JUSTMATTER

Artificial Intelligence (AI) Responsible Use Policy

Version: 1.0
Release Date: January 2026

Contents

1. Purpose and Scope

1.1 Purpose

This policy defines principles, responsibilities, and governance for the responsible use of artificial intelligence (AI) technologies in audit activities, including risk assessment, analytics, documentation, reporting, and assurance work.

It ensures AI use is trustworthy, auditable, ethical, and aligned with professional auditing standards, relevant regulatory considerations, and sound risk management practices.

1.2 Scope

This policy applies to:

- All auditors and audit teams (internal or external)
- AI tools and systems used in audit work (e.g., data analytics engines, large language models, automation tools, predictive models)
- Third-party AI services and platforms integrated into audit workflows
- Audit documentation, deliverables, and reporting that involve or are informed by AI outputs

2. Governance Framework

2.1 Alignment with AI RMF and ISO 42001

Audit functions shall build AI governance by combining:

- The NIST AI Risk Management Framework (AI RMF) for risk-based identification, assessment, measurement, and mitigation of AI risks, tailored to audit contexts.
- The ISO/IEC 42001 AI Management System standard for an enterprise-wide, auditable AI governance system with documented policies, roles, controls, continuous improvement cycles, and internal audit processes.

This dual approach embeds NIST's risk guidance into the formal management structure ISO 42001 expects.

3. Principles for Responsible AI Use

3.1 Trustworthiness and Risk Awareness

AI must be used in ways that promote reliability, accuracy, fairness, and resilience. Audit teams must:

- Identify and classify AI risks relevant to the audit engagement
- Assess impacts on audit outcomes, quality, and independence
- Use risk registers, profiles, and mitigation plans consistent with AI RMF principles.

3.2 Human Oversight and Judgment

Auditors must exercise professional judgment over AI outputs. AI tools are assistive and must not replace:

- Critical thinking
- Evidence evaluation
- Professional skepticism
- Conclusions and audit opinions

4. Roles and Responsibilities

4.1 AI Governance Sponsor

The Managing Director is designated as the AI Governance Sponsor, who has the following roles and responsibilities:

- Establish and update the AI policy
- Champion AI governance aligned with organizational priorities
- Ensure alignment with ISO 42001 structure (leadership accountability, management reviews).

4.2 AI Risk and Controls Committee

The Executive Team serves as the AI Risk and Controls Committee, with the following roles and responsibilities:

- Responsible for risk tiering, control selection, and oversight cycles
- Validates that AI tools used in audits comply with policies and risk thresholds

4.3 Individual Auditors and Teams

- Apply policy consistently in daily audit work
- Document AI use, decisions, validations, and overrides
- Support internal audit assurance activities related to AI governance

4.4 Internal Audit Function

Per IIA guidance, internal audit should:

- Understand where, how, and why AI is used across the organization
- Provide assurance on AI governance structures, controls, and ethical use
- Increase auditors' AI literacy to effectively assess risk and controls
- Use the IIA's AI Auditing Framework tools and AI literature as practical guides.

5. Risk Management and Controls

5.1 Inventory and Classification

Maintain an AI systems inventory covering:

- Purpose and context of use
- Data inputs and sources
- Model assumptions and limitations

This supports risk identification and aligns with both ISO 42001 audit documentation and NIST function "Map."

5.2 Impact and Risk Assessments

Before using an AI tool:

- Conduct risk assessments considering fairness, bias, privacy, security, and reliability
- Document risk treatment actions and monitoring plans

These assessments form a core part of responsible use and support ISO 42001's "Plan" and AI RMF's "Map" and "Measure" functions.

5.3 Validation and Testing

- Validate AI outputs against independent benchmarks

- Require evidence of accuracy and relevance before reliance
- Log decisions, overrides, and human validations

6. Documentation and Audit Trails

Audit documentation must include:

- AI tool identification, version, and configuration
- Risk assessments and control evidence
- Rationale for using or not using AI outputs in audit conclusions
- Prompt documentation where generative AI is used (input and output)
- Audit trails sufficient for internal and external quality reviews

This meets ISO 42001's emphasis on documented processes and internal control records.

7. Training and Competence

Provide tailored training for auditors covering:

- AI fundamentals and risks
- Risk management per NIST AI RMF
- AI governance per ISO 42001
- Ethical considerations and human oversight best practices

The IIA's AI knowledge center and related frameworks reinforce the need for auditors to develop AI risk awareness and control evaluation skills.

8. Monitoring and Continuous Improvement

- Establish regular reviews of AI policy compliance
- Use internal audits to assess AI governance maturity
- Update controls and policy based on new risk insights, standards updates, and technology evolution
- Drive continuous improvement through internal review cycles (ISO PDCA) and risk reassessments (NIST RMF ongoing cycles)

This dynamic approach aligns with ISO 42001's management system requirements and NIST's risk lifecycle perspective.

9. Ethics, Accountability, and Transparency

Audit teams must ensure:

- AI use supports ethical principles and audit independence
- Transparency to stakeholders about how AI tools influence audit methodology, without revealing confidential information
- Governance and accountability through documented roles and conditions

The IIA framework highlights ethics and human oversight as foundational to responsible AI audits.

10. Policy Maintenance and Review

This policy shall be:

- Reviewed at least annually
- Updated for changes in standards (e.g., AI RMF updates, ISO 42001 revisions)
- Revalidated after material changes in AI tools, regulatory requirements, or audit practice needs