lifecycle framework.
- ✓ List of AI Governance Tasks (source) is a complete list of tasks included in the AIGA AI Governance Framework. The tasks are divided into the following categories: AI System, Algorithms, Data operations, Risk and impacts, Transparency, explainability and contestability (TEC), Accountability and ownership, Development and operations, Compliance.

Key aspects of the AIGA AI Governance Framework include:

1. Multistakeholder Collaboration: effective AI governance requires collaboration across sectors.
2. Structured Approach: AIGA's three-workstream structure (Safe Systems, Responsible Applications, and Resilient Governance) demonstrates the value of a structured, holistic approach. Leaders should similarly organise their AI governance efforts around key areas like system safety, responsible application, and regulatory compliance.
3. Proactive Risk Management: The Presidio AI Framework, introduced in one of AIGA's papers, emphasises early risk identification and proactive risk management. Leaders should implement robust guardrails and shared responsibility models to anticipate and mitigate AI-related risks.
4. Use-Case Based Evaluation: Leaders should assess AI tools based on specific use cases, ensuring multistakeholder governance, transparent communication, and value-based change management.

4.7 Useful Sources

The Open Data Institute's Data Ethics Canvas (source) summarises the key criteria to consider in order to ethically implement technology initiatives *(see right).*

DLA Piper AI Governance Report (source) examines AI deployment, Common AI challenges and risks, AI governance effectiveness and Key sector differences

Implementing Gen AI with speed and safety (source) This McKinsey article provides a blueprint for developing an approach to implementing Gen AI responsibly.

The art of AI maturity (source): Based on an Accenture survey of 1,600 C-Suite executives, this report looks at how organisations are advancing AI maturity including responsible implementation.

The AI Safety Institute (AISI) (source): The AISI helps governments understand advanced AI for informed policy-making and public accountability and advise on building in-house capabilities to test the safety of advanced AI systems, particularly large language models and AI assistants. They've released an open-source testing framework called 'Inspect' for the wider research community to use and build upon.

About Winmark Research

Acknowledgments

We would like to thank Winmark's AI Advisory Board, and all of the Winmark members who shared their valuable insights and experiences during the development of this guide.

All Winmark reports, including AI Governance in 2024, can be found in 'member area' on the Winmark portal

What we do

- Identify opportunities, segments and targets
- Assess the competitive performance of people, products and services
- Forecast market trends based on consumer behaviour and economic indicators
- Tests new concepts to develop your product / service
- Investigate potential takeover targets with strategic, financial and cultural fit
- Collate best practices and processes, and benchmark against industry standards
- Elevate Thought Leadership by bringing unique foresights, new growth opportunities, and risk mitigation strategies

Winmark's research helps our members and clients…

Stay ahead of industry trends and adapt to changing market conditions

Establish credibility and trust both internally, and externally

Become a leader in your field, attracting clients, and top talent

Share knowledge and perspectives to shape industry standards and practices

Leverage your strengths, open up new opportunities

Enhance brand reputation, increase visibility and prestige

Anticipate customer needs, strengthen satisfaction and loyalty

Foster a culture of continuous learning and development

Guide long-term planning and decision-making

What our clients say…

> Few reports on trends in the legal industry are as thorough as the Winmark's annual Looking Glass report.
>
> THE TIMES

> One word – excellent. Honestly the best [report] I have read so far and believe me, I have read a fair number.
>
> BCG

> Not only was the content itself excellent, but the fact it came from Winmark instantly ensured it had credibility.
>
> Smith & Williamson

> Winmark consistently deliver on two critical criteria that we seek in a partner – clear ROI and on time.
>
> Canon

> The last Winmark report is one of the best I have seen on strategy – it simplifies what can be overly complicated.
>
> BDO

> A very comprehensive report with very good content. Great work!
>
> Pinsent Masons

Contact us

John Jeffcock,
Chief Executive Officer

M +44 (0) 7957 831284
T +44 (0) 207 605 8000
E john.jeffcock@winmarkglobal.com

Catherine Qi
Head of Research

M +44 (0) 7860842081
T +44 (0) 207 605 8000
E catherine.qi@winmarkglobal.com

Membership of **Winmark's C-Suite Network** is made up of a diverse group of approximately **2,000 member organisations** and **1000+ individuals** across a **multitude of industry sectors**

Our leadership networks operate on a **peer-to-peer model,** in which members **learn** from each other, **benchmark** against others and **gain insights, new ideas** and **assurance** through **engaging with peers**

www.winmarkglobal.com | LinkedIn
Winmark Ltd, 7 Berghem Mews,
Blythe Road, London W14 0HN