



WWW.AUDITT.ORG.UK

Auditt Governance Framework

AI Governance Policy

Minimum Viable AI Policy

The framework for governing all AI systems auditt uses — the principles, responsibilities and requirements that ensure AI is adopted and operated in ways that are safe, secure, lawful and aligned with our values.

APPROVED

20 October 2026

VERSION

1.0 — Minimum Viable

NEXT REVIEW

By 20 October 2027

ENTITY

Auditt Technology Consulting Ltd UK · Reg. 15072334 · UKIPO Patent P152528.GB-RPA

AI Governance Policy

This Policy applies to every employee, contractor and third-party user who uses AI systems in the course of their work for Auditt.

PURPOSE AND SCOPE

AI is adopted and used across auditt in ways that are safe, secure, lawful and aligned with our values — because trust in every transaction and transparency in every audit begin with how we govern the tools we build with.

1.1 Purpose

This Policy establishes the framework for governing all AI systems we use. It sets out the principles, responsibilities and requirements to ensure that AI is adopted and used in ways that are safe, secure, lawful and aligned with our values, and provides practical guidance for everyone who uses AI tools in their work.

1.2 Applicability

This Policy applies to all AI systems we procure or operate, including cloud-based AI services, AI features embedded in business software and any pilot or proof-of-concept deployments. All employees and contractors who use AI systems for work purposes must comply with this Policy.

1.3 Exclusions

Low-risk or experimental AI activities may be granted exceptions where they do not pose significant material, legal, ethical or operational risks.

1.4 Related Frameworks

This Policy operates alongside our existing policies, including those for data protection and information security.

KEY TERMS

For the purposes of this Policy, the following definitions shall apply.

"AI System" means any software application that uses AI models to generate outputs such as predictions, recommendations, decisions or content — including chatbots, content generators, recommendation engines, coding assistants and AI features embedded in business software. ◆

"AI Model" means the computational component within an AI system that produces outputs from inputs, typically using machine learning or statistical techniques; AI systems combine models with data, interfaces and other components. ◆ **"AI Incident"** means any event where an AI system operates outside its intended parameters, produces harmful or incorrect outputs, or violates policy or legal requirements. ◆ **"AI Governance Lead"** means the senior leader responsible for coordinating AI governance implementation; maintains this Policy, approves low and medi-

um-impact AI systems, confirms classifications, oversees incident response, ensures training exists and reports to the GRC Committee. ◆

"GRC Committee" means the existing Governance, Risk and Compliance Committee; provides strategic oversight of AI governance, reviews AI risks and decides on high-impact AI systems and policy matters. ◆

"System Owner" means the designated individual accountable for governance and compliance of a specific AI system throughout its use. ◆

"Mechanism Owner" means the designated individual accountable for the effective operation of governance mechanisms that implement specified controls — including AI system inventory, incident reporting and risk assessment.

GUIDING PRINCIPLES

Our approach to AI is guided by six principles that carry practical implications for how we select, manage and use AI.

3.1 Trustworthiness and Reliability

AI systems must be dependable in their intended contexts. We adopt tools that are fit for purpose and operate predictably within defined boundaries; we monitor for degradation or unexpected behaviour, and investigate inconsistent or questionable results before relying on them.

3.4 Security and Privacy Protection

Security and privacy are embedded by design and sustained throughout the system lifecycle. We apply data minimisation, do not enter personal or confidential information into unapproved tools, and review protections when vendors update their systems or terms.

3.2 Fairness and Bias Prevention

AI systems must treat individuals and groups equitably. We assess for bias before adopting a system, remain alert to disparate impacts during use, and adjust or discontinue systems where unacceptable disparities are identified.

3.5 Accountability and Oversight

Clear accountability exists for every AI system in use. Employees remain accountable for work produced with AI assistance. AI augments human judgment rather than replacing it, and does not make consequential decisions without human review and approval.

3.3 Transparency and Explainability

People affected by AI decisions should be able to understand how those decisions are influenced. We disclose material AI use, document the systems we rely on, and ensure staff can explain, at a general level, what each tool does and where it may fall short.

3.6 Societal Impact

We consider effects beyond immediate business outcomes, evaluating whether tools could cause harm to individuals, communities or society, and engaging constructively with regulatory developments and evolving expectations around responsible AI use.

ACCOUNTABILITY

We are ultimately accountable for how AI is used across our operations. This accountability cannot be delegated to vendors or automated systems. The roles below ensure responsibility for AI is clearly assigned and decisions are made by people with appropriate authority.

Governance, Risk & Compliance Committee

Reviews and approves high-impact AI systems, sets risk tolerance, approves policy changes and receives regular reporting on AI governance matters. Escalates to executive leadership as appropriate.

System Owners

Every AI system has a designated owner accountable for compliance with this Policy — understanding the system's capabilities and limitations, ensuring monitoring is in place, maintaining documentation and reporting issues through appropriate channels.

All Employees

Must comply with this Policy, complete required training, review and validate AI outputs before use, and report incidents promptly. Employees remain accountable for work produced with AI assistance.

AI Governance Lead

Maintains this Policy, approves low and medium-impact AI systems and their classification, oversees incident response, ensures training exists and reports to the GRC Committee. High-impact systems require Committee approval.

Mechanism Owners

Accountable for the effective operation of assigned governance mechanisms (inventory, incident reporting, risk assessment). Maintain supporting documentation and templates and recommend improvements based on operational experience.

Specialist Functions

Information Security advises on security requirements; the Data Protection Officer oversees privacy compliance; Legal and Compliance advises on regulatory requirements and reviews vendor contracts. These functions support, but do not replace, the accountability of the AI Governance Lead and System Owners.

RISK SCREENING AND CLASSIFICATION

5.1 Classification Requirement

All AI systems must be classified before deployment. The System Owner proposes classification, and the AI Governance Lead confirms it. Classification is reviewed when scope, use or operating environment changes materially.

5.2 Classification Factors

Classification considers the nature and reversibility of decisions influenced, degree of human oversight, number and vulnerability of people affected, sensitivity of data processed, regulatory requirements and whether the system operates autonomously.

LEVEL 01 · LOW	LEVEL 02 · MEDIUM	LEVEL 03 · HIGH
Advisory, Non-Sensitive Advisory outputs with human decision-making, non-sensitive data, limited populations, minimal harm potential. Examples: drafting tools, document summarisation. Requires: registration · responsible use	Significant Decisions, Personal Data Systems influencing significant decisions, processing personal data, operating at scale or presenting moderate harm. Examples: customer service AI, operational analytics. Requires: documented risk assessment · Governance Lead approval	Consequential Decisions Systems making or substantially influencing consequential decisions affecting rights, financial standing, employment or service access. Examples: recruitment screening, credit decisions. Requires: comprehensive risk assessment · executive approval · human oversight · ongoing monitoring

5.3 Prohibited Uses

We will not use AI that violates applicable laws, makes fully automated consequential decisions without human oversight, breaches data protection requirements, or presents unacceptable risks to individuals or our organisation. Uncertain cases must be referred to the AI Governance Lead.

5.4 Risk Assessment

Medium and High Impact systems require documented risk assessment before deployment, identifying potential harms, evaluating likelihood and severity, documenting controls and confirming residual risks fall within acceptable bounds.

AI SYSTEM INVENTORY

6.1 Inventory Requirement

We maintain a central inventory of all AI systems in use. Every AI system must be registered before deployment, including AI embedded in business software where those features are actively used.

6.2 Inventory Contents and Update

The inventory records system name and description, vendor, System Owner, business purpose, classification level, key dates and data types processed. Medium and High Impact systems link to supporting documentation including risk assessments and approvals. System Owners register their systems and update entries when material changes occur; the designated Mechanism Owner maintains the infrastructure; the AI Governance Lead reviews the inventory periodically for completeness.

ACCEPTABLE USE

7.1 Permitted Uses

Employees are encouraged to use approved AI tools for drafting content, summarising documents, automating repetitive tasks, brainstorming ideas and generating initial drafts for human refinement. AI analytics may inform decisions where humans validate results and understand limitations.

7.2 Prohibited Uses

Employees must not input confidential, personal or sensitive information into AI tools not approved for that data category. AI must not make consequential decisions without human review. Employees must not use AI to generate misleading, discriminatory or harmful content, misrepresent AI-generated content as human-created where disclosure is required, or bypass security controls or violate intellectual property rights.

7.3 Uses Requiring Care

External AI tools should only be used where approved. AI outputs for significant decisions should be validated against authoritative sources. Customer-facing AI use should be disclosed where material. When uncertain, seek guidance before proceeding.

7.4 Additional Guidance

The Appendix to this Policy provides practical examples of permitted uses, prohibited uses and situations requiring extra caution. All employees should familiarise themselves with these guidelines before using AI tools. The AI Governance Lead may publish additional guidance for specific tools.

PROCUREMENT AND VENDOR MANAGEMENT

8.1 Approval

AI systems must be approved by the AI Governance Lead before procurement or deployment, with input from Information Security, Data Protection and Legal as appropriate.

8.2 Vendor Assessment

Before adopting a vendor-supplied AI system, we assess how it handles data (storage, retention, use for training), security controls, testing for bias and harmful outputs, transparency about capabilities and limitations, and vendor track record.

8.3 Evidence Requirements

For Medium and High Impact systems, vendors should provide evidence of appropriate testing — including methodology, training data information, known limitations and safeguards. Where evidence is inadequate, additional internal controls may be required.

8.4 Contracts

Contracts must address data handling, security and privacy, and include performance standards, incident notification and clear allocation of responsibilities. Legal and Compliance reviews contracts for Medium and High Impact systems.

8.5 Ongoing Oversight

System Owners monitor vendor communications about updates, term changes or security issues. Material changes trigger review of classification and controls.

HUMAN OVERSIGHT AND CONTROL

9.1 Meaningful Oversight

Humans retain meaningful oversight of AI systems, proportionate to the system's autonomy and the stakes involved. AI outputs must be reviewed before use, with review depth matching the significance of the decision or communication.

9.2 Consequential Decisions

AI must not make final decisions in high-consequence areas such as employment, financial standing, access to services or safety without human review and approval. Where AI informs such decisions, a qualified person makes the final determination.

9.3 Override and Continuity

Users must know how to override, pause or discontinue AI systems they work with. High Impact systems require documented intervention procedures. Critical business functions must not depend solely on AI without alternative pathways.

9.4 Training

People using AI systems must understand the system's capabilities, limitations and failure modes, proportionate to classification and role.

REPORTING AND SUPPORT

10.1 Reporting Incidents

If you observe an AI system producing harmful, incorrect or unexpected outputs, or suspect a violation of this Policy, report it promptly to your Director or through our incident reporting channels. For urgent matters affecting customers or safety, notify a senior Director immediately. The designated Mechanism Owner maintains incident reporting channels and ensures incidents are properly tracked and escalated.

10.2 Reporting Content

Provide as much detail as practical: what happened, when, which system was involved and any relevant outputs. Good faith reporting is encouraged and will not result in adverse consequences.

10.3 Questions and Guidance

If uncertain whether a particular use of AI is appropriate, seek guidance before proceeding. Your Director is the first point of contact. For questions involving data protection, security or legal risk, consult the relevant specialist teams.

10.4 Feedback

Suggestions for improving this Policy or our AI practices should be directed to the AI Governance Lead.

EXCEPTIONS

11.1 Exception Requests

Requests for exceptions to this Policy must be documented and submitted to the AI Governance Lead. Each request must include the business need, an analysis of potential risks and any compensating controls to be implemented.

11.2 Approval

The AI Governance Lead may grant temporary or conditional exceptions if overall risk remains acceptable. Exceptions are time-limited and subject to review.

POLICY REVIEW

12.1 Maintenance

The AI Governance Lead is responsible for maintaining this Policy. The Policy is reviewed at least annually or earlier if prompted by significant changes in technology, regulation or organisational circumstances.

12.2 Revisions

Substantive revisions require approval from executive leadership and must be communicated to all affected staff.

APPENDIX — ACCEPTABLE USE GUIDELINES

PERMITTED — WHAT YOU CAN DO

Automate repetitive tasks, summarise documents, draft content, brainstorm, inform decisions with validated analytics, draft customer communications in approved tools, and propose pilots in controlled environments after informing your Director.

PROHIBITED — WHAT YOU MUST NOT DO

Disclose confidential or personal data to unapproved tools; bypass security controls; make high-stakes decisions without human review; generate deceptive, harmful or impersonating content; infringe IP; or conceal AI involvement where transparency is required.

USE WITH CARE — BE CAREFUL WHEN...

Using external or unapproved AI tools; handling AI-generated content before official use; integrating AI into workflows; using personal AI tools for work; or acting in regulated or sensitive areas — seek guidance where uncertain.

SIGNED *Dr. Gopalakrishnan Thyagarajan*, Director · Approved 20 October 2026 · AI Governance Policy v1.0