AI Risk Management Framework

Version 2026 & Integrated Edition

This Document is a Repurposing of the NIST AI RMF 2023

Shaped Specifically on the Integration of

~

ISO/IEC 42001 Artificial Intelligence Management System (AIMS)

~

ISO/IEC 27001 Information Security Management System (ISMS)

January 2026

Background

Ever wounder how the "Govern, Map, Measure, Manage" was created? Well the structure did not emerge from nowhere - it draws on several decades of risk management thinking. The most direct ancestor is NIST's own Cybersecurity Framework (CSF) from 2014, which used the five functions: Identify, Protect, Detect, Respond, and Recover. This established NIST's approach of organizing risk management into distinct functional categories.

But the deeper roots go back further. The concepts reflect influence from:

- Enterprise Risk Management (ERM) frameworks, particularly COSO's ERM framework (2004, updated 2017), which emphasized governance, objective-setting, risk assessment, and monitoring as core functions
- ISO standards like ISO 31000 (risk management) and ISO/IEC 27001 (information security), which promoted systematic approaches to identifying, analyzing, and treating risks
- Quality management traditions like Plan-Do-Check-Act (PDCA) cycles, which influenced the cyclical nature of Map→Measure→Manage

The specific articulation as "*Govern*, Map, Measure, Manage" for AI was NIST's synthesis, published in the AI RMF 1.0 in January 2023. *Govern* sits at a different level - it's about establishing the strategic framework, policies, and oversight structure before you enter the PDCA cycle. NIST AI RMF working group adapted these established risk management principles specifically for AI systems' unique challenges - things like opacity, emergent behaviors, and sociotechnical impacts.

If you trace it back far enough, you get to some pretty fundamental human activities. The core insight behind all these frameworks - that you should **think before you act, check what happened, and adjust** - is ancient. Maritime insurance in the 1600s, agricultural planning, military strategy... humans have always done informal risk management.

What's interesting is how we **formalized** it. The modern frameworks emerged roughly like this:

1. **Quality control** (1920s-50s) - Shewhart, Deming, and others developed statistical process control and PDCA cycles for manufacturing
2. **Systems thinking** (1950s-70s) - People started seeing organizations as interconnected systems that needed holistic management
3. **Enterprise risk management** (1990s-2000s) - Financial scandals and corporate failures drove frameworks like COSO that said "governance should be baked in, not bolted on"
4. **Domain-specific adaptations** (2000s-present) - Cybersecurity, AI, privacy, etc. took those general principles and tailored them

So in a way, the "egg" was the practical need to manage complex systems, and the "chicken" was the formalization into frameworks. But then those frameworks became eggs that hatched new, more specific frameworks!

This AI RMF 2026 is really the latest chicken in a long line of chickens, if that makes sense. What's novel is applying these concepts to systems that are probabilistic, opaque, and can exhibit emergent behaviors - things traditional risk frameworks were not really designed for.

NIST AI Risk Management Framework: My Analysis and Update

Evaluation of Framework Currency and Alignment with Emerging Standards

Analysis Date: January 7, 2026

Prepared for: Framework Review Assessment

Executive Summary

Since the 2023 release of the NIST AI Risk Management Framework (AI RMF 1.0), much in the world of national-international AI Standards, Frameworks and Guidelines have evolved significantly through supplementary guidance. While the core framework remains fundamentally sound, **the framework DOES need targeted updates** to address:

1. **Emerging generative AI risks** (partially addressed through the July 2024 Generative AI Profile)
2. **Enhanced cybersecurity integration** (in progress via Cyber AI Profile and SP 800-53 overlays)
3. **Supply chain and third-party AI dependencies** (gaps identified in March 2025 updates)
4. **Agentic and multi-agent AI systems** (emerging risk category)
5. **Global regulatory harmonization** (ongoing through crosswalk development)
6. **ISO/IEC 42001 Artificial Intelligence Management Systems (AIMS)** (provides a framework for organizations to responsibly develop, use, and manage AI, ensuring governance, risk mitigation, ethical practices, and compliance with regulations like the EU AI Act)

Key Finding: Rather than requiring a complete overhaul, NIST is appropriately addressing gaps through a **modular enhancement approach** with profiles, overlays, and updated crosswalks. However, while those that have adopted the NIST view of AI Risk Management, I've created a different **2026 version update** that I feel would be valuable to consolidate all of these developments and address newly identified gaps.

Current State Assessment

AI RMF 2026 Evolution Timeline

January 2023: NIST AI RMF 1.0 released

- Core functions: Govern, Map, Measure, Manage
- Voluntary, technology-neutral framework
- Initial crosswalks published

July 2024: Generative AI Profile (NIST AI 600-1) released

- Addresses GenAI-specific risks: hallucinations, data leakage, CBRN information
- Provides supplementary guidance without replacing core framework
- Recognized gaps: jailbreaking, prompt injection, model extraction

December 2024: Cyber AI Profile (NISTIR 8596) preliminary draft released

- Three focus areas: securing AI systems, AI-enabled cyber defense, thwarting AI-enabled attacks
- Integrates with NIST Cybersecurity Framework 2.0
- Comments due January 30, 2026

August 2025: SP 800-53 Control Overlays for Securing AI Systems (COSAIS) announced

- Five initial use cases: generative AI, predictive AI, single/multi-agent systems, AI developer controls
- Implementation-focused guidance building on existing SP 800-53 catalog
- Public comment period ongoing

2025 Ongoing Developments:

- SP 800-53 Release 5.2.0 (August 2025) added AI-specific controls
- Revision planned per AI Action Plan
- Enhanced crosswalks to ISO 42001, EU AI Act, Singapore AI Verify

International Standards Landscape

ISO/IEC 42001:2023 (AI Management Systems)

Status: Published December 2023, certifiable standard

Key Characteristics:

- Plan-Do-Check-Act (PDCA) management system approach
- Certifiable through accredited bodies (3-year validity)
- Strong alignment with ISO 27001 for information security
- Requirements for AI governance, risk assessment, lifecycle management

AI RMF Alignment:

- Official NIST crosswalk published mapping AI RMF subcategories to ISO 42001 clauses
- Approximately 40-50% overlap in requirements
- AI RMF's Govern function maps well to ISO organizational structure clauses
- Both emphasize risk management, transparency, human oversight

Gap Analysis:

- ISO 42001 requires formal AIMS documentation; NIST AI RMF 2023 is more flexible
- ISO specifies certifiable audit requirements; NIST is guidance-based
- AI RMF 2026 provides more detailed trustworthiness characteristics
- ISO 42001 includes stronger supply chain oversight requirements

EU AI Act (Regulation 2024/1689)

Status: Entered force August 1, 2024; phased implementation

Implementation Timeline:

- February 2, 2025: Prohibited AI systems ban effective
- August 2, 2025: GPAI provider obligations, transparency requirements
- August 2, 2026: High-risk AI obligations, conformity assessments
- August 2, 2027: Extended deadline for embedded high-risk systems

Key Requirements:

- Risk-based classification (unacceptable, high, limited, minimal)
- CE marking for high-risk systems
- Mandatory transparency and record-keeping
- Post-market monitoring and incident reporting
- Penalties up to €35 million or 7% global turnover

NIST Relationship:

- EU AI Act is legally binding regulation; AI RMF 2026 is voluntary guidance
- ISO 42001 serves as bridge between AI RMF 2026 and EU AI Act compliance
- NIST principles align with EU requirements for transparency, accountability, human oversight
- Gap: EU Act more prescriptive on conformity assessment procedures

Singapore AI Governance Framework

Current Framework Components:

- Model AI Governance Framework (updated 2024 for Generative AI)
- AI Verify toolkit (government-developed testing framework)
- AI Verify Foundation (open-source community since 2023)
- ISAGO 2.0 (self-assessment guide)
- Singapore Standard SS ISO/IEC 42001:2024 (national adoption)

Global Harmonization Efforts:

- October 2023: AI Verify mapped to NIST AI RMF 2023 (interoperability achieved)
- June 2024: AI Verify mapped to ISO/IEC 42001:2023
- February 2025: Global AI Assurance Pilot launched
- Integration with OECD AI Principles and GPAI Code of Practice

Singapore's Approach:

- Voluntary, non-binding frameworks
- Strong emphasis on practical testing and validation
- Nine governance dimensions for Generative AI
- Focus on cross-border alignment and reducing compliance costs

Other National/Regional Standards

United Kingdom:

- UK AI Safety Institute established
- Inspect AI safety testing platform (open-source)
- Emphasis on frontier model evaluation and red-teaming
- Close coordination with NIST on standards development

China:

- AI Safety Governance Framework published 2024
- Interim Measures for Generative AI Services
- MIIT establishing AI Standardization Technical Committee
- Goal: 50+ AI standards by 2026

Japan:

- AI Promotion Bill passed February 2025
- Social Principles of Human-Centric AI (2019 baseline)
- Mandatory cooperation on safe AI development
- Japan AI Safety Institute established

Australia:

- Voluntary AI Safety Standard (10 guardrails)
- Consultation on mandatory guardrails for high-risk settings
- Alignment with international frameworks

Cybersecurity Framework Integration

NIST Cybersecurity Framework (CSF) 2.0 Integration

Current Integration Status:

- Cyber AI Profile (NISTIR 8596) preliminary draft released December 2024
- Maps CSF 2.0 Functions/Categories/Subcategories to AI-specific considerations
- Provides AI-specific guidance without creating separate framework

Three Focus Areas:

1. **Securing AI Systems:** Protecting AI models, data, infrastructure from attacks
2. **AI-Enabled Cyber Defense:** Using AI to enhance security operations
3. **Thwarting AI-Enabled Cyberattacks:** Defending against adversaries using AI

Integration Benefits:

- Organizations can use existing CSF programs for AI security
- Reduces compliance burden by building on familiar framework
- Maps to SP 800-53 controls for detailed implementation

Identified Gaps:

- Initial draft lacks depth on adversarial ML attacks
- Limited coverage of AI supply chain security
- Needs stronger integration with Zero Trust architecture

SP 800-53 Control Overlays (COSAIS Project)

Purpose: Adapt SP 800-53 security controls for AI-specific use cases

Five Initial Use Cases:

1. Generative AI (LLM assistants with RAG)
2. Predictive AI (business workflow automation)
3. Single-agent AI systems
4. Multi-agent AI systems
5. AI developer-specific controls

Key Innovations:

- Addresses model integrity, data provenance, adversarial robustness
- Supplements existing controls rather than replacing them
- Assumes baseline enterprise security controls already implemented
- Library approach allows mix-and-match based on use case

Development Status:

- Concept paper released August 14, 2025
- Public comment period ongoing
- Slack collaboration channel active
- Expected finalization: 2026

Existing NIST AI RMF 2023 Crosswalks

NIST has published official crosswalks mapping AI RMF to:

- **ISO/IEC 42001:2023** - AI Management Systems
- **NIST Cybersecurity Framework 2.0**
- **Singapore AI Verify Framework**
- **OECD AI Principles**

Additional crosswalks in development:

- EU AI Act (unofficial but widely developed by third parties)
- Various sector-specific frameworks (healthcare, financial services)

Crosswalk Effectiveness:

- Enable organizations to leverage work across frameworks
- Reduce duplication of compliance efforts
- Support international operations
- Generally well-received by implementers

Limitations:

- Static documents requiring manual updates
- Some mappings are high-level rather than detailed
- Limited guidance on conflict resolution when frameworks diverge
- Need for interactive tools (some third parties have created these)

Gap Analysis: What NIST AI RMF 2023 Needs

Critical Updates Required

A. Generative AI & Foundation Models

Current Coverage: Partial through AI 600-1 Profile (July 2024)
Gaps Identified:

- Insufficient guidance on prompt injection and jailbreaking attacks
- Limited coverage of model extraction and inversion attacks
- Weak guidance on synthetic content provenance and watermarking
- Inadequate treatment of training data copyright and licensing
- Missing guidance on red-teaming methodologies for LLMs

Recommendation: Expand core framework or create comprehensive GenAI addendum integrating AI 600-1 findings with new threat intelligence.

B. Multi-Agent and Agentic AI Systems

Current Coverage: Minimal; being addressed in COSAIS (Control Overlays for Securing AI Systems) use cases
Gaps Identified:

- No specific guidance on agent-to-agent interaction risks
- Limited treatment of emergent behaviors in multi-agent systems
- Insufficient coverage of autonomous decision-making boundaries
- Missing guidance on agent oversight and kill-switch mechanisms
- Weak treatment of agent goal misalignment

Recommendation: Add dedicated section or category in next framework version addressing agentic AI governance.

C. AI Supply Chain Risk Management

Current Coverage: General third-party risk in Govern function
Gaps Identified:

- Insufficient guidance on foundation model provider assessment
- Limited treatment of AI Bill of Materials (AI-BOM) requirements
- Weak guidance on model card verification and validation
- Missing risk assessment for fine-tuning and RAG data sources
- Inadequate coverage of vendor lock-in and exit strategies

Recommendation: Integrate C-SCRM principles specifically for AI dependencies; expand AI-BOM guidance (reference emerging standards).

D. Adversarial Machine Learning

Current Coverage: Referenced but not detailed in core framework
Progress: NIST AI 100-2e2025 (Adversarial ML taxonomy) published
Gaps Identified:

- Limited practical guidance on implementing adversarial defenses
- Insufficient treatment of evasion, poisoning, extraction attacks
- Weak guidance on adversarial testing requirements
- Missing integration with security operations and SIEM tools
- Inadequate coverage of model drift due to adversarial adaptation

Recommendation: Integrate AI 100-2e2025 taxonomy into core framework with actionable implementation guidance.

E. AI Incident Response and Forensics

Current Coverage: General incident management in Manage function
Gaps Identified:

- No specific guidance on AI-related incident classification
- Limited treatment of model behavior forensics
- Weak guidance on preserving evidence from AI systems
- Missing integration with existing IR frameworks (NIST SP 800-61)
- Inadequate coverage of notification requirements across areas

Recommendation: Develop AI incident response playbook as companion document; integrate with SP 800-61.

F. Continuous Monitoring and Model Drift

Current Coverage: General monitoring in Measure function
Gaps Identified:

- Insufficient guidance on establishing baseline model performance
- Limited treatment of detecting data drift vs. concept drift
- Weak guidance on retraining triggers and approval processes
- Missing metrics for ongoing trustworthiness validation
- Inadequate coverage of automated monitoring tool integration

Recommendation: Expand Measure function with specific AI monitoring subcategories and metrics.

G. Explainability and Interpretability

Current Coverage: Addressed as trustworthiness characteristic
Gaps Identified:

- Limited practical guidance on implementing explainable AI techniques
- Insufficient treatment of regulatory requirements for explainability
- Weak guidance on balancing performance vs. interpretability
- Missing integration with sector-specific explainability standards
- Inadequate coverage of explaining ensemble and neural network decisions

Recommendation: Develop explainability implementation guide with sector-specific examples.

H. Environmental and Sustainability Impacts

Current Coverage: Minimal to none
Emerging Requirement: Growing regulatory focus (EU AI Act considers environmental impact)
Gaps Identified:

- No guidance on measuring AI carbon footprint
- Limited treatment of energy-efficient model design
- Missing consideration of computational resource optimization
- No integration with sustainability reporting frameworks
- Inadequate coverage of data center environmental impact

Recommendation: Add environmental sustainability as governance consideration; develop metrics aligned with sustainability standards.

References
Key documents reviewed for this analysis:

- AI RMF 2026 1.0 (AI 100-1, January 2023)
- NIST Generative AI Profile (AI 600-1, July 2024)
- NIST Cyber AI Profile Preliminary Draft (IR 8596, December 2024)
- NIST SP 800-53 Release 5.2.0 (August 2025)
- COSAIS Concept Paper (August 2025)
- ISO/IEC 42001:2023
- EU AI Act (Regulation 2024/1689)
- Singapore Model AI Governance Framework (2024)
- Multiple crosswalk documents and international standards

Assessment completed: January 7, 2026

Executive Summary

This AI Risk Management Framework 2026 (AI RMF 2026) is an Integrated Edition which provides ***the first comprehensive framework that seamlessly integrates NIST guidance with ISO/IEC 42001 (AI Management Systems) and ISO/IEC 27001 (Information Security Management Systems).*** This integration enables organizations to efficiently implement world-class AI governance while positioning themselves for international certification and regulatory compliance.

Key Integration Features

- Direct clause-by-clause mapping of NIST categories to ISO 42001 requirements
- AI-specific extensions of ISO 27001 Annex A controls
- PDCA (Plan-Do-Check-Act) cycle alignment with NIST's four functions
- Unified evidence generation satisfying all three standards simultaneously
- ISO 42001 certification readiness guidance and audit preparation
- 40-60% reduction in implementation effort vs. separate frameworks

"This document began as a tool for my own work. I'm now releasing it to the global community in good faith, hoping it helps others make sense of the many AI standards, guidelines, and frameworks emerging worldwide."

"We form a global community bound by common interest in AI—and we need to support each other through its adoption, governance, and use. ~ Ash Moore, Bluefox Consulting Service LLC".

Contents

What's New in My Personal Version of AI RMF 2026

This version includes significant enhancements:

- **Expanded coverage of generative AI risks** including hallucinations, prompt injection, data leakage, and synthetic content generation.
- **New guidance on agentic and multi-agent AI systems** addressing autonomous decision-making and emergent behaviors.
- **Enhanced AI supply chain risk management** including AI Bill of Materials (AI-BOM) requirements and third-party model assessment.
- **Comprehensive adversarial machine learning guidance** covering evasion, poisoning, extraction, and inference attacks.
- **Strengthened cybersecurity integration** with direct alignment to NIST Cybersecurity Framework 2.0 and SP 800-53 controls.
- **Updated international standards crosswalks** including ISO/IEC 42001, EU AI Act, and Singapore AI Verify.
- **New environmental sustainability considerations** addressing AI's energy consumption and carbon footprint.
- **Enhanced implementation guidance** with sector-specific examples and maturity models

Core Framework Structure

The AI RMF 2026 maintains the proven four-function structure introduced in version 1.0, while expanding and refining each function:

- **GOVERN:** Cultivates a culture of risk management and establishes accountability structures across the AI lifecycle
- **MAP:** Identifies context, categorizes AI systems, and assesses associated risks and impacts
- **MEASURE:** Employs quantitative and qualitative methods to analyze and track AI risks throughout the lifecycle
- **MANAGE:** Implements processes to respond to, mitigate, and monitor AI risks on an ongoing basis

Trustworthy AI Characteristics

The framework continues to emphasize seven key characteristics that define trustworthy AI systems:

- **Valid and Reliable:** Consistently operating as intended in accordance with specifications.
- **Safe:** Not posing unacceptable risks to safety, including physical safety and cybersecurity
- **Secure and Resilient:** Protected against unauthorized access and able to withstand adverse conditions.
- **Accountable and Transparent:** Enabling clear understanding of system behavior and decision-making.

- **Explainable and Interpretable:** Providing meaningful information about system operations appropriate to stakeholders.
- **Privacy-Enhanced:** Protecting personal information and maintaining confidentiality.
- **Fair with Harmful Bias Managed:** Avoiding perpetuation of discriminatory outcomes and unjust impacts.

Using This Framework

The AI RMF 2026 is designed to be used in several ways:

- **As a standalone framework** for organizations beginning their AI risk management journey
- **In conjunction with existing frameworks** such as ISO/IEC 42001, NIST Cybersecurity Framework, or ISO 27001
- **For compliance alignment** with regulatory requirements including the EU AI Act
- **As an assessment tool** to evaluate the maturity of current AI risk management practices

Organizations should tailor the framework to their specific context, considering factors such as:

- Sector and regulatory environment.
- Organization size and resources
- AI system complexity and criticality
- Stakeholder expectations and risk tolerance
- Existing risk management and governance structures

Relationship with International Standards

The AI RMF 2026 has been designed with international harmonization as a priority. Detailed crosswalks are provided for:

- **ISO/IEC 42001:2023** (Artificial Intelligence Management Systems)
- **ISO/IEC 27001:2022**
- **EU AI Act** (Regulation 2024/1689)
- **Singapore AI Verify Framework** and Model AI Governance Framework
- **NIST Cybersecurity Framework 2.0** and SP 800-53 security controls
- **OECD AI Principles** and other international guidance

These crosswalks enable organizations to leverage work across multiple frameworks, reducing compliance burden and promoting consistent global practices.

1. Introduction

1.1 Background and Context

Artificial intelligence has rapidly evolved from experimental technology to a fundamental component of modern infrastructure. AI systems now influence critical decisions in healthcare, finance, transportation, employment, education, criminal justice, and national security. This widespread adoption has brought both tremendous benefits and significant risks that require systematic management.

The original NIST AI Risk Management Framework (version 1.0), released in January 2023, provided foundational guidance for organizations seeking to manage AI-related risks. Since that release, the field has experienced rapid advancement, particularly in generative AI, foundation models, and autonomous systems. These developments have revealed new risk categories and highlighted the need for enhanced guidance.

This version “AI RMF Version 2026” represents a comprehensive update informed by:

- Early adoption experiences and stakeholder feedback from version 1.0
- Emerging risks from generative AI and large language models
- Development of international standards including ISO/IEC 42001 and the EU AI Act
- Research on adversarial machine learning and AI security
- Increased focus on AI supply chain risks and third-party dependencies
- Recognition of environmental and sustainability impacts

1.2 Scope and Applicability

This framework applies to all AI systems, defined as engineered or machine-based systems that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

In scope:

- Traditional machine learning systems (supervised, unsupervised, reinforcement learning)
- Deep Learning and Neural Networks
- Generative AI including large language models and multimodal systems
- Foundation models and general-purpose AI
- Autonomous and agentic AI systems
- Multi-agent systems and swarm intelligence
- Edge AI and embedded systems
- AI-enabled decision support systems

Out of scope:

- Simple rule-based systems without learning capabilities
- Traditional statistical analysis without predictive components
- Standard database queries and business intelligence dashboards

1.3 Framework Organization

The AI RMF 2026 is organized into several complementary components:

Component	Description
Core Framework	Four Functions (GOVERN, MAP, MEASURE, MANAGE) with Categories and Subcategories defining outcomes
Implementation Guide	Step-by-step procedures, templates, and practical examples for applying the framework
Profiles	Sector-specific and technology-specific adaptations (e.g., Healthcare Profile, GenAI Profile)
Crosswalks	Mappings to international standards and regulatory frameworks for harmonization
Appendices	Reference materials including glossary, risk scenarios, and assessment tools

1.4 Key Terminology

This section defines key terms used throughout the framework. For a comprehensive glossary, see Appendix A.

AI Actor: An entity involved in design, development, deployment, evaluation, or use of AI systems, including organizations, individuals, or automated systems.

AI System: An engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments.

Foundation Model: An AI model trained on broad data that can be adapted to a wide range of downstream tasks. Examples include large language models, vision transformers, and multimodal models.

Generative AI: AI systems capable of generating new content including text, images, audio, video, code, or other data. These systems learn patterns from training data to produce novel outputs.

Agentic AI: AI systems capable of autonomous action in pursuit of defined goals, including the ability to plan, execute actions, and adapt based on environmental feedback.

AI Bill of Materials (AI-BOM): A comprehensive inventory of all components, dependencies, and artifacts that comprise an AI system, including models, datasets, libraries, and third-party services.

Model Card: Documentation that provides transparent information about an AI model's development, capabilities, limitations, and intended use cases.

Trustworthy AI: AI systems that are valid and reliable, safe, secure, and resilient, accountable, and transparent, explainable, and interpretable, privacy-enhanced, and fair with harmful bias managed.

2. AI Risks and Impacts

2.1 Understanding AI Risks

AI risks differ from traditional technology risks in several fundamental ways. AI systems learn from data, make probabilistic decisions, can exhibit emergent behaviors, and may operate with varying degrees of autonomy. These characteristics create unique risk profiles that require specialized management approaches.

2.1.1 Categories of AI Risks

AI risks can be categorized into several overlapping dimensions:

- **Technical Risks:** Issues arising from system design, implementation, or operation including model errors, data quality problems, algorithmic failures, and technical debt.
- **Security Risks:** Threats to AI system confidentiality, integrity, and availability including adversarial attacks, data poisoning, model extraction, and backdoor vulnerabilities
- **Safety Risks:** Potential for AI systems to cause physical harm, property damage, or operational failures in critical systems.
- **Privacy Risks:** Unauthorized disclosure, inference, or misuse of personal information through AI systems
- **Fairness and Bias Risks:** Discriminatory outcomes or perpetuation of societal biases through AI decision-making
- **Accountability Risks:** Inability to determine responsibility when AI systems cause harm or make erroneous decisions.
- **Transparency and Explainability Risks:** Lack of understanding about how AI systems reach decisions, limiting trust and oversight.
- **Supply Chain Risks:** Dependencies on third-party models, data, or services that introduce vulnerabilities or compliance issues.
- **Environmental Risks:** Significant energy consumption and carbon emissions from AI model training and deployment

2.1.2 Emerging AI Risk Categories

AI RMF 2026 identifies several emerging risk categories that have become prominent since the release of version 1.0:

Generative AI Risks

- **Hallucinations:** Generation of plausible but factually incorrect or nonsensical outputs
- **Prompt Injection:** Malicious manipulation of system behavior through crafted inputs.
- **Data Leakage:** Unintended exposure of training data through model outputs
- **Synthetic Content Misuse:** Creation of deepfakes, misinformation, or harmful content
- **CBRN Information:** Potential to assist in creation of chemical, biological, radiological, or nuclear threats.

Agentic AI Risks

- **Goal Misalignment:** Autonomous agents pursuing objectives in unintended or harmful ways.
- **Emergent Behaviors:** Unexpected capabilities or actions arising from agent interactions.
- **Oversight Gaps:** Insufficient human monitoring of autonomous decision-making.
- **Cascading Failures:** Errors propagating through multi-agent systems.

2.2 Risk Taxonomy and Classification

The following table provides a comprehensive taxonomy of AI risks, organized by category, with severity indicators and mitigation priorities.

Category	Risk Type	Severity	Primary Mitigation
Technical Risks	Model Performance Degradation	High	Continuous monitoring and retraining
	Data Quality Issues	High	Robust data validation and governance
	System Integration Failures	Medium	Comprehensive testing and staged deployment
Security Risks	Adversarial Attacks	**Critical**	Adversarial training and input validation
	Data Poisoning	**Critical**	Secure data pipelines and provenance tracking
	Model Extraction	High	API rate limiting and watermarking
Safety Risks	Physical Harm	**Critical**	Safety-critical design and fail-safes
	Critical System Failures	**Critical**	Redundancy and graceful degradation
Privacy Risks	Personal Data Exposure	**Critical**	Privacy-preserving techniques and encryption

	Re-identification Attacks	High	De-identification and differential privacy
Fairness Risks	Discriminatory Outcomes	High	Bias testing and fairness metrics
	Disparate Impact	High	Diverse training data and regular audits
GenAI Risks	Hallucinations	Medium	Grounding techniques and fact-checking
	Prompt Injection	High	Input sanitization and output filtering
	Data Leakage	**Critical**	Training data curation and privacy audits
Agentic AI Risks	Goal Misalignment	**Critical**	Human-in-the-loop and value alignment
	Emergent Behaviors	High	Extensive testing and capability monitoring
Supply Chain Risks	Third-Party Model Vulnerabilities	High	Vendor assessment and AI-BOM
	Dependency Failures	Medium	Redundancy and fallback mechanisms
Environmental Risks	Excessive Energy Consumption	Medium	Efficient architecture and optimization

3. Core Framework: The Four Functions

The AI RMF 2026 Core consists of four Functions that represent the key activities for managing AI risks throughout the system lifecycle. These Functions provide a high-level strategic view that organizations can use to structure their AI risk management programs.

Function	Purpose and Key Activities
GOVERN	**Cultivate the culture of risk management and establish accountability.** Establish policies, assign roles, allocate resources, engage stakeholders, and integrate AI risk management into organizational governance
MAP	**Establish context and identify AI system characteristics.** Categorize AI systems, identify impacts, assess risks, and understand legal/regulatory requirements
MEASURE	**Quantify and track AI risks throughout lifecycle.** Define metrics, assess trustworthiness, monitor performance, and evaluate effectiveness of controls
MANAGE	**Respond to and mitigate identified risks.** Prioritize risks, implement controls, respond to incidents, and continuously improve risk posture

Document Structure Note

This is a comprehensive framework document. The complete document includes detailed guidance on all four Functions (GOVERN, MAP, MEASURE, MANAGE), implementation playbooks, sector-specific profiles, international standards crosswalks, and comprehensive appendices. This excerpt demonstrates the professional structure and formatting used throughout the full 150+ page framework.

Complete sections include:

Chapter 1: GOVERN Function

Complete coverage of all 6 GOVERN categories:

- GOVERN 1: Organizational AI Governance (1.1-1.4)
- GOVERN 2: Accountability and Responsibility (2.1)
- GOVERN 3: Workforce Diversity and Team Composition (3.1)
- GOVERN 4: Risk Management Culture (4.1)
- GOVERN 5: Oversight and Monitoring (5.1)
- GOVERN 6: Trustworthy AI Characteristics (6.1)

Includes detailed implementation guidance, all seven trustworthiness characteristics, ISO 42001 and ISO 27001 mappings, and comprehensive summary tables.

Chapter 2: MAP Function

Complete coverage of all 5 MAP categories:

- MAP 1: Context and Requirements (1.1-1.2)
- MAP 2: Categorize AI Systems (2.1)
- MAP 3: Impacts and Benefits (3.1-3.2)
- MAP 4: Risks and Impacts (4.1)
- MAP 5: Impact Assessment (5.1-5.2)

Includes risk categories, classification dimensions, stakeholder identification, and complete ISO mappings.

Chapter 3: MEASURE Function

Complete coverage of all 4 MEASURE categories:

- MEASURE 1: Appropriate Methods and Metrics (1.1-1.2)
- MEASURE 2: Data Quality (2.1)
- MEASURE 3: System Performance (3.1-3.2)
- MEASURE 4: Risk Tracking and Monitoring (4.1)

Includes trustworthiness metrics, data quality dimensions, measurement methods, and monitoring elements.

Chapter 4: MANAGE Function

Complete coverage of all 4 MANAGE categories:

- MANAGE 1: Risk Response (1.1-1.2)
- MANAGE 2: Incident Management (2.1-2.2)
- MANAGE 3: Communication and Transparency (3.1)
- MANAGE 4: Continuous Improvement (4.1-4.2)

This demonstration highlights the framework's professional formatting, comprehensive structure, and practical implementation focus that organizations need for AI governance.

Chapter 1-- GOVERN Function

AI RMF 2026 – ISO Standards Integrated Edition
January 2026

Overview

The GOVERN Function establishes and nurtures a culture of AI risk management throughout the organization. It emphasizes organizational structures, policies, processes, and accountability mechanisms that enable responsible AI development and deployment across all stages of the AI lifecycle.

GOVERN provides the foundation for all other functions by establishing leadership commitment, organizational culture, policies, and governance structures necessary for effective AI risk management.

GOVERN Function Structure

Category	Focus Area
GOVERN 1	Organizational AI Governance and Policies
GOVERN 2	Accountability and Responsibility
GOVERN 3	Workforce Diversity, Equity, Inclusion, and Accessibility (DEIA)
GOVERN 4	Organizational Culture and AI Risk Management
GOVERN 5	Oversight and Monitoring
GOVERN 6	Trustworthy AI Characteristics

GOVERN 1: Organizational AI Governance

Outcome: Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.

GOVERN 1.1: Legal and Regulatory Requirements

Organizations identify, track, and manage applicable legal and regulatory requirements for AI systems throughout their lifecycle.

Implementation Guidance:

- Establish compliance register tracking AI-related laws and regulations.
- Monitor regulatory developments (EU AI Act, state laws, sector-specific regulations)
- Assign compliance ownership for each requirement.
- Conduct regular compliance assessments.
- Document compliance evidence for audit purposes.

ISO/IEC 42001 Mapping:

- Clause 4.2: Understanding the needs and expectations of interested parties.
- Clause 6.3: Compliance obligations

ISO/IEC 27001 Mapping:

- Clause 4.2: Understanding interested parties.
- A.5.1: Policies for information security (applicable to AI)

GOVERN 1.2: Roles and Responsibilities

Clear assignment of roles, responsibilities, and authorities for AI governance across the organization.

Key Roles:

- Board/Executive Leadership: Strategic oversight and accountability
- Chief AI Officer (CAIO): Overall AI strategy and governance coordination
- Chief Risk Officer: AI risk assessment and management
- Chief Information Security Officer: AI security and resilience
- Data Protection Officer: Privacy and data governance
- AI Ethics Committee: Ethical review and fairness assessment
- AI Developers/Engineers: System design and implementation
- Business Units: AI deployment and operational monitoring

ISO/IEC 42001 Mapping:

- Clause 5.3: Organizational roles, responsibilities, and authorities

ISO/IEC 27001 Mapping:

- Clause 5.3: Organizational roles and responsibilities

GOVERN 1.3: Diversity, Equity, Inclusion, and Accessibility (DEIA)

AI design and development teams reflect diversity across multiple dimensions to reduce bias and improve outcomes.

Implementation Guidance:

- Establish DEIA goals for AI teams
- Implement inclusive hiring and retention practices
- Provide DEIA and bias awareness training
- Include diverse perspectives in AI design decisions
- Ensure accessibility throughout AI system design

ISO/IEC 42001 Mapping:

- Clause 6.1.3: AI impact assessment (considers fairness and inclusivity)
- Clause 7.2: Competence (includes diversity considerations)

GOVERN 1.4: Organizational AI Risk Management Culture
Foster a culture where identifying and addressing AI risks is encouraged, valued, and rewarded.

Implementation Guidance:

- Leadership demonstrates visible commitment to responsible AI
- Establish speak-up culture for AI concerns
- Reward identification and mitigation of AI risks
- Share lessons learned from AI incidents organization-wide
- Integrate AI risk awareness into performance evaluations

ISO/IEC 42001 Mapping:

- Clause 5.1: Leadership and commitment
- Clause 7.3: Awareness

GOVERN 2: Accountability and Responsibility

Outcome: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.

GOVERN 2.1: Accountability Structures

Establish clear accountability for AI system decisions, outcomes, and impacts throughout the lifecycle.

Implementation Guidance:

- Define decision authority at each AI lifecycle stage
- Document approval requirements for high-risk AI systems
- Establish escalation paths for AI risk issues
- Create accountability documentation (RACI matrix)

- Implement audit trails for key AI decisions

ISO/IEC 42001 Mapping:
- Clause 5.3: Organizational roles, responsibilities, and authorities
- Clause 8.1: Operational planning and control

ISO/IEC 27001 Mapping:
- Clause 5.3: Organizational roles

GOVERN 3: Workforce Diversity and Team Composition

Outcome: AI design, development, and deployment teams are diverse and include subject matter experts from across disciplines.

GOVERN 3.1: Diverse AI Teams

Build multidisciplinary teams with diverse backgrounds, expertise, and perspectives.

Team Composition:
- Technical experts: AI/ML engineers, data scientists, software developers
- Domain experts: Subject matter specialists for application area
- Social scientists: Ethicists, sociologists, psychologists
- Legal and compliance: Attorneys, regulatory specialists
- User representatives: End users and affected stakeholders

ISO/IEC 42001 Mapping:
- Clause 7.2: Competence

GOVERN 4: Risk Management Culture

Outcome: Organizational culture supports addressing AI risks effectively.

GOVERN 4.1: Training and Awareness
Ensure all AI stakeholders have appropriate training and awareness of AI risks and responsible practices.

Training Program Elements:
- AI fundamentals for non-technical staff
- Responsible AI principles and trustworthiness characteristics
- Bias identification and mitigation techniques
- Privacy and security for AI systems
- Incident reporting and response procedures
- Role-specific technical and governance training

ISO/IEC 42001 Mapping:
- Clause 7.2: Competence
- Clause 7.3: Awareness

ISO/IEC 27001 Mapping:
- Clause 7.2: Competence
- A.6.3: Awareness training

GOVERN 5: Oversight and Monitoring

Outcome: Organizational oversight and monitoring processes ensure AI systems are developed and deployed in accordance with policies and risk management practices.

GOVERN 5.1: Governance Bodies
Establish oversight bodies with appropriate authority, expertise, and independence.

Key Oversight Mechanisms:
- AI Governance Committee: Cross-functional oversight and policy decisions
- AI Ethics Review Board: Ethical assessment of high-risk systems
- Internal Audit: Independent assessment of AIMS effectiveness
- Management Review: Executive evaluation of AI governance
- External Audit: Third-party certification and validation

ISO/IEC 42001 Mapping:
- Clause 9.2: Internal audit
- Clause 9.3: Management review

ISO/IEC 27001 Mapping:
- Clause 9.2: Internal audit
- Clause 9.3: Management review

GOVERN 6: Trustworthy AI Characteristics

Outcome: Policies and procedures are in place to address trustworthy AI characteristics including validity, reliability, safety, security, resilience, accountability, transparency, explainability, interpretability, privacy enhancement, and fairness.

GOVERN 6.1: Trustworthy AI Policy
Establish comprehensive policies addressing all trustworthiness characteristics.

Seven Trustworthiness Characteristics:

1. Valid and Reliable
- Systems perform consistently and accurately for intended purposes
- Testing and validation procedures ensure fitness for use

2. Safe
- Systems do not pose unacceptable risk of harm
- Safety mechanisms prevent dangerous failures

3. Secure and Resilient
- Protected against unauthorized access and adversarial attacks
- Can recover from failures and continue operating

4. Accountable and Transparent
- Clear responsibility for system decisions and outcomes
- Information about capabilities, limitations, and operation available

5. Explainable and Interpretable
- Meaningful explanations of system behavior and decisions
- Users can understand how outputs were generated

6. Privacy-Enhanced
- Protects individual privacy and data rights
- Implements privacy-by-design principles

7. Fair - with Harmful Bias Managed
- Does not systematically disadvantage individuals or groups
- Bias identification and mitigation throughout lifecycle

ISO/IEC 42001 Mapping:
- Clause 5.2: AI management system policy

GOVERN Function: Complete Mapping Summary

AI RMF	Description	ISO 42001	ISO 27001
GOVERN 1.1	Legal and regulatory requirements	4.2, 6.3	4.2, A.5.1
GOVERN 1.2	Roles and responsibilities	5.3	5.3
GOVERN 1.3	DEIA in design	6.1.3, 7.2	7.2
GOVERN 1.4	Risk management culture	5.1, 7.3	5.1, 7.3
GOVERN 2.1	Accountability structures	5.3, 8.1	5.3
GOVERN 3.1	Diverse teams	7.2	7.2
GOVERN 4.1	Training and awareness	7.2, 7.3	7.2, A.6.3
GOVERN 5.1	Oversight bodies	9.2, 9.3	9.2, 9.3
GOVERN 6.1	Trustworthy AI policy	5.2	5.2

Chapter 2- MAP Function

AI RMF 2026 – ISO Integrated Edition
January 2026

Overview

The MAP Function establishes context by identifying business requirements, AI system capabilities, stakeholders, and risks. It provides the foundation for subsequent measurement and management activities by creating a comprehensive understanding of each AI system's operational environment and potential impacts.

MAP 1: Context and Requirements

Outcome: The context in which AI systems will be developed, deployed, and used is established, including legal, regulatory, and business requirements.

MAP 1.1: Mission and Stakeholders

Identify business purpose, define success criteria, and engage relevant stakeholders throughout the AI lifecycle.

Implementation:

- Document business objectives and use cases
- Identify all stakeholders: users, affected parties, decision-makers
- Establish stakeholder engagement mechanisms
- Define success metrics aligned with trustworthiness

ISO 42001: 4.2, 4.4 | **ISO 27001:** 4.2

MAP 1.2: AI Capabilities and Scope

Define what the AI system can and cannot do, including technical capabilities and limitations.

ISO 42001: 8.1 | **ISO 27001:** 4.3

MAP 2: Categorize AI Systems

Outcome: AI systems are categorized based on characteristics, intended use, and potential impacts.

MAP 2.1: AI Type Classification

Classify by technical approach, capability level, autonomy, and deployment model.

Classification Dimensions:

- Technical: supervised, unsupervised, reinforcement learning
- Capability: narrow AI, general-purpose, foundation model, agentic

- Autonomy: fully automated, semi-autonomous, human-in-loop
- Deployment: on-premises, cloud, edge, hybrid

ISO 42001: 6.1.3, 8.1 | **ISO 27001:** A.8.1

MAP 3: Impacts and Benefits

Outcome: AI system benefits and potential negative impacts are identified and documented.

MAP 3.1: Expected Benefits

Document intended positive outcomes for individuals, organizations, and society.

ISO 42001: 6.1.3 | **ISO 27001:** 6.1.1

MAP 3.2: Potential Harms

Identify negative impacts across dimensions: fairness, privacy, safety, security, transparency.

ISO 42001: 6.1.2, 6.1.3 | **ISO 27001:** 6.1.2

MAP 4: Risks and Impacts

Outcome: AI risks and related impacts are identified and documented.

MAP 4.1: Risk Identification

Systematically identify AI risks across categories: technical, fairness, security, privacy, safety, operational, legal.

Risk Categories:

- Technical: performance degradation, model drift, hallucinations
- Fairness: discriminatory outcomes, bias amplification
- Security: adversarial attacks, model theft, data poisoning
- Privacy: data exposure, re-identification risks
- Safety: physical harm, critical infrastructure impacts
- Operational: system failures, integration issues
- Legal/Regulatory: non-compliance, liability

ISO 42001: 6.1.2 | **ISO 27001:** 6.1.2

MAP 5: Impact Assessment

Outcome: Impacts to individuals, groups, communities, organizations, and society are assessed and documented.

MAP 5.1: Individual and Group Impacts

Assess impacts on individuals and demographic groups, including potential for discrimination.

ISO 42001: 6.1.3 | **ISO 27001:** A.5.30

MAP 5.2: Societal and Environmental Impacts

Assess broader societal consequences, including environmental, cultural, and community impacts.

ISO 42001: 6.1.3 | **ISO 27001:** 4.2

MAP Function: Complete Mapping Summary

AI RMF	Description	ISO 42001	ISO 27001
MAP 1.1	Mission and stakeholders	4.2, 4.4	4.2
MAP 1.2	AI capabilities and scope	8.1	4.3
MAP 2.1	AI type classification	6.1.3, 8.1	A.8.1
MAP 3.1	Expected benefits	6.1.3	6.1.1
MAP 3.2	Potential harms	6.1.2, 6.1.3	6.1.2
MAP 4.1	Risk identification	6.1.2	6.1.2
MAP 5.1	Individual/group impacts	6.1.3	A.5.30
MAP 5.2	Societal impacts	6.1.3	4.2

Chapter 3- MEASURE Function

AI RMF 2026 - Integrated Edition
January 2026

Overview

The MEASURE Function employs quantitative and qualitative methods to assess AI system trustworthiness, capabilities, and impacts. It establishes metrics, test methodologies, and ongoing monitoring to verify that AI systems perform as intended and risks are appropriately managed.

MEASURE 1: Appropriate Methods and Metrics

Outcome: Appropriate methods and metrics are identified and applied to measure AI system trustworthiness.

MEASURE 1.1: Trustworthiness Metrics

Define metrics for each trustworthiness characteristic: validity, reliability, safety, security, resilience, accountability, transparency, explainability, interpretability, privacy, fairness.

Example Metrics:

- Validity: accuracy, precision, recall, F1 score
- Fairness: demographic parity, equalized odds, disparate impact ratio
- Security: adversarial robustness, attack success rate
- Privacy: k-anonymity, differential privacy epsilon
- Explainability: SHAP values, LIME scores, feature importance

ISO 42001: 9.1.1 | **ISO 27001:** 9.1

MEASURE 1.2: Measurement Methods

Select appropriate quantitative and qualitative measurement approaches.

Methods:

- Automated testing and evaluation
- Human evaluation and expert review
- Red team exercises and adversarial testing
- User feedback and satisfaction surveys
- External audits and third-party assessments

ISO 42001: 8.2.3, 9.1 | **ISO 27001:** 9.1, A.8.29

MEASURE 2: Data Quality

Outcome: AI system test datasets, training data, and operational data quality are evaluated.

MEASURE 2.1: Dataset Representativeness

Verify training and test data represent the deployment environment and affected populations.

Quality Dimensions:

- Accuracy: correct and error-free
- Completeness: no critical missing values
- Consistency: uniform across sources
- Timeliness: current and up-to-date
- Representativeness: reflects real-world diversity
- Relevance: appropriate for intended use

ISO 42001: 8.2.3 | **ISO 27001:** A.8.11

MEASURE 3: System Performance

Outcome: AI system performance is evaluated and documented.

MEASURE 3.1: Technical Performance

Measure accuracy, latency, throughput, resource utilization, and other technical metrics.

ISO 42001: 8.2.3, 9.1 | **ISO 27001:** A.8.6

MEASURE 3.2: Trustworthiness Evaluation

Assess all seven trustworthiness characteristics systematically.

ISO 42001: 8.2.3 | **ISO 27001:** A.8.7

MEASURE 4: Risk Tracking and Monitoring

Outcome: Mechanisms are in place to track and monitor AI risks over time.

MEASURE 4.1: Ongoing Monitoring

Implement continuous monitoring of AI system performance, data quality, and risk indicators.

Monitoring Elements:

- Model performance degradation detection
- Data drift and distribution shift monitoring
- Fairness metric tracking across demographic groups
- Security event logging and analysis
- User feedback and complaint tracking
- Incident and near-miss reporting

ISO 42001: 9.1 | **ISO 27001:** 9.1

MEASURE Function: Complete Mapping Summary

AI RMF	Description	ISO 42001	ISO 27001
MEASURE 1.1	Trustworthiness metrics	9.1.1	9.1
MEASURE 1.2	Measurement methods	8.2.3, 9.1	9.1, A.8.29
MEASURE 2.1	Dataset representativeness	8.2.3	A.8.11
MEASURE 3.1	Technical performance	8.2.3, 9.1	A.8.6
MEASURE 3.2	Trustworthiness evaluation	8.2.3	A.8.7
MEASURE 4.1	Ongoing monitoring	9.1	9.1

Chapter 4- MANAGE Function

AI RMF 2026 - Integrated Edition
January 2026

Overview

The MANAGE Function allocates resources to mapped and measured AI risks and responds to identified incidents. It ensures that risks are treated appropriately, incidents are handled effectively, and continuous improvement mechanisms are in place.

MANAGE 1: Risk Response

Outcome: AI risks are prioritized and managed according to risk management strategies.

MANAGE 1.1: Risk Treatment Strategy

Document and implement risk response strategies for identified AI risks.

Risk Treatment Options:

- Avoid: eliminate the risk by not pursuing the activity
- Reduce: implement controls to mitigate likelihood or impact
- Transfer: share risk through insurance, contracts, or partnerships
- Accept: informed decision to retain risk within tolerance

ISO 42001: 6.1.4 | **ISO 27001:** 6.1.3

MANAGE 1.2: Control Implementation

Implement technical and organizational controls to manage AI risks.

Control Categories:

- Technical: model architecture, data processing, security measures
- Organizational: policies, procedures, training programs
- Physical: infrastructure security, access controls
- Legal: contracts, terms of use, regulatory compliance

ISO 42001: 8.1 | **ISO 27001:** 6.1.3, Annex A

MANAGE 2: Incident Management

Outcome: AI incidents are identified, documented, managed, and used to improve trustworthiness.

MANAGE 2.1: Incident Response

Establish and implement AI incident response procedures.

Incident Response Phases:
- Detection: identify and report incidents
- Triage: assess severity and classify incident type
- Containment: limit impact and prevent escalation
- Investigation: root cause analysis
- Remediation: fix underlying issues
- Recovery: restore normal operations
- Post-incident review: document lessons learned

ISO 42001: 8.2.5 | **ISO 27001:** A.5.24, A.5.26

MANAGE 2.2: Incident Documentation

Maintain comprehensive records of AI incidents for analysis and improvement.

ISO 42001: 8.2.5, 7.5 | **ISO 27001:** A.5.28

MANAGE 3: Communication and Transparency

Outcome: Information about AI systems and their risks is communicated to stakeholders.

MANAGE 3.1: Stakeholder Communication

Provide appropriate information to stakeholders about AI system capabilities, limitations, and risks.

Communication Elements:
- System purpose and intended use
- Known limitations and failure modes
- Data sources and training methodology
- Performance metrics and testing results
- Human oversight and appeal mechanisms
- Privacy practices and data handling

ISO 42001: 7.4 | **ISO 27001:** 7.4

MANAGE 4: Continuous Improvement

Outcome: Organizational practices incorporate lessons learned from AI measurement and management activities.

MANAGE 4.1: Improvement Process

Establish systematic processes for continuous improvement of AI systems and governance.

Improvement Mechanisms:

- Regular review of AI system performance and trustworthiness
- Integration of lessons learned from incidents
- Updates based on emerging research and best practices
- Stakeholder feedback incorporation
- Audit findings remediation
- Model retraining and updating procedures

ISO 42001: 10.2 | **ISO 27001:** 10.2

MANAGE 4.2: Lessons Learned

Document and share lessons from AI experiences across the organization.

ISO 42001: 10.1, 10.2 | **ISO 27001:** 10.1

MANAGE Function: Complete Mapping Summary

AI RMF	Description	ISO 42001	ISO 27001
MANAGE 1.1	Risk treatment strategy	6.1.4	6.1.3
MANAGE 1.2	Control implementation	8.1	6.1.3, Annex A
MANAGE 2.1	Incident response	8.2.5	A.5.24, A.5.26
MANAGE 2.2	Incident documentation	8.2.5, 7.5	A.5.28
MANAGE 3.1	Stakeholder communication	7.4	7.4
MANAGE 4.1	Improvement process	10.2	10.2
MANAGE 4.2	Lessons learned	10.1, 10.2	10.1

1. Understanding the Three-Standard Integration

1.1 Why Integration Matters

Organizations deploying AI systems today must navigate multiple standards simultaneously. This framework solves that challenge by providing unified guidance that satisfies AI RMF 2026, ISO 42001, and ISO 27001 requirements through a single implementation effort.

The Three Standards:

Standard	Type	Purpose	Certification
AI RMF 2026	Voluntary guidance	AI risk management practices	No (assessment only)
ISO 42001	International standard	AI management system	Yes (3-year cycle)
ISO 27001	International standard	Information security	Yes (3-year cycle)

1.2 Integration Methodology

This framework uses three integration layers:

Layer	Description
Structural Alignment	AI RMF GOVERN/MAP/MEASURE/MANAGE aligns with ISO 42001 PDCA (Plan-Do-Check-Act) and ISO 27001 ISMS structure
Clause-Level Mapping	Every AI RMF Category explicitly references ISO 42001 clauses and ISO 27001 Annex A controls
Evidence Generation	Implementation guidance shows how to create artifacts satisfying all three standards simultaneously

1.3 PDCA Alignment with NIST Functions

The NIST functions map directly to ISO's Plan-Do-Check-Act cycle:

NIST Function	ISO 42001 PDCA	ISO 27001 Phase	Key Activities
GOVERN	PLAN	Establish	Policy, leadership, planning, resources
MAP	PLAN	Plan	Context, risk assessment, impact assessment
MEASURE	CHECK	Monitor & Review	Metrics, monitoring, audit, management review
MANAGE	DO + ACT	Implement & Improve	Controls, incident response, continual improvement

2. ISO/IEC 42001:2023 Structure and AI RMF Alignment

2.1 ISO 42001 Clause Overview

ISO 42001 consists of 10 main clauses (Clauses 4-10 are normative requirements):

Clause	Title	AI RMF Alignment	Key Requirements
4	Context	GOVERN, MAP	Understanding organization, stakeholders, AIMS scope
5	Leadership	GOVERN	Top management commitment, AI policy, roles
6	Planning	GOVERN, MAP	Risk assessment, impact assessment, objectives
7	Support	GOVERN	Resources, competence, awareness, communication
8	Operation	MAP, MANAGE	Operational planning, AI lifecycle, change control
9	Performance evaluation	MEASURE	Monitoring, measurement, audit, management review
10	Improvement	MANAGE	Nonconformity, corrective action, continual improvement

3. ISO 27001:2022 Annex A Controls for AI Systems

3.1 Control Categories and AI Extensions

ISO 27001 Annex A contains 93 controls across four categories. The following shows key controls requiring AI-specific implementation:

Section	Category	Key AI Controls	AI-Specific Considerations
A.5	Organizational (37)	A.5.1 Policies, A.5.9 Asset inventory, A.5.23 Cloud services	AI policy, model inventory, AI-BOM, ML platform security
A.6	People (8)	A.6.2 Awareness, A.6.3 Sanctions	AI ethics training, responsible use, sanctions for misuse
A.7	Physical (14)	A.7.4 Monitoring, A.7.14 Disposal	AI infrastructure monitoring, secure model/data disposal

A.8	Technological (34)	A.8.8 Backup, A.8.16 Monitoring, A.8.24 Cryptography	Model versioning, inference monitoring, model encryption

4. Comprehensive NIST-ISO Crosswalk

4.1 GOVERN Function Mappings

The following table maps AI RMF GOVERN categories to ISO 42001 clauses and ISO 27001 controls:

AI RMF Category	ISO 42001 Clause	ISO 27001 Control	Alignment Type
GOVERN 1: Policies & Procedures	5.2 AI Policy, 6.1 Actions	A.5.1 Information security policies	Direct
GOVERN 1.1: Legal & Regulatory	4.2 Understanding needs, 6.3 Compliance	A.5.31 Legal requirements	Direct
GOVERN 1.2: Roles & Responsibilities	5.3 Roles, authorities	A.5.2 Information security roles	Direct
GOVERN 1.3: Diversity & Inclusion	7.2 Competence, 6.1.3 Impact assessment	A.6.2 Awareness training	Complementary
GOVERN 1.4: Organizational Culture	5.1 Leadership commitment	A.5.1 Policies, A.6.2 Awareness	Direct
GOVERN 1.5: Oversight Functions	9.2 Internal audit, 9.3 Management review	A.5.35 Independent review	Direct

4.2 MAP Function Mappings

AI RMF Category	ISO 42001 Clause	ISO 27001 Control	Alignment Type
MAP 1: Context & Requirements	4.1 Organization context, 4.4 AIMS scope	A.5.7 Threat intelligence	Direct
MAP 1.1: Mission & Stakeholders	4.2 Stakeholder needs, 8.1 Planning	A.5.9 Inventory	Direct
MAP 1.2: AI Capabilities	6.1.3 AI system impact assessment	A.5.9 Asset inventory	Direct
MAP 2: Risk Assessment	6.1.2 AI risk assessment	6.1.2 Information security risk assessment	Direct
MAP 2.1: Risk Identification	6.1.2.1 Risk identification	6.1.2 a) Risk identification	Direct
MAP 2.2: Risk Analysis	6.1.2.2 Risk analysis	6.1.2 b) Risk analysis	Direct
MAP 2.3: Risk Prioritization	6.1.2.3 Risk evaluation	6.1.2 c) Risk evaluation	Direct

4.3 MEASURE Function Mappings

AI RMF Category	ISO 42001 Clause	ISO 27001 Control	Alignment Type
MEASURE 1: Test & Validation	8.2 AI system lifecycle, 9.1 Monitoring	A.8.29 Testing	Direct
MEASURE 1.1: Validation	8.2.3 AI system validation	A.8.29 Security testing	Direct
MEASURE 1.2: Error Tracking	10.1 Nonconformity	A.8.16 Monitoring activities	Direct
MEASURE 2: Metrics	9.1.1 Performance metrics	A.8.16 Monitoring	Direct
MEASURE 2.1: Trustworthiness	6.1.3 Impact assessment indicators	A.8.16 Monitoring activities	Complementary
MEASURE 3: Monitoring	9.1 Monitoring & measurement	A.8.16 Monitoring activities	Direct

4.4 MANAGE Function Mappings

AI RMF Category	ISO 42001 Clause	ISO 27001 Control	Alignment Type
MANAGE 1: Risk Response	6.1.4 AI risk treatment	6.2 Information security risk treatment	Direct
MANAGE 1.1: Risk Prioritization	6.1.4 Treatment selection	6.1.3 Risk treatment	Direct
MANAGE 1.2: Risk Treatment	8.1 Operational controls	A.8 Technological controls	Direct
MANAGE 2: Incident Response	8.2.5 Incident management	A.5.24-A.5.28 Incident management	Direct
MANAGE 2.1: Incident Plan	8.2.5 Planning	A.5.26 Response planning	Direct
MANAGE 3: Disclosure	7.4 Communication	A.5.6 Contact with authorities	Complementary
MANAGE 4: Continuous Improvement	10.2 Continual improvement	10.2 Continual improvement	Direct

5. ISO 42001 Certification Readiness

5.1 Certification Process

ISO 42001 certification follows a two-stage audit process:

Stage	Focus	Key Activities	Typical Duration
Stage 1	Documentation Review	Review AIMS scope, policy, procedures, risk assessment	1-3 days
Stage 2	Implementation Verification	Verify controls, interview staff, test processes, review evidence	3-7 days
Surveillance	Ongoing Compliance	Annual audits to verify AIMS maintenance and improvement	1-2 days annually
Recertification	Full Re-Assessment	Complete re-audit at end of 3-year cycle	Same as initial

5.2 Evidence Requirements by Clause

The following evidence from this AI RMF implementation supports ISO 42001 certification:

ISO Clause	Required Evidence	NIST Source	Certification Notes
4 Context	Context analysis, stakeholder register, AIMS scope	GOVERN 1.1, MAP 1.1	Must show evidence of annual review
5 Leadership	AI policy (approved), organizational chart with roles	GOVERN 1, 1.2	Top management approval required
6 Planning	Risk assessment, impact assessment, objectives with KPIs	MAP 2, MEASURE 2	Must demonstrate risk-based approach
7 Support	Competency matrix, training records, communication plan	GOVERN 1.3, 1.4	Evidence of awareness campaign needed
8 Operation	Lifecycle procedures, change control, AI system register	MAP 1.2, MANAGE 1.2	Must cover full AI lifecycle
9 Performance	Monitoring logs, audit reports, management review minutes	MEASURE 3, GOVERN 1.5	Annual management review required
10 Improvement	Corrective action records, improvement register	MANAGE 4	Must show closed-loop improvement

6. Integrated Implementation Guide

Section 6.1: Implementation Pathways

Complete Guide to AI RMF & ISO Integration

Introduction

Organizations approach AI governance from different starting points. This section provides detailed implementation pathways tailored to your current state, with realistic timelines, resource requirements, and step-by-step guidance.

Selecting Your Implementation Pathway

Use the decision tree below to identify which pathway best fits your organization:

Current State	Recommended Pathway	Expected Timeline
No existing frameworks; starting AI governance from scratch	Pathway 1: Greenfield Implementation	12-18 months to ISO 42001/27001 dual certification
Have ISO 27001 certification; adding AI governance	Pathway 2: ISO 27001 Extension	6-9 months to ISO 42001 certification
Implementing NIST AI RMF; want ISO certification	Pathway 3: AI RMF to ISO Bridge	9-12 months to dual certification
Have multiple frameworks (e.g., ISO 27001 + sector frameworks)	Pathway 4: Multi-Framework Consolidation	6-12 months depending on existing coverage

Pathway 1: Greenfield Implementation

Starting Point: No existing formal AI governance or ISO certifications

Target: ISO 42001 and ISO 27001 dual certification with AI RMF implementation

Timeline: 12-18 months

Phase 1: Foundation (Months 1-3)

Objectives:

- Establish governance structure and leadership commitment
- Define AIMS and ISMS scope
- Build core team and assign roles
- Create AI system inventory

Key Activities:

Week	Activity	Deliverable	Resources
1-2	Executive workshop on AI governance, Secure executive sponsorship	Executive commitment letter, Budget approval	Executive team, External consultant (optional)
3-4	Define governance structure, Appoint AI Risk Officer, Form AI governance committee	Governance charter, RACI matrix	Legal, Risk, IT, Business leads
5-6	Conduct AI system discovery, Create initial inventory	AI system register	IT team, Business units, 2-3 FTE
7-8	Define AIMS and ISMS scope, Document organizational context	Scope statement, Context analysis	Governance team, 1-2 FTE
9-12	Develop integrated AI policy, Identify stakeholders, Document compliance obligations	AI Management System Policy, Stakeholder register, Compliance register	Legal, Compliance, Risk, 2 FTE

Resources Required:

- **Team:** Program Manager (1 FTE), AI Risk Officer (0.5 FTE), Legal/Compliance (0.25 FTE), IT/Security (0.5 FTE)
- **Budget:** $50,000-$100,000 (consulting, tools, training)
- **Skills:** ISO standards knowledge, AI/ML basics, Risk management, Project management

Phase 2: Risk Assessment (Months 4-6)

Objectives:

- Complete AI risk assessments for all systems
- Conduct AI impact assessments
- Perform information security risk assessment
- Develop risk treatment plans

Week	Activity	Deliverable	Resources
13-16	Develop risk assessment methodology, Create risk criteria and appetite	Risk assessment procedure, Risk criteria document	Risk team, 2 FTE
17-20	Conduct AI risk assessments, Identify technical, fairness, privacy, safety risks	Risk register with 50-100+ risks	Risk analysts, AI experts, 3 FTE
21-23	Perform AI impact assessments, Evaluate fairness, privacy, accessibility impacts	Impact assessments for high-risk systems	Ethics team, Domain experts, 2 FTE
24-26	Conduct ISO 27001 information security risk assessment	Information security risk register	Security team, 2 FTE

Resources Required:

- **Team:** Risk Manager (1 FTE), AI Risk Analysts (2 FTE), Security Analyst (1 FTE), AI Ethics specialist (0.5 FTE)
- **Budget:** $75,000-$150,000 (risk assessment tools, workshops, external expertise)
- **Skills:** Risk assessment, AI/ML expertise, Security, Ethics, Stakeholder engagement

Phase 3: Control Implementation (Months 7-12)

Objectives:

- Implement risk treatment controls
- Deploy technical controls for AI security
- Establish monitoring and measurement
- Create documentation and evidence repository

Key Activities by Month:

Month 7-8: Documentation and Procedures

- Develop AI lifecycle procedures (design, develop, deploy, monitor)
- Create data governance framework
- Document AI supply chain management procedures
- Establish document control system

Month 9-10: Technical Controls

- Implement access controls for AI systems
- Deploy model monitoring and drift detection
- Establish AI security testing (adversarial testing)
- Implement logging and audit trails
- Set up incident response procedures

Month 11-12: Training and Evidence

- Deliver organization-wide AI awareness training
- Conduct role-specific AI training
- Organize evidence repository by ISO clause
- Document control implementation evidence

Resources Required:

- **Team:** Implementation Manager (1 FTE), AI Engineers (2-3 FTE), Security Engineers (2 FTE), Data Governance (1 FTE), Training Coordinator (0.5 FTE)
- **Budget:** $150,000-$300,000 (tools, infrastructure, training)
- **Skills:** MLOps, Security engineering, Documentation, Training development

Phase 4: Validation and Improvement (Months 13-15)

Objectives:

- Conduct internal audits
- Perform management review
- Address gaps and nonconformities
- Prepare for certification audit

Activity	Details	Timeline
Internal Audit	Full audit of ISO 42001 and ISO 27001 requirements, Test controls and procedures, Document findings	Month 13 (3-4 weeks)
Gap Remediation	Address nonconformities, Implement corrective actions, Collect additional evidence	Month 14 (4-6 weeks)
Management Review	Present AIMS performance to leadership, Review objectives and KPIs, Approve for certification	Month 15 (1 week)
Pre-Assessment	Optional readiness review by certification body, Identify any remaining gaps	Month 15 (optional)

Resources Required:

- **Team:** Lead Auditor (1 FTE), Audit team (2-3 people), Management team for review
- **Budget:** $25,000-$50,000 (internal audit, pre-assessment)
- **Skills:** ISO auditing, Root cause analysis, Corrective action

Phase 5: Certification (Months 16-18)

Objectives:

- Complete Stage 1 and Stage 2 audits
- Address any audit findings
- Achieve dual ISO 42001/27001 certification

Audit Stage	Focus	Duration
Stage 1: Documentation Review	Review AIMS and ISMS documentation, Verify scope and readiness, Identify documentation gaps	1-2 days on-site, 2-4 weeks gap closure
Stage 2: Implementation Audit	Audit all ISO 42001 and 27001 requirements, Interview personnel, Review evidence, Test controls	3-5 days on-site for mid-size org
Nonconformity Closure	Address any major/minor NCs, Submit evidence to auditor, Verification of corrections	2-4 weeks depending on findings
Certification Decision	Certification body reviews audit report, Issues certificates (3-year validity)	2-4 weeks after NC closure

Resources Required:

- **Team:** Audit coordinator (0.5 FTE), Subject matter experts for interviews
- **Budget:** $40,000-$80,000 (certification body fees for dual audit)
- **Skills:** Audit preparation, Evidence presentation

Pathway 1: Complete Resource Summary

Phase	Duration	Team Size	Budget
Phase 1: Foundation	3 months	2-3 FTE	$50K-$100K
Phase 2: Risk Assessment	3 months	4-5 FTE	$75K-$150K
Phase 3: Implementation	6 months	6-8 FTE	$150K-$300K
Phase 4: Validation	3 months	3-4 FTE	$25K-$50K
Phase 5: Certification	3 months	2 FTE	$40K-$80K
TOTAL	18 months	Peak: 6-8 FTE	$340K-$680K

Pathway 2: ISO 27001 Extension

Starting Point: Current ISO 27001 certification, adding AI governance

Target: Add ISO 42001 certification while maintaining ISO 27001

Timeline: 6-9 months

Key Advantages:

- Existing ISMS provides foundation (30-40% of ISO 42001 requirements)
- Documentation and audit processes already established
- Management system maturity reduces learning curve
- Can leverage ISO 27001 Annex A controls for AI systems

Implementation Phases

Phase 1: Gap Assessment (Month 1)

- Compare current ISMS against ISO 42001 requirements
- Identify AI-specific gaps in existing controls
- Map current security controls to AI systems
- Deliverable: Gap analysis report, Implementation roadmap

Phase 2: AI-Specific Requirements (Months 2-3)

- Expand ISMS scope to cover AI systems
- Create AI system inventory
- Conduct AI risk assessments (ISO 42001 Clause 6.1.2)
- Perform AI impact assessments (ISO 42001 Clause 6.1.3)
- Deliverable: AI risk register, Impact assessments, AI-specific policies

Phase 3: AI Lifecycle Controls (Months 4-5)

- Implement AI lifecycle procedures (ISO 42001 Clause 8.2)
- Establish data governance for AI (ISO 42001 Clause 8.2.1)
- Deploy AI monitoring and drift detection
- Implement AI supply chain management (ISO 42001 Clause 8.3)
- Deliverable: AI procedures, Monitoring system, AI-BOM

Phase 4: Integration and Audit (Months 6-9)

- Update existing documentation with AI components
- Conduct combined internal audit (ISO 27001 + 42001)
- Management review of integrated system
- ISO 42001 certification audit
- Deliverable: ISO 42001 certificate

Pathway 2: Resource Summary

Phase	Duration	Team Size	Budget
Gap Assessment	1 month	2 FTE	$15K-$25K
AI Requirements	2 months	3-4 FTE	$50K-$100K
AI Lifecycle Controls	2 months	4-5 FTE	$75K-$125K
Integration and Audit	4 months	2-3 FTE	$40K-$60K
TOTAL	9 months	Peak: 4-5 FTE	$180K-$310K

Pathway 3: AI RMF to ISO Bridge

Starting Point: Implementing NIST AI RMF, want ISO certification

Target: ISO 42001 and ISO 27001 dual certification

Timeline: 9-12 months

Key Advantages:

- AI RMF content maps 80-90% to ISO 42001 requirements
- AI risk management already understood
- Focus on formalizing management system and documentation
- Add ISO 27001 information security foundation

Critical Gap Areas to Address

ISO Requirement	Typical AI RMF Gap	Action Needed
Formal AIMS scope (ISO 42001 4.4)	AI RMF guidance informal	Document formal scope statement with boundaries, exclusions, justifications
Management system policy (ISO 42001 5.2)	May have AI principles but not formal policy	Create ISO-compliant policy with all required elements, executive approval
Internal audit program (ISO 42001 9.2)	May lack formal audit program	Establish audit program, train auditors, conduct audits, document results
Management review (ISO 42001 9.3)	Reviews may not follow ISO structure	Formalize management review with required inputs/outputs, document minutes

Document control (ISO 42001 7.5)	Documentation may be informal	Implement document control procedure, master list, version control
ISO 27001 ISMS	AI focus; may lack comprehensive information security	Implement ISO 27001 Annex A controls, conduct info security risk assessment

Implementation Phases

Phase 1: Formalization (Months 1-3)

- Map existing AI RMF work to ISO 42001 requirements
- Create formal AIMS scope and policy
- Establish document control system
- Formalize governance structure with ISO-compliant roles

Phase 2: ISO 27001 Foundation (Months 4-6)

- Conduct information security risk assessment
- Implement ISO 27001 Annex A controls for AI systems
- Create Statement of Applicability (SoA)
- Extend monitoring to cover information security

Phase 3: Management System Maturity (Months 7-9)

- Establish internal audit program
- Conduct first internal audits
- Implement corrective action process
- Hold formal management review

Phase 4: Certification (Months 10-12)

- Organize evidence repository
- Conduct certification audits (Stage 1 and 2)
- Achieve dual certification

Pathway 3: Resource Summary

Phase	Duration	Team Size	Budget
Formalization	3 months	2-3 FTE	$40K-$75K
ISO 27001 Foundation	3 months	3-4 FTE	$75K-$125K
Management System Maturity	3 months	2-3 FTE	$50K-$75K
Certification	3 months	2 FTE	$40K-$60K
TOTAL	12 months	Peak: 3-4 FTE	$205K-$335K

Pathway 4: Multi-Framework Consolidation

Starting Point: Multiple existing frameworks (e.g., ISO 27001 + sector frameworks like HIPAA, SOC 2, NIST CSF)

Target: Consolidated AI governance aligned to ISO 42001

Timeline: 6-12 months depending on existing framework maturity

Key Advantages:

- Significant existing governance infrastructure
- Mature risk management and audit capabilities
- Can leverage existing controls for AI-specific adaptations
- Opportunity to streamline and reduce duplication

Common Framework Combinations

Current Frameworks	Coverage Assessment	Integration Approach
ISO 27001 + HIPAA	Strong security, privacy controls. Need AI-specific lifecycle, fairness	Extend ISMS to AI, add ISO 42001 AI lifecycle and impact assessment. HIPAA privacy maps well to AI
ISO 27001 + SOC 2	Strong controls, risk management. Need AI governance, bias management	Map SOC 2 controls to ISO 42001, add AI-specific controls, formalize AI governance structure
NIST CSF + ISO 27001	Strong cybersecurity foundation. Need AI-specific risk management	Add NIST AI RMF on top of CSF, formalize for ISO 42001, integrate AI into existing risk programs
Industry frameworks (e.g., PCI-DSS, FISMA)	Strong compliance, security. Need AI lifecycle, transparency	Map existing controls to ISO standards, add AI-specific requirements, create unified governance

Implementation Approach

Step 1: Framework Mapping and Gap Analysis (Month 1-2)

- Map all existing frameworks to ISO 42001 and ISO 27001
- Identify overlaps and redundancies
- Identify AI-specific gaps not covered by existing frameworks
- Create unified control matrix

Step 2: Consolidation Strategy (Month 2-3)

- Design integrated governance structure
- Streamline documentation (single policy library)
- Unified risk management approach
- Consolidated audit and compliance calendar

Step 3: AI-Specific Additions (Month 3-6)

- Implement AI risk and impact assessments
- Add AI lifecycle management (ISO 42001 Clause 8.2)
- Establish AI monitoring and drift detection
- Add fairness and bias controls
- Implement AI supply chain management

Step 4: Integration and Optimization (Month 6-9)

- Merge documentation into unified system
- Train team on integrated approach
- Conduct combined internal audits
- Demonstrate efficiency gains to stakeholders

Step 5: Certification (Month 9-12)

- ISO 42001 certification audit
- Maintain existing certifications (ISO 27001, etc.)
- Establish ongoing surveillance audit schedule

Pathway 4: Resource Summary

Phase	Duration	Team Size	Budget
Framework Mapping	2 months	2-3 FTE	$30K-$50K
Consolidation Strategy	1 month	2 FTE	$20K-$30K
AI-Specific Additions	3 months	3-4 FTE	$75K-$100K
Integration/Optimization	3 months	2-3 FTE	$40K-$60K
Certification	3 months	1-2 FTE	$30K-$50K
TOTAL	12 months	Peak: 3-4 FTE	$195K-$290K

Pathway Comparison and Selection Guide

Quick Comparison Table

Pathway	Timeline	Peak Team	Budget Range	Best For
1: Greenfield	12-18 months	6-8 FTE	$340K-$680K	Starting from scratch, building comprehensive program
2: ISO 27001 Extension	6-9 months	4-5 FTE	$180K-$310K	Have ISMS, adding AI governance
3: AI RMF to ISO	9-12 months	3-4 FTE	$205K-$335K	Implementing AI RMF, want certification
4: Multi-Framework	6-12 months	3-4 FTE	$195K-$290K	Multiple frameworks, seeking consolidation

Success Factors Across All Pathways

Leadership and Commitment

- Executive sponsorship and visible support
- Adequate budget and resources
- Patience for cultural and process change

Team Composition

- Blend of AI/ML technical expertise
- Risk management and compliance knowledge
- ISO standards experience (consider consultants if lacking)
- Project management capabilities

Realistic Expectations

- Certification is a journey, not a destination
- Initial audit findings are normal - plan for remediation time
- Continuous improvement required after certification
- Surveillance audits every 6-12 months

Tool Selection

- GRC platform for documentation and compliance tracking

- AI monitoring and observability tools
- Model registry and versioning system
- Evidence repository structure

Decision Tree: Selecting Your Pathway

Use this decision tree to determine the optimal pathway:

1. **Do you have ISO 27001 certification?**
   → YES: Choose Pathway 2 (ISO 27001 Extension) - 6-9 months
   → NO: Continue to question 2

2. **Are you currently implementing NIST AI RMF?**
   → YES: Choose Pathway 3 (AI RMF to ISO Bridge) - 9-12 months
   → NO: Continue to question 3

3. **Do you have other established frameworks (SOC 2, HIPAA, FISMA, etc.)?**
   → YES: Choose Pathway 4 (Multi-Framework Consolidation) - 6-12 months
   → NO: Choose Pathway 1 (Greenfield Implementation) - 12-18 months

Next Steps

Once you have selected your pathway:

4. Review the detailed phase breakdown for your chosen pathway
5. Secure executive sponsorship and budget approval
6. Assemble your core implementation team
7. Create detailed project plan with milestones
8. Consider engaging external consultants for ISO expertise
9. Begin Phase 1 activities for your pathway

7. Example: Creating Integrated AI Governance Policy

7.1 Policy Structure

An integrated AI governance policy must satisfy all three standards:

Policy Section	Required Content	Standards Satisfied
1. Purpose & Scope	Define AI systems covered, organizational objectives	[AI RMF GOVERN 1] [ISO 42001 5.2] [ISO 27001 5.2]
2. Policy Statement	Commitment to trustworthy AI, risk management, compliance	[AI RMF GOVERN 1] [ISO 42001 5.2]
3. Trustworthiness Principles	Seven NIST characteristics: valid, safe, secure, accountable, explainable, private, fair	[AI RMF Core] [ISO 42001 6.1.3]
4. Risk Appetite	Acceptable risk levels for AI use cases	[AI RMF MAP 2] [ISO 42001 6.1.2] [ISO 27001 6.1.2]
5. Roles & Responsibilities	Define AI governance roles, decision authority	[AI RMF GOVERN 1.2] [ISO 42001 5.3] [ISO 27001 A.5.2]
6. Compliance Commitments	Reference to NIST, ISO 42001, ISO 27001, regulations	[All standards]
7. Review & Approval	Annual review cycle, approval authority	[ISO 42001 5.2] [ISO 27001 5.2]

Conclusion

The AI Risk Management Framework 2026 Integrated Edition represents a paradigm shift in AI governance. By seamlessly integrating AI RMF 2026 with ISO 42001 and ISO 27001, organizations can:

- Reduce implementation effort by 40-60% compared to separate frameworks
- Achieve ISO 42001 certification demonstrating world-class AI governance
- Satisfy multiple regulatory requirements with unified evidence
- Build customer and partner trust through internationally recognized standards
- Scale governance consistently across global operations

This framework provides the roadmap for organizations to implement responsible AI governance efficiently, demonstrate that commitment through certification, and position themselves for success in an increasingly regulated AI landscape.

Appendices

The complete integrated framework includes the following appendices (implementation detail continues in full version):

- Appendix A: Complete AI RMF-to-ISO 42001 Subcategory Crosswalk
- Appendix B: Complete AI RMF-to-ISO 27001 Control Crosswalk
- Appendix C: ISO 42001-to-ISO 27001 Integration Matrix
- Appendix D: EU AI Act Compliance Mapping
- Appendix E: Singapore AI Verify Alignment
- Appendix F: Document Templates (Policy, Risk Assessment, Audit Checklist)
- Appendix G: EU AI Act Templates (Ready-to-Use Templates for EU AI Act Compliance)
- Appendix H: Glossary - Unified Terminology (AI RMF, ISO 42001, ISO 27001)
- Appendix I: Evidence Repository Structure for Certification Audits
- Appendix J: Certification Body Selection Guide
- Appendix K: Common Audit Findings and Remediation

Appendix A1-A2

AI RMF 2026 to ISO/IEC 42001 Complete Crosswalk

Version 1.0 | January 2026

Introduction

This comprehensive crosswalk maps all AI RMF 2026 categories and subcategories to ISO/IEC 42001:2023 clauses, enabling organizations to implement both standards efficiently.

Alignment Types

- **Direct:** AI RMF 2026 directly satisfies ISO requirement
- **Substantial:** AI RMF 2026 addresses majority; some ISO-specific documentation needed
- **Partial:** AI RMF 2026 covers some aspects; additional work needed

GOVERN Function Mappings

Complete AI RMF to ISO 42001 Crosswalk

This comprehensive crosswalk maps all GOVERN function categories and subcategories to ISO/IEC 42001:2023 clauses and controls. Each mapping includes alignment type and implementation notes.

Alignment Legend

Direct: AI RMF directly satisfies ISO requirement with minimal additional documentation
Substantial: AI RMF addresses majority of requirement; some ISO-specific documentation needed
Partial: AI RMF covers some aspects; significant additional ISO work required

GOVERN 1: Organizational AI Governance

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 1.1: Legal and regulatory requirements are identified and managed	4.2, 6.3	Substantial	Need formal compliance register and regular review process
GOVERN 1.2: Roles and responsibilities for AI governance are clearly defined	5.3	Direct	AI RMF guidance aligns with ISO requirements
GOVERN 1.3: Policies and procedures are in place for AI development and deployment	5.2, 8.1	Substantial	Policies must use ISO management system language

GOVERN 1.4: Diversity, equity, inclusion, and accessibility (DEIA) processes are prioritized	6.1.3, 7.2	Partial	ISO requires documented DEIA objectives and metrics
GOVERN 1.5: Organizational culture supports responsible AI development	5.1, 7.3	Substantial	Need documented leadership commitment and awareness program
GOVERN 1.6: Mechanisms are in place to inventory AI systems	8.1, 8.2	Direct	AI system inventory is core requirement for both standards
GOVERN 1.7: Processes support transparent decision-making about AI systems	5.2, 7.4	Substantial	Transparency policy must address stakeholder communication

GOVERN 2: Accountability and Responsibility

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 2.1: Accountability structures are established with clear assignment of responsibilities	5.3, 8.1	Direct	RACI matrix recommended for both standards
GOVERN 2.2: Oversight mechanisms exist for AI systems throughout lifecycle	9.2, 9.3	Substantial	ISO requires formal audit and management review

GOVERN 2.3: Processes enable appeal or contestation of AI system outputs	8.2.4	Partial	ISO 42001 requires documented appeal mechanism

GOVERN 3: Workforce Diversity and Team Composition

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 3.1: AI development teams include diverse perspectives and domain expertise	7.2	Substantial	ISO requires competency assessments for all roles
GOVERN 3.2: Multidisciplinary teams are assembled to address AI impacts	7.2, 8.2.1	Substantial	Document team composition and expertise for each AI system

GOVERN 4: Risk Management Culture

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 4.1: Organizational culture emphasizes risk-aware AI development	5.1, 7.3	Substantial	Culture demonstrated through training, communication, and leadership
GOVERN 4.2: Training and awareness programs address AI risks	7.2, 7.3	Direct	Both standards require documented training programs
GOVERN 4.3: Incentives and accountability measures promote responsible AI	5.1, 7.1	Partial	ISO requires performance evaluation and disciplinary process

GOVERN 5: Organizational Oversight and Monitoring

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 5.1: Mechanisms exist for oversight of AI systems	9.2, 9.3	Substantial	ISO requires internal audit and management review processes
GOVERN 5.2: Independent review of AI systems is conducted	9.2	Direct	Internal audit provides independent review

GOVERN 6: Trustworthy AI Characteristics

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
GOVERN 6.1: Policies address AI system validity and reliability	5.2, 8.2.3	Direct	Testing and validation requirements in both standards
GOVERN 6.2: Policies address AI system safety	5.2, 6.1.3	Substantial	ISO 42001 requires AI impact assessment including safety
GOVERN 6.3: Policies address AI system security and resilience	5.2, 8.2	Direct	ISO 27001 Annex A provides comprehensive security controls
GOVERN 6.4: Policies address AI system accountability and transparency	5.2, 7.4	Substantial	Transparency policy and stakeholder communication required
GOVERN 6.5: Policies address	5.2, 8.2.4	Substantial	ISO 42001 requires information to deployers and users

AI system explainability and interpretability			
GOVERN 6.6: Policies address privacy enhancement	5.2, 8.2.3	Direct	Privacy protection core requirement in both standards
GOVERN 6.7: Policies address fairness and harmful bias management	5.2, 6.1.3	Substantial	ISO 42001 impact assessment must address fairness

GOVERN Function Summary

The GOVERN function shows strong alignment (80-90%) between AI RMF and ISO standards. Key implementation requirements for ISO certification include:

- Formal AIMS policy using ISO management system language
- Documented organizational structure with roles and responsibilities
- Formal internal audit program (ISO 42001 Clause 9.2)
- Management review process (ISO 42001 Clause 9.3)
- Training and competency records (ISO 42001 Clause 7.2)
- Documented compliance obligations register

MAP Function Mappings

Complete AI RMF to ISO 42001 Crosswalk

This comprehensive crosswalk maps all MAP function categories and subcategories to ISO/IEC 42001:2023 clauses and controls.

Alignment Legend

Direct: AI RMF directly satisfies ISO requirement
Substantial: AI RMF addresses majority; some ISO documentation needed
Partial: AI RMF covers some aspects; significant ISO work required

MAP 1: Context and Requirements

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
MAP 1.1: Context is established and mapped to organizational mission and goals	4.1, 4.4	Direct	Both require understanding organizational context
MAP 1.2: Intended purpose and scope of AI systems are defined	4.4, 8.1	Direct	System scope definition required for both standards
MAP 1.3: Business value and expected benefits are documented	6.1.3, 6.2	Substantial	ISO requires documented objectives and expected outcomes
MAP 1.4: Stakeholders and their expectations are identified	4.2	Direct	Stakeholder analysis core to ISO 42001 Clause 4.2

MAP 1.5: Legal and regulatory requirements are identified	6.3	Direct	Compliance obligations must be documented
MAP 1.6: AI system interactions and interdependencies are mapped	8.1, 8.3	Substantial	Asset inventory must include system dependencies

MAP 2: Categorize AI Systems

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
MAP 2.1: AI systems are categorized by type, application, and risk level	6.1.3, 8.1	Direct	Classification required for risk-based controls
MAP 2.2: AI system autonomy level is determined	6.1.3, 8.2	Substantial	Autonomy impacts risk assessment and controls
MAP 2.3: Technical approach and model architecture are documented	8.2.3	Substantial	Technical documentation required for both standards
MAP 2.4: Data sources and data quality requirements are defined	8.2.3	Direct	Data governance fundamental to both standards
MAP 2.5: Third-party components and dependencies are identified	8.3	Direct	Supply chain mapping required (AI-BOM)

MAP 3: Impacts and Benefits

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
MAP 3.1: Positive and negative impacts are identified and documented	6.1.3	Direct	AI impact assessment required by ISO 42001
MAP 3.2: Expected benefits to individuals and society are documented	6.1.3, 6.2	Substantial	Benefits assessment supports objectives setting
MAP 3.3: Potential harms across multiple dimensions are identified	6.1.2, 6.1.3	Direct	Risk and impact assessment cover potential harms
MAP 3.4: Demographic impacts and equity implications are assessed	6.1.3	Substantial	Fairness assessment required in impact analysis
MAP 3.5: Environmental impacts are considered	6.1.3	Partial	Environmental impact optional but recommended

MAP 4: Risks and Impacts

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
MAP 4.1: Technical risks are identified and documented	6.1.2	Direct	Technical risk assessment required by both
MAP 4.2: Fairness and bias risks are assessed	6.1.2, 6.1.3	Substantial	Bias assessment part of ISO 42001 impact assessment
MAP 4.3: Security and privacy risks are identified	6.1.2	Direct	ISO 27001 provides comprehensive security framework
MAP 4.4: Safety risks are evaluated	6.1.2, 6.1.3	Substantial	Safety must be addressed in risk assessment
MAP 4.5: Legal and regulatory compliance risks are assessed	6.1.2, 6.3	Direct	Compliance risk assessment required
MAP 4.6: Reputational and organizational risks are considered	6.1.2	Substantial	Business impact should include reputation

MAP 5: Impact Assessment

AI RMF Subcategory	ISO 42001 Clause	Alignment	Notes
MAP 5.1: Impacts on individuals and groups are assessed	6.1.3	Direct	Impact assessment required by ISO 42001 Clause 6.1.3
MAP 5.2: Societal and community impacts are evaluated	6.1.3	Substantial	Broader impacts should be considered in assessment
MAP 5.3: Environmental impacts are assessed	6.1.3	Partial	Consider energy consumption and carbon footprint
MAP 5.4: Accessibility and inclusion impacts are evaluated	6.1.3	Substantial	Accessibility should be part of impact assessment
MAP 5.5: Impact assessment results are documented and shared with stakeholders	6.1.3, 7.4	Substantial	Documentation and communication required

MAP Function Summary

The MAP function demonstrates excellent alignment (85-95%) with ISO 42001.

Key implementation requirements:

- Formal AI impact assessment (ISO 42001 Clause 6.1.3) covering fairness, safety, privacy, accessibility
- Comprehensive risk assessment (ISO 42001 Clause 6.1.2) with documented methodology
- AI system inventory and classification (ISO 42001 Clause 8.1, ISO 27001 A.5.9)
- Stakeholder identification and engagement (ISO 42001 Clause 4.2)
- Supply chain mapping including AI-BOM (ISO 42001 Clause 8.3)
- Context analysis and scope definition (ISO 42001 Clause 4.1, 4.4)

MEASURE Function Mappings

Complete AI RMF to ISO 42001 Crosswalk

MEASURE 1: Appropriate Methods and Metrics

AI RMF Subcategory	ISO 42001	Alignment	Notes
MEASURE 1.1: Metrics for AI system trustworthiness are identified	8.2.3, 9.1	Substantial	Define metrics for validity, fairness, security, privacy
MEASURE 1.2: Measurement methodologies are established and validated	8.2.3, 9.1	Direct	Testing procedures required by both standards
MEASURE 1.3: Metrics for validity and reliability are defined	8.2.3	Direct	Accuracy, precision, recall, F1 score
MEASURE 1.4: Fairness metrics across demographic groups are established	6.1.3, 8.2.3	Substantial	Demographic parity, equalized odds, disparate impact
MEASURE 1.5: Security and robustness metrics are defined	8.2.3	Direct	Adversarial robustness, attack resistance

MEASURE 2: Data Quality

AI RMF Subcategory	ISO 42001	Alignment	Notes
MEASURE 2.1: Training data quality is assessed	8.2.3	Direct	Data quality dimensions: accuracy, completeness, consistency
MEASURE 2.2: Test data representativeness is evaluated	8.2.3	Substantial	Test data must reflect deployment population
MEASURE 2.3: Data provenance and lineage are documented	8.2.3	Direct	Track data sources and transformations
MEASURE 2.4: Bias in datasets is identified and quantified	6.1.3, 8.2.3	Substantial	Statistical analysis of demographic representation
MEASURE 2.5: Data freshness and relevance are monitored	8.2.3, 9.1	Substantial	Monitor for data drift and staleness

MEASURE 3: System Performance

AI RMF Subcategory	ISO 42001	Alignment	Notes
MEASURE 3.1: Technical performance is evaluated and documented	8.2.3, 9.1	Direct	Accuracy, latency, throughput, resource utilization
MEASURE 3.2: Trustworthiness characteristics are assessed	8.2.3	Substantial	All seven trustworthiness characteristics
MEASURE 3.3: Performance across demographic	6.1.3, 8.2.3	Substantial	Disaggregated performance metrics by group

groups is evaluated			
MEASURE 3.4: System behavior in edge cases is tested	8.2.3	Substantial	Boundary testing and stress testing

MEASURE 4: Risk Tracking and Monitoring

AI RMF Subcategory	ISO 42001	Alignment	Notes
MEASURE 4.1: Ongoing monitoring mechanisms are established	9.1	Direct	Continuous monitoring of performance and risks
MEASURE 4.2: Model drift is detected and tracked	9.1	Substantial	Monitor for data drift and concept drift
MEASURE 4.3: Performance degradation is identified	9.1	Direct	Automated alerts for performance thresholds
MEASURE 4.4: Security events and anomalies are monitored	8.2.5, 9.1	Direct	SIEM integration for AI systems
MEASURE 4.5: User feedback and complaints are tracked	9.1, 10.1	Substantial	Feedback mechanism and complaint tracking

MEASURE Function Summary

The MEASURE function shows strong alignment (80-90%) with ISO standards.

Key requirements:

- Performance monitoring program (ISO 42001 Clause 9.1)
- Documented testing methodology (ISO 42001 Clause 8.2.3)
- Metrics for all trustworthiness characteristics
- Data quality assessment framework
- Continuous monitoring infrastructure (ISO 27001 A.8.16)

MANAGE Function Mappings

Complete AI RMF to ISO 42001 crosswalk

MANAGE 1: Risk Response

AI RMF Subcategory	ISO 42001	Alignment	Notes
MANAGE 1.1: Risk treatment strategies are selected and documented	6.1.4	Direct	Avoid, reduce, transfer, or accept risks
MANAGE 1.2: Controls are implemented to address identified risks	6.1.4, 8.1	Direct	Technical and organizational controls
MANAGE 1.3: Residual risks are assessed and accepted	6.1.4	Direct	Management acceptance of residual risks required
MANAGE 1.4: Risk treatment plans are executed and tracked	6.1.4, 8.1	Substantial	Implementation tracking and evidence collection

MANAGE 2: Incident Management

AI RMF Subcategory	ISO 42001	Alignment	Notes
MANAGE 2.1: Incident response procedures are established	8.2.5	Direct	Detection, triage, containment, investigation, remediation
MANAGE 2.2: AI incidents are identified and classified	8.2.5	Substantial	Incident classification by severity and type

MANAGE 2.3: Incidents are documented and analyzed	8.2.5, 7.5	Direct	Incident records and root cause analysis
MANAGE 2.4: Lessons learned are captured and shared	10.1, 10.2	Substantial	Post-incident review and knowledge sharing
MANAGE 2.5: Notification and reporting requirements are met	8.2.5	Substantial	Regulatory and stakeholder notification

MANAGE 3: Communication and Transparency

AI RMF Subcategory	ISO 42001	Alignment	Notes
MANAGE 3.1: Information about AI systems is communicated to stakeholders	7.4, 8.2.4	Direct	Transparency documentation and communication
MANAGE 3.2: Model cards and documentation are published	8.2.4	Substantial	Information to deployers and users required
MANAGE 3.3: Limitations and known issues are disclosed	8.2.4	Substantial	Honest disclosure of capabilities and limitations
MANAGE 3.4: Stakeholder feedback mechanisms are provided	7.4, 9.1	Substantial	Feedback channels and response process

MANAGE 4: Continuous Improvement

AI RMF Subcategory	ISO 42001	Alignment	Notes
MANAGE 4.1: Improvement processes are established	10.2	Direct	Continual improvement of AIMS
MANAGE 4.2: Performance data informs system improvements	9.1, 10.2	Direct	Data-driven improvement decisions
MANAGE 4.3: Model retraining and updating procedures are followed	8.2.3	Substantial	Change management for model updates
MANAGE 4.4: Corrective actions are implemented and verified	10.1	Direct	Nonconformity and corrective action process
MANAGE 4.5: Best practices are identified and adopted	10.2	Substantial	Learning from industry and research

MANAGE Function Summary

The MANAGE function demonstrates excellent alignment (85-95%) with ISO standards.

Key requirements:

- Risk treatment plan (ISO 42001 Clause 6.1.4)
- Incident response procedure (ISO 42001 Clause 8.2.5, ISO 27001 A.5.24)
- Stakeholder communication plan (ISO 42001 Clause 7.4)
- Continual improvement process (ISO 42001 Clause 10)
- Corrective action tracking (ISO 42001 Clause 10.1)
- Model update and change management procedures

Appendix A-2

Complete AI RMF to ISO 42001 Crosswalk

Version 1.0 | *January 2026*

Introduction

This appendix provides a comprehensive mapping of all AI RMF 2026 categories to ISO/IEC 42001:2023 clauses. Organizations can use this crosswalk to understand how implementing AI RMF guidance contributes to ISO 42001 certification readiness.

Alignment Types

- **Direct:** AI RMF directly satisfies ISO 42001 requirement with minimal additional documentation
- **Substantial:** AI RMF addresses majority of requirement; some ISO-specific documentation needed (e.g., formal procedures, records)
- **Partial:** AI RMF covers some aspects; significant additional work required to meet ISO requirements

ISO 42001 Structure Overview

ISO 42001 uses a high-level structure (HLS) common to ISO management system standards:

- Clause 4: Context of the organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

ISO 42001 Clause 4: Context of the Organization

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
4.1: Understanding organization and context	MAP 1.1, GOVERN 1.1	Direct	AI RMF covers; formal documentation required
4.2: Understanding needs and expectations of interested parties	MAP 1.4, GOVERN 2.3	Direct	Stakeholder register with documented requirements
4.3: Determining scope of AIMS	MAP 1.2, GOVERN 1.6	Substantial	Formal scope statement with boundaries and exclusions
4.4: AI management system	GOVERN 1, All Functions	Substantial	AIMS processes documented and implemented

ISO 42001 Clause 5: Leadership

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
5.1: Leadership and commitment	GOVERN 1.5, GOVERN 4.1	Substantial	Executive endorsement and resource allocation evidence
5.2: AI management system policy	GOVERN 6.1-6.7	Substantial	Formal policy using ISO language, approved and published
5.3: Organizational roles, responsibilities and authorities	GOVERN 1.2, GOVERN 2.1	Direct	RACI matrix and job descriptions documented

ISO 42001 Clause 6: Planning

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
6.1.1: General (risk and opportunities)	MAP 3, MAP 4	Direct	Risk and opportunity assessment documented
6.1.2: AI risk assessment	MAP 4.1-4.6	Direct	Formal risk assessment with methodology and register
6.1.3: AI impact assessment	MAP 3, MAP 5	Direct	Impact assessment covering all dimensions
6.1.4: Risk treatment	MANAGE 1.1-1.4	Direct	Risk treatment plan with controls and ownership
6.2: AI objectives and planning	MAP 1.3, GOVERN 1	Substantial	SMART objectives with measurable KPIs
6.3: Compliance obligations	MAP 1.5, GOVERN 1.1	Direct	Compliance register with tracking

ISO 42001 Clause 7: Support

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
7.1: Resources	GOVERN 1.2, GOVERN 3	Substantial	Resource allocation plan and evidence
7.2: Competence	GOVERN 3.1, GOVERN 4.2	Direct	Competency matrix and training records
7.3: Awareness	GOVERN 4.2, GOVERN 1.5	Direct	Awareness program and attendance records

7.4: Communication	MANAGE 3.1-3.4, GOVERN 1.7	Substantial	Communication plan and stakeholder records
7.5: Documented information	All Functions	Partial	Document control procedure and master list required

ISO 42001 Clause 8: Operation

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
8.1: Operational planning and control	All Functions, GOVERN 1.3	Substantial	AI lifecycle procedures documented
8.2: AI system lifecycle processes	MAP 2, MEASURE 3, MANAGE 4.3	Substantial	Lifecycle stages defined with gates and approval
8.2.1: Data management	MAP 2.4, MEASURE 2	Direct	Data governance framework and quality controls
8.2.2: Design and development	MAP 2.3, GOVERN 3.2	Substantial	Design controls and development procedures
8.2.3: Validation and testing	MEASURE 1, MEASURE 3	Direct	Validation protocol and test results
8.2.4: Information to deployers and users	MANAGE 3.2, MANAGE 3.3	Substantial	Model cards and user documentation
8.2.5: AI system operation and monitoring	MEASURE 4, MANAGE 2	Direct	Monitoring plan and incident procedures
8.3: Management of AI supply chain	MAP 2.5	Substantial	Vendor assessment and AI-BOM required

ISO 42001 Clause 9: Performance Evaluation

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
9.1: Monitoring, measurement, analysis and evaluation	MEASURE 1, MEASURE 4, MANAGE 4.2	Direct	Performance metrics and monitoring dashboard
9.2: Internal audit	GOVERN 5.1, GOVERN 5.2	Partial	Internal audit program and schedule required
9.3: Management review	GOVERN 5.1, GOVERN 2.2	Partial	Management review process and minutes required

ISO 42001 Clause 10: Improvement

ISO 42001 Requirement	AI RMF Mapping	Alignment	Implementation Gap
10.1: Nonconformity and corrective action	MANAGE 4.4, MANAGE 2.4	Substantial	Corrective action procedure and tracking register
10.2: Continual improvement	MANAGE 4.1, MANAGE 4.2, MANAGE 4.5	Direct	Improvement process and evidence of implementation

Summary and Key Gaps

This crosswalk demonstrates 80-90% alignment between AI RMF 2026 and ISO 42001. Organizations implementing AI RMF guidance are well-positioned for ISO 42001 certification with targeted additions.

Critical ISO 42001 Requirements Not Fully Covered by AI RMF:

- Formal AIMS scope document (Clause 4.4)
- Management system policy using ISO language (Clause 5.2)
- Internal audit program with documented audits (Clause 9.2)
- Management review process with formal minutes (Clause 9.3)
- Document control procedure (Clause 7.5)
- Formal corrective action tracking system (Clause 10.1)

Implementation Recommendations:

- Use AI RMF as implementation guide for ISO 42001 content requirements
- Add formal management system documentation and procedures
- Establish internal audit and management review processes
- Implement document control and records management
- Prepare evidence repository organized by ISO 42001 clause

End of Appendix A

Appendix B

AI RMF 2026 to ISO 27001:2022

Control Crosswalk

AI-Specific Implementation of Information Security Controls

Version 1.0 | January 2026

AI-Specific Control Implementation

All 93 Controls with AI Guidance

Introduction

This appendix provides comprehensive AI-specific implementation guidance for all 93 ISO/IEC 27001:2022 Annex A controls. Each control includes mapping to AI RMF categories, alignment assessment, and detailed AI-specific implementation requirements.

How to Use This Appendix

For each control:

1. AI RMF Mapping: Shows which AI RMF categories address this control
2. Alignment: Direct (AI RMF fully covers), Substantial (mostly covers), or Partial (additional work needed)
3. AI Implementation: Specific guidance for implementing this control for AI systems

AI Asset Classes Requiring Protection

AI Models: Trained weights, architectures, hyperparameters
Training Data: Datasets for training and fine-tuning
AI Algorithms: Proprietary techniques and methods
AI Infrastructure: GPUs, TPUs, specialized hardware
AI-BOM: Third-party models, libraries, dependencies

A.5 Organizational Controls (37 Controls)

Control	AI RMF Mapping	Align	AI-Specific Implementation
A.5.1 Policies for information security	GOVERN 6.1-6.7, GOVERN 1.3	Substantial	AI policy must address: (1) Model security and integrity, (2) Training data protection and provenance, (3) Fairness and bias management, (4) Transparency and explainability requirements, (5) Accountability structures for AI decisions, (6) Privacy-preserving techniques, (7) AI-specific incident response
A.5.2 Information security roles and responsibilities	GOVERN 1.2, GOVERN 2.1	Direct	Define AI-specific roles: AI Risk Officer, AI Ethics Committee, Model Validation Team, AI Security Analyst, Data Governance Lead. Document responsibilities for AI lifecycle stages: development, deployment, monitoring, incident response
A.5.3 Segregation of duties	GOVERN 2.1	Substantial	Separate duties for: (1) Model development vs. validation, (2) Training data preparation vs. quality review, (3) Model deployment approval vs. implementation, (4) AI system monitoring vs. performance evaluation. Prevent single individual from controlling entire AI pipeline
A.5.4 Management responsibilities	GOVERN 1.5, GOVERN 5.1	Direct	Management accountable for: AI risk management program, resource allocation for AI governance, AI policy compliance, ethical AI oversight, AI incident escalation
A.5.5 Contact with authorities	GOVERN 1.1, MANAGE 2.5	Substantial	Establish contacts with: AI regulatory authorities, data protection authorities (for AI/ML), law enforcement (for AI-related incidents), AI standards bodies. Document escalation procedures for AI regulatory issues

A.5.6 Contact with special interest groups	MAP 1.4	Partial	Engage with: AI ethics boards, ML security research community, fairness in AI working groups, industry AI consortia. Stay informed on emerging AI threats and best practices
A.5.7 Threat intelligence	MAP 4.3, MEASURE 4.4	Substantial	Monitor AI-specific threats: (1) Adversarial attacks (evasion, poisoning, backdoor), (2) Model extraction and inversion, (3) Data poisoning campaigns, (4) Prompt injection techniques, (5) Model stealing, (6) Training data extraction. Subscribe to AI security threat feeds
A.5.8 Information security in project management	GOVERN 1.3, MAP 2.2	Substantial	Integrate security into AI project lifecycle: Security requirements in project charter, Threat modeling for AI systems, Security gates at development milestones, AI-specific security testing, Privacy and fairness reviews before deployment
A.5.9 Inventory of information and other associated assets	MAP 2.1, GOVERN 1.6	Direct	AI asset inventory includes: (1) Models: architecture, versions, weights, hyperparameters, (2) Datasets: training, validation, test data with lineage, (3) AI infrastructure: GPUs, TPUs, training clusters, (4) AI code repositories and notebooks, (5) Third-party AI components (AI-BOM), (6) Model serving endpoints and APIs. Track ownership, classification, and location
A.5.10 Acceptable use of information and other associated assets	GOVERN 1.3	Substantial	Define acceptable use for: AI models (authorized use cases only), Training data (purpose limitation), Model outputs (proper interpretation and limitations), AI infrastructure (approved workloads), Pre-trained models (licensing compliance). Prohibit: Unauthorized model fine-tuning, Data exfiltration, Adversarial testing without approval

A.5.11 Return of assets	GOVERN 1.3	Partial	When personnel leave: Return access to AI systems and models, Delete local copies of training data, Remove from AI infrastructure access, Revoke API keys and credentials, Transfer ownership of AI projects, Document knowledge transfer for AI systems
A.5.12 Classification of information	MAP 2.1, MAP 2.2	Direct	Classify AI systems by: (1) Risk level: High/Medium/Low based on impact, (2) Data sensitivity: PII, confidential, public, (3) Autonomy level: Fully automated, human-in-loop, human-on-loop, (4) Decision impact: High-stakes (hiring, credit) vs. low-stakes. Classify training data by: Sensitivity, Source, Quality level, Bias risk
A.5.13 Labelling of information	MAP 2.1	Substantial	Label AI assets: Model classification tags, Dataset sensitivity labels, Model version and lineage metadata, Training data provenance markers, AI system risk classification badges. Use metadata standards for AI artifacts
A.5.14 Information transfer	MANAGE 3.2	Substantial	Secure transfer of: Model weights and architectures (encrypted), Training datasets (data loss prevention), Model cards and documentation, Inference results (privacy-preserving). Control cross-border AI model and data transfers per regulations
A.5.15 Access control	MANAGE 1.2	Direct	Implement access control for: Model repositories (version control), Training data stores (need-to-know), AI infrastructure (role-based), Model serving endpoints (authentication), MLOps tools and platforms. Use principle of least privilege for AI systems
A.5.16 Identity management	MANAGE 1.2	Direct	Manage identities for: AI developers and data scientists, Automated AI agents and systems, Service accounts for AI pipelines, API consumers of AI services. Track who/what accesses AI assets

A.5.17 Authentication information	MANAGE 1.2	Direct	Protect credentials for: AI infrastructure access, Model repositories, Cloud AI services, API keys for AI endpoints, Database connections for training data. Rotate AI service credentials regularly
A.5.18 Access rights	MANAGE 1.2	Direct	Define access rights to: View/modify models, Access training data, Deploy AI systems, Monitor AI performance, Approve model changes. Implement approval workflows for sensitive AI operations
A.5.19 Information security in supplier relationships	MAP 2.5	Direct	Assess AI vendors for: Model security practices, Data handling procedures, Model provenance and transparency, Incident notification commitments, Subprocessor disclosure (for AI services), Audit rights for AI systems. Maintain AI-BOM for third-party components
A.5.20 Addressing information security within supplier agreements	MAP 2.5	Direct	Supplier agreements must address: Model licensing and usage rights, Training data sources and quality, Model performance guarantees, Bias and fairness commitments, Security incident notification (24-48 hours), Model update and patching, IP ownership of fine-tuned models, Data retention and deletion, Audit and inspection rights
A.5.21 Managing information security in ICT supply chain	MAP 2.5	Substantial	AI supply chain includes: Foundation model providers, AI-as-a-Service platforms, Training data vendors, Labeled data providers, MLOps tool vendors, AI hardware suppliers. Assess: Model poisoning risks, Data quality assurance, Component vulnerabilities in AI stack

A.5.22 Monitoring, review and change management of supplier services	MAP 2.5, MANAGE 4.3	Substantial	Monitor AI suppliers for: Model performance degradation, Service availability and latency, API changes and deprecations, Security vulnerabilities, Compliance with SLAs. Review: Model updates and their impacts, Data quality changes, New AI risks from supplier changes
A.5.23 Information security for use of cloud services	MAP 2.5, MANAGE 1.2	Direct	AI-as-a-Service assessment: Model security in multi-tenant environment, Data residency and sovereignty, Inference data privacy and encryption, API security and rate limiting, Model isolation between customers, Training data handling by provider, Audit logs and monitoring, Vendor lock-in and portability
A.5.24 Information security incident management planning and preparation	MANAGE 2.1	Direct	AI incident response plan covering: Model failures and hallucinations, Fairness violations and bias incidents, Data poisoning detection, Adversarial attack response, Privacy breaches from models, Model theft or extraction, Unauthorized model deployment. Define incident classification, escalation, and response teams
A.5.25 Assessment and decision on information security events	MANAGE 2.2	Substantial	Assess AI events for: Severity (impact on decisions), Affected population size, Bias or fairness implications, Privacy risk, Reputational damage, Regulatory reporting requirements. Decision criteria for incident declaration
A.5.26 Response to information security incidents	MANAGE 2.1	Direct	AI incident response: Containment (disable model, fallback to baseline), Investigation (analyze model behavior, review training data), Remediation (retrain, adjust thresholds, add guardrails), Communication (notify affected parties, regulators), Recovery (gradual re-deployment with monitoring)

A.5.27 Learning from information security incidents	MANAGE 2.4, MANAGE 4.1	Substantial	Post-incident review for AI: Root cause (model, data, or deployment issue), Contributing factors (drift, adversarial input), Lessons learned, Process improvements, Model enhancements, Training data updates, Detection capability improvements
A.5.28 Collection of evidence	MANAGE 2.3	Substantial	Preserve AI incident evidence: Model snapshots and weights, Input data that triggered incident, Model predictions and confidence scores, Training data version, System logs and monitoring data, Configuration and hyperparameters. Maintain chain of custody for forensics
A.5.29 Information security during disruption	MANAGE 2.1	Partial	AI continuity planning: Fallback to simpler models or rules, Manual override procedures, Cached predictions for critical functions, Model redundancy and failover, Alternative data sources
A.5.30 ICT readiness for business continuity	MANAGE 1.2	Partial	AI system continuity: Backup of trained models, Training data backup and versioning, AI infrastructure redundancy, Model serving high availability, Recovery time objectives for AI systems
A.5.31 Legal, statutory, regulatory and contractual requirements	MAP 1.5, GOVERN 1.1	Direct	Track AI regulations: EU AI Act compliance, Sector-specific AI rules (healthcare, finance), Data protection laws (GDPR, CCPA) for training data, Bias and discrimination laws, Model explainability requirements, AI transparency mandates, Cross-border data transfer restrictions

A.5.32 Intellectual property rights	MAP 2.5, GOVERN 1.1	Substantial	Protect AI IP: Model architecture patents, Proprietary training techniques, Licensed model usage compliance, Training data copyright, Generated content ownership, Open source model compliance. Respect: Training data licenses, Pre-trained model terms, AI software dependencies
A.5.33 Protection of records	GOVERN 6.6, MEASURE 2.1	Substantial	Protect AI records: Model development documentation, Training records and data lineage, Validation and testing results, Deployment approvals, Monitoring logs, Incident reports, Audit trails. Define retention periods per regulatory requirements
A.5.34 Privacy and protection of personal information	GOVERN 6.6, MEASURE 2.1	Direct	AI privacy protection: Minimize PII in training data, Implement differential privacy, Prevent model inversion and membership inference, Data anonymization and pseudonymization, Right to explanation for decisions, Right to be forgotten (model unlearning), Privacy impact assessment for AI systems
A.5.35 Independent review of information security	GOVERN 5.2	Substantial	Independent AI review: Third-party model audits, External fairness assessments, Security penetration testing, Privacy compliance review, Algorithm audits, Bias testing by independent evaluators
A.5.36 Compliance with policies and standards	GOVERN 1.1, MANAGE 1.1	Substantial	AI compliance monitoring: Policy adherence checks, Standards alignment verification, Control effectiveness assessment, Gap analysis, Remediation tracking. Regular compliance attestation for AI systems

A.5.37 Documented operating procedures	GOVERN 1.3	Substantial	Document AI procedures: Model development lifecycle, Data preparation and labeling, Training and validation processes, Deployment and release management, Monitoring and alerting, Incident response, Model retirement. Keep procedures current with AI practices

A.6 People Controls (8 Controls)

Control	AI RMF Mapping	Align	AI-Specific Implementation
A.6.1 Screening	GOVERN 3.1	Substantial	Screen AI personnel for: Technical competency in ML/AI, Understanding of AI ethics and bias, Background checks for sensitive AI roles, Verification of credentials and experience. Consider risk level of AI systems they will access
A.6.2 Terms and conditions of employment	GOVERN 1.2	Partial	Employment agreements address: AI confidentiality and IP, Responsible AI practices, Prohibition of unauthorized model use, Data handling requirements, Ethical guidelines for AI work, Consequences of AI policy violations
A.6.3 Information security awareness, education and training	GOVERN 4.2, GOVERN 1.5	Direct	AI training program: AI security fundamentals, Adversarial ML and threat landscape, Responsible AI and ethics, Bias identification and mitigation, Privacy-preserving techniques, Secure ML development practices, AI incident reporting. Role-specific training for: AI developers, Data scientists, Model validators, AI operators
A.6.4 Disciplinary process	GOVERN 4.3	Partial	Disciplinary actions for: Unauthorized AI model deployment, Data misuse or exfiltration, Bypassing AI governance controls, Bias introduction or fairness violations, Security policy violations in AI work

A.6.5 Responsibilities after termination or change of employment	GOVERN 1.2	Partial	Post-employment: Revoke AI system access, Remove from model repositories, Delete training data copies, Disable API credentials, Transfer AI project ownership, Knowledge transfer for critical AI systems
A.6.6 Confidentiality or non-disclosure agreements	GOVERN 1.2	Partial	NDAs cover: Proprietary AI models and techniques, Training data and sources, Model performance metrics, AI system vulnerabilities, AI research and development, Customer AI implementations
A.6.7 Remote working	MANAGE 1.2	Substantial	Remote AI work security: Secure access to training infrastructure, VPN for AI resources, Encrypted storage for models and data, Prohibition of local training data downloads, Secure development environments, Monitoring of remote AI activities
A.6.8 Information security event reporting	MANAGE 2.2, MEASURE 4.5	Direct	Report AI events: Model failures or anomalies, Suspected adversarial attacks, Data quality issues, Bias or fairness concerns, Privacy incidents, Unauthorized access to AI systems, Performance degradation. Provide clear reporting channels and non-retaliation

A.7 Physical Controls (14 Controls)

Control	AI RMF Mapping	Align	AI-Specific Implementation
A.7.1 Physical security perimeters	MANAGE 1.2	Partial	Secure AI infrastructure: Data center access for AI training clusters, GPU/TPU farm physical security, Research lab access controls, Protection of AI development facilities
A.7.2 Physical entry	MANAGE 1.2	Partial	Control access to: AI training facilities, Model development labs, Data storage locations, AI hardware rooms. Use badge access, biometrics, visitor logs
A.7.3 Securing offices, rooms and facilities	MANAGE 1.2	Partial	Secure AI work areas: Lock AI development offices, Secure model training facilities, Protected storage for AI data, Clean desk for AI notebooks and data
A.7.4 Physical security monitoring	MANAGE 1.2	Partial	Monitor AI facilities: Video surveillance of data centers, Access logs for AI labs, Environmental monitoring (for AI hardware), Intrusion detection for AI infrastructure areas
A.7.5 Protecting against physical and environmental threats	MANAGE 1.2	Partial	Protect AI infrastructure from: Fire (AI hardware generates heat), Flood, Power failure (UPS for training), HVAC failure (GPU cooling critical), Natural disasters affecting AI operations
A.7.6 Working in secure areas	MANAGE 1.2	Partial	Secure area procedures for: Sensitive AI model development, Proprietary training data handling, AI research and experimentation, High-risk AI system development
A.7.7 Clear desk and clear screen	MANAGE 1.2	Partial	Clear desk for AI work: Lock away training data notebooks, Secure model documentation, Clear screens showing AI development, No unattended AI workstations

A.7.8 Equipment siting and protection	MANAGE 1.2	Partial	AI equipment protection: GPU/TPU placement and cooling, Training cluster physical security, Protection from unauthorized viewing of AI screens, Secure disposal of AI hardware
A.7.9 Security of assets off-premises	MANAGE 1.2	Substantial	Off-premises AI assets: Encrypted laptops with models, Secure transport of AI hardware, Protection of backup media with training data, Security for remote AI development, Controlled sharing of model artifacts
A.7.10 Storage media	MEASURE 2.3	Substantial	AI storage media: Label drives containing training data, Encrypt model storage media, Secure backup of AI artifacts, Version control for model storage, Protect against magnetic/electronic interference
A.7.11 Supporting utilities	MANAGE 1.2	Partial	AI infrastructure utilities: Redundant power for training clusters, Cooling systems for GPU farms, Backup generators for AI operations, Network redundancy for AI services
A.7.12 Cabling security	MANAGE 1.2	Partial	Protect AI network cabling: Secure connections to AI infrastructure, Protected pathways for AI data networks, Prevent tampering with AI hardware connections
A.7.13 Equipment maintenance	MANAGE 4.3	Partial	AI equipment maintenance: GPU/TPU servicing procedures, Data sanitization before AI hardware repair, Vendor access controls for AI infrastructure, Maintenance logs for AI equipment
A.7.14 Secure disposal or re-use of equipment	GOVERN 6.6	Substantial	AI equipment disposal: Secure erasure of models from hardware, Sanitize training data from storage, Degauss or destroy AI data drives, Certificate of destruction for sensitive AI hardware, Ensure no model artifacts remain on reused equipment

A.8 Technological Controls (34 Controls)

Control	AI RMF Mapping	Align	AI-Specific Implementation
A.8.1 User endpoint devices	MANAGE 1.2	Substantial	Secure AI development endpoints: Encrypted laptops for AI developers, Hardened workstations for model training, Mobile device management for AI access, Prohibit unauthorized AI tools, Secure configuration for data science environments
A.8.2 Privileged access rights	MANAGE 1.2	Direct	Control privileged access to: Model production deployment, Training infrastructure administration, Master datasets, AI platform admin functions, Model registry management. Use just-in-time privileged access, MFA for privileged AI operations
A.8.3 Information access restriction	MANAGE 1.2	Direct	Restrict access to: Sensitive training data, Production models, Model weights and parameters, Proprietary algorithms, Customer AI data, High-risk AI systems. Implement need-to-know and least privilege
A.8.4 Access to source code	MANAGE 1.2	Direct	Control access to: AI model code repositories, Training pipeline code, Preprocessing scripts, Custom algorithms, Model serving code. Use code review and version control
A.8.5 Secure authentication	MANAGE 1.2	Direct	Strong authentication for: AI platform access, Model repositories, Training infrastructure, API endpoints, Cloud AI services. Implement MFA for sensitive AI systems
A.8.6 Capacity management	MEASURE 3.1	Substantial	AI capacity planning: Training cluster capacity, GPU/TPU utilization, Model serving capacity, Storage for training data and models, Network bandwidth for AI workloads. Monitor and forecast AI resource needs

A.8.7 Protection against malware	MEASURE 3.1, GOVERN 6.3	Direct	AI malware protection: Scan training data for malicious content, Validate model integrity (checksums, signatures), Detect backdoors in models, Monitor for data poisoning, Protect model artifacts from tampering, Secure ML libraries and dependencies. Use model signing and provenance verification
A.8.8 Management of technical vulnerabilities	MANAGE 1.2	Substantial	AI vulnerability management: Track AI framework vulnerabilities (TensorFlow, PyTorch), Patch AI infrastructure, Monitor AI-specific CVEs, Update ML libraries, Scan for vulnerable dependencies in AI stack, Assess adversarial robustness
A.8.9 Configuration management	MANAGE 4.3	Substantial	AI configuration management: Model hyperparameters as code, Infrastructure as code for AI platforms, Baseline configurations for AI environments, Change control for AI configurations, Version control for training configs
A.8.10 Information deletion	GOVERN 6.6, MANAGE 1.2	Direct	AI-specific deletion: Model unlearning when required (GDPR right to be forgotten), Secure deletion of training data, Remove personal data from datasets, Versioned model retirement and archival, Delete deprecated AI artifacts, Sanitize AI development environments
A.8.11 Data masking	MEASURE 2.1, GOVERN 6.6	Direct	Privacy-preserving AI techniques: Differential privacy in training, Federated learning (data stays local), Synthetic data generation, Homomorphic encryption for inference, Anonymization of training datasets, K-anonymity for sensitive attributes, Data minimization in AI systems

A.8.12 Data leakage prevention	GOVERN 6.6	Direct	Prevent AI data leakage: DLP for training data transfers, Monitor model exfiltration attempts, Prevent unauthorized dataset downloads, Control model weight exports, Detect data extraction from models, API rate limiting to prevent scraping
A.8.13 Information backup	MANAGE 1.2	Substantial	Backup AI assets: Trained model weights and architectures, Training datasets (with versioning), Model metadata and documentation, Training configurations and hyperparameters, Validation results, Model serving configurations. Test restore procedures for AI systems
A.8.14 Redundancy of information processing facilities	MANAGE 1.2	Partial	AI redundancy: Multiple model serving instances, Backup training infrastructure, Failover for critical AI systems, Geographic distribution of AI services, Alternative data sources
A.8.15 Logging	MEASURE 4.1	Direct	AI logging: Model training logs, Inference requests and responses, Model performance metrics, Data access logs, Model deployment events, Configuration changes, Failed predictions, API usage. Retain logs per compliance requirements
A.8.16 Monitoring activities	MEASURE 4.1-4.5	Direct	AI monitoring: Model performance degradation, Data drift (distribution shift), Concept drift (relationship changes), Fairness metrics by demographic group, Prediction confidence trends, Adversarial attack detection, Unusual inference patterns, API abuse, Training anomalies. Implement automated alerts for AI-specific thresholds
A.8.17 Clock synchronization	MEASURE 4.1	Partial	Synchronize time across: AI training clusters, Model serving infrastructure, Distributed AI systems, Logging systems for AI. Critical for: Correlating AI events, Drift detection, Performance analysis

A.8.18 Use of privileged utility programs	MANAGE 1.2	Substantial	Control AI utility programs: Model deployment tools, Data migration utilities, Bulk model operations, Training job schedulers, Model conversion tools. Log and audit privileged AI utility use
A.8.19 Installation of software on operational systems	MANAGE 4.3	Substantial	Control AI software installation: ML framework updates, New AI libraries, Model serving software, Monitoring tools, Data processing utilities. Use change management for AI infrastructure software
A.8.20 Networks security	MANAGE 1.2	Substantial	AI network security: Segment AI training networks, Protect model serving endpoints, Secure API gateways, Network isolation for sensitive AI workloads, Encrypted communications for AI services, DDoS protection for AI APIs
A.8.21 Security of network services	MANAGE 1.2	Substantial	Secure AI network services: API authentication and authorization, Rate limiting for AI endpoints, TLS for model serving, VPN for remote AI access, Secure inter-service communication
A.8.22 Segregation of networks	MANAGE 1.2	Substantial	Network segregation for AI: Separate training and production networks, Isolate high-risk AI systems, Segment by data sensitivity, DMZ for public AI APIs, Separate development/test/prod AI environments
A.8.23 Web filtering	MANAGE 1.2	Partial	Filter AI-related web access: Block malicious model repositories, Control download of untrusted AI libraries, Prevent access to adversarial attack tools, Monitor AI research site access

A.8.24 Use of cryptography	GOVERN 6.3, MEASURE 2.1	Direct	AI cryptography: Encrypt models at rest (AES-256), TLS for model serving APIs, Encrypt training data storage, Secure key management for AI systems, Encrypted backups of models, Homomorphic encryption for privacy-preserving inference, Secure multi-party computation for federated learning
A.8.25 Secure development life cycle	MAP 2.3, MEASURE 3.4	Direct	AI-specific SDLC: Threat modeling for AI systems, Secure training pipeline design, Adversarial testing in development, Fairness validation gates, Privacy review checkpoints, Security testing of AI code, Code review for model implementations, Secure defaults for AI systems, Supply chain security for AI dependencies
A.8.26 Application security requirements	MAP 2.3	Substantial	AI application security requirements: Input validation for model inputs, Output sanitization for predictions, API security (authentication, rate limiting), Protection against adversarial inputs, Model inference DoS prevention, Secure handling of sensitive features, XSS/injection prevention in AI UIs
A.8.27 Secure system architecture and engineering principles	MAP 2.3, MANAGE 1.2	Substantial	AI architecture security: Defense in depth for AI systems, Fail-safe defaults (reject on uncertainty), Least privilege for AI components, Separation of duties (training vs deployment), Model isolation in multi-tenant systems, Secure model versioning, Audit trails for AI decisions
A.8.28 Secure coding	MAP 2.3	Substantial	Secure AI coding: Validate all inputs to models, Sanitize training data inputs, Prevent code injection in dynamic models, Use safe deserialization for models, Avoid hardcoded secrets in AI code, Input bounds checking, Secure random number generation

A.8.29 Security testing in development and acceptance	MEASURE 1.2, MEASURE 3.4	Direct	AI security testing: Adversarial attack testing (FGSM, PGD, C&W), Model extraction attempts, Membership inference attacks, Data poisoning tests, Robustness evaluation, Input fuzzing for AI systems, API penetration testing, Bias and fairness testing, Privacy leakage assessment, Red team exercises for AI. Test throughout development and before deployment
A.8.30 Outsourced development	MAP 2.5	Substantial	Outsourced AI development: Security requirements in contracts, Code review of outsourced AI work, Model validation from vendors, IP ownership clarity, Data handling agreements, Security testing of delivered AI components, Source code escrow for critical AI
A.8.31 Separation of development, test and production environments	MANAGE 1.2	Direct	AI environment separation: Isolated training environments, Separate validation infrastructure, Staging for model testing, Production model serving isolation, No production data in dev/test, Synthetic data for development, Strict promotion controls between environments, Separate credentials per environment
A.8.32 Change management	MANAGE 4.3	Direct	AI change management: Model retraining approval workflow, Version control for models (Git, DVC), A/B testing for model updates, Gradual rollout of new models, Rollback procedures for models, Impact assessment before deployment, Change documentation for AI systems, Approval for hyperparameter changes, Emergency change process for critical fixes

A.8.33 Test information	MEASURE 2.1	Substantial	AI test data management: Protect test datasets (may contain real data), Synthetic test data generation, Anonymize test data, Separate test from production data, Version control test datasets, Representative test data for fairness validation
A.8.34 Protection of information systems during audit testing	GOVERN 5.2	Partial	AI audit protection: Read-only access for auditors to production models, Test in non-production environments, Monitor audit activities, Protect model IP during audits, Secure audit evidence containing AI data

Implementation Summary

This complete crosswalk covers all 93 ISO 27001:2022 Annex A controls with AI-specific implementation guidance. Organizations should:

1. Review all controls for applicability to AI systems
2. Document applicability decisions in Statement of Applicability (SoA)
3. Implement controls with AI-specific adaptations as described
4. Collect evidence of implementation for certification audit
5. Regularly review and update controls as AI systems evolve

Key AI-Specific Controls

Controls requiring significant AI-specific implementation:

- A.5.9 - Inventory (must include AI models, datasets, infrastructure)
- A.5.7 - Threat Intelligence (adversarial ML attacks)
- A.5.19-20 - Supplier Security (AI-BOM, model provenance)
- A.5.34 - Privacy (model unlearning, differential privacy)
- A.8.7 - Malware Protection (model integrity, backdoor detection)
- A.8.10 - Information Deletion (model unlearning)
- A.8.11 - Data Masking (privacy-preserving ML)
- A.8.16 - Monitoring (drift detection, fairness metrics)
- A.8.25 - Secure Development (AI-specific SDLC)
- A.8.29 - Security Testing (adversarial testing, red teaming)
- A.8.32 - Change Management (model retraining, version control)

End of Appendix B

Appendix C

ISO 42001-to-ISO 27001 Integration Matrix

Efficient Dual Management System Implementation

Version 1.0 | January 2026

Introduction

This appendix provides a comprehensive integration matrix showing how ISO/IEC 42001 (Artificial Intelligence Management Systems) and ISO/IEC 27001 (Information Security Management Systems) can be implemented together efficiently. Organizations pursuing dual certification can leverage significant overlaps between the two standards to reduce implementation effort by 40-60%.

Why Integrate Both Standards?

- **Complementary Coverage:** ISO 42001 addresses AI-specific risks; ISO 27001 provides comprehensive security controls
- **Customer Requirements:** Clients increasingly demand both AI governance (ISO 42001) and security (ISO 27001) certification
- **Regulatory Alignment:** EU AI Act and other regulations reference both AI management and information security
- **Operational Efficiency:** Unified documentation, single audit process, shared governance structures
- **Risk Management Synergy:** AI risks and information security risks addressed holistically

Integration Approach

This matrix shows three integration levels:

Integration Level	Description
Direct Overlap	ISO 42001 clause directly satisfied by ISO 27001 control with minimal AI-specific additions
Substantial Overlap	ISO 42001 and ISO 27001 requirements significantly overlap; unified implementation possible with AI extensions
Complementary	ISO 42001 and ISO 27001 address distinct aspects; both needed but can share documentation structure

High-Level Standards Comparison

Common Ground: Both Are Management Systems

ISO 42001 and ISO 27001 share the same Annex SL high-level structure, making integration straightforward:

Clause	Topic	ISO 42001 Focus	ISO 27001 Focus
4	Context	AI stakeholders, AI scope	Information security context, ISMS scope
5	Leadership	AI policy, AI roles	Information security policy, security roles
6	Planning	AI risk assessment, AI impact assessment	Information security risk assessment
7	Support	AI competence, AI awareness	Security competence, security awareness
8	Operation	AI system lifecycle	Security controls implementation
9	Performance	AI monitoring, AI audit	Security monitoring, security audit
10	Improvement	AI continual improvement	ISMS continual improvement

Key Insight: Because both standards follow the same structure, organizations can create a unified management system with AI-specific and security-specific sections rather than maintaining two separate systems.

Clause-by-Clause Integration Matrix

Clause 4: Context of the Organization

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
4.1 Understanding	Understand AI context, issues affecting AIMS	Understand security context, issues affecting ISMS	90%	Single context analysis covering both AI and security
4.2 Stakeholders	Understand AI stakeholder needs	Understand security stakeholder needs	85%	Unified stakeholder analysis with AI and security perspectives
4.3 Scope	Determine AIMS boundaries	Determine ISMS boundaries	95%	Single scope document covering both systems (typically identical)
4.4 Management System	Establish, implement AIMS	Establish, implement ISMS	100%	Unified management system with AI and security components

- **Unified Document:** 'Context Analysis' covering AI and information security factors
- **Shared Scope:** Single 'AI & Information Security Management System (AIMS-ISMS) Scope Statement'

Clause 5: Leadership

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
5.1 Leadership	Top management demonstrates AI leadership	Top management demonstrates security leadership	95%	Single leadership commitment statement for both
5.2 Policy	Establish AI policy	Establish information security policy	80%	Unified 'AI & Information Security Policy'
5.3 Roles	Assign AI roles and responsibilities	Assign security roles and responsibilities	85%	Combined role matrix with AI and security responsibilities

- **Unified Policy:** Single policy document addressing both AI governance and information security
- **Combined Roles:** CISO role expanded to include AI security; AI Ethics Officer role includes security considerations
- **Example Roles:**
  - Chief AI & Information Security Officer (combined CISO role)
  - AI System Owner (responsible for both AI performance and security)
  - Data Protection Officer (covers both security and AI privacy)

Clause 6: Planning

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
6.1.1 General	Actions to address AI risks and opportunities	Actions to address security risks and opportunities	90%	Unified risk treatment planning
6.1.2 Risk Assessment	AI risk assessment process	Information security risk assessment	75%	Single risk assessment methodology with AI-specific criteria
6.1.3 Impact Assessment	AI system impact assessment (NEW to ISO 42001)	N/A (use 27001 A.5.34 DPIA)	50%	AI impact assessment references security impact analysis
6.1.4 Risk Treatment	AI risk treatment	Information security risk treatment	85%	Unified risk treatment plan covering both domains
6.2 Objectives	AI objectives and planning	Information security objectives	90%	Combined objectives addressing both AI and security goals
6.3 Planning Changes	Plan changes to AIMS	Plan changes to ISMS	100%	Single change planning process

- **Key Integration Point:** Risk assessment methodology extended to include AI-specific risk criteria alongside traditional security risks
- **Unified Risk Register:** Single risk register with risk types: AI risks (bias, drift, explainability) and security risks (confidentiality, integrity, availability)

Clause 7: Support

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
7.1 Resources	Provide AI resources	Provide security resources	95%	Unified resource planning and allocation
7.2 Competence	Ensure AI competence	Ensure security competence	85%	Combined competency framework for AI and security
7.3 Awareness	AI awareness program	Security awareness program	90%	Unified awareness training covering both topics
7.4 Communication	AI communication plan	Security communication plan	95%	Single communication strategy for both
7.5 Documented Info	AIMS documentation control	ISMS documentation control	100%	Single document management system for both

- **Training Program:** Unified 'AI & Security Awareness Training' covering both disciplines
- **Document Repository:** Single controlled document library with AI and security policies, procedures, records

Clause 8: Operation

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
8.1 Planning	Operational planning and control for AI	Plan, implement, control security processes	85%	Unified operational procedures
8.2 AI Lifecycle	AI system lifecycle management (NEW)	N/A (use 27001 A.8.25 SDLC)	60%	AI lifecycle procedures reference security SDLC
8.3 Supply Chain	AI supply chain management (NEW)	Supplier security (A.5.19-A.5.22)	70%	Integrated supply chain security with AI-specific criteria

- **Critical Integration:** AI system lifecycle (ISO 42001 8.2) must incorporate security controls from ISO 27001 A.8 (Technological controls)
- **Example Integration:** AI model development (ISO 42001) + Secure development (ISO 27001 A.8.25-A.8.28)

Clause 9: Performance Evaluation

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
9.1 Monitoring	Monitor, measure, analyze AI performance	Monitor, measure, analyze security performance	80%	Unified monitoring dashboard covering both
9.2 Internal Audit	AIMS internal audit	ISMS internal audit	95%	Combined audit program addressing both standards
9.3 Management Review	AIMS management review	ISMS management review	100%	Single management review meeting covering both systems

- **Unified Audit Program:** Single internal audit covering both ISO 42001 and ISO 27001 requirements
- **Combined Management Review:** Quarterly/annual review addressing both AIMS and ISMS performance
- **Monitoring Metrics:** AI performance metrics (accuracy, fairness, drift) + Security metrics (incidents, vulnerabilities, compliance)

Clause 10: Improvement

Sub-Clause	ISO 42001 Requirement	ISO 27001 Requirement	Overlap	Integration Approach
10.1 Nonconformity	Address AI nonconformities	Address security nonconformities	95%	Single corrective action process for both
10.2 Continual Improvement	Continually improve AIMS	Continually improve ISMS	100%	Unified improvement program

- **Corrective Action Register:** Single register tracking AI and security nonconformities
- **Improvement Register:** Unified tracking of improvements to both systems

ISO 42001 AI-Specific Requirements and ISO 27001 Control Mapping

ISO 42001 introduces AI-specific requirements that extend beyond traditional ISO 27001. Here is how they integrate:

AI Impact Assessment (ISO 42001 6.1.3)

ISO 42001 Requirement	Related ISO 27001 Controls	Integration Approach
AI system impact assessment considering: individual rights, societal impacts, environmental impacts, fairness, bias	A.5.34 Privacy and protection of PII, A.5.31 Legal requirements, A.5.7 Threat intelligence	Extend ISO 27001 privacy impact assessment (DPIA) to include AI-specific impacts: bias, fairness, environmental sustainability, algorithmic transparency

AI System Lifecycle (ISO 42001 8.2)

ISO 42001 Requirement	Related ISO 27001 Controls	Integration Approach
8.2.1 Data management for AI	A.8.11 Data masking, A.5.34 Privacy, A.5.12 Classification	Apply ISO 27001 data security controls to training/inference data with AI-specific extensions
8.2.2 AI system design and development	A.8.25-A.8.28 Secure development lifecycle	Integrate AI development into secure SDLC; add AI-specific validation steps
8.2.3 AI system verification and validation	A.8.29 Security testing in development	Extend security testing to include AI-specific validation: fairness testing, bias detection, adversarial testing
8.2.4 AI system deployment	A.8.31-A.8.32 Change management, deployment	Apply secure deployment controls to AI model deployment; add AI-specific checks
8.2.5 AI system operation and monitoring	A.8.16 Monitoring activities, A.8.15 Logging	Extend security monitoring to AI-specific metrics: model drift, performance degradation, bias metrics
8.2.6 AI system continual learning	A.8.8 Management of technical vulnerabilities	Treat model retraining like patching; apply change control and testing

AI Supply Chain (ISO 42001 8.3)

ISO 42001 Requirement	Related ISO 27001 Controls	Integration Approach
Third-party AI models, foundation models, AI services	A.5.19-A.5.22 Supplier relationships, A.5.23 Cloud services	Apply ISO 27001 supplier security with AI-specific criteria: model provenance, AI-BOM, bias testing, performance SLAs
Open-source AI components	A.5.21 ICT supply chain security	Extend software supply chain security to include open-source AI models, datasets, libraries

Unified Documentation Structure

Organizations can dramatically reduce documentation burden by creating unified documents that satisfy both standards:

Unified Document Name	Satisfies ISO 42001	Satisfies ISO 27001
AI & Information Security Policy	Clause 5.2 AI Policy	Clause 5.2 Information Security Policy
Context Analysis & Scope Statement	Clause 4 Context and Scope	Clause 4 Context and Scope
Risk Assessment Methodology	Clause 6.1.2 AI Risk Assessment	Clause 6.1.2 Information Security Risk Assessment
Risk Register	Clause 6.1.2 AI Risks	Clause 6.1.2 Security Risks
Risk Treatment Plan	Clause 6.1.4 AI Risk Treatment	Clause 6.2 Risk Treatment
Roles & Responsibilities Matrix	Clause 5.3 AI Roles	Clause 5.3 Security Roles
Awareness Training Program	Clause 7.3 AI Awareness	Clause 7.3 Security Awareness
Operational Procedures Manual	Clause 8 AI Operations	Clause 8 Security Operations
Internal Audit Program	Clause 9.2 AIMS Audit	Clause 9.2 ISMS Audit
Management Review Template	Clause 9.3 AIMS Review	Clause 9.3 ISMS Review
Corrective Action Register	Clause 10.1 AI Nonconformities	Clause 10.1 Security Nonconformities
Supplier Security Assessment	Clause 8.3 AI Supply Chain	A.5.19-A.5.22 Supplier Controls
Incident Response Plan	Clause 8.2.5 AI Incidents	A.5.24-A.5.28 Incident Management
Change Management Procedure	Clause 6.3, 8.2.4 AI Changes	A.8.32 Change Management

Dual Certification Audit Strategy

Sequential vs. Simultaneous Certification

Organizations have two main pathways to dual certification:

Approach	Advantages	Considerations
Sequential: ISO 27001 First, Then ISO 42001	Build security foundation first; ISMS provides structure for AIMS; Many auditors more familiar with 27001	Longer total timeline (12-18 months); May need to retrofit AI-specific requirements
Sequential: ISO 42001 First, Then ISO 27001	Focus on AI governance priorities; Build AI-specific controls from start	Less common path; Harder to find AI auditors first; May need to add detailed security controls later
Simultaneous: Both Together	Shortest total timeline (12-15 months); Unified system from start; Single integrated audit	More complex initial planning; Requires experienced auditors familiar with both; Higher upfront effort

Recommended Approach: Simultaneous Certification

For organizations implementing both standards, simultaneous certification is most efficient:

- **Month 0-3:** Foundation - Unified scope, policy, roles, context analysis
- **Month 3-6:** Risk Management - Combined risk assessment, treatment planning
- **Month 6-9:** Implementation - Deploy controls, procedures, monitoring
- **Month 9-12:** Validation - Internal audits, management review, gap remediation
- **Month 12-15:** Certification - Stage 1 audits (both standards), Stage 2 audits (both standards)

Combined Audit Approach

Request certification body to conduct combined audits:

Audit Phase	ISO 42001 Focus	ISO 27001 Focus	Duration
Stage 1: Documentation	AIMS scope, policy, procedures, risk assessment, AI lifecycle	ISMS scope, policy, procedures, risk assessment, Annex A controls	2-4 days (combined)
Stage 2: Implementation	AI system implementation, impact assessments, monitoring, AI supply chain	Security controls implementation, incident response, access control, monitoring	4-8 days (combined)
Surveillance Year 1-2	AI system changes, new AI projects, AI risk reviews	Security control effectiveness, new risks, incidents	1-2 days/year (combined)
Recertification Year 3	Full AIMS reassessment	Full ISMS reassessment	Same as initial (combined)

Cost Savings: Combined audits typically cost 30-40% less than separate audits for each standard.

Effort Reduction Through Integration

Quantifying the benefits of integrated implementation:

Activity	Separate Implementation	Integrated Implementation	Effort Reduction
Policy Development	2 policies (AI + Security)	1 unified policy	50% reduction
Risk Assessment	2 separate assessments	1 unified assessment	40% reduction
Internal Audits	2 audit programs	1 combined audit	45% reduction
Management Reviews	2 separate meetings	1 combined meeting	50% reduction
Training Programs	2 separate programs	1 unified program	35% reduction
Documentation Control	2 document systems	1 unified system	40% reduction
Certification Audits	2 separate audits	1 combined audit	35% reduction
Annual Surveillance	2 separate audits/year	1 combined audit/year	40% reduction

Overall Implementation Effort Reduction: 40-50%

Annual Maintenance Effort Reduction: 35-45%

Common Integration Pitfalls and How to Avoid Them

Pitfall	Impact	How to Avoid
Treating standards as separate silos	Duplicate documentation, wasted effort, inconsistent approaches	Create unified management system from day one; use integrated documentation structure
Focusing only on AI, neglecting security	ISO 42001 without proper security controls; vulnerable AI systems	Ensure every AI system has security controls from ISO 27001 Annex A
Focusing only on security, neglecting AI-specific risks	ISO 27001 without AI governance; blind to bias, fairness, explainability risks	Extend ISMS to include AI-specific risk assessment and impact assessment
Different teams for ISO 42001 vs ISO 27001	Lack of coordination, duplicate work, conflicting requirements	Single combined team with both AI and security expertise
Separate audit schedules	More disruption, higher costs, coordination burden	Negotiate combined audit schedule with certification body
AI system inventory separate from asset inventory	Inconsistent asset tracking, gap in coverage	Extend ISO 27001 A.5.9 asset inventory to include AI systems (models, data, infrastructure)
Different risk registers	Inconsistent risk treatment, missed dependencies between AI and security risks	Single unified risk register with both AI and security risk types

Dual Certification Implementation Checklist

Phase 1: Foundation (Months 0-3)

- ☐ Establish executive sponsorship for dual certification
- ☐ Form unified AI & Security governance team
- ☐ Create unified context analysis (ISO 42001 4.1 + ISO 27001 4.1)
- ☐ Define unified AIMS-ISMS scope (ISO 42001 4.3 + ISO 27001 4.3)
- ☐ Draft unified AI & Information Security Policy (ISO 42001 5.2 + ISO 27001 5.2)
- ☐ Assign combined roles and responsibilities (ISO 42001 5.3 + ISO 27001 5.3)
- ☐ Create AI system inventory extending asset inventory (ISO 42001 8.1 + ISO 27001 A.5.9)

Phase 2: Risk Management (Months 3-6)

- ☐ Develop unified risk assessment methodology (ISO 42001 6.1.2 + ISO 27001 6.1.2)
- ☐ Conduct combined risk assessment covering AI and security risks
- ☐ Perform AI system impact assessments (ISO 42001 6.1.3)
- ☐ Create unified risk treatment plan (ISO 42001 6.1.4 + ISO 27001 6.2)
- ☐ Define combined objectives and KPIs (ISO 42001 6.2 + ISO 27001 6.2)
- ☐ Document Statement of Applicability for ISO 27001 Annex A controls

Phase 3: Implementation (Months 6-9)

- ☐ Implement AI system lifecycle procedures (ISO 42001 8.2)
- ☐ Deploy security controls from ISO 27001 Annex A with AI extensions
- ☐ Establish unified monitoring and measurement (ISO 42001 9.1 + ISO 27001 9.1)
- ☐ Deploy unified awareness training program (ISO 42001 7.3 + ISO 27001 7.3)
- ☐ Implement combined incident response plan (ISO 42001 8.2.5 + ISO 27001 A.5.24-A.5.28)
- ☐ Establish AI supply chain security (ISO 42001 8.3 + ISO 27001 A.5.19-A.5.22)

Phase 4: Validation (Months 9-12)

- ☐ Conduct unified internal audit (ISO 42001 9.2 + ISO 27001 9.2)
- ☐ Hold combined management review (ISO 42001 9.3 + ISO 27001 9.3)
- ☐ Remediate findings from internal audit
- ☐ Complete 3+ months of operational evidence
- ☐ Select certification body with dual certification capability

Phase 5: Certification (Months 12-15)

- ☐ Schedule combined Stage 1 audit (both standards)
- ☐ Address Stage 1 findings
- ☐ Schedule combined Stage 2 audit (both standards)
- ☐ Address Stage 2 findings
- ☐ Receive dual certification

Summary: Key Integration Principles

- **1. Single Management System:** Create one unified AIMS-ISMS, not two separate systems
- **2. Unified Documentation:** Single policy, scope, risk register, audit program, management review
- **3. AI Extensions to Security:** Extend ISO 27001 controls with AI-specific implementations
- **4. Security Foundations for AI:** Apply ISO 27001 security controls to every AI system
- **5. Combined Governance:** Single team, single leadership, unified objectives
- **6. Integrated Audits:** Request combined certification audits for efficiency
- **7. Shared PDCA Cycle:** Plan-Do-Check-Act applies to both AI and security

Result: 40-50% reduction in implementation effort, 35-45% reduction in ongoing maintenance

Document Control

Document Information	Details
Document Title	Appendix C: ISO 42001-to-ISO 27001 Integration Matrix
Version	1.0
Date	January 2026
Author	AI RMF 2026 Integration Project
Classification	Public
Review Cycle	Annual or upon standard updates
Related Documents	ISO 42001:2023, ISO 27001:2022, Appendices A and B
Purpose	Enable efficient dual certification through integrated implementation

End of Appendix C

Appendix D1-D2

EU AI Act Compliance Mapping

AI RMF 2026, ISO 42001, ISO 27001 Alignment with EU Regulation 2024/1689

Version 1.0 | January 2026

Introduction

The EU Artificial Intelligence Act (AI Act), formally known as Regulation (EU) 2024/1689, entered into force on August 1, 2024, and represents the world's first comprehensive legal framework for artificial intelligence. This appendix demonstrates how implementing AI RMF 2026, ISO 42001, and ISO 27001 positions organizations for EU AI Act compliance.

EU AI Act Overview

- **Status:** Entered into force August 1, 2024; phased implementation through 2027
- **Scope:** Applies to providers and deployers of AI systems in the EU market
- **Approach:** Risk-based classification (Unacceptable, High-Risk, Limited Risk, Minimal Risk)
- **Penalties:** Up to €35M or 7% of global turnover for serious violations
- **Key Requirements:** Risk management, data governance, transparency, human oversight, accuracy, robustness

Implementation Timeline

Date	Milestone	Requirements
Aug 1, 2024	Entered into force	General obligation to understand applicability begins
Feb 2, 2025	Prohibited AI ban	Unacceptable risk AI systems must be discontinued
Aug 2, 2025	Governance obligations	AI governance structures, codes of practice must be established
Aug 2, 2026	General-purpose AI	GPAI model requirements, transparency obligations apply
Aug 2, 2027	High-risk AI systems	Full compliance for high-risk AI systems required

EU AI Act Risk Classification

The AI Act categorizes AI systems into four risk levels. Understanding your classification is the first step:

Risk Level	Definition	Examples	Compliance Approach
Unacceptable Risk	AI prohibited due to threats to safety, livelihoods, rights	Social scoring, real-time biometric ID in public, exploitation of vulnerabilities	Discontinue immediately (banned Feb 2025)
High-Risk	AI with significant impact on health, safety, fundamental rights	Critical infrastructure, employment, law enforcement, education, credit scoring	Full AI Act compliance + conformity assessment
Limited Risk	AI with transparency obligations	Chatbots, emotion recognition, biometric categorization, deepfakes	Transparency requirements only
Minimal Risk	AI with no/low risk	AI-enabled video games, spam filters, inventory management	Voluntary codes of conduct

- **AI RMF/ISO Support:** AI RMF 2026 MAP function + ISO 42001 Clause 6.1.3 (Impact Assessment) provides systematic approach to risk classification

High-Risk AI System Requirements

Organizations with high-risk AI systems must comply with comprehensive requirements in Title III, Chapter 2 of the AI Act. This section maps those requirements to AI RMF 2026, ISO 42001, and ISO 27001:

Article 9: Risk Management System

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Establish risk management system throughout lifecycle	MAP 4.1, MANAGE 1.1	Clause 6.1.2 AI Risk Assessment	Clause 6.1.2 Risk Assessment
Identify and analyze known and foreseeable risks	MAP 4.2, 4.3	Clause 6.1.2 Risk Identification	Clause 6.1.2 Risk Identification
Estimate and evaluate risks	MAP 2.3	Clause 6.1.2 Risk Analysis	Clause 6.1.2 Risk Analysis
Adopt risk mitigation measures	MANAGE 1.2	Clause 6.1.4 Risk Treatment	Clause 6.2 Risk Treatment
Test risk mitigation effectiveness	MEASURE 1.3, 4.3	Clause 8.2.3 Validation	A.8.29 Security Testing
Consider risks from foreseeable misuse	MAP 3.2	Clause 6.1.2 Risk Assessment	A.5.7 Threat Intelligence

Compliance Pathway: Organizations implementing MAP + MANAGE functions with ISO 42001 Clause 6 substantially satisfy Article 9.

Article 10: Data and Data Governance

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Training, validation, testing datasets relevant, representative, free of errors	MEASURE 2.1	Clause 8.2.1 Data Management	A.8.11 Data Masking
Data governance practices for quality of datasets	MAP 2.3	Clause 8.2.1 Data Governance	A.5.12 Classification of Information
Examination of biases in datasets	MAP 5.3, MEASURE 2.5	Clause 6.1.3 Impact Assessment	A.5.34 Privacy and PII
Detection and correction of biases	MANAGE 1.2, 4.2	Clause 10.2 Continual Improvement	A.8.8 Management of Vulnerabilities
Data processing in compliance with GDPR	GOVERN 6.2, MAP 5.4	Clause 6.3 Compliance Obligations	A.5.34 Privacy and Protection of PII

Compliance Pathway: ISO 42001 Clause 8.2.1 (Data Management for AI) directly addresses Article 10 requirements.

Article 11: Technical Documentation

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
General description of AI system	MAP 1.2, 2.2	Clause 8.2.2 AI System Documentation	A.5.9 Inventory of Assets
Detailed description of elements and development process	MAP 1.3, 3.3	Clause 8.2.2 Development Documentation	A.8.25 Secure Development Lifecycle
Information on monitoring, functioning, control of AI system	MEASURE 3.1, 3.2	Clause 9.1 Monitoring and Measurement	A.8.16 Monitoring Activities
Description of risk management system	MANAGE 1.1	Clause 6.1.2 Risk Assessment Documentation	Clause 6.1.2 Risk Assessment
Description of changes made throughout lifecycle	MANAGE 4.3	Clause 8.2.4 Deployment, 8.2.6 Continual Learning	A.8.32 Change Management
List of harmonized standards applied	GOVERN 1.1	Clause 6.3 Compliance	Clause 6.1.3 Legal Requirements

Compliance Pathway: ISO 42001 Clause 8.2.2 + ISO 27001 Clause 7.5 (Documented Information) provide structure for Article 11 documentation.

Article 12: Record-Keeping (Logging)

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Automatic recording of events (logs)	MEASURE 3.1	Clause 9.1 Monitoring	A.8.15 Logging
Logs enable monitoring throughout lifecycle	MEASURE 3.2	Clause 8.2.5 Operation and Monitoring	A.8.16 Monitoring Activities
Logs facilitate post-market monitoring	MEASURE 3.3	Clause 9.1 Performance Evaluation	A.8.16 Monitoring Activities
Appropriate logging level (functionality, risks, context)	MEASURE 2.2	Clause 9.1.1 Metrics	A.8.15 Logging

Compliance Pathway: ISO 27001 A.8.15 (Logging) + A.8.16 (Monitoring) extended for AI-specific logs satisfy Article 12.

Article 13: Transparency and Information to Deployers

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Instructions for use (intended purpose, specifications)	MANAGE 3.1, 3.2	Clause 8.2.2 Documentation	A.5.10 Acceptable Use
Information on human oversight measures	MANAGE 3.1	Clause 8.2.2 Human Oversight Documentation	A.6.2 Terms and Conditions
Information on expected lifetime and maintenance	MANAGE 3.2	Clause 8.2.2 Lifecycle Information	A.7.13 Equipment Maintenance
Description of known or foreseeable risks	MAP 3.2, MANAGE 3.2	Clause 6.1.2 Risk Communication	A.5.7 Threat Intelligence

Compliance Pathway: AI RMF 2026 MANAGE 3 (Disclosure) + ISO 42001 Clause 7.4 (Communication) address Article 13.

Article 14: Human Oversight

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Human oversight measures integrated into system	GOVERN 2.1, MANAGE 1.2	Clause 8.2.2 Human Oversight Design	A.5.18 Access Rights
Humans can understand AI system capabilities and limitations	MANAGE 3.2	Clause 7.3 Awareness	A.6.3 Information Security Awareness
Humans can monitor operation and interpret outputs	MEASURE 3.1	Clause 9.1 Monitoring	A.8.16 Monitoring Activities
Humans can intervene or interrupt the system	MANAGE 2.1	Clause 8.2.5 Incident Management	A.5.26 Response to Incidents
Deployers assign oversight to competent persons	GOVERN 1.2	Clause 7.2 Competence	A.6.2 Terms and Conditions

Compliance Pathway: AI RMF 2026 GOVERN 2 (Accountability) + ISO 42001 human oversight requirements satisfy Article 14.

Article 15: Accuracy, Robustness, and Cybersecurity

EU AI Act Requirement	AI RMF 2026	ISO 42001	ISO 27001
Appropriate level of accuracy	MEASURE 1.1, 2.2	Clause 9.1 Performance Metrics	A.8.29 Security Testing
Robustness against errors and faults	MEASURE 2.5, MANAGE 1.3	Clause 8.2.3 Validation	A.8.14 Redundancy
Resilience against attempts to alter use or performance	MANAGE 1.2	Clause 6.1.2 Risk Assessment (Adversarial)	A.8.29 Security Testing
Cybersecurity measures	MANAGE 1.2	Clause 6.1.2 Security Risks	ALL of ISO 27001 Annex A

Compliance Pathway: AI RMF 2026 MEASURE function + ISO 27001 comprehensive security controls satisfy Article 15.

Provider vs. Deployer Obligations

The AI Act distinguishes between providers (who develop/supply AI) and deployers (who use AI). Understanding your role is critical:

Role	Definition	Key Obligations
Provider	Person/entity that develops AI system or has it developed, places it on market under their name/trademark	Risk management, data governance, technical documentation, conformity assessment, CE marking, post-market monitoring
Deployer	Person/entity that uses AI system under their authority (except personal non-professional use)	Use AI according to instructions, monitor operation, human oversight, report serious incidents, data protection impact assessment (if required)
Importer	Person/entity established in EU that places on market AI system bearing name of provider outside EU	Ensure conformity assessment completed, keep documentation, inform authorities of non-conforming systems
Distributor	Person/entity in supply chain that makes AI system available on EU market	Verify CE marking exists, verify documentation provided, inform authorities of non-conforming systems

- **Critical Note:** Deployers can become providers if they substantially modify the AI system or change its intended purpose

Conformity Assessment for High-Risk AI

High-risk AI systems require conformity assessment before placing on the market. The AI Act allows different assessment procedures:

Assessment Type	When Applicable	Procedure
Internal Control (Annex VI)	Provider has ISO 42001 certification OR applied harmonized standards OR common specifications	Self-assessment based on technical documentation and quality management system
Third-Party Assessment (Annex VII)	AI system for biometric identification/categorization, critical infrastructure, law enforcement	Notified body assesses technical documentation and quality management system
Special Procedure (Article 43)	AI systems by law enforcement, immigration, asylum authorities	Assessment by designated competent authority

- **ISO 42001 Advantage:** Organizations with ISO 42001 certification can use internal control procedure (faster, less expensive) instead of mandatory third-party assessment
- **Path to Internal Control:** Implement AI RMF 2026 + achieve ISO 42001 certification → qualify for self-assessment

General-Purpose AI Models (GPAI)

The AI Act includes specific requirements for general-purpose AI models, particularly those with systemic risks:

GPAI Category	Definition	Requirements	AI RMF 2026 Alignment
Standard GPAI	Foundation models for general tasks	Technical documentation, transparency info, copyright compliance	AI RMF MAP 2.2, ISO 42001 8.2.2, ISO 27001 A.5.32
GPAI with Systemic Risk	High-impact capability or reach (e.g., >10^25 FLOPs training)	Above + model evaluation, adversarial testing, serious incident tracking, cybersecurity	AI RMF MEASURE 4.3, ISO 42001 6.1.2, ISO 27001 A.8.29
Downstream Provider	Uses GPAI to build specific system	Comply with high-risk requirements if applicable, cooperate with GPAI provider	Full AI RMF 2026 42001/27001 framework

- **Key Obligation:** GPAI providers must make summary of training content available (copyright concerns)
- **Systemic Risk Threshold:** ≥10^25 FLOPs OR equivalent performance/reach/impact as determined by Commission

Transparency Obligations (Limited Risk)

Even AI systems that are not high-risk have transparency obligations if they fall into these categories:

AI System Type	Transparency Requirement	AI RMF 2026 Implementation
AI systems interacting with people	Inform users they are interacting with AI (unless obvious from context)	AI RMF MANAGE 3.1, ISO 42001 7.4 Communication
Emotion recognition systems	Inform users that emotion recognition is taking place	AI RMF MANAGE 3.1, ISO 42001 7.4 Communication
Biometric categorization	Inform users that biometric categorization is occurring	AI RMF MANAGE 3.1, ISO 42001 7.4 Communication
AI-generated content (deepfakes)	Clearly label content as artificially generated/manipulated; machine-readable disclosure	AI RMF MANAGE 3.3, ISO 42001 7.4 Communication
AI-generated text content	Disclose that AI generates content	AI RMF MANAGE 3.3, ISO 42001 7.4 Communication

- **Exception:** Transparency not required if obvious from circumstances (e.g., clearly labeled chatbot interface)

AI Literacy and Organizational Governance

The AI Act requires providers and deployers to ensure sufficient AI literacy among their staff:

AI Act Requirement	AI RMF 2026 Alignment	ISO 42001/27001 Alignment
Providers/deployers ensure staff have sufficient AI literacy	GOVERN 4.1, 4.2 AI Awareness	ISO 42001 7.3 Awareness, ISO 27001 7.3 Awareness, A.6.3
AI literacy appropriate to level of responsibility	GOVERN 1.3 Competence	ISO 42001 7.2 Competence, ISO 27001 7.2 Competence
Understanding of AI capabilities, limitations, impact	GOVERN 4.2 Awareness Training	ISO 42001 7.3 AI Awareness Program
Ability to interpret AI outputs appropriately	GOVERN 4.2, MEASURE 3.1	ISO 42001 7.3 + 9.1 Monitoring
Awareness of risks from misuse	GOVERN 4.3 Supply Chain Awareness	ISO 42001 7.3, ISO 27001 A.6.3

Comprehensive Compliance Matrix

This matrix shows how implementing the integrated framework addresses all major EU AI Act requirements:

AI Act Article	Requirement	AI RMF 2026	ISO 42001	ISO 27001	Coverage
Art. 9	Risk Management	MAP, MANAGE	6.1.2-6.1.4	6.1.2-6.2	95%
Art. 10	Data Governance	MAP, MEASURE	8.2.1	A.8.11, A.5.34	90%
Art. 11	Documentation	MAP 2.2	8.2.2, 7.5	7.5, A.5.9	95%
Art. 12	Logging	MEASURE 3	9.1	A.8.15, A.8.16	100%
Art. 13	Transparency	MANAGE 3	7.4	A.5.10	90%
Art. 14	Human Oversight	GOVERN 2, MANAGE	8.2.2	A.5.18, A.6.2	85%
Art. 15	Accuracy/Robustness	MEASURE	9.1, 8.2.3	Annex A	90%
Art. 16	Quality Management	GOVERN, All	All Clauses	All Clauses	95%
Art. 17	Post-Market Monitoring	MEASURE 3	9.1	A.8.16	90%
Art. 52	Transparency (Limited)	MANAGE 3	7.4	N/A	90%
Art. 53	AI Literacy	GOVERN 4	7.2, 7.3	7.2, 7.3	95%

Overall Compliance Coverage: 90-95%

Gaps and Additional EU AI Act-Specific Requirements

While AI RMF 2026 implementation provides 90-95% coverage, organizations must address these AI Act-specific requirements:

1. CE Marking and Declaration of Conformity

- **Requirement:** Affix CE marking to high-risk AI systems; draw up EU declaration of conformity
- **AI RMF 2026 Gap:** Neither standard addresses CE marking procedures
- **Action Needed:** Follow EU conformity assessment procedures (Annex V, VI, or VII)

2. Registration in EU Database

- **Requirement:** Register high-risk AI systems in EU database before placing on market
- **AI RMF 2026 Gap:** Not addressed in standards
- **Action Needed:** Register in EU database (details to be provided by Commission)

3. Serious Incident Reporting

- **Requirement:** Report serious incidents and malfunctions to national authorities within 15 days
- **AI RMF 2026 Coverage:** Incident management covered (MANAGE 2, ISO 42001 8.2.5, ISO 27001 A.5.24-A.5.28)
- **Gap:** Specific 15-day authority notification requirement
- **Action Needed:** Add EU authority notification to incident response procedures

4. Cooperation with Authorities

- **Requirement:** Provide authorities with documentation, access, cooperation on request
- **AI RMF 2026 Coverage:** Communication covered (ISO 42001 7.4, ISO 27001 A.5.6)
- **Action Needed:** Document authority cooperation procedures

EU AI Act Compliance Roadmap

Recommended phased approach for organizations implementing AI RMF 2026 framework to achieve EU AI Act compliance:

Phase 1: Assessment (Months 1-3)

- Inventory all AI systems in organization
- Classify each system: Unacceptable, High-Risk, Limited Risk, Minimal Risk
- Determine if you are provider, deployer, or both for each system
- Identify which systems require conformity assessment
- Gap analysis: current state vs. EU AI Act requirements

Phase 2: Foundation (Months 3-9)

- Implement AI RMF 2026 (all four functions)
- Establish ISO 42001 AIMS (target certification)
- Implement/extend ISO 27001 ISMS for AI systems
- Discontinue any unacceptable risk AI systems

Phase 3: EU-Specific Requirements (Months 9-15)

- Prepare technical documentation per Article 11
- Implement transparency measures for limited risk systems
- Add EU authority notification to incident procedures
- Prepare for conformity assessment (internal or third-party)

Phase 4: Certification and Conformity (Months 15-24)

- Achieve ISO 42001 certification (enables internal conformity assessment)
- Complete conformity assessment for high-risk systems
- Affix CE marking and draw up EU declaration of conformity
- Register high-risk AI systems in EU database
- Establish post-market monitoring per Article 72

Target: Full EU AI Act compliance by August 2027 (high-risk deadline)

Summary: The Strategic Value of Integrated Implementation

Organizations implementing AI RMF 2026, ISO 42001, and ISO 27001 gain significant advantages for EU AI Act compliance:

Coverage Advantage

- 90-95% of EU AI Act requirements already satisfied
- Comprehensive risk management, data governance, documentation foundation
- Only EU-specific procedural requirements (CE marking, registration) need addition

Conformity Assessment Advantage

- ISO 42001 certification enables internal control (self-assessment)
- Avoids costly and time-consuming third-party conformity assessment
- Faster time to market for high-risk AI systems

Global Standards Alignment

- Single framework satisfies: NIST (US), ISO (global), EU AI Act (Europe)
- Positions for other regulations: UK AI framework, Singapore, Japan
- Future-proof as standards converge globally

Business Value

- Demonstrate compliance to EU customers and partners
- Reduce legal and regulatory risk exposure (penalties up to €35M/7% turnover)
- Build trust through internationally recognized standards and EU compliance
- Competitive advantage in EU market where AI Act compliance is mandatory

Document Control

Document Information	Details
Document Title	Appendix D: EU AI Act Compliance Mapping
Version	1.0
Date	January 2026
Author	AI RMF 2026 Integration Project
Classification	Public
Review Cycle	Quarterly (during AI Act implementation period); Annual thereafter
Related Documents	EU Regulation 2024/1689, AI RMF 2026 1.0, ISO 42001:2023, ISO 27001:2022
Regulatory Status	AI Act entered force Aug 2024; high-risk requirements apply Aug 2027
Purpose	Enable EU AI Act compliance through integrated AI RMF 2026 implementation

Appendix D2

EU AI Act

Articles 9-15 Requirements

& Complete Compliance Matrices

High-Risk AI Systems Implementation Guide

Version 1.0 | January 2026

Document Purpose

This document provides comprehensive guidance on implementing the requirements for high-risk AI systems under Articles 9-15 of the EU AI Act (Regulation (EU) 2024/1689). It includes detailed compliance matrices showing how AI RMF and ISO 42001/27001 implementations satisfy EU AI Act requirements.

Scope

This guide applies to:

- Providers of high-risk AI systems placing products on the EU market
- Deployers of high-risk AI systems operating in the EU
- Organizations with existing AI RMF or ISO 42001/27001 implementations seeking EU AI Act compliance
- Technical teams responsible for AI system development, deployment, and monitoring

How to Use This Document

Each article section contains:

1. **Legal Text:** Exact requirements from the EU AI Act
2. **Detailed Requirements:** Breaking down what must be implemented
3. **Compliance Matrix:** Mapping to AI RMF categories and ISO clauses
4. **Implementation Guidance:** Practical steps and best practices
5. **Evidence Requirements:** What documentation auditors will expect

Contents

Appendix A: Complete Cross-Reference Matrix
All EU AI Act Requirements mapped to AI RMF and ISO Standards

Appendix B: Evidence Collection Guide
Required documentation for conformity assessment

Article 9: Risk Management System

9.1 Legal Requirements

Article 9(1) - EU AI Act:

"A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems, consisting of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and update."

The risk management system shall comprise the following steps:

6. **Identification and analysis of known and reasonably foreseeable risks** associated with each high-risk AI system
7. **Estimation and evaluation of the risks** that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse
8. **Evaluation of other possibly arising risks** based on the analysis of data gathered from the post-market monitoring system
9. **Adoption of suitable risk management measures** in accordance with the provisions of the following paragraphs
10. **Testing to ensure risk management measures** are effective and functioning properly

9.2 Detailed Implementation Requirements

9.2.1 Risk Identification and Analysis

Scope of Risk Identification:

- **Health and Safety Risks:** Physical harm, psychological harm, health impacts from AI system failures or outputs
- **Fundamental Rights Risks:** Privacy violations, discrimination, bias, freedom of expression, due process, access to justice, right to fair trial, protection of personal data
- **Technical Risks:** Model inaccuracy, robustness failures, adversarial attacks, data poisoning, model drift, system failures
- **Operational Risks:** Misuse, unintended use cases, interaction with other systems, dependency failures
- **Environmental Risks:** Deployment context changes, edge cases, novel scenarios not seen in training

Risk Analysis Methods Required:

- Hazard analysis (HAZOP, FMEA, or equivalent)
- Threat modeling for adversarial scenarios
- Bias and fairness analysis across demographic groups
- Privacy impact assessment (DPIA where applicable)

- Fundamental rights impact assessment
- Use case analysis including reasonably foreseeable misuse

9.2.2 Risk Estimation and Evaluation

Risk Assessment Criteria Must Include:

- **Severity:** Impact on health, safety, fundamental rights (catastrophic, critical, major, minor, negligible)
- **Probability:** Likelihood of occurrence (frequent, probable, occasional, remote, improbable)
- **Affected Population:** Number of individuals potentially impacted
- **Vulnerable Groups:** Special consideration for children, elderly, persons with disabilities, marginalized groups
- **Detectability:** Whether the issue can be identified before causing harm

Risk Matrix (Example Framework):

Severity	Very Low Probability	Low Probability	Medium Probability	High Probability
Catastrophic (Life, fundamental rights)	High Risk	High Risk	Critical Risk	Critical Risk
Critical (Serious harm)	Medium Risk	High Risk	High Risk	Critical Risk
Major (Significant impact)	Low Risk	Medium Risk	High Risk	High Risk
Minor (Limited impact)	Low Risk	Low Risk	Medium Risk	Medium Risk
Negligible (No significant impact)	Acceptable	Low Risk	Low Risk	Medium Risk

9.2.3 Risk Treatment Measures

Hierarchy of Risk Management (Article 9(4)):

11. **Eliminate or reduce risks as far as possible** through adequate design and development (design controls)
    - Technical design modifications to prevent risks
    - Algorithm selection to minimize bias
    - Architecture changes for robustness
    - Data quality improvements

12. **Implement adequate mitigation and control measures** for risks that cannot be eliminated (operational controls)
    - Human oversight mechanisms
    - Monitoring and alerting systems
    - Fail-safe mechanisms and fallback procedures
    - Access controls and usage restrictions

13. **Provide appropriate information to deployers** (residual risk communication)
    - Instructions for use (Article 13)
    - Known limitations and contraindications
    - Required oversight and intervention procedures
    - Training requirements for users

14. **Where appropriate, provide training to deployers** on proper use and risk awareness

9.2.4 Continuous Risk Management Throughout Lifecycle

Ongoing Requirements:

- **Testing During Development:** Validate risk management measures work as intended
- **Post-Market Monitoring:** Article 9(2)(c) requires evaluation of emerging risks based on post-market data
- **Regular Systematic Updates:** Review and update risk management system at defined intervals
- **Incident-Triggered Reviews:** Update risk assessment when serious incidents occur
- **Change Management:** Re-assess risks when AI system is substantially modified

9.3 Article 9 Compliance Matrix

The following matrix demonstrates how AI RMF and ISO 42001/27001 implementations satisfy Article 9 requirements:

EU AI Act Article 9 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Establish, implement, document, maintain risk management system	GOVERN 1.3 MAP 4 MANAGE 1	6.1.2 (AI risk assessment) 6.1.4 (Risk treatment)	6.1.3 (Info security risk assessment)	Direct
Continuous iterative process throughout lifecycle	MANAGE 4 (Continuous Improvement)	10.2 (Continual improvement)	10.2 (Continual improvement)	Direct
Regular systematic review and update	GOVERN 5.1 (Oversight) MANAGE 4.2	9.3 (Management review)	9.3 (Management review)	Direct
Identify and analyze known and foreseeable risks to health, safety, fundamental rights	MAP 3 (Impacts) MAP 4.1-4.6	6.1.3 (AI impact assessment)	A.5.7 (Threat intelligence)	Direct
Consider risks from intended purpose and reasonably foreseeable misuse	MAP 1.2 (Intended purpose) MAP 4	6.1.2 (Risk assessment methodology)	6.1.3 (Risk assessment process)	Direct
Estimate and evaluate risks with severity and probability	MAP 4 (Risk assessment)	6.1.2 (AI risk assessment)	6.1.3 (Risk assessment)	Direct

Evaluate emerging risks from post-market monitoring data	MEASURE 4 (Monitoring) MANAGE 4.2	9.1 (Monitoring and measurement) 10.2 (Improvement)	A.8.16 (Monitoring activities)	Substantial
Eliminate or reduce risks through design and development	MAP 2.3 (Design) MANAGE 1.2	8.2.2 (Design and development) 6.1.4 (Risk treatment)	A.8.27 (Secure system architecture)	Direct
Implement adequate mitigation and control measures	MANAGE 1.1-1.4 (Risk treatment)	6.1.4 (Risk treatment plan)	6.1.3 (Control selection) Annex A (Controls)	Direct
Provide information to deployers about residual risks	MANAGE 3.1-3.3 (Transparency)	8.2.4 (Information to deployers and users)	A.5.1 (Information security policies)	Direct
Provide training to deployers where appropriate	GOVERN 4.2 (Training)	7.2 (Competence) 7.3 (Awareness)	A.6.3 (Information security awareness)	Substantial
Test risk management measures for effectiveness	MEASURE 1.2 (Validation) MEASURE 3	8.2.3 (Validation and testing)	A.8.29 (Security testing)	Direct

Alignment Level Key:

- **Direct:** AI RMF/ISO directly satisfies EU AI Act requirement with minimal additional work
- **Substantial:** AI RMF/ISO addresses majority of requirement; some EU-specific additions needed

EU AI Act: Article 10: Data and Data Governance

Complete Implementation Guide

10.1 Legal Requirements

Article 10(1) - EU AI Act:

"High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5."

Article 10(2) - Data Quality Criteria:

"Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular:"

- *the relevant design choices;*
- *data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;*
- *relevant data preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;*
- *the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;*
- *an assessment of the availability, quantity and suitability of the data sets that are needed;*
- *examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations.*

Article 10(3) - Dataset Quality Standards:

"Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used."

Article 10(4) - Contextual Appropriateness:

"Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioral or functional setting within which the high-risk AI system is intended to be used."

Article 10(5) - Special Categories of Personal Data:

"To the extent that it is strictly necessary for the purposes of ensuring bias detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons."

10.2 Detailed Implementation Requirements

10.2.1 Data Governance Framework

Required Data Governance Practices:

- **1. Design Choices Documentation:**
  - Rationale for data collection approach
  - Feature selection methodology
  - Sampling strategy and justification
  - Trade-offs considered (e.g., quantity vs. quality)

- **2. Data Collection Processes:**
  - **Collection Methodology:**
  - - Sources identified and documented
  - - Collection procedures standardized
  - - Time period of collection specified
  - - Quality checks at point of collection
  - **Data Origin and Provenance:**
  - - Complete lineage from source to use
  - - Original purpose documented (for personal data)
  - - Legal basis for collection and use
  - - License and usage rights

- **3. Data Preparation Processing:**
  - **Annotation and Labeling:**
  - - Annotation guidelines and procedures
  - - Annotator training and qualification
  - - Inter-annotator agreement measurement
  - - Quality assurance processes
  - **Cleaning Operations:**
  - - Duplicate removal procedures
  - - Outlier detection and handling
  - - Missing data imputation methods
  - - Error correction procedures

- **Updating and Enrichment:**
- - Version control for datasets
- - Change tracking and documentation
- - Feature engineering documentation
- **Aggregation:**
- - Aggregation rules and procedures
- - Impact on statistical properties

- **4. Formulation of Assumptions:**
  - Document what data is supposed to measure
  - What data is supposed to represent
  - Limitations of representation
  - Known gaps between data and reality
- **5. Availability, Quantity, and Suitability Assessment:**
  - Data sufficiency analysis for intended purpose
  - Coverage of edge cases and rare events
  - Temporal coverage (historical period)
  - Geographic and demographic coverage
- **6. Bias Examination:**
  - Systematic analysis for biases affecting health and safety
  - Impact on fundamental rights assessment
  - Discrimination testing per EU law
  - Feedback loop analysis (outputs influencing future inputs)

10.2.2 Data Quality Criteria (Article 10(3))

1. Relevance:

Definition: Data must be directly related to and appropriate for the intended purpose of the AI system.

Implementation Requirements:

- Features align with decision-making needs
- No extraneous data creating spurious correlations
- Data coverage matches use case requirements
- Documented justification for each feature included

2. Sufficiently Representative:

Definition: Data must adequately represent the population and contexts where AI will be deployed.

Implementation Requirements:

Dimension	Assessment Method	Acceptability Criteria
Demographic Representation	Compare dataset demographics to target population using census data or representative surveys	No underrepresented group <5% of target population; proportional representation within ±10% where feasible
Geographic Coverage	Map data sources to deployment regions; identify geographic gaps	All deployment regions represented; major regions have adequate sample size (n>100)
Temporal Coverage	Analyze time distribution of data; check for seasonal patterns	Multiple time periods; seasonal variations captured; recent data included
Edge Cases	Identify rare but important scenarios; assess coverage	Known edge cases present in dataset; rare events represented proportionally
Class Balance	Calculate class distribution; compare to expected deployment distribution	Imbalance justified and documented; mitigation applied if needed (resampling, reweighting)

3. Free of Errors:

Definition: Data must be accurate, with systematic errors identified, quantified, and minimized.

Error Types and Mitigation:

- **Measurement Errors:** Sensor calibration, instrument validation, error bounds documented
- **Label Errors:** Inter-annotator agreement >80%, quality audits, correction procedures
- **Transcription Errors:** Automated validation, double-entry verification, checksums
- **Systematic Bias:** Statistical tests, comparison to ground truth, bias correction
- **Acceptable Error Rate:** <5% for high-risk systems; <1% for safety-critical; documented and justified

4. Complete:

Definition: Data must have all necessary features and adequate sample sizes; missing data minimized and handled appropriately.

Completeness Assessment:

- **Feature Completeness:** All required attributes present; documented rationale for exclusions
- **Sample Size Adequacy:** Statistical power analysis; sufficient data for all subgroups; minimum n documented
- **Missing Data Handling:**
  - Missing data rate calculated and documented
  - Pattern analysis (MCAR, MAR, MNAR)
  - Imputation method justified (mean, median, ML-based, deletion)
  - Impact of imputation on model performance assessed

5. Appropriate Statistical Properties:

Definition: Data must have statistical characteristics suitable for intended ML techniques and target population.

Required Statistical Analysis:

- **Distribution Analysis:**
  - Feature distributions documented (mean, median, std dev, skewness, kurtosis)
  - Comparison to expected population distributions
  - Normality tests where required by model
- **Correlation Analysis:**
  - Feature correlation matrix computed
  - Multicollinearity identified and addressed
  - Proxy features for protected attributes identified
- **Subgroup Analysis:**
  - Statistical properties computed for each demographic subgroup
  - Significant differences between groups documented and explained

10.2.3 Training, Validation, and Testing Data Sets

Data Set Separation Requirements:

Data Set	Purpose	Requirements
Training Set	Used to train/fit the AI model parameters	Typically 60-80% of total data; Must be representative of intended use; Separate from validation/test sets; Documented splits and rationale; All quality criteria apply; No data leakage
Validation Set	Tune hyperparameters and prevent overfitting during development	Typically 10-20% of total data; Independent from training set; Used for model selection and early stopping; Same distribution as training; Prevents information leakage
Testing Set	Final evaluation of model performance before deployment	Typically 10-20% of total data; Never used during training/tuning; Held out until final evaluation; Provides unbiased performance estimate; Representative of deployment conditions

Split Methodology Requirements:

- **Random Splitting:** Use stratified sampling to maintain class proportions; Set and document random seed for reproducibility
- **Temporal Splitting:** For time-series: earlier data for training, later data for testing; Prevents look-ahead bias
- **Group-Based Splitting:** Keep related instances together (same patient, user, entity); Prevents data leakage through grouping
- **Documentation:** Record exact split methodology, dates, sample sizes, random seeds, verification of no overlap

Data Leakage Prevention:

- **Strict Separation:** No overlap between train/validation/test sets
- **Temporal Integrity:** Future data never used to inform past predictions
- **Preprocessing Integrity:** Normalization parameters computed only on training data
- **Feature Selection:** Feature engineering based only on training data

10.2.4 Contextual Appropriateness (Article 10(4))

Context Dimensions to Consider:

- **Geographical Characteristics:**
  - Regional variations in language, dialect, terminology
  - Climate and environmental differences
  - Infrastructure and technology availability
  - Urban vs. rural deployment contexts
- **Contextual Setting:**
  - Industry-specific terminology and practices
  - Organizational culture and workflows
  - Regulatory environment differences
- **Behavioral Characteristics:**
  - User behavior patterns and expectations
  - Cultural norms and preferences
  - Age-related behavioral differences
- **Functional Setting:**
  - Different use cases and workflows
  - Performance requirements by setting
  - Integration with existing systems

10.2.5 Special Categories of Personal Data (Article 10(5))

Special Categories (GDPR Article 9):

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for unique identification
- Health data
- Sex life or sexual orientation

Strict Necessity Requirement:

Special category data may ONLY be processed when:

- It is STRICTLY NECESSARY for bias detection and correction
- No alternative methods exist to achieve bias mitigation
- Processing is proportionate to the risk being addressed

Required Safeguards:

Safeguard Category	Requirements	Implementation Examples
Legal Basis	Establish legal grounds under GDPR Article 9(2); Document necessity assessment	Data Protection Impact Assessment (DPIA); Legal opinion; Documented necessity justification
Data Minimization	Collect and process only what is strictly necessary; Regular review of necessity	Collect aggregate statistics instead of individual data where possible; Use proxies if sufficient
Purpose Limitation	Use solely for bias detection/correction; No secondary purposes	Access controls limiting use; Automated deletion after bias analysis complete
Technical Safeguards	Encryption, pseudonymization, anonymization where possible	End-to-end encryption; Differential privacy; Federated learning; Secure multi-party computation
Organizational Safeguards	Limited access; Training; Audit trails; Breach procedures	Role-based access control; Privacy training; Logging all access; Incident response plan
Transparency	Inform data subjects of processing for bias mitigation	Privacy notice explaining bias detection use; Transparency in AI documentation
Time Limitation	Delete data when no longer needed for bias detection	Automated deletion schedule; Regular review of retention necessity

Privacy-Preserving Bias Detection Techniques:

- **Differential Privacy:** Add noise to data/outputs to protect individual privacy while detecting bias
- **Federated Learning:** Train on distributed data without centralizing sensitive information
- **Synthetic Data:** Generate synthetic samples preserving statistical properties without real individuals
- **Aggregated Analysis:** Analyze group-level statistics rather than individual records

10.3 Article 10 Compliance Matrix

EU AI Act Article 10 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Training, validation, testing data sets with quality criteria	MEASURE 2.1-2.4 (Data Quality)	8.2.1 (Data for AI) 8.2.2 (Data design)	A.8.11 (Data masking) A.5.9 (Inventory)	Direct
Data governance and management practices	GOVERN 1.5 (Data governance) MAP 2.1	8.2.1 (Data management)	A.5.33 (Records) A.8.10 (Deletion)	Direct
Design choices documented	MAP 2.3 (Design documentation)	8.2.2 (Design and development) 7.5 (Documentation)	A.5.37 (Procedures)	Direct
Data collection processes and origin	GOVERN 3.2 (Provenance) MEASURE 2.1	8.2.1 (Data collection)	A.5.9 (Asset inventory)	Direct
Data preparation: annotation, labeling, cleaning, updating, enrichment, aggregation	MEASURE 2.2 (Data preprocessing)	8.2.1 (Data preparation)	A.8.24 (Cryptography)	Direct
Formulation of assumptions about data	MAP 1.1 (Context) MEASURE 2.1	8.2.1 (Data assumptions) 7.5 (Documentation)	A.5.1 (Policies)	Substantial
Assessment of availability, quantity, suitability	MEASURE 2.1 (Data assessment)	8.2.1 (Data assessment)	A.5.9 (Inventory)	Substantial

Examination for biases affecting health, safety, fundamental rights, discrimination	MEASURE 2.3 (Bias examination) MAP 3.3	8.2.1 (Bias examination) 6.1.3 (Impact assessment)	N/A	Direct
Data relevant, representative, free of errors, complete	MEASURE 2.1-2.4 (Data validity)	8.2.1 (Data quality)	A.8.24 (Cryptography)	Direct
Appropriate statistical properties for target population	MEASURE 2.2 (Dataset properties) MAP 3.4	8.2.1 (Statistical properties)	N/A	Substantial
Consider geographical, contextual, behavioral, functional settings	MAP 1.1-1.3 (Context) MAP 3.4	4.1-4.2 (Context of organization)	4.1 (Context)	Substantial
Process special category data with safeguards for bias detection	MAP 3.3 (Bias) GOVERN 1.5	8.2.1 (Special categories) 6.1.3 (Impact assessment)	A.5.34 (Privacy) A.8.11 (Data masking)	Substantial

10.4 Implementation Guidance and Tools

Recommended Tools:

- **Data Versioning:** DVC (Data Version Control), MLflow Data, Pachyderm
- **Data Quality:** Great Expectations, Deequ, TensorFlow Data Validation
- **Bias Detection:** AI Fairness 360 (IBM), Fairlearn (Microsoft), What-If Tool (Google)
- **Data Documentation:** Datasheets for Datasets, Dataset Nutrition Labels
- **Lineage Tracking:** Apache Atlas, OpenLineage, Amundsen

Implementation Checklist:

1. ☐ Establish data governance team and procedures
2. ☐ Document data collection methodology and sources
3. ☐ Implement data quality assessment framework
4. ☐ Conduct bias examination across demographic groups
5. ☐ Create train/validation/test splits with documented methodology
6. ☐ Implement data versioning and lineage tracking
7. ☐ Assess contextual appropriateness for deployment settings
8. ☐ If using special category data: conduct DPIA and implement safeguards
9. ☐ Document all data governance decisions and trade-offs
10. ☐ Create data sheets for all datasets used

Article 11: Technical Documentation

11.1 Legal Requirements

Article 11(1) - EU AI Act:

"The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up to date. The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in this Section and to provide national competent authorities and notified bodies with the information necessary to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV."

Annex IV - Technical Documentation Contents:

The technical documentation must include the following minimum elements:

1. **General description of the AI system:**
   - Intended purpose, persons or groups at whom the system is directed
   - Level of accuracy and accuracy metrics
   - Robustness and cybersecurity measures
   - Any known or foreseeable circumstances related to use by unauthorized persons
   - System versions and previous iterations

2. **Detailed description of elements and development:**
   - Methods and steps for development including design specifications
   - System architecture and computational resources
   - Data requirements and data collection methodology
   - Pre-trained systems and training methodologies

3. **Detailed information on monitoring, functioning, and control:**
   - Capabilities and limitations
   - All relevant information regarding data, data governance, and data management
   - Human oversight measures

4. **Detailed description of risk management system:**
   - Risk management process per Article 9
   - Identified risks and mitigation measures

5. **Changes made to the system through its lifecycle:**
   - Documentation of substantial modifications

6. **List of standards applied:**
   - Harmonized standards, technical specifications, or other means used

7. **EU declaration of conformity:**

- Copy of the declaration per Article 47

8. **Detailed description of the system for assessment and verification:**
   - Testing procedures, validation results, performance metrics

11.2 Detailed Implementation Requirements

11.2.1 General System Description

Required Content:

- **Intended Purpose Statement:**
  - Specific use cases and applications
  - Geographic scope and deployment environments
  - Target user populations and affected persons
  - Contraindications and prohibited uses

- **Performance Characteristics:**
  - Accuracy metrics with confidence intervals
  - Performance across demographic subgroups
  - False positive and false negative rates
  - Precision, recall, F1 scores as applicable

- **Robustness Measures:**
  - Performance under adversarial conditions
  - Resilience to input perturbations
  - Failure modes and fallback mechanisms

- **Cybersecurity Measures:**
  - Security architecture and controls
  - Authentication and authorization mechanisms
  - Encryption methods for data in transit and at rest
  - Vulnerability assessment results and remediation

11.2.2 System Development and Architecture

Development Methodology Documentation:

- Design specifications and requirements analysis
- Development lifecycle methodology (Agile, Waterfall, DevOps)
- Version control and change management processes
- Quality assurance and testing protocols

System Architecture Documentation:

- **Architecture Diagrams:**
  - High-level system architecture
  - Data flow diagrams
  - Model architecture (neural network topology, decision trees, etc.)

    - Integration points with external systems

- **Computational Resources:**
    - Hardware requirements (CPU, GPU, memory)
    - Software dependencies and libraries
    - Infrastructure specifications (cloud, on-premise)

- **Algorithm Description:**
    - ML/AI techniques employed (supervised learning, deep learning, reinforcement learning)
    - Model type and architecture details
    - Hyperparameters and configuration
    - Training algorithms and optimization methods

11.2.3 Data Documentation

Comprehensive Data Requirements:

- **Data Collection Methodology:**
    - Sources of training, validation, testing data
    - Collection time period and geographic scope
    - Sampling methodology and rationale
    - Consent and licensing information

- **Data Characteristics:**
    - Dataset size (number of samples, features)
    - Data types and formats
    - Statistical properties and distributions
    - Demographic composition and representativeness analysis

- **Data Preprocessing:**
    - Cleaning procedures and quality filters applied
    - Normalization, standardization techniques
    - Feature engineering and selection methods
    - Augmentation strategies if applied

- **Data Governance:**
    - Data versioning and lineage tracking
    - Access controls and security measures
    - Retention and deletion policies

11.2.4 Validation and Testing Documentation

Testing Procedures:

- **Validation Methodology:**
    - Cross-validation approach (k-fold, stratified, time-series)
    - Hyperparameter tuning procedures
    - Model selection criteria

- **Performance Testing:**
  - Accuracy metrics on test set
  - Performance across demographic subgroups
  - Fairness metrics (demographic parity, equalized odds, etc.)
  - Robustness testing results
- **Security Testing:**
  - Adversarial attack testing (evasion, poisoning)
  - Penetration testing results
  - Vulnerability scanning reports
- **User Acceptance Testing:**
  - Pilot deployment results
  - User feedback and satisfaction metrics

11.3 Article 11 Compliance Matrix

EU AI Act Article 11 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Technical documentation drawn up before market placement	GOVERN 1.3 (Documentation)	7.5 (Documented information) 8.2.4 (Pre-market docs)	A.5.1 (Policies) A.5.37 (Procedures)	Direct
Keep documentation up to date throughout lifecycle	GOVERN 5.1 (Oversight) MANAGE 4	7.5.3 (Control of documented information)	A.5.37 (Documented procedures)	Direct
Demonstrate compliance with all requirements	All AI RMF categories	9.2 (Internal audit) 9.3 (Management review)	9.2 (Internal audit)	Direct
General description: intended purpose, accuracy, robustness	MAP 1 (Context) MEASURE 3	8.2.4 (System description)	A.5.1 (Policies)	Direct
Development methods and steps	MAP 2 (Categorization) MAP 5	8.2.2 (Design and development)	A.8.25 (Secure development)	Direct
System architecture and computational resources	MAP 2.3 (Technical design)	8.2.2 (Architecture)	A.8.27 (System architecture)	Direct
Data requirements and governance	MEASURE 2 (Data quality) GOVERN 1.5	8.2.1 (Data for AI)	A.5.33 (Records protection)	Direct

Monitoring, functioning, and control information	MEASURE 4 (Monitoring) GOVERN 5	9.1 (Monitoring and measurement)	A.8.16 (Monitoring activities)	Direct
Human oversight measures	GOVERN 1.6 (Human-AI config) MANAGE 3	8.2.5 (Human oversight)	A.6.2 (Roles/responsibilities)	Direct
Risk management system description	MAP 4 (Risks) MANAGE 1	6.1.2 (AI risk assessment)	6.1.3 (Risk assessment)	Direct
Changes made through lifecycle	MANAGE 4.1 (Change management)	8.1 (Operational planning) 10.2 (Improvement)	A.8.32 (Change management)	Direct
List of applied standards	GOVERN 1.2 (Standards)	6.1.5 (Compliance obligations)	4.2 (Interested parties)	Direct
EU declaration of conformity	GOVERN 2.1 (Accountability)	8.2.4 (Conformity)	9.2 (Internal audit)	Direct
System assessment and verification procedures	MEASURE 1 (Validation) MEASURE 3	8.2.3 (Validation and testing)	A.8.29 (Security testing)	Direct

11.4 Technical Documentation Checklist

Use this checklist to ensure your technical documentation is complete before placing your high-risk AI system on the market:

☐	Documentation Element	Evidence Required
☐	Intended purpose and use case description	Written statement with specific use cases, target users, deployment contexts, contraindications
☐	System performance specifications	Accuracy metrics, performance benchmarks, confidence intervals, subgroup analysis
☐	Robustness testing results	Adversarial testing reports, stress testing results, failure mode analysis
☐	Cybersecurity measures documentation	Security architecture diagrams, penetration testing reports, vulnerability assessments
☐	Development methodology documentation	Design specifications, development process description, version control logs
☐	System architecture diagrams	High-level architecture, data flow diagrams, integration points, model architecture
☐	Computational resource specifications	Hardware requirements, software dependencies, infrastructure specifications
☐	Algorithm and model description	ML techniques used, model architecture details, hyperparameters, training methods
☐	Data collection methodology	Data sources, collection procedures, sampling methodology, consent documentation
☐	Data quality analysis	Relevance assessment, representativeness analysis, error analysis, completeness report
☐	Bias examination and mitigation	Demographic analysis, bias detection results, mitigation strategies implemented

☐	Data governance procedures	Data versioning system, lineage tracking, access controls, retention policies
☐	Training, validation, testing data documentation	Dataset descriptions, split methodology, statistical properties, version information
☐	Human oversight measures	Oversight procedures, human-in-the-loop design, intervention capabilities
☐	Risk management system documentation	Risk register, risk assessment reports, mitigation measures, residual risks
☐	Validation and testing procedures	Test plans, validation methodology, performance test results, acceptance criteria
☐	Change management documentation	Version history, substantial modifications log, impact assessments for changes
☐	Applied standards list	Harmonized standards, technical specifications, conformity assessment methods
☐	EU Declaration of Conformity	Signed declaration per Article 47, list of requirements satisfied

Documentation Retention:

- Technical documentation must be kept for 10 years after the AI system is placed on the market or put into service
- Documentation must be available to national competent authorities upon request
- Updates to documentation must be reflected within reasonable timeframes

Article 12: Record-Keeping

12.1 Legal Requirements

Article 12(1) - EU AI Act:

"High-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system."

Article 12(2) - Logging Capabilities:

"The logging capabilities shall conform to recognized standards or common specifications. The logs shall be kept for a period of time that is appropriate in the light of the intended purpose of the AI system and applicable legal obligations under Union or national law."

Article 12(3) - Log Content Requirements:

"Logs shall record the period of each use of the high-risk AI system, the input data and output data that led to the output that is provided by the AI system, and, where the AI system is used by natural persons, the identification of the natural person."

Article 12(4) - Deployer Access:

"Deployers of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, where such logs are under their control. The logs shall be kept for a period of time that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law."

12.2 Detailed Implementation Requirements

12.2.1 Automatic Logging System Architecture

Technical Requirements for Logging Infrastructure:

- **Automated Recording:** System must automatically log events without manual intervention
- **Reliability:** Logging system must be fault-tolerant and not fail silently
- **Tamper-Proof:** Logs must be protected against unauthorized modification or deletion
- **Completeness:** All required events must be captured without gaps
- **Performance:** Logging must not significantly degrade system performance
- **Scalability:** Logging infrastructure must scale with system usage

Implementation Architecture Patterns:

- **Centralized Logging:** All logs aggregated in central repository

  - Tools: Elasticsearch/Logstash/Kibana (ELK), Splunk, CloudWatch
  - Benefits: Easy querying, correlation, analysis

- **Immutable Log Storage:** Write-once, read-many storage
  - Technologies: Blockchain, WORM storage, cryptographic signatures
  - Benefits: Tamper-evident, audit trail integrity

- **Structured Logging:** Use standardized log formats
  - Formats: JSON, Common Event Format (CEF), Syslog
  - Benefits: Easier parsing, analysis, interoperability

12.2.2 Required Log Content

Mandatory Log Fields (Article 12(3)):

Log Element	Description	Implementation Details
Period of Use	Start and end time of each AI system interaction or inference	ISO 8601 timestamp format with timezone; Millisecond precision recommended; Session ID linking related events
Input Data	Data that was provided to the AI system to produce the output	Full input payload or reference to stored input; Preserve input data integrity; Handle large inputs with checksums/hashes
Output Data	Results, predictions, decisions, or recommendations produced by the AI system	Complete output including confidence scores; Any intermediate results if relevant; Classification labels, probabilities, rankings
User Identification	When used by natural persons, identification of the person operating the system	User ID, username, or other identifier; Role/privileges at time of use; Authentication method used; IP address or device ID where appropriate
Model Version	Specific version of AI model that generated the output	Model version ID; Training timestamp; Configuration parameters; Deployment identifier
System State	Relevant system state at time of inference	Active configuration settings; Feature flags; A/B test group assignment; Environmental conditions if relevant

Additional Recommended Log Elements:

- Processing time and latency metrics
- Human oversight interventions (if overridden or modified)
- Errors, warnings, or anomalies detected
- Data quality assessments (if performed)
- Explainability artifacts (feature importance, saliency maps)

12.2.3 Log Retention and Management

Retention Period Determination:

Retention periods must consider:

- **Intended Purpose:** High-consequence decisions (e.g., credit, hiring, law enforcement) require longer retention
- **Legal Obligations:**
  - GDPR data retention limits
  - Sector-specific regulations (healthcare, finance, employment)
  - National laws requiring specific retention periods
- **Risk Level:** Higher risk systems generally require longer retention
- **Statute of Limitations:** Consider legal claim periods

Typical Retention Periods by Use Case:

AI System Category	Recommended Retention	Justification
Employment/HR decisions	3-5 years minimum	Employment discrimination claim periods; Evidence for legal disputes
Credit/Financial decisions	5-7 years	Financial regulations; Loan lifecycle; Dispute resolution periods
Law enforcement	7-10 years minimum	Criminal proceedings; Appeals; Post-conviction challenges
Healthcare/Medical AI	10 years minimum	Medical record retention; Malpractice claims; Long-term outcomes
Education/Training	3-5 years	Student record requirements; Assessment challenges
Critical infrastructure	5-10 years	Safety investigations; Incident analysis; Regulatory audits

Log Management Procedures:

- **Access Controls:** Restrict log access to authorized personnel only
- **Audit Trail:** Log all access to logs (meta-logging)
- **Backup and Recovery:** Regular backups with tested restore procedures
- **Secure Deletion:** Cryptographic erasure or physical destruction after retention period
- **Log Monitoring:** Automated monitoring for anomalies, gaps, or integrity issues

12.3 Article 12 Compliance Matrix

EU AI Act Article 12 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Automatic recording of events (logs) over lifetime	GOVERN 3.2 (Provenance) MEASURE 4.1	9.1 (Monitoring) 8.2.6 (Logging)	A.8.15 (Logging) A.8.16 (Monitoring)	Direct
Logging capabilities conform to recognized standards	GOVERN 1.2 (Standards)	6.1.5 (Compliance obligations)	A.8.15 (Logging standards)	Substantial
Logs kept for appropriate period based on purpose and legal obligations	GOVERN 1.4 (Records)	7.5 (Documented information retention)	A.5.33 (Records protection) A.8.10 (Information deletion)	Direct
Record period of each use (timestamps)	MEASURE 4.1 (System tracking)	8.2.6 (Record-keeping)	A.8.15 (Logging)	Direct
Record input data that led to output	MEASURE 4.1 (Input logging) GOVERN 3.2	8.2.6 (Input recording)	A.8.15 (Logging)	Direct
Record output data provided by system	MEASURE 4.1 (Output logging) GOVERN 3.2	8.2.6 (Output recording)	A.8.15 (Logging)	Direct
Identify natural persons using the system	GOVERN 2.2 (User accountability)	9.1 (Monitoring)	A.9.2 (User access management) A.8.15 (Logging)	Direct
Deployers keep logs under their control	GOVERN 2 (Accountability)	5.3 (Organizational roles) 7.5 (Document control)	A.5.33 (Records protection)	Direct
Log protection and integrity	GOVERN 5.2 (Monitoring)	9.1 (Monitoring integrity)	A.8.15 (Logging) A.8.24 (Cryptography)	Direct

12.4 Implementation Guidance

Log Implementation Checklist:

1. **Design Logging Architecture:**
   - Select centralized logging platform
   - Define structured log schema with all mandatory fields
   - Implement immutable storage or cryptographic signatures
2. **Implement Logging in AI System:**
   - Instrument all inference/decision points
   - Capture complete input-output pairs
   - Record user identification for human-operated systems
   - Include model version and configuration
3. **Set Up Log Management:**
   - Define retention policies per use case
   - Implement automated retention enforcement
   - Configure access controls and audit logging
   - Establish backup and disaster recovery procedures
4. **Test and Validate:**
   - Verify all required fields are captured
   - Test log completeness under various scenarios
   - Validate log integrity and tamper-resistance
   - Ensure performance impact is acceptable
5. **Document and Monitor:** Create logging procedures, train deployers on log access, monitor for logging failures, regularly audit log quality and completeness

Sample Log Entry Template (JSON):

```
{   "timestamp": "2026-01-17T14:23:45.123Z",   "session_id": "abc-123-def-456",   "system_id": "hr-ai-screening-v2.3",   "model_version": "2.3.1",   "user_id": "user_789",   "user_role": "hr_manager",   "input": {     "resume_id": "res_12345",     "job_posting_id": "job_67890",     "feature_vector": [0.72, 0.85, ...]   },   "output": {     "candidate_score": 0.87,     "recommendation": "interview",     "confidence": 0.92,     "explanation": "Strong match for required skills"   },   "processing_time_ms": 234,   "human_oversight": false,   "environment": "production" }
```

Article 13: Transparency and Information to Deployers

13.1 Legal Requirements

Article 13(1) - EU AI Act:

"High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable deployers to interpret the system's output and use it appropriately."

Article 13(2) - Instructions for Use:

"High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers."

Required Information in Instructions for Use (Article 13(3)):

- **Identity and contact details of the provider**
- **Characteristics, capabilities and limitations of performance** of the high-risk AI system
- **Changes to the high-risk AI system and its performance** which have been pre-determined by the provider
- **Human oversight measures** including the technical measures
- **Expected lifetime of the high-risk AI system and maintenance measures**
- **Where applicable, description of financial, computational and other resources** required
- **Information to enable deployers to correctly interpret the output**
- **Where appropriate, specifications for the input data**

13.2 Detailed Implementation Requirements

13.2.1 System Transparency Design

Transparency by Design Requirements:

- **Interpretable Outputs:**
  - Outputs must be presented in human-understandable format
  - Include confidence scores or uncertainty measures
  - Provide context for understanding what the output means
  - Avoid technical jargon in user-facing outputs

- **Explainability Features:**
  - Feature importance or contributing factors to decision
  - Similar examples or precedents from training data
  - Counterfactual explanations (what would change the outcome)
  - Visualizations where appropriate (saliency maps, attention)

- **Uncertainty Communication:**
  - Clearly indicate when system is uncertain
  - Provide confidence intervals or probability distributions
  - Flag edge cases or out-of-distribution inputs

- **Decision Rationale:**
  - Provide reasoning for recommendations or classifications
  - Link to relevant rules, policies, or training examples
  - Allow deployers to understand the basis for outputs

13.2.2 Instructions for Use - Required Content

Section 1: Provider Information

- Provider legal name and registered address
- Contact information (email, phone, website)
- Authorized representative in EU (if provider outside EU)
- Support channels and response times

Section 2: System Characteristics and Capabilities

- **Intended Purpose:**
  - Specific use cases and applications
  - Target user groups and affected populations
  - Deployment contexts and environments

- **Performance Characteristics:**
  - Accuracy levels with confidence intervals
  - Performance metrics across demographic subgroups
  - False positive and false negative rates
  - Benchmark comparisons to alternative methods

- **Limitations:**
  - Known failure modes and edge cases
  - Conditions under which system may underperform
  - Types of inputs that may produce unreliable outputs
  - Scenarios where human judgment should override AI

- **Contraindications:**
  - Prohibited or inappropriate uses
  - Populations for whom system is not suitable
  - Environmental conditions to avoid

Section 3: System Changes and Updates

- **Pre-determined Changes:**
  - Automatic updates or retraining schedules
  - Expected performance evolution over time
  - Model drift monitoring and recalibration procedures
- **Version Management:**
  - Current system version and release date
  - Versioning scheme and changelog
  - Notification process for updates
- **Impact of Changes:**
  - How updates may affect performance
  - Testing and validation before deployment of updates

Section 4: Human Oversight Measures

- **Oversight Capabilities Required:**
  - How humans can monitor the AI system
  - Intervention points and override mechanisms
  - Escalation procedures for problematic outputs
- **Technical Measures:**
  - User interface features for oversight
  - Alert mechanisms for edge cases or high uncertainty
  - Tools for reviewing and correcting outputs
- **Training Requirements:**
  - Required competencies for deployers
  - Training materials and resources provided

Section 5: Lifecycle and Maintenance

- **Expected Lifetime:**
  - Anticipated operational lifespan
  - End-of-life indicators and replacement triggers
- **Maintenance Requirements:**
  - Periodic revalidation or recalibration schedules
  - Performance monitoring procedures
  - Quality assurance and testing requirements

-

- **Support Services:**
  - Technical support availability and channels
  - Service level agreements and response times

Section 6: Resource Requirements

- **Computational Resources:**
  - Hardware specifications (CPU, GPU, RAM)
  - Network bandwidth and latency requirements
  - Storage capacity needed

- **Financial Resources:**
  - Licensing costs and pricing model
  - Ongoing maintenance and support fees
  - Cost per transaction or usage-based fees

- **Human Resources:**
  - Personnel requirements (roles, FTE)
  - Required training time and expertise levels

Section 7: Output Interpretation Guidance

- **Understanding Outputs:**
  - Explanation of output format and structure
  - How to interpret confidence scores and probabilities
  - Meaning of classifications, categories, or predictions

- **Contextual Factors:**
  - When outputs should be considered reliable
  - Factors that may affect output validity
  - How to assess output quality

- **Decision Support:**
  - How to use AI output in decision-making process
  - When to seek additional information or consultation
  - Combining AI recommendations with other inputs

Section 8: Input Data Specifications

- **Data Format Requirements:**
  - Required data types, formats, and schemas
  - Data validation rules and constraints
  - Preprocessing steps required
- **Data Quality Requirements:**
  - Minimum data quality standards
  - Acceptable ranges and distributions
  - Handling of missing or incomplete data
- **Input Validation:**
  - Automated validation checks performed
  - Error messages and troubleshooting guidance

13.3 Article 13 Compliance Matrix

EU AI Act Article 13 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Design for transparent operation enabling output interpretation	MANAGE 3.1-3.3 (Transparency)	8.2.2 (Design for transparency)	A.5.1 (Information security policies)	Direct
Instructions for use in appropriate digital format	MANAGE 3.1 (Documentation)	8.2.4 (Information to deployers)	A.5.37 (Documented procedures)	Direct
Instructions must be concise, complete, correct, clear, relevant, accessible, comprehensible	MANAGE 3.1 (Clear communication)	7.4 (Communication)	A.5.1 (Policies)	Substantial
Provider identity and contact details	GOVERN 2.1 (Accountability)	5.3 (Organizational roles) 4.1 (Context)	A.5.2 (Information security roles)	Direct
Characteristics, capabilities, and limitations of performance	MEASURE 3 (Performance) MAP 1.2	8.2.4 (System description)	A.5.1 (Policies)	Direct
Pre-determined changes and performance impacts	MANAGE 4.1 (Change management)	8.1 (Operational planning) 10.2 (Improvement)	A.8.32 (Change management)	Direct
Human oversight measures and technical measures	GOVERN 1.6 (Human-AI config) MANAGE 3.2	8.2.5 (Human oversight)	A.6.2 (Roles and responsibilities)	Direct

Expected lifetime and maintenance measures	MANAGE 4.3 (Lifecycle management)	8.2 (AI system lifecycle)	A.5.29 (Information security in project management)	Substantial
Resources required (financial, computational, other)	GOVERN 4.1 (Resourcing)	7.1 (Resources)	A.5.1 (Policies)	Substantial
Information to enable correct output interpretation	MANAGE 3.1 (Transparency)	8.2.4 (Deployer information)	A.5.1 (Policies)	Direct
Specifications for input data where appropriate	MEASURE 2.1 (Data requirements) MAP 2.1	8.2.1 (Data for AI)	A.5.9 (Inventory of assets)	Direct

13.4 Instructions for Use Template

The following template can be adapted for your high-risk AI system instructions for use:

INSTRUCTIONS FOR USE

[AI System Name and Version]

High-Risk AI System - Article 13 EU AI Act

1. PROVIDER INFORMATION

Provider: [Legal name]

Address: [Registered address]

Contact: [Email, phone, website]

EU Authorized Representative: [If applicable]

2. SYSTEM IDENTIFICATION

Product Name: [Name]

Version: [Version number]

Release Date: [Date]

CE Marking: [Mark applied - Yes/No]

3. INTENDED PURPOSE

[Detailed description of intended use cases]
Target Users: [Description]
Affected Persons: [Groups impacted by AI decisions]

4. PERFORMANCE CHARACTERISTICS

Accuracy: [Metrics with confidence intervals]
Performance by Subgroup: [Demographic analysis]
Benchmark Comparisons: [How it compares to alternatives]

5. LIMITATIONS AND CONTRAINDICATIONS

Known Limitations: [List specific limitations]
Failure Modes: [When system may fail]
Prohibited Uses: [Contraindicated applications]

6. HUMAN OVERSIGHT REQUIREMENTS

Oversight Measures: [How humans monitor the system]
Intervention Capabilities: [How to override or modify outputs]
Required Training: [Competencies needed by deployers]

7. OUTPUT INTERPRETATION GUIDE

Output Format: [Description of how outputs are presented]
Confidence Scores: [How to interpret probabilities]
Decision Support: [How to use AI output in decision-making]

8. SYSTEM LIFECYCLE

Expected Lifetime: [Duration]
Maintenance Schedule: [Revalidation, updates]
Pre-determined Changes: [Automatic updates, retraining]

9. RESOURCE REQUIREMENTS

Computational: [Hardware, software, network]
Financial: [Costs and fees]
Human: [Personnel and training requirements]

10. INPUT DATA SPECIFICATIONS

Required Format: [Data types, schemas]
Quality Requirements: [Standards for input data]
Validation: [Automated checks performed]

Article 14: Human Oversight

14.1 Legal Requirements

Article 14(1) - EU AI Act:

"High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use."

Article 14(2) - Purpose of Human Oversight:

"Human oversight shall aim to prevent or minimize the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse."

Article 14(3) - Oversight shall ensure natural persons:

- **Fully understand the capacities and limitations** of the high-risk AI system
- **Are able to properly monitor its operation**
- **Are able to correctly interpret the system's output**
- **Are able to decide not to use the system or disregard, override or reverse the output**
- **Are able to intervene in the operation or interrupt the system**

Article 14(4) - Technical Measures:

"Human oversight shall be ensured through either one or all of the following measures: (a) measures identified and built into the high-risk AI system by the provider; (b) measures identified by the provider and implemented by the deployer."

Article 14(5) - Measures for remote biometric identification:

"For high-risk AI systems referred to in point 1(a) of Annex III [real-time remote biometric identification], the measures shall ensure that no action or decision is taken by the deployer on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons."

14.2 Detailed Implementation Requirements

14.2.1 Human Oversight Design Patterns

Pattern 1: Human-in-the-Loop (HITL)

Description: Human actively participates in every decision cycle. AI provides recommendations; human must approve before action is taken.

Use Cases:

- High-consequence decisions (credit approval, hiring, law enforcement)
- Safety-critical applications (medical diagnosis, autonomous systems)

Implementation:

- AI generates recommendation with explanation
- Human reviews AI output and supporting information
- Explicit approval required (button click, signature)
- Human decision logged with rationale

Pattern 2: Human-on-the-Loop (HOTL)

Description: AI operates autonomously but human monitors and can intervene. System provides alerts when human attention needed.

Use Cases:

- High-volume routine decisions with exception handling
- Real-time systems where delays would impact performance

Implementation:

- AI makes decisions automatically within defined parameters
- Dashboard shows AI activity in real-time
- Alerts triggered for: low confidence, edge cases, unusual patterns, errors
- Human can pause, override, or reverse AI decisions

Pattern 3: Human-in-Command (HIC)

Description: Human sets objectives and constraints; AI operates within boundaries. Human maintains ultimate authority and can intervene at any time.

Use Cases:

- Strategic decision support systems
- Complex multi-step processes with AI assistance

Implementation:

- Human defines goals, constraints, and risk tolerance
- AI proposes action plans within human-defined boundaries
- Human approves strategy before AI execution
- Continuous monitoring with intervention capability

14.2.2 Human-Machine Interface Requirements

Interface Design Principles:

- **Transparency:** Clear visibility into AI reasoning and confidence
- **Control:** Intuitive mechanisms to override, pause, or stop AI
- **Feedback:** Immediate confirmation of human interventions
- **Situational Awareness:** Context about current AI state and recent actions
- **Error Prevention:** Guard rails against accidental actions

Required Interface Elements:

Interface Element	Purpose	Implementation Example
Override Button	Allow human to reject AI recommendation and input own decision	Prominent "Override" button with confirmation dialog; logs reason for override
Confidence Display	Show AI certainty level in its output	Percentage confidence score; color-coded (green/yellow/red); warning for low confidence
Explanation View	Provide rationale for AI decision	Expandable panel showing key factors, feature importance, similar cases
Pause/Stop Control	Immediately halt AI operations	Emergency stop button; pauses all automated actions; requires human restart
Alert System	Notify human of issues requiring attention	Visual/audio alerts for edge cases, errors, low confidence; priority levels
Activity Log	Show recent AI actions and decisions	Scrollable log with timestamps, inputs, outputs, confidence; searchable/filterable
Parameter Controls	Adjust AI behavior and thresholds	Sliders for risk tolerance, confidence threshold; takes effect immediately
Manual Input Mode	Allow human to bypass AI entirely	Toggle to manual mode; AI provides info only, no automated actions

14.2.3 Special Requirements for Biometric Identification

Dual Verification Requirement (Article 14(5)):

For real-time remote biometric identification systems:

- AI system provides candidate matches with confidence scores
- **First human reviewer** independently evaluates match quality
- **Second human reviewer** (different person) independently verifies
- Both reviewers must confirm before any action taken
- Reviewers cannot see each other's assessments initially
- Discrepancies escalated to senior reviewer or rejected

14.3 Article 14 Compliance Matrix

EU AI Act Article 14 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Design for effective oversight by natural persons	GOVERN 1.6 (Human-AI configuration)	8.2.5 (Human oversight)	A.6.2 (Roles and responsibilities)	Direct
Appropriate human-machine interface tools	MANAGE 3.2 (User interface)	8.2.5 (Interface design)	A.5.16 (Identity management)	Substantial
Prevent or minimize risks to health, safety, fundamental rights	MAP 4 (Risk mitigation) MANAGE 1	6.1.2 (AI risk assessment) 6.1.4 (Risk treatment)	6.1.3 (Risk assessment)	Direct
Humans fully understand capacities and limitations	MANAGE 3.1 (Transparency) GOVERN 4.2	7.2 (Competence) 7.3 (Awareness)	A.6.3 (Awareness)	Direct
Able to properly monitor system operation	GOVERN 5.1-5.2 (Oversight)	9.1 (Monitoring and measurement)	A.8.16 (Monitoring activities)	Direct
Able to correctly interpret system output	MANAGE 3.1 (Output interpretation) MAP 1.2	8.2.4 (Information to deployers)	A.5.1 (Policies)	Direct
Able to decide not to use or disregard/override/reverse output	GOVERN 1.6 (Human authority)	8.2.5 (Override capability)	A.6.2 (Roles)	Direct
Able to intervene or interrupt system operation	GOVERN 1.6 (Intervention)	8.2.5 (Intervention measures)	A.5.23 (Information security in use of cloud)	Direct
Measures built into system by provider OR	GOVERN 2 (Accountability)	5.3 (Organizational roles) 8.2.5	A.5.2 (Information security roles)	Direct

implemented by deployer		(Oversight design)		
Biometric ID: Dual verification by two natural persons required	GOVERN 1.6 (Multi-person oversight)	8.2.5 (Verification procedures)	A.9.2 (User access management)	Substantial

14.4 Human Oversight Implementation Checklist

1. **Select Oversight Pattern:** Determine which pattern (HITL, HOTL, HIC) best fits use case and risk level
2. **Design Interface:** Build human-machine interface with override, explanation, monitoring capabilities
3. **Implement Controls:** Add technical measures for pause, stop, override, manual mode
4. **Develop Training:** Create programs to ensure humans understand system capabilities and limitations
5. **Test Oversight:** Validate that humans can effectively monitor and intervene
6. **Document Procedures:** Create operating procedures for oversight and intervention

Article 15: Accuracy, Robustness, and Cybersecurity

15.1 Legal Requirements

Article 15(1) - EU AI Act:

"High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle."

Article 15(2) - Accuracy Levels:

"The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions for use. High-risk AI systems shall be as accurate as possible in view of their intended purpose."

Article 15(3) - Robustness:

"High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans."

Article 15(4) - Cybersecurity:

"High-risk AI systems shall be resilient as regards attempts by unauthorized third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions to address AI-specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training dataset, inputs designed to cause the AI system to malfunction, or model flaws."

15.2 Detailed Implementation Requirements

15.2.1 Accuracy Requirements and Metrics

Appropriate Accuracy Levels:

Accuracy requirements depend on intended purpose and consequences:

Use Case Risk Level	Typical Accuracy Requirement	Rationale
Life/safety critical (medical diagnosis, autonomous vehicles)	95-99%+ accuracy; very low false negative rate	Errors can result in serious harm or death; must minimize missed cases
High-consequence decisions (credit, hiring, law enforcement)	90-95%+ accuracy; balanced FP/FN rates	Significant life impact; fairness requires minimizing both error types
Moderate-consequence (content moderation, fraud detection)	85-90% accuracy; error tolerance based on review process	Errors can be caught in review; balance accuracy with operational efficiency
Lower-consequence (recommendations, prioritization)	80-85% accuracy; errors have minimal direct harm	Sub-optimal suggestions acceptable; user maintains control

Required Accuracy Metrics:

- **Overall Accuracy:** Percentage of correct predictions
- **Precision:** Of positive predictions, what percentage are correct (TP / (TP + FP))
- **Recall (Sensitivity):** Of actual positives, what percentage are identified (TP / (TP + FN))
- **F1 Score:** Harmonic mean of precision and recall
- **AUC-ROC:** Area under receiver operating characteristic curve
- **Confidence Intervals:** Statistical uncertainty in accuracy estimates
- **Subgroup Performance:** Accuracy broken down by demographic groups

Accuracy Throughout Lifecycle:

- **Initial Validation:** Accuracy measured on held-out test set before deployment
- **Continuous Monitoring:** Track accuracy on production data over time
- **Drift Detection:** Identify when accuracy degrades due to data drift
- **Revalidation:** Periodic reassessment with current ground truth data

15.2.2 Robustness Requirements

Resilience to Errors and Faults:

- **Input Validation:**
  - Reject malformed or out-of-range inputs
  - Handle missing or incomplete data gracefully
- **Error Handling:**
  - Graceful degradation when components fail
  - Clear error messages to users
  - Logging of errors for debugging
- **Edge Case Handling:**
  - Identify and test edge cases during development
  - Flag unusual inputs for human review

Technical Redundancy Solutions:

- **Backup Systems:** Alternative AI models or rule-based fallbacks when primary system fails
- **Fail-Safe Plans:** Predetermined actions when system cannot operate safely
- **Circuit Breakers:** Automatic shutdown triggers for anomalous behavior
- **Manual Override:** Human intervention capability

15.2.3 Cybersecurity Requirements

AI-Specific Threat Landscape:

Attack Type	Description	Mitigation Measures
Data Poisoning	Attacker injects malicious data into training set to corrupt model	Data provenance verification; outlier detection; data sanitization; trusted sources only
Model Evasion	Adversarial inputs crafted to cause misclassification	Adversarial training; input preprocessing; anomaly detection; confidence thresholds
Model Extraction	Attacker queries model to reverse-engineer it	Rate limiting; query monitoring; watermarking; differential privacy
Model Inversion	Reconstruct training data from model outputs	Differential privacy; output perturbation; query restrictions
Backdoor Attack	Trigger pattern causes model to produce attacker-chosen output	Model inspection; activation clustering; neural cleanse techniques
Prompt Injection	For LLMs, malicious instructions embedded in inputs	Input sanitization; prompt validation; output filtering; context isolation

Comprehensive Security Measures:

- **Prevention:**
  - Secure model development lifecycle
  - Code review and security testing
  - Access controls on training data and models
- **Detection:**
  - Adversarial input detection
  - Anomaly detection in outputs
  - Model integrity verification
- **Response:**
  - Incident response plan for AI security events
  - Model rollback capability
  - Communication protocols
- **Control:**
  - Patch management for vulnerabilities
  - Continuous security monitoring

15.3 Article 15 Compliance Matrix

EU AI Act Article 15 Requirement	AI RMF Mapping	ISO 42001 Clause	ISO 27001 Control	Alignment Level
Appropriate level of accuracy throughout lifecycle	MEASURE 3.1-3.3 (Accuracy)	8.2.3 (Validation and testing) 9.1 (Monitoring)	A.8.29 (Security testing)	Direct
Declare accuracy levels and metrics in instructions	MEASURE 3 (Metrics) MANAGE 3.1	8.2.4 (Information to deployers)	A.5.37 (Documented procedures)	Direct
Accuracy as high as possible given intended purpose	MEASURE 3.1 (Performance optimization)	8.2.2 (Design and development) 10.2 (Improvement)	10.2 (Continual improvement)	Direct
Robustness - resilient to errors, faults, inconsistencies	MEASURE 3.4 (Robustness) MAP 4.5	8.2.3 (Testing for robustness)	A.8.14 (Redundancy)	Direct
Technical redundancy, backup, fail-safe plans	MANAGE 2.2 (Resilience) MAP 4.5	8.1 (Operational planning)	A.8.13 (Information backup) A.8.14 (Redundancy)	Substantial
Cybersecurity - resilient to unauthorized manipulation	MEASURE 3.5 (Cybersecurity) MAP 4.6	6.1.2 (Security risk assessment)	All ISO 27001 Annex A controls	Direct
Address AI-specific vulnerabilities (data poisoning, adversarial)	MAP 4.6 (AI security risks)	6.1.2 (AI risk assessment)	A.8.7 (Malware protection) A.8.16 (Monitoring)	Substantial
Prevent, detect, respond, resolve, control attacks on AI system	MANAGE 2.1 (Incident response)	5.26-5.28 (Incident management)	A.5.24-5.28 (Incident management)	Direct
Perform consistently throughout lifecycle	MEASURE 4.2 (Drift detection) MANAGE 4.2	9.1 (Monitoring and measurement) 10.2 (Improvement)	A.8.16 (Monitoring)	Direct

15.4 Testing and Validation Framework

Comprehensive Testing Program:

7. **Accuracy Testing:** Measure performance on representative test set; Subgroup analysis; Confidence interval calculation; Benchmark comparisons
8. **Robustness Testing:** Edge case testing; Stress testing; Fault injection; Data quality degradation tests
9. **Adversarial Testing:** Evasion attacks; Poisoning simulations; Model extraction attempts; Backdoor detection
10. **Security Testing:** Penetration testing; Vulnerability scanning; Code security analysis; Dependency checks
11. **Continuous Monitoring:** Production performance tracking; Drift detection; Anomaly monitoring; Security event logging

---

This comprehensive document provides complete implementation guidance for EU AI Act Articles 9-15, including:

- Full legal text and requirements for each article
- Detailed implementation guidance with specific procedures
- Complete compliance matrices mapping to AI RMF and ISO 42001/27001
- Practical checklists and templates
- Real-world implementation examples and patterns

EU AI Act Compliance: CE Marking Procedures & Declaration Templates

Complete Conformity Assessment Guide

Document Purpose and Scope

Purpose: This document provides comprehensive guidance on CE marking procedures, conformity assessment pathways, and EU Declaration of Conformity requirements for high-risk AI systems under the EU AI Act.

Scope:

- Conformity assessment procedures (Articles 43-44)
- CE marking requirements (Article 48)
- EU Declaration of Conformity (Article 47)
- Step-by-step implementation procedures
- Complete declaration templates ready for use

Section 1: Conformity Assessment Overview

1.1 Legal Requirements

Article 43 - Conformity Assessment:

Providers of high-risk AI systems shall ensure that their systems undergo a conformity assessment procedure prior to their placing on the market or putting into service.

Article 48(1) - CE Marking:

High-risk AI systems that have been assessed to be in conformity with the requirements set out in this Regulation shall bear the CE marking of conformity.

Article 47 - EU Declaration of Conformity:

The provider shall draw up an EU declaration of conformity for each high-risk AI system and keep it at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service.

1.2 Conformity Assessment Procedures

Two Main Procedures (Article 43):

Procedure	Description	When Applicable
Annex VI: Internal Control (Self-Assessment)	Provider conducts conformity assessment based on internal control of design and production; Quality management system required	Default procedure for most high-risk AI systems; No notified body involvement unless harmonized standards not fully applied
Annex VII: Quality Management System + Assessment by Notified Body	Provider establishes quality management system; Notified body assesses technical documentation and QMS	Required when harmonized standards not applied or applied incompletely; Required for certain Annex III systems (biometric, critical infrastructure)

1.3 Decision Tree: Which Procedure Applies?

Follow this decision tree to determine your conformity assessment procedure:

Step 1: Is your AI system classified as high-risk under Annex III?

- YES → Continue to Step 2
- NO → AI Act does not apply (unless general-purpose AI)

Step 2: Are you using harmonized standards?

- YES and applied FULLY → Continue to Step 3
- NO or only PARTIALLY → Annex VII (Notified Body) REQUIRED

Step 3: Is your system in specific high-risk categories?

- Biometric identification/categorization (Annex III, point 1)
- Critical infrastructure (Annex III, point 2)
- If YES to above → Annex VII (Notified Body) REQUIRED

Step 4: Default procedure

- If you reached this step → Annex VI (Internal Control) applies

Section 2: Annex VI - Internal Control Procedure

2.1 Procedure Overview

This is the self-assessment procedure where the provider demonstrates conformity without notified body involvement (unless harmonized standards not fully applied).

Required Elements:

- Quality management system per Article 17
- Technical documentation per Article 11 and Annex IV
- Compliance with all requirements of Chapter III, Section 2 (Articles 9-15)
- EU Declaration of Conformity

2.2 Step-by-Step Implementation

1. **Establish Quality Management System**

Article 17 Quality Management System Requirements:

- **Strategy for Regulatory Compliance:**
  - Policy for compliance with EU AI Act
  - Processes to ensure compliance
  - Assignment of responsibilities
- **Design, Development, Quality Control Techniques:**
  - Procedures for AI system design and development
  - Quality control processes
  - Testing and validation procedures
- **Examination, Test, Validation Procedures:**
  - Pre-market testing protocols
  - Validation methodology
  - Verification procedures
- **Post-Market Monitoring System:**
  - Continuous monitoring plan (Article 72)
  - Serious incident reporting procedures (Article 73)
  - Performance monitoring and updates
- **Reporting Procedures:**
  - Serious incident reporting to authorities
  - Malfunctions and corrective actions
  - Communication to deployers
- **Record-Keeping:**
  - Automatic logging per Article 12
  - Documentation retention (10 years)

Deliverable: Quality Management System documentation demonstrating compliance with Article 17

Timeline: 2-4 months to establish and document

2. **Prepare Technical Documentation (Article 11, Annex IV)**

Required Contents (see Article 11 document for full details):

- General system description
- Detailed description of elements and development
- Monitoring, functioning, and control information
- Risk management system description
- Changes made throughout lifecycle
- List of applied standards
- EU declaration of conformity
- Assessment and verification procedures

Deliverable: Complete technical documentation package

Timeline: 3-6 months to compile comprehensive documentation

3. **Ensure Compliance with Articles 9-15**

Verify that your AI system meets all requirements:

- Article 9: Risk management system ✓
- Article 10: Data and data governance ✓
- Article 11: Technical documentation ✓
- Article 12: Record-keeping ✓
- Article 13: Transparency and information ✓
- Article 14: Human oversight ✓
- Article 15: Accuracy, robustness, cybersecurity ✓

Deliverable: Evidence of compliance for each article

Timeline: Ongoing throughout development; 6-12 months for full compliance

4. **Draw Up EU Declaration of Conformity**

Complete the EU Declaration of Conformity using the template in Section 4.

Deliverable: Signed EU Declaration of Conformity

Timeline: 1-2 weeks once all documentation complete

5. **Affix CE Marking**

Apply CE marking to your AI system per Article 48 (see Section 3).

Deliverable: CE marking affixed to system/documentation

Timeline: 1 week

6. **Keep Documentation Available**

Maintain all documentation for 10 years after placing on market or putting into service.

Deliverable: Document retention system

Timeline: Ongoing for 10 years

Section 3: CE Marking Requirements

3.1 Legal Requirements (Article 48)

Article 48(2) - CE Marking Rules:

"The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate."

Article 48(3) - Identification Number:

"Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number shall be affixed by the notified body itself or, under its instructions, by the provider or by the provider's authorized representative."

3.2 CE Marking Specifications

Physical Requirements:

- **Visible:** Clearly visible to users and authorities
- **Legible:** Easy to read; minimum height 5mm (unless different size justified)
- **Indelible:** Permanent; cannot be easily removed or altered

Placement Options (in order of preference):

Option	When to Use	Example
1. On the AI System Itself	When system has physical form (hardware, embedded systems, robots)	Affixed to hardware casing, device label, nameplate
2. On the Packaging	When affixing to system not possible/warranted (software-only systems)	Printed on software box, USB drive packaging, delivery media
3. In Accompanying Documentation	When neither system nor packaging available (cloud services, APIs, SaaS)	Included in digital instructions for use, user manual, technical documentation cover page

CE Marking Format:

The CE marking consists of the letters "CE" in a specific format:

CE

With Notified Body (if applicable):

CE 1234 (where 1234 is notified body identification number)

3.3 Additional Information to Include

Along with CE marking, include:

- Provider name and registered address
- Product name, type, batch or serial number
- Year of manufacture
- Notified body identification number (if applicable)

Section 4: EU Declaration of Conformity

4.1 Legal Requirements (Article 47)

Required Contents:

- Provider name and address
- Statement that declaration issued under sole responsibility of provider
- AI system identification (type, batch, serial number)
- Statement of conformity with EU AI Act requirements
- References to harmonized standards applied or other means of demonstrating conformity
- Where applicable, notified body name, identification number, and certificate details
- Place and date of issue
- Signature of authorized person

4.2 EU Declaration of Conformity Template

Use this template for your EU Declaration of Conformity:

EU DECLARATION OF CONFORMITY

Regulation (EU) 2024/1689 - Artificial Intelligence Act

1. AI SYSTEM IDENTIFICATION

Product Name: [AI System Name]

Product Type/Model: [Type/Model Number]

Batch or Serial Number: [Number or Range]

Version: [Software/Firmware Version]

Intended Purpose: [Description of intended use]

2. PROVIDER INFORMATION

Provider Name: [Legal Entity Name]

Registered Address: [Full Address]

Country: [Country]

Contact: [Email, Phone]

3. AUTHORIZED REPRESENTATIVE (If applicable, for providers outside EU)

Name: [Representative Name]

Address: [EU Address]

Contact: [Email, Phone]

4. DECLARATION

This declaration of conformity is issued under the sole responsibility of the provider.

The AI system identified above is in conformity with Regulation (EU) 2024/1689 (Artificial Intelligence Act), and where applicable, with the following Union harmonisation legislation:

☐ [Other relevant EU legislation, e.g., Medical Device Regulation, Machinery Regulation]

☐ [Add others as applicable]

5. CONFORMITY ASSESSMENT PROCEDURE

The conformity assessment was performed according to:

☐ Annex VI - Internal control based on quality management system

☐ Annex VII - Conformity assessment based on quality management system and assessment of technical documentation

6. APPLIED STANDARDS AND SPECIFICATIONS

The following harmonized standards and technical specifications were applied:

☐ [Harmonized Standard Name and Reference Number]

☐ [Common Specifications if applicable]

☐ [Technical Specifications]

☐ Other means of demonstrating conformity: [Describe]

7. NOTIFIED BODY (If applicable)

Notified Body Name: [Name]
Notified Body Number: [4-digit ID]
Certificate Number: [Certificate Reference]
Certificate Issue Date: [Date]
Certificate Expiry Date: [Date]

8. ADDITIONAL INFORMATION

[Any additional relevant information]

9. SIGNATURE

Signed for and on behalf of: [Provider Name]
Place of issue: [City, Country]
Date of issue: [DD/MM/YYYY]

_____

Name: [Authorized Person Name]
Position: [Job Title]
Signature: [Handwritten or Digital Signature]

Section 5: Implementation Timeline

Typical Timeline for Annex VI (Internal Control) Procedure:

Phase	Activities	Duration
Preparation	Gap analysis, team formation, resource allocation	1-2 months
QMS Development	Establish quality management system per Article 17	2-4 months
Technical Documentation	Compile comprehensive documentation per Article 11 and Annex IV	3-6 months (parallel with QMS)
Compliance Verification	Verify compliance with Articles 9-15; testing and validation	2-4 months (parallel)
Internal Review	Internal audit, gap remediation, final checks	1-2 months
Declaration & CE Marking	Complete EU Declaration of Conformity, affix CE marking	2-4 weeks
Total	End-to-end conformity assessment	9-18 months

This document provides complete CE marking procedures and EU Declaration of Conformity templates for EU AI Act compliance.

EU AI Act Compliance: EU Database Registration & Incident Reporting

Complete Registration and Reporting Procedures

Document Purpose and Scope

Purpose: This document provides comprehensive guidance on EU database registration requirements and serious incident reporting procedures for high-risk AI systems under the EU AI Act.

Scope:

- EU database registration (Article 71)
- Registration information requirements
- Post-market monitoring (Article 72)
- Serious incident reporting (Article 73)
- Step-by-step procedures and templates

Section 1: EU Database Registration

1.1 Legal Requirements (Article 71)

Article 71(1) - Database Obligation:

"Before placing on the market or putting into service a high-risk AI system listed in Annex III, with the exception of high-risk AI systems listed in point 2 of Annex III, the provider or, where applicable, the authorised representative shall register itself and its high-risk AI system in the EU database referred to in Article 71."

Article 71(4) - Information to be Registered:

The EU database shall contain personal and non-personal data entered by providers, notified bodies and national competent authorities in accordance with their respective obligations under this Regulation.

1.2 Who Must Register

Obligated Parties:

- **Providers** of high-risk AI systems (primary responsibility)
- **Authorized Representatives** (when provider is outside EU)

Systems Requiring Registration:

- All high-risk AI systems listed in Annex III
- **EXCEPTION:** Systems in Annex III point 2 (critical infrastructure) are exempt from registration

Timing:

- **BEFORE** placing on market or putting into service

1.3 Required Registration Information

Provider Information:

- Provider name and legal form
- Registered address
- Contact details (email, phone, website)
- Authorized representative details (if applicable)

AI System Information:

- Trade name and additional unambiguous reference
- Intended purpose
- Status of the AI system (on market, in service, withdrawn, recalled)
- Type, category, and Annex III classification

- Brief description of system and how it works
- Member States where system available or deployed
- Link to instructions for use (publicly accessible)

Conformity Assessment Information:

- Conformity assessment procedure applied
- Summary of conformity assessment activities
- CE marking affixation date
- Notified body details (if applicable): name, ID number, certificate number

Post-Market Monitoring Information:

- Post-market monitoring plan summary
- Contact for post-market monitoring queries

1.4 Registration Procedure

Step-by-Step Registration Process:

1. **Access EU Database**
   - Access the EU database for high-risk AI systems
   - URL: [To be provided by European Commission]
   - Create account or login with EU Login credentials

2. **Register as Provider**
   - Complete provider organization profile
   - Verify legal entity information
   - Designate authorized users for registration

3. **Register AI System**
   - Create new AI system entry
   - Complete all required fields (see Section 1.3)
   - Upload supporting documentation
   - Provide link to publicly accessible instructions for use

4. **Submit Registration**
   - Review all information for accuracy
   - Submit registration
   - Receive registration confirmation and unique identifier

5. **Maintain Registration**
   - Update registration when system changes substantially
   - Update status (on market, withdrawn, recalled)
   - Keep contact information current

1.5 Registration Checklist

☐	Requirement	Details/Evidence
☐	Provider information complete and verified	Legal name, address, contact details, legal form
☐	AI system identified and classified	Trade name, Annex III classification, intended purpose
☐	Conformity assessment completed	Procedure applied, CE marking affixed, declaration signed
☐	Instructions for use publicly accessible	URL to instructions, confirmed accessible
☐	Post-market monitoring plan prepared	Plan summary, monitoring procedures established
☐	Notified body information (if applicable)	Body name, ID number, certificate details
☐	Authorized representative designated (if non-EU provider)	Representative name, EU address, contact
☐	Registration submitted before market placement	Confirmation received, unique identifier obtained
☐	Registration maintenance procedure established	Update triggers defined, responsible person assigned

Section 2: Post-Market Monitoring

2.1 Legal Requirements (Article 72)

Article 72(1) - Monitoring Obligation:

"Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system."

Article 72(2) - Monitoring Activities:

The post-market monitoring system shall actively and systematically collect, document and analyse relevant data which may be provided by deployers or which may be collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2.

2.2 Post-Market Monitoring Plan Components

Required Elements:

- **1. Data Collection Strategy:**
  - **Sources of Information:**
  - - Deployer feedback and reports
  - - User complaints and inquiries
  - - System logs and automated monitoring
  - - Performance metrics from deployment
  - - Literature and scientific publications
  - - Market surveillance findings

- **2. Performance Monitoring:**
  - Accuracy tracking over time
  - Model drift detection
  - Performance across demographic subgroups
  - Comparison to pre-deployment performance

- **3. Safety Monitoring:**
  - Incident tracking and analysis
  - Near-miss events
  - Malfunction patterns
  - Emerging risks

- **4. Compliance Monitoring:**
  - Continuous verification of Article 9-15 compliance
  - Quality management system effectiveness
  - Human oversight effectiveness

- **5. Analysis and Evaluation:**
  - Regular data analysis procedures
  - Root cause analysis for incidents
  - Trend identification
- **6. Corrective and Preventive Actions:**
  - Action triggers and escalation criteria
  - Corrective action procedures
  - System updates and improvements
  - Communication to deployers
- **7. Reporting:**
  - Internal reporting to management
  - Serious incident reporting to authorities (Article 73)
  - Database updates

Section 3: Serious Incident Reporting

3.1 Legal Requirements (Article 73)

Article 73(1) - Reporting Obligation:

"Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred."

Article 73(2) - Timeline:

The report shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the provider becomes aware of the serious incident.

3.2 Definition of Serious Incident

Article 3(49) - "Serious Incident":

An incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

- **(a) Death of a person** or serious harm to a person's health
- **(b) Serious and irreversible disruption** of the management or operation of critical infrastructure
- **(c) Infringement of obligations** under Union law intended to protect fundamental rights
- **(d) Serious damage to property or the environment**

Examples of Serious Incidents:

Category	Example Scenarios
Death or Serious Health Harm	Medical AI misdiagnosis leading to death; Autonomous vehicle causing fatal accident; Healthcare AI delay in emergency detection causing permanent injury
Critical Infrastructure Disruption	AI controlling power grid causes extended blackout; Transportation management AI failure causing service disruption; Water treatment AI malfunction affecting supply
Fundamental Rights Infringement	Biometric ID system wrongly identifies person leading to false arrest; Employment AI discriminates based on protected characteristics; Credit scoring AI systematically denies loans to specific groups
Property or Environmental Damage	Industrial AI causes significant environmental contamination; Autonomous system damages valuable property; AI-controlled process causes fire or explosion

3.3 Reporting Procedure

Step-by-Step Reporting Process:

6. **Incident Detection and Assessment (Immediate)**
   - Become aware of incident through any source
   - Assess whether incident meets "serious incident" criteria
   - Document initial incident details
   - Activate incident response team

7. **Investigate Causal Link (Within days)**
   - Gather evidence about incident
   - Analyze system logs and data
   - Interview witnesses/deployers if relevant
   - Determine if causal link exists or is reasonably likely

8. **Prepare Report (Maximum 15 days from awareness)**
   - Complete incident report using template (Section 3.5)
   - Include all required information
   - Gather supporting evidence and documentation

9. **Submit Report (Immediately upon establishing link, max 15 days)**
   - Submit to market surveillance authority in Member State(s) where incident occurred
   - Submit through official reporting channel (as established by each Member State)
   - Obtain confirmation of receipt

10. **Follow-Up and Cooperation (Ongoing)**
    - Cooperate with authority investigation
    - Provide additional information as requested
    - Submit follow-up reports if new information emerges
    - Implement corrective actions as required

3.4 Required Report Information

Minimum Information to Include:

- **Provider Information:**
  - Name and contact details
  - Database registration number

- **AI System Identification:**
  - Product name and model
  - Serial/batch number
  - Version/configuration involved

-

- **Incident Details:**
  - Date, time, and location of incident
  - Description of what occurred
  - Consequences (death, injury, damage, etc.)
  - Persons affected (anonymized if necessary)
- **Causal Analysis:**
  - Evidence of causal link to AI system
  - Root cause analysis findings
  - Contributing factors
- **Corrective Actions:**
  - Immediate actions taken
  - Planned preventive measures
  - Timeline for implementation

3.5 Serious Incident Report Template

SERIOUS INCIDENT REPORT

Article 73 - EU AI Act

SECTION 1: PROVIDER INFORMATION

Provider Name: [Legal Entity Name]

Address: [Full Address]

Contact Person: [Name, Title]

Email: [Email]

Phone: [Phone]

EU Database Registration Number: [Number]

SECTION 2: AI SYSTEM IDENTIFICATION

Product Name: [Name]

Model/Type: [Model]

Serial/Batch Number: [Number]

Software Version: [Version]

Annex III Classification: [Classification]

Intended Purpose: [Purpose]

SECTION 3: INCIDENT DETAILS

Date of Incident: [DD/MM/YYYY]

Time of Incident: [HH:MM]

Location: [City, Country, Member State]

Date Provider Became Aware: [DD/MM/YYYY]

How Provider Became Aware: [Deployer report / User complaint / System monitoring / Other]

SECTION 4: INCIDENT DESCRIPTION

Detailed Description of What Occurred:

[Provide detailed narrative of the incident]

SECTION 5: CONSEQUENCES

Severity Classification (check all that apply):

☐ Death of person(s)

☐ Serious harm to person's health

☐ Serious and irreversible disruption of critical infrastructure

☐ Infringement of fundamental rights obligations

☐ Serious damage to property

☐ Serious damage to environment

Number of Persons Affected: [Number]
Detailed Description of Consequences: [Description]

SECTION 6: CAUSAL ANALYSIS

Evidence of Causal Link to AI System:
[Describe evidence establishing or suggesting causal link]

Root Cause (if determined):
[Describe identified root cause]

Contributing Factors:
[List any contributing factors]

SECTION 7: CORRECTIVE ACTIONS

Immediate Actions Taken:
[List immediate actions]

Planned Corrective Measures:
[Describe planned corrections]

Implementation Timeline:
[Provide timeline]

SECTION 8: ADDITIONAL INFORMATION

[Any other relevant information]

SECTION 9: DECLARATION

I declare that the information provided in this report is accurate and complete to the best of my knowledge.

Prepared by: [Name, Position]
Date: [DD/MM/YYYY]
Signature: _____

Section 4: Implementation Checklist

Use this checklist to ensure compliance with database registration and reporting requirements:

☐	Requirement	Status/Notes
☐	EU Database registration completed before market placement	Date: _____ Registration #: _____
☐	Post-market monitoring plan documented	Version: _____ Last review: _____
☐	Post-market monitoring system operational	Active since: _____ Responsible: _____
☐	Incident detection and assessment procedures established	Documented in: _____
☐	Serious incident reporting procedures established	Procedure doc: _____ Training: _____
☐	Contact established with Member State market surveillance authorities	Contacts documented: Yes / No
☐	Staff trained on incident identification and reporting	Training date: _____ Attendees: _____
☐	Incident response team designated	Team lead: _____ Members: _____
☐	Database registration update procedures established	Review frequency: _____ Responsible: _____

This document provides complete EU database registration procedures and serious incident reporting templates for EU AI Act compliance.

End of Appendix D

Appendix E

AI RMF 2026 to ISO/IEC 42001 Complete Crosswalk

Version 1.0 | January 2026

Introduction

This comprehensive crosswalk maps all AI RMF 2026 categories and subcategories to ISO/IEC 42001:2023 clauses, enabling organizations to implement both standards efficiently.

Alignment Types

- **Direct:** AI RMF directly satisfies ISO requirement
- **Substantial:** AI RMF addresses majority; some ISO-specific documentation needed
- **Partial:** AI RMF covers some aspects; additional work needed

GOVERN Function Mappings

AI RMF	Description	ISO 42001	Alignment	Notes
GOVERN 1.1	Legal/regulatory requirements managed	4.2, 6.3	Direct	Compliance register
GOVERN 1.2	Roles and responsibilities defined	5.3	Direct	AIMS roles documented
GOVERN 1.3	DEI in AI design	6.1.3, 7.2	Substantial	Impact assessment
GOVERN 1.4	Responsible AI culture	5.1, 7.3	Substantial	Awareness programs
GOVERN 2.1	Accountability structures exist	5.3, 8.1	Direct	Decision authority defined
GOVERN 3.1	AI teams diverse	7.2	Partial	Competency planning
GOVERN 4.1	Risk management culture	5.1, 7.3	Substantial	Training records
GOVERN 5.1	Oversight bodies exist	9.2, 9.3	Direct	Audit, management review
GOVERN 6.1	Trustworthy AI policies	5.2	Direct	AI policy approved

MAP Function Mappings

AI RMF	Description	ISO 42001	Alignment	Notes
MAP 1.1	Mission and stakeholders documented	4.2, 4.4	Direct	Stakeholder analysis; scope
MAP 1.2	AI application and uses defined	8.1	Direct	AI system register
MAP 2.1	AI systems categorized by risk	6.1.3	Direct	Impact assessment
MAP 3.1	Potential benefits documented	6.1.3	Substantial	Business case
MAP 3.2	Known risks documented	6.1.2	Direct	Risk register
MAP 4.1	Systematic risk assessment	6.1.2	Direct	Risk methodology
MAP 5.1	Individual impacts assessed	6.1.3	Direct	Rights impact analysis
MAP 5.2	Societal impacts assessed	6.1.3	Direct	Community engagement

MEASURE Function Mappings

AI RMF	Description	ISO 42001	Alignment	Notes
MEASURE 1.1	Trustworthiness metrics defined	9.1.1	Substantial	Define KPIs
MEASURE 2.1	Test datasets representative	8.2.3	Substantial	Validation data
MEASURE 2.2	Performance evaluated	8.2.3, 9.1	Direct	Testing, monitoring
MEASURE 3.1	Risk tracking mechanisms	9.1	Direct	Risk tracking system
MEASURE 4.1	AI system validation performed	8.2.3	Direct	Validation reports

MANAGE Function Mappings

AI RMF	Description	ISO 42001	Alignment	Notes
MANAGE 1.1	Risk response strategy documented	6.1.4	Direct	Treatment plan
MANAGE 1.2	Risk responses implemented	8.1	Direct	Control implementation
MANAGE 2.1	Incident response plan established	8.2.5	Direct	Response procedures
MANAGE 3.1	Information shared with stakeholders	7.4	Direct	Transparency docs
MANAGE 4.1	Continuous improvement processes	10.2	Direct	Improvement register
MANAGE 4.2	Lessons learned incorporated	10.1, 10.2	Direct	Post-incident reviews

Summary

This crosswalk demonstrates 80-90% alignment between AI RMF 2026 and ISO 42001. Organizations implementing AI RMF 2026 guidance can achieve ISO 42001 certification with targeted additions of formal management system documentation.

Key Gaps

- Formal AIMS scope document (ISO Clause 4.4)
- Management system policy with ISO language (Clause 5.2)
- Internal audit program (Clause 9.2)
- Document control procedures (Clause 7.5)

End of Appendix E

Appendix F

Document Templates for ISO 42001 & 27001 Integration

Appendix F

Introduction

This appendix provides standardized document templates to support implementation of the integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 framework. These templates ensure consistency, completeness, and alignment with certification requirements.

Template Usage Guidelines

Each template includes:

Element	Description
Purpose	Intended use and objectives
Instructions	Guidance for completing each section
Mappings	References to AI RMF 2026, ISO 42001, and ISO 27001 requirements

Template F.1

AI System Inventory Record

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a standardized method for documenting all AI systems within an organization's AI Management System (AIMS). It supports comprehensive system tracking, lifecycle management, and compliance verification across AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 requirements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-1.1 (Inventory of AI systems), MAP-1.1 (Context of use), MANAGE-1.1 (System documentation)
- **ISO/IEC 42001:** Clause 4.1 (Understanding organization context), Clause 7.5 (Documented information), Clause 8.1 (Operational planning)
- **ISO/IEC 27001:** Clause 7.5 (Documented information), Annex A.8.1 (Inventory of assets)

Instructions for Use

1. Complete one inventory record for each AI system

Fill in all required fields. Mark optional fields as "N/A" if not applicable.

2. Assign unique system identifier

Use organizational naming convention (e.g., AIS-2024-001, ML-PROD-002).

3. Update inventory regularly

Review and update at least quarterly or when significant changes occur.

4. Maintain version control

Track all changes to the inventory record in the change log.

5. Store securely

Maintain inventory records as controlled documents per ISO/IEC 42001 requirements.

AI SYSTEM INVENTORY RECORD

Section 1: Basic Identification

1.1 System Identifier (Unique ID): _____

1.2 System Name: _____

1.3 System Version: _____

1.4 Record Creation Date: _____

1.5 Last Updated: _____

1.6 Record Owner: _____

Section 2: System Classification

2.1 System Type (check all that apply):

☐ Machine Learning System

☐ Deep Learning System

☐ Natural Language Processing

☐ Computer Vision

☐ Expert System / Rule-Based

☐ Robotic Process Automation

☐ Recommendation System

☐ Other (specify): _____

2.2 AI Technique (primary method):

☐ Supervised Learning

☐ Unsupervised Learning

☐ Reinforcement Learning

☐ Semi-Supervised Learning

☐ Transfer Learning

☐ Ensemble Methods

☐ Other (specify): _____

2.3 Deployment Status:

☐ Development

☐ Testing

☐ Staging

☐ Production

☐ Retired

☐ Decommissioned

2.4 Risk Level Classification (per AI RMF MEASURE):

☐ Critical - High impact on safety, rights, or critical operations

☐ High - Significant impact requiring close monitoring

☐ Medium - Moderate impact with standard controls

☐ Low - Limited impact, minimal risk

Risk Assessment Reference: _____

Section 3: Business Context

3.1 Business Unit/Department: _____

3.2 System Owner: _____

3.3 Technical Lead: _____

3.4 Business Sponsor: _____

3.5 Intended Purpose:

[Describe primary business purpose and objectives]

_____

_____

_____

3.6 Use Cases:

[List specific use cases or applications]

_____

_____

_____

3.7 Expected Benefits:

☐ Improved efficiency

☐ Cost reduction

☐ Enhanced accuracy

☐ Better customer experience

☐ New capabilities

☐ Risk reduction

☐ Other: _____

Section 4: Technical Specifications

4.1 Model Architecture:

[Describe neural network type, algorithm, or approach]

_____

_____

4.2 Development Framework/Platform: _____

4.3 Programming Languages Used: _____

4.4 Key Libraries/Dependencies: _____

_____

4.5 Input Data Specifications:

Data Types: _____

Data Format: _____

Expected Volume: _____

Data Sources: _____

4.6 Output Specifications:

Output Type: _____

Output Format: _____

Confidence/Probability Provided: ☐ Yes ☐ No

4.7 Performance Metrics:

Primary Metric: _____

Target Performance: _____

Current Performance: _____

Section 5: Data Governance (ISO/IEC 42001 Clause 7.4)

5.1 Training Data:

Dataset Name/ID: _____

Dataset Size: _____

Data Collection Period: _____

Data Source(s): _____

Data Quality Assessment: ☐ Complete ☐ Pending ☐ Not Required

5.2 Data Sensitivity Classification:

☐ Public - No restrictions

☐ Internal - Organization use only

☐ Confidential - Restricted access

☐ Highly Confidential - Strictly controlled

5.3 Personal Data Processing:

Processes Personal Data: ☐ Yes ☐ No

If Yes, Data Protection Impact Assessment (DPIA) Completed: ☐ Yes ☐ No

DPIA Reference Number: _____

Legal Basis for Processing: _____

Data Retention Period: _____

5.4 Bias Assessment:

Bias Testing Performed: ☐ Yes ☐ No ☐ Planned

Bias Assessment Reference: _____

Identified Biases: _____

Section 6: Infrastructure and Deployment

6.1 Deployment Environment:

☐ On-Premises

☐ Cloud (specify provider): _____

☐ Hybrid

☐ Edge/IoT Devices

6.2 Geographic Location(s): _____

6.3 Availability Requirements: _____

6.4 Scalability Requirements: _____

6.5 Integration Points:

[List systems this AI system integrates with]

_____

_____

6.6 API Endpoints:

Has External APIs: ☐ Yes ☐ No

API Documentation Location: _____

Section 7: Security and Controls (ISO/IEC 27001 Alignment)

7.1 Access Controls:

☐ Role-Based Access Control (RBAC) implemented

☐ Multi-Factor Authentication (MFA) required

☐ Least privilege principle applied

☐ Access logs maintained

7.2 Data Protection Measures:

☐ Encryption at rest

☐ Encryption in transit (TLS/SSL)

☐ Data masking/anonymization

☐ Secure key management

☐ Data backup and recovery procedures

7.3 Model Security:

☐ Model versioning and integrity checks

☐ Protection against model theft

☐ Adversarial robustness testing performed

☐ Input validation and sanitization

7.4 Monitoring and Logging:

☐ Real-time performance monitoring

☐ Security event logging

☐ Audit trail maintained

☐ Anomaly detection enabled

Log Retention Period: _____

Section 8: Governance and Accountability (AI RMF GOVERN)

8.1 Human Oversight:

☐ Human-in-the-loop

☐ Human-on-the-loop

☐ Human-in-command

☐ Fully automated (no human oversight)

Oversight Roles/Personnel: _____

Override Capability: ☐ Yes ☐ No

8.2 Explainability and Transparency:

☐ Model explanations available

☐ Decision rationale provided

☐ User documentation complete

Explainability Method: _____

8.3 Ethical Review:

Ethics Review Completed: ☐ Yes ☐ No ☐ Not Required

Review Date: _____

Reviewer(s): _____

Ethical Concerns Identified: _____

8.4 Regulatory Compliance:

[List applicable regulations and compliance status]

_____

_____

Section 9: Lifecycle Management

9.1 Development Start Date: _____

9.2 Initial Deployment Date: _____

9.3 Last Major Update: _____

9.4 Planned Retirement Date (if known): _____

9.5 Update/Retraining Schedule:

☐ Continuous (automated)

☐ Monthly

☐ Quarterly

☐ Annually

☐ As needed

☐ Not scheduled

9.6 Change Management:

Change Control Process Defined: ☐ Yes ☐ No

Change Log Reference: _____

Section 10: Documentation References

Document Type	Reference Number/Location	Last Updated
System Requirements Specification	[Reference]	[Date]
Risk Assessment	[Reference]	[Date]
Technical Documentation	[Reference]	[Date]
User Documentation	[Reference]	[Date]
Test/Validation Reports	[Reference]	[Date]
Model Card	[Reference]	[Date]
Data Governance Documentation	[Reference]	[Date]
Security Assessment	[Reference]	[Date]
Incident Response Plan	[Reference]	[Date]

Section 11: Approval and Sign-Off

Prepared By:

Name: _____

Title: _____

Date: _____

Signature: _____

Reviewed By:

Name: _____

Title: _____

Date: _____

Signature: _____

Approved By:

Name: _____

Title: _____

Date: _____

Signature: _____

END OF AI SYSTEM INVENTORY RECORD

Document Control Information:

Template Version: 1.0

Effective Date: [Date]

Next Review Date: [Date]

Owner: [AI Governance Office/CISO/CTO]

Template F.2
AI Risk Assessment Worksheet

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a systematic methodology for identifying, analyzing, and evaluating AI-specific risks throughout the AI system lifecycle.

Framework Alignment:

- **AI RMF 2026:** MAP-2.3, MAP-3.1, MAP-3.2, MEASURE-2.1, MANAGE-2.1
- **ISO/IEC 42001:** Clause 6.1, Clause 8.1.2, Clause 9.1
- **ISO/IEC 27001:** Clause 6.1.2, Clause 6.1.3, Clause 8.2

Instructions for Use

1. Assessment Timing:

- • Conduct initial assessment during system design phase
- • Update before major deployments or changes
- • Review at least annually for production systems

2. Risk Rating Methodology:

- • Use 5-point scales for Impact and Likelihood
- • Calculate Risk Score = Impact × Likelihood
- • Apply risk matrix to determine risk level

RISK ASSESSMENT WORKSHEET

Section 1: Assessment Information

1.1 AI System Name: _____
1.2 System ID: _____
1.3 Assessment Date: _____
1.4 Assessment Version: _____
1.5 Previous Assessment Date:
_____

1.6 Assessment Type:
☐ Initial Assessment (new system)
☐ Pre-Deployment Assessment
☐ Periodic Review
☐ Change-Triggered Assessment
☐ Incident-Triggered Assessment

1.7 Assessment Team:

Name	Role/Title	Area of Expertise
[Name]	[Title]	[Expertise]
[Name]	[Title]	[Expertise]
[Add rows as needed]		

Section 2: Risk Rating Scales

2.1 Impact Scale (1-5)

Score	Level	Description
5	Catastrophic	Severe harm; major financial loss; permanent reputation damage; regulatory sanctions; loss of life
4	Major	Significant harm; substantial financial loss; serious reputation damage; legal liability
3	Moderate	Noticeable harm; moderate financial loss; reputation concerns; compliance violations
2	Minor	Limited harm; small financial loss; minor reputation impact; inconvenience
1	Negligible	Minimal or no harm; negligible financial impact; no reputation impact

2.2 Likelihood Scale (1-5)

Score	Level	Probability	Description
5	Almost Certain	>90%	Expected to occur frequently
4	Likely	60-90%	Will probably occur
3	Possible	30-60%	Might occur
2	Unlikely	10-30%	Could occur but doubtful
1	Rare	<10%	May occur in exceptional circumstances

2.3 Risk Matrix

Risk Score = Impact × Likelihood

Impact↓/Likelihood→	1-Rare	2-Unlikely	3-Possible	4-Likely	5-Almost Certain
5-Catastrophic	5-Medium	10-High	15-High	20-Critical	25-Critical
4-Major	4-Medium	8-Medium	12-High	16-High	20-Critical
3-Moderate	3-Low	6-Medium	9-Medium	12-Medium	15-High
2-Minor	2-Low	4-Low	6-Medium	8-Medium	10-High
1-Negligible	1-Low	2-Low	3-Low	4-Low	5-Medium

Risk Level Definitions:
Critical (20-25): Unacceptable risk. Immediate action required.
High (10-19): Significant risk. Senior management attention required.
Medium (4-9): Moderate risk. Mitigation measures should be implemented.
Low (1-3): Acceptable risk. Monitor through standard procedures.

Section 3: Risk Categories

Assess risks in each applicable category:

3.1 Technical/Performance Risks

Examples:
- • Insufficient model accuracy
- • Model drift over time
- • Lack of robustness

3.2 Fairness and Bias Risks

Examples:
- • Discriminatory outcomes
- • Underrepresentation in training data
- • Disparate impact across groups

3.3 Security Risks

Examples:
- • Adversarial attacks
- • Model theft
- • Data poisoning

3.4 Privacy Risks

Examples:

- • Personal data exposure
- • Re-identification risks
- • Membership inference attacks

3.5 Transparency Risks

Examples:

- • Lack of model interpretability
- • Black box decision-making

3.6 Safety Risks

Examples:

- • Physical harm to individuals
- • Critical infrastructure failures

3.7 Operational Risks

Examples:

- • System deployment failures
- • Integration issues

3.8 Legal/Regulatory Risks

Examples:

- • Non-compliance with regulations
- • Liability for AI decisions

3.9 Ethical/Social Risks

Examples:

- • Erosion of human autonomy
- • Social manipulation

Section 4: Risk Assessment Entry

RISK ID: R-001

Risk Category:
☐ Technical/Performance
☐ Fairness and Bias
☐ Security
☐ Privacy
☐ Transparency
☐ Safety
☐ Operational
☐ Legal/Regulatory
☐ Ethical/Social

Risk Description:
[Describe the risk in detail - what could go wrong and how]

_____
_____

Potential Consequences:
[What harm or damage could occur]

_____

Affected Stakeholders:
[Who would be impacted]

_____

Inherent Risk Assessment (before controls):
Impact Rating (1-5): _____ Justification: _____
Likelihood Rating (1-5): _____ Justification: _____
Risk Score (Impact × Likelihood): _____
Risk Level: ☐ Critical ☐ High ☐ Medium ☐ Low

Existing Controls/Mitigations:
[List current measures in place]

_____
_____

Control Effectiveness:
☐ Highly Effective ☐ Moderately Effective ☐ Minimally Effective ☐ Not Effective

Residual Risk Assessment (after controls):
Impact Rating (1-5): _____
Likelihood Rating (1-5): _____
Risk Score: _____
Risk Level: ☐ Critical ☐ High ☐ Medium ☐ Low

Risk Treatment Decision:
☐ Accept - Risk is acceptable at current level
☐ Mitigate - Implement additional controls
☐ Transfer - Share or transfer risk
☐ Avoid - Do not proceed with this aspect

Additional Mitigation Measures Required:
[List specific additional controls to implement]
_____
_____

Responsible Party: _____
Target Completion Date: _____
Status: ☐ Not Started ☐ In Progress ☐ Complete

[Copy this risk entry template for each additional identified risk (R-002, R-003, etc.)]

Section 5: Risk Summary Dashboard

Risk ID	Description	Category	Inherent Score	Inherent Level	Residual Score	Residual Level	Treatment
R-001	[Brief description]	[Category]	[Score]	[Level]	[Score]	[Level]	[Treatment]
R-002	[Brief description]						
[Add rows as needed]							

Risk Profile Statistics

Metric	Count
Total Risks Identified	[Number]
Critical Risks (Residual)	[Number]
High Risks (Residual)	[Number]
Medium Risks (Residual)	[Number]
Low Risks (Residual)	[Number]
Risks Requiring Additional Mitigation	[Number]

Section 6: Overall Assessment and Recommendations

6.1 Overall Risk Profile:

☐ Acceptable - Risks are well-managed
☐ Manageable - Acceptable with stated mitigations
☐ Concerning - Significant risks require attention
☐ Unacceptable - Critical risks make deployment inadvisable

6.2 Key Findings:

[Summarize main risk assessment findings]

_____

_____

_____

6.3 Critical Recommendations:
[List must-do recommendations before deployment]

_____

_____

6.4 Deployment Recommendation:
☐ Approve for deployment
☐ Approve with conditions
☐ Defer deployment pending risk mitigation
☐ Do not deploy

Section 7: Assessment Approval

Risk Assessment Lead:
Name: _____
Title: _____
Date: _____
Signature: _____

Reviewed By (Risk Manager/CISO):
Name: _____
Title: _____
Date: _____
Signature: _____

Approved By (AI Governance Board):
Name: _____
Title: _____
Date: _____
Signature: _____

END OF RISK ASSESSMENT WORKSHEET

Document Control Information:
Template Version: 1.0
Effective Date: [Date]
Next Review Date: [Date]
Owner: Risk Management/AI Governance Office

Template F.3
AI Governance Committee Charter

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This charter establishes the AI Governance Committee, defining its authority, responsibilities, composition, and operating procedures. The committee provides oversight and governance for AI systems throughout their lifecycle, ensuring alignment with organizational strategy, ethical principles, and regulatory requirements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-1.1 (Accountability structures), GOVERN-1.2 (Roles and responsibilities), GOVERN-1.3 (Governance processes)
- **ISO/IEC 42001:** Clause 5.1 (Leadership and commitment), Clause 5.3 (Organizational roles and responsibilities), Clause 9.3 (Management review)
- **ISO/IEC 27001:** Clause 5.1 (Leadership and commitment), Clause 5.3 (Organizational roles)

Instructions for Use

1. Customization:

- • Adapt sections to organizational structure and needs
- • Modify committee composition based on organization size
- • Adjust meeting frequency as appropriate

2. Approval Process:

- • Review draft charter with executive leadership
- • Obtain board or senior management approval
- • Communicate charter to all stakeholders

3. Implementation:

- • Appoint committee members formally
- • Schedule inaugural meeting
- • Establish supporting processes and documentation

4. Maintenance:

- • Review charter annually
- • Update as organizational needs evolve
- • Document all amendments with approval

AI GOVERNANCE COMMITTEE CHARTER

Section 1: Committee Establishment

1.1 Committee Name:
[Organization Name] AI Governance Committee

1.2 Effective Date:
[DD/MM/YYYY]

1.3 Authority:
This committee is established by [Board of Directors / Executive Leadership / CEO] and operates under the authority of [specify governing body]. The committee has the authority to:

- • Review and approve AI system development and deployment decisions
- • Establish AI policies, standards, and guidelines
- • Request information and reports from any organizational unit
- • Commission assessments, audits, or external reviews
- • Escalate critical issues to executive leadership or board
- • Make binding decisions within defined scope of authority

1.4 Reporting Relationship:
The committee reports to: [CEO / CTO / Board of Directors / Risk Committee]
Reporting frequency: [Quarterly / As needed / After each meeting]

Section 2: Committee Purpose and Objectives

2.1 Primary Purpose:
The AI Governance Committee provides oversight, guidance, and decision-making authority for all AI initiatives within the organization, ensuring responsible AI development and deployment aligned with organizational values, ethical principles, and regulatory requirements.

2.2 Key Objectives:
Strategic Alignment:

- • Ensure AI initiatives align with organizational strategy and objectives
- • Prioritize AI investments and resource allocation
- • Identify strategic AI opportunities and risks

Risk Management:

- • Oversee AI risk identification, assessment, and mitigation
- • Review and approve risk assessments for high-risk AI systems
- • Monitor emerging AI risks and trends

Compliance and Ethics:

- • Ensure compliance with AI regulations and standards
- • Uphold ethical AI principles and responsible practices
- • Review ethical considerations for AI applications

Operational Oversight:

- • Approve AI system deployments based on established criteria
- • Monitor AI system performance and incidents
- • Review AI Management System (AIMS) effectiveness

Stakeholder Engagement:

- • Facilitate communication between AI teams and leadership
- • Consider stakeholder interests and concerns
- • Promote transparency and accountability

Section 3: Committee Composition

3.1 Membership Structure:

Role	Position/Title	Name (if appointed)
Committee Chair	[CTO / Chief AI Officer / VP Technology]	[Name]
Executive Sponsor	[CEO / COO / Board Member]	[Name]
Technical Lead	[Head of AI/ML / Chief Data Scientist]	[Name]
Risk & Compliance Officer	[Chief Risk Officer / Compliance Director]	[Name]
Security Representative	[CISO / Security Director]	[Name]
Legal Counsel	[General Counsel / Legal Director]	[Name]
Privacy Officer	[DPO / Privacy Director]	[Name]
Ethics Representative	[Ethics Officer / Advisory role]	[Name]
Business Representative	[Business Unit Leader]	[Name]
External Advisor (Optional)	[Independent Expert / Academic]	[Name]

3.2 Member Qualifications:

Committee members should possess:

- • Relevant expertise in AI, technology, risk, compliance, or related fields
- • Senior-level decision-making authority
- • Understanding of organizational strategy and operations
- • Commitment to responsible and ethical AI practices
- • Ability to dedicate time to committee responsibilities

3.3 Terms of Service:

• Standard term: [2 years / 3 years / At leadership discretion]
• Term limits: [No limit / Maximum 2 consecutive terms]
• Renewal process: [Describe renewal/reappointment process]

3.4 Chair Responsibilities:

The Committee Chair shall:

- • Set meeting agendas in consultation with members
- • Preside over committee meetings
- • Serve as primary liaison to executive leadership
- • Ensure committee decisions are documented and communicated
- • Facilitate consensus-building and conflict resolution
- • Sign off on committee reports and recommendations

3.5 Member Appointment and Removal:

Appointment:

- • Members are appointed by [CEO / Board / Executive Committee]
- • Appointments are documented and communicated organization-wide

Removal:

- • Members may be removed for cause by appointing authority
- • Voluntary resignation with [30 / 60] days notice
- • Automatic removal upon change in qualifying position

Section 4: Roles and Responsibilities

4.1 Committee Responsibilities:

Strategy and Planning

- • Review and approve organizational AI strategy
- • Prioritize AI initiatives and allocate resources
- • Align AI investments with business objectives
- • Monitor AI industry trends and emerging technologies

Governance and Oversight

- • Establish and maintain AI governance framework
- • Define AI policies, standards, and procedures
- • Approve high-impact or high-risk AI system deployments
- • Review AI system performance metrics and KPIs
- • Monitor compliance with governance requirements

Risk Management

- • Review and approve risk assessments for AI systems
- • Establish risk appetite and tolerance levels for AI
- • Monitor risk mitigation effectiveness
- • Review significant incidents and corrective actions
- • Escalate critical risks to appropriate leadership

Ethics and Responsible AI

- • Define and uphold AI ethical principles
- • Review ethical implications of AI applications
- • Ensure fairness, transparency, and accountability
- • Address bias and discrimination concerns
- • Consider societal and stakeholder impacts

Compliance and Legal

- • Ensure compliance with AI regulations and standards
- • Monitor regulatory developments and assess impact
- • Review legal and liability considerations
- • Oversee audit and certification processes

Communication and Reporting

- • Report regularly to executive leadership/board
- • Communicate decisions to relevant stakeholders
- • Promote transparency in AI governance
- • Facilitate cross-functional collaboration

4.2 Individual Member Responsibilities:

Each committee member shall:

- • Attend meetings regularly and participate actively
- • Review materials in advance of meetings
- • Contribute expertise and perspective to discussions
- • Maintain confidentiality of sensitive information
- • Declare conflicts of interest promptly
- • Support implementation of committee decisions

- • Stay informed about AI developments and best practices

Section 5: Meeting Procedures

5.1 Meeting Frequency:
• Regular meetings: [Monthly / Quarterly / Bi-monthly]
• Special meetings: Called as needed by Chair or majority of members
• Annual strategic planning session: [Date/timeframe]

5.2 Meeting Format:
• Duration: [Typical duration, e.g., 2 hours]
• Location: [In-person / Hybrid / Virtual]
• Technology: [Video conferencing platform if applicable]

5.3 Quorum:
A quorum consists of [majority / two-thirds / specific number] of voting members. Decisions require quorum to be valid.

5.4 Voting and Decision-Making:
• Decision method: [Consensus preferred / Majority vote / Chair decides]
• Voting eligibility: [All members / Specific roles only]
• Tie-breaking: [Chair has deciding vote / Escalate to executive sponsor]
• Abstentions: Permitted when conflicts of interest exist

5.5 Meeting Agenda:
Standing agenda items:
1. 1. Call to order and attendance
2. 2. Approval of previous meeting minutes
3. 3. Review of action items from previous meeting
4. 4. New AI system deployment approvals
5. 5. Risk assessment reviews
6. 6. Incident reports and corrective actions
7. 7. Compliance and regulatory updates
8. 8. AI system performance metrics
9. 9. Policy and standard updates
10. 10. Other business
11. 11. Next meeting date and preliminary agenda

5.6 Meeting Materials:
• Agenda distributed: [3 / 5 / 7] business days before meeting
• Supporting materials provided in advance
• Materials marked with appropriate confidentiality level

5.7 Minutes and Documentation:
• Secretary/designated member records meeting minutes
• Minutes include: attendees, decisions, action items, votes
• Draft minutes circulated within [5 / 7] business days
• Approved minutes filed in [document management system]
• Retention period: [7 years / Per records retention policy]

5.8 Attendance Requirements:
• Members expected to attend [80% / 75%] of scheduled meetings
• Proxy voting: [Permitted / Not permitted]
• Delegation: Members may send designees with prior notice

Section 6: Decision-Making Authority

6.1 Approval Authority:
The committee has approval authority for:

Decision Type	Authority Level
High-risk AI system deployments	Committee approval required
AI policies and standards	Committee approval required
Significant AI investments (above threshold)	Committee recommends, executive approves
Risk treatment plans for critical/high risks	Committee approval required
AI strategy and roadmap	Committee recommends, board/exec approves
Medium/low risk AI deployments	Delegated to AI teams with reporting
Emergency responses to critical incidents	Chair authority with committee ratification

6.2 Escalation Criteria:
The committee shall escalate to executive leadership/board:
- • Critical AI risks with potential for severe harm
- • Significant regulatory compliance issues
- • Major ethical concerns or controversies
- • Resource allocation conflicts beyond committee authority
- • Strategic decisions requiring board/executive input

6.3 Delegation:
The committee may delegate authority for routine decisions to:
- • AI project teams (for low-risk systems)
- • Committee subcommittees (for specialized topics)
- • Committee chair (for time-sensitive matters)

All delegated decisions shall be reported to the committee.

Section 7: Subcommittees and Working Groups

7.1 Subcommittee Formation:
The committee may establish subcommittees or working groups for:

- • Deep-dive analysis of specific topics
- • Development of policies or standards
- • Investigation of incidents or issues
- • Ongoing monitoring of specialized areas

7.2 Example Subcommittees:
• Technical Review Subcommittee: Evaluates technical aspects of AI systems
• Ethics Review Board: Examines ethical implications
• Risk Assessment Working Group: Conducts detailed risk analyses
• Incident Response Team: Manages AI system incidents

7.3 Subcommittee Operations:
• Charter: Each subcommittee operates under defined charter
• Leadership: Chaired by committee member or designee
• Membership: May include non-committee subject matter experts
• Reporting: Regular reports to main committee
• Authority: Recommend to main committee; limited independent authority

Section 8: Reporting and Communication

8.1 Regular Reporting:

Report Type	Audience	Frequency	Content
Executive Summary	CEO/Executive Team	Quarterly	Key decisions, risks, initiatives
Board Report	Board of Directors	Annually or as requested	Strategic overview, major risks
Operational Report	AI Teams	After each meeting	Decisions affecting operations
Annual Report	Organization-wide	Annually	Comprehensive governance review

8.2 Communication Channels:
• Committee portal: [Document repository location]
• Email distribution list: [governance-committee@organization]
• Stakeholder notifications: [Process for communicating decisions]
• Public communications: [Approach to external transparency]

8.3 Confidentiality:
• Committee deliberations are confidential
• Decisions and rationale are documented for transparency
• Sensitive information protected according to classification
• Public communications approved by Chair and [Communications/Legal]

Section 9: Performance and Effectiveness

9.1 Committee Performance Metrics:

Metric	Target
Meeting attendance rate	>80%
Decision turnaround time	[Target timeframe]
Action item completion rate	>90% on time
AI incidents requiring escalation	[Track and review]
Stakeholder satisfaction	[Survey score target]
Regulatory compliance rate	100%

9.2 Annual Self-Assessment:
The committee shall conduct an annual self-assessment evaluating:

- • Achievement of committee objectives
- • Effectiveness of governance processes
- • Quality of decision-making
- • Committee composition and expertise
- • Meeting efficiency and participation
- • Stakeholder feedback and satisfaction

9.3 Continuous Improvement:
Based on assessment results, the committee shall:

- • Identify areas for improvement
- • Develop and implement action plans
- • Update charter and processes as needed
- • Enhance training and development for members

Section 10: Resources and Support

10.1 Administrative Support:
The committee is supported by:

- • Secretary/Coordinator: [Role/person responsible]
- • Meeting logistics and scheduling
- • Document management and distribution
- • Minutes preparation and archiving

10.2 Budget and Resources:
• Annual budget allocation: [Amount or process]
• External advisor fees: [If applicable]
• Training and development funds: [If applicable]
• Technology and tools: [Collaboration platforms, document systems]

10.3 Access to Information:
Committee members have access to:

- • All AI system documentation and records
- • Risk assessments and audit reports
- • Incident reports and investigations
- • Performance metrics and dashboards
- • Legal and regulatory guidance

10.4 Training and Development:
Committee members receive:

- • Onboarding for new members
- • Regular updates on AI regulations and standards
- • Training on emerging AI risks and best practices
- • Access to relevant conferences and workshops

Section 11: Charter Review and Amendment

11.1 Review Schedule:
This charter shall be reviewed:

- • Annually as part of committee self-assessment
- • Following significant organizational changes
- • When new regulations or standards are introduced
- • Upon request of committee Chair or majority of members

11.2 Amendment Process:

1. 1. Proposed amendments submitted to Committee Chair
2. 2. Review and discussion by committee members
3. 3. Approval by [majority / two-thirds] vote of committee
4. 4. Final approval by [CEO / Board / Executive Committee]
5. 5. Updated charter distributed to stakeholders

11.3 Version Control:

• All charter versions maintained in document repository
• Amendment history tracked and documented
• Previous versions archived for reference

Section 12: Charter Approval

12.1 Approval Signatures:

Committee Chair:
Name: _____
Title: _____
Date: _____
Signature: _____

Executive Sponsor:
Name: _____
Title: _____
Date: _____
Signature: _____

Final Approval (CEO/Board Chair):
Name: _____
Title: _____
Date: _____
Signature: _____

END OF AI GOVERNANCE COMMITTEE CHARTER

Document Control Information:
Charter Version: 1.0
Effective Date: [Date]
Next Review Date: [Date]
Document Owner: [Committee Chair / AI Governance Office]
Distribution: Executive Leadership, Committee Members, AI Teams

Template F.4
AI Policy Template

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a standardized structure for creating AI-related policies. It ensures consistency across all AI governance policies and compliance with framework requirements for documented policy statements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-1.3 (Policies and procedures), GOVERN-2.1 (Transparency), GOVERN-5.1 (Organizational culture)
- **ISO/IEC 42001:** Clause 5.2 (AI management system policy), Clause 7.5 (Documented information), Clause 8.1 (Operational planning and control)
- **ISO/IEC 27001:** Clause 5.2 (Information security policy), Clause 7.5 (Documented information)

Instructions for Use

1. Policy Development Process:

- • Identify policy need based on governance requirements or risk assessment
- • Assign policy owner with appropriate authority
- • Engage stakeholders from affected departments
- • Draft policy using this template structure
- • Review with legal, compliance, and risk teams

2. Required Sections:

- • All numbered sections (1-10) are required for every policy
- • Subsections may be tailored to policy subject matter
- • Additional sections may be added as needed
- • Appendices may be used for supporting content

3. Approval and Distribution:

- • Obtain required approvals per organizational process
- • Publish in central policy repository
- • Communicate to all affected personnel
- • Provide training on policy requirements

4. Policy Maintenance:

- • Review policy at scheduled intervals (typically annually)
- • Update when regulations, technology, or risks change
- • Track compliance and effectiveness metrics
- • Retire or consolidate outdated policies

[POLICY TITLE]

[Organization Name]

Policy Number:	**[e.g., AI-POL-001]**
Version:	[e.g., 1.0]
Effective Date:	[DD/MM/YYYY]
Last Review Date:	[DD/MM/YYYY]
Next Review Date:	[DD/MM/YYYY]
Policy Owner:	[Title/Department]
Approved By:	[Title]
Classification:	[Public / Internal / Confidential]

1. Purpose

[Clearly state the purpose of this policy. Explain why it exists and what it aims to achieve.]

Example:

> The purpose of this policy is to [primary objective]. This policy establishes [what it establishes] and ensures [what it ensures]. By implementing this policy, [Organization Name] seeks to [desired outcomes].

2. Scope

[Define the scope of this policy - what and who it covers.]

2.1 Applicability:

[Specify what this policy applies to]

This policy applies to:

- • [Organizational units, departments, or functions]
- • [Types of AI systems or activities covered]
- • [Specific processes or operations]
- • [Geographic locations if applicable]

2.2 Covered Personnel:

[Specify who must comply with this policy]

This policy applies to:

- • All employees (full-time, part-time, temporary)

- • Contractors and consultants
- • Third-party vendors and service providers
- • [Other stakeholders as applicable]

2.3 Exclusions:
[Specify any explicit exclusions or exceptions]

This policy does not apply to:
- • [Specific exclusions]
- • [Systems or processes excluded]

3. Definitions

[Define key terms used in this policy to ensure common understanding]

Term	Definition
[Term 1]	[Definition]
[Term 2]	[Definition]
[Term 3]	[Definition]
[Term 4]	[Definition]
[Add rows as needed]	

Common AI Terms (include as relevant):
- • Artificial Intelligence (AI): [Organization-specific definition]
- • Machine Learning (ML): [Definition]
- • High-Risk AI System: [Definition based on risk framework]
- • AI System Owner: [Definition]
- • Model Bias: [Definition]

4. Policy Statement

[This is the core of the policy - state the policy requirements clearly and concisely]

4.1 General Principles:
[State overarching principles that guide this policy]

[Organization Name] is committed to:
- • [Principle 1]
- • [Principle 2]
- • [Principle 3]

- • [Principle 4]

4.2 Requirements:
[State specific, actionable requirements. Use "must," "shall," or "will" for mandatory requirements]

[Requirement Category 1]

- • [Organization/personnel] must [specific requirement]
- • [Organization/personnel] shall [specific requirement]
- • [Organization/personnel] will [specific requirement]

[Requirement Category 2]

- • [Specific requirement]
- • [Specific requirement]
- • [Specific requirement]

[Requirement Category 3]

- • [Specific requirement]
- • [Specific requirement]

4.3 Prohibited Actions:
[Explicitly state what is not allowed]

The following actions are prohibited:
- • [Prohibited action 1]
- • [Prohibited action 2]
- • [Prohibited action 3]

5. Roles and Responsibilities

[Define who is responsible for what under this policy]

Role	Responsibilities
Policy Owner	• Maintain and update policy • Ensure policy compliance • Report to governance committee • [Add specific responsibilities]
[Executive Leadership/Board]	• Approve policy and major revisions • Provide resources for implementation • Oversee policy effectiveness • [Add specific responsibilities]
[AI Governance Committee]	• Review and recommend policy updates • Monitor compliance metrics • Address policy violations • [Add specific responsibilities]
[AI System Owners]	• Implement policy requirements for their systems • Report compliance status • Address non-compliance issues • [Add specific responsibilities]
[All Employees]	• Comply with policy requirements • Report policy violations • Complete required training • [Add specific responsibilities]
[Compliance/Risk Function]	• Monitor policy compliance • Conduct audits and assessments • Investigate violations • [Add specific responsibilities]

6. Procedures and Implementation

[Describe how the policy will be implemented and any supporting procedures]

6.1 Implementation Approach:
[Describe the approach for implementing this policy]

This policy will be implemented through:

- • [Implementation step 1]
- • [Implementation step 2]
- • [Implementation step 3]

6.2 Supporting Procedures:
[Reference supporting procedures, standards, or guidelines]

This policy is supported by the following procedures:

- • [Procedure name and reference number]
- • [Procedure name and reference number]
- • [Procedure name and reference number]

6.3 Training Requirements:
[Specify training requirements for policy compliance]

• All personnel covered by this policy must complete [training name] within [timeframe]
• Refresher training required [frequency]
• New employees must complete training within [timeframe] of hire/assignment
• Training records maintained for [retention period]

6.4 Documentation Requirements:
[Specify what documentation must be maintained]

The following documentation must be maintained:

- • [Document type 1] - Retained for [period]
- • [Document type 2] - Retained for [period]
- • [Document type 3] - Retained for [period]

7. Compliance and Monitoring

[Describe how compliance with this policy will be monitored and measured]

7.1 Compliance Monitoring:

[Describe monitoring approach]

Compliance with this policy will be monitored through:

- • Regular audits conducted [frequency]
- • Automated compliance checks where applicable
- • Self-assessments by [responsible parties] [frequency]
- • Review of compliance metrics and KPIs
- • Incident and violation reporting

7.2 Key Performance Indicators:

[Define metrics for measuring policy effectiveness]

KPI	Target	Measurement Frequency
[KPI 1]	[Target value/threshold]	[Monthly/Quarterly/Annually]
[KPI 2]	[Target value/threshold]	[Monthly/Quarterly/Annually]
[KPI 3]	[Target value/threshold]	[Monthly/Quarterly/Annually]
[Add rows as needed]		

7.3 Reporting:

[Describe reporting requirements]

• Compliance status reported to [governance body] [frequency]
• Significant non-compliance issues escalated immediately
• Annual compliance report prepared by [responsible party]
• Audit findings reviewed and action plans developed

8. Non-Compliance and Enforcement

[Describe consequences of policy violations and enforcement mechanisms]

8.1 Policy Violations:
[Define what constitutes a policy violation]

Policy violations include but are not limited to:
- • Failure to comply with mandatory requirements
- • Engaging in prohibited actions
- • Circumventing policy controls or safeguards
- • Falsifying compliance documentation
- • Failing to report known violations

8.2 Reporting Violations:
[Describe how to report policy violations]

• Policy violations must be reported immediately to [reporting channel]
• Violations can be reported through:
- - Direct supervisor or manager
- - Compliance hotline: [phone number]
- - Email: [compliance email]
- - Anonymous reporting system: [details]

• No retaliation against good faith reporters

8.3 Consequences:
[Describe potential consequences of violations]

Violations of this policy may result in:
- • Verbal or written warning
- • Mandatory retraining
- • Performance improvement plan
- • Suspension of system access or privileges
- • Disciplinary action up to and including termination
- • Legal action if applicable

8.4 Investigation Process:
[Describe how violations will be investigated]

17. 1. Violation reported to [designated authority]
18. 2. Preliminary assessment conducted within [timeframe]
19. 3. Formal investigation initiated if warranted
20. 4. Findings documented and reported
21. 5. Corrective actions implemented
22. 6. Follow-up to ensure compliance

9. Policy Review and Revision

[Describe the policy review and update process]

9.1 Review Schedule:
This policy will be reviewed:

- • Annually by [policy owner] on [month/quarter]
- • Following significant organizational changes
- • When new regulations or standards are introduced
- • After major incidents or compliance issues
- • Upon request of [governance committee/executive leadership]

9.2 Review Process:
Policy reviews will include:

- • Assessment of policy effectiveness and compliance
- • Review of regulatory and standard changes
- • Stakeholder feedback collection
- • Benchmarking against industry best practices
- • Identification of needed updates or improvements

9.3 Revision Process:
Policy revisions follow this process:

23. 1. Policy owner initiates revision based on review findings
24. 2. Draft revisions prepared and stakeholders consulted
25. 3. Legal and compliance review conducted
26. 4. Revisions submitted to [governance committee] for approval
27. 5. Final approval obtained from [executive sponsor/board]
28. 6. Updated policy communicated to all affected parties
29. 7. Version control and change history maintained

9.4 Version Control:
• All policy versions maintained in [document repository]
• Version numbering: [Major.Minor format - e.g., 2.1]
• Change history documented in policy revision log
• Previous versions archived and retained per records policy

10. References and Related Documents

[List related policies, procedures, standards, and external references]

10.1 Related Policies:
- • [Policy Name] - [Policy Number]
- • [Policy Name] - [Policy Number]
- • [Policy Name] - [Policy Number]

10.2 Supporting Procedures and Standards:
- • [Procedure/Standard Name] - [Document Number]
- • [Procedure/Standard Name] - [Document Number]
- • [Procedure/Standard Name] - [Document Number]

10.3 Regulatory and Framework References:
- • NIST AI Risk Management Framework (AI RMF 2026)
- • ISO/IEC 42001:2023 - Artificial Intelligence Management System
- • ISO/IEC 27001:2022 - Information Security Management
- • [Applicable regulations - e.g., EU AI Act, GDPR, etc.]
- • [Industry-specific standards]

10.4 Additional Resources:
- • [Guidance documents]
- • [Training materials]
- • [Tools and templates]

11. Policy Approval

[Document formal approval of this policy]

Role	Name	Signature	Date
Policy Owner	[Name, Title]	_____	_____
Legal Review	[Name, Title]	_____	_____
Compliance Review	[Name, Title]	_____	_____
Governance Committee	[Chair Name, Title]	_____	_____
Executive Approval	[Name, Title]	_____	_____

12. Revision History

[Maintain a log of all policy revisions]

Version	Date	Author	Description of Changes	Approved By
1.0	[Date]	[Name]	Initial policy creation	[Name]
[Version]	[Date]	[Name]	[Description of changes]	[Name]
[Add rows for each revision]				

END OF POLICY

Note to Policy Developers:
• Remove all bracketed instructional text [like this] before finalizing
• Remove example content and replace with actual policy content
• Ensure all sections are complete and accurate
• Obtain all required approvals before publication
• File approved policy in central repository

Template Information:
Template Version: 1.0
Template Owner: AI Governance Office
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001

Template F.5
AI Procedure Template

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a standardized structure for creating AI-related procedures. Procedures translate policy requirements into step-by-step instructions for implementation, ensuring consistency and compliance with framework requirements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-1.3 (Procedures), MAP-4.1 (Operational procedures), MANAGE-3.1 (Process documentation)
- **ISO/IEC 42001:** Clause 7.5 (Documented information), Clause 8.1 (Operational planning and control), Clause 9.1 (Monitoring and measurement)
- **ISO/IEC 27001:** Clause 7.5 (Documented information), Clause 8.1 (Operational planning and control)

Instructions for Use

1. When to Create a Procedure:

- • To implement policy requirements
- • When process consistency is critical
- • For complex, multi-step processes
- • To ensure compliance with standards
- • When training or cross-functional coordination is needed

2. Procedure Development:

- • Map the current process (as-is state)
- • Identify improvements and standardization opportunities
- • Engage process owners and subject matter experts
- • Document step-by-step instructions clearly
- • Include decision points, inputs, outputs, and roles
- • Test procedure with actual users before finalizing

3. Writing Best Practices:

- • Use active voice and imperative mood (e.g., "Submit the form")
- • Number steps sequentially
- • Include only one action per step when possible

- • Add decision points as separate steps
- • Reference supporting documents and tools
- • Include visual aids (flowcharts, screenshots) when helpful

4. Maintenance:

- • Review procedures when policies change
- • Update when process improvements are identified
- • Solicit feedback from users regularly
- • Keep procedures current with system/tool updates

[PROCEDURE TITLE]

[Organization Name]

Procedure Number:	**[e.g., AI-PROC-001]**
Version:	[e.g., 1.0]
Effective Date:	[DD/MM/YYYY]
Last Review Date:	[DD/MM/YYYY]
Next Review Date:	[DD/MM/YYYY]
Process Owner:	[Title/Department]
Procedure Author:	[Name, Title]
Approved By:	[Title]
Related Policy:	[Policy Name and Number]

1. Purpose

[State the purpose of this procedure - what it accomplishes and why it exists]

Example:

This procedure defines the step-by-step process for [process name]. It ensures that [objectives achieved] in compliance with [relevant policy/standard]. Following this procedure will [benefits/outcomes].

2. Scope

[Define when and where this procedure applies]

2.1 Applicability:

This procedure applies to:

- • [Specific processes, systems, or activities]
- • [Organizational units or departments]
- • [Types of AI systems or projects]
- • [Geographic locations if applicable]

2.2 When to Use This Procedure:

Follow this procedure when:

- • [Trigger condition 1]
- • [Trigger condition 2]
- • [Trigger condition 3]

2.3 Exclusions:

This procedure does not apply to:

- • [Specific exclusions]
- • [Exceptions - reference alternate procedures]

3. Definitions and Acronyms

[Define technical terms, abbreviations, and acronyms used in this procedure]

Term/Acronym	Definition
[Term 1]	[Definition]
[Term 2]	[Definition]
[Acronym 1]	[Full name and explanation]
[Acronym 2]	[Full name and explanation]
[Add rows as needed]	

4. Roles and Responsibilities

[Define who does what in this procedure]

Activity/Task	Responsible	Accountable	Consulted	Informed
[Activity 1]	[Role]	[Role]	[Role(s)]	[Role(s)]
[Activity 2]	[Role]	[Role]	[Role(s)]	[Role(s)]
[Activity 3]	[Role]	[Role]	[Role(s)]	[Role(s)]
[Activity 4]	[Role]	[Role]	[Role(s)]	[Role(s)]
[Add rows as needed]				

RACI Key:

- • Responsible: Performs the work
- • Accountable: Ultimately answerable for completion
- • Consulted: Provides input and expertise
- • Informed: Kept updated on progress

5. Prerequisites and Requirements

[Identify what must be in place before starting this procedure]

5.1 Required Permissions/Access:

- • [System access or permission level required]
- • [Authorization or approval needed]
- • [Security clearance or credentials]

5.2 Required Training:

- • [Training course or certification required]
- • [Minimum experience level]

5.3 Required Tools and Systems:

- • [Software/application name and version]
- • [Equipment or hardware]
- • [Access to specific environments]

5.4 Required Documents/Information:

- • [Document name and location]
- • [Data or information needed]
- • [Forms or templates required]

5.5 Prerequisites:

Before beginning this procedure:

- • [Prerequisite condition or task 1]
- • [Prerequisite condition or task 2]
- • [Prerequisite condition or task 3]

6. Procedure Steps

[Provide detailed, sequential steps to complete the process]

Note: Steps are numbered sequentially. Sub-steps are lettered (a, b, c). Decision points are clearly marked.

[Phase 1 Name - e.g., Initiation]

Phase 2 Name - e.g., Execution]

30. 5. [Action]
31. 6. [Action]

Note: [Important information or caution]
32. 7. [Action involving system/tool]

a. Navigate to [location/screen]
b. Select [option/button]
c. Enter [required information]:
• Field 1: [Instructions]
• Field 2: [Instructions]
d. Click [Submit/Save/Confirm]
33. 8. [DECISION POINT] Is [validation check] successful?

- If YES: Proceed to Step 9
- If NO: [Error handling procedure]

[Phase 3 Name - e.g., Review and Approval]

34. 9. [Action]
35. 10. [Action]

[Phase 4 Name - e.g., Closure]

36. 11. [Action]
37. 12. [Final action]
38. 13. Document completion in [tracking system/log]

a. Record [information]
b. Update status to [final status]
c. Notify [stakeholders]

End of Procedure

7. Process Flowchart

[Include a visual flowchart of the procedure]

[INSERT FLOWCHART HERE]

Flowchart symbols:

- • Oval: Start/End
- • Rectangle: Process step/action
- • Diamond: Decision point
- • Arrow: Flow direction
- • Parallelogram: Input/Output

Note: Flowchart should align with steps in Section 6. Use flowcharting software (e.g., Visio, Lucidchart, Draw.io) and insert as image.

8. Forms, Templates, and Tools

[List and describe supporting materials needed for this procedure]

Item	Type	Location/Link	Used in Step
[Form/Template name]	Form	[File path or URL]	Step [#]
[System/Tool name]	System	[URL or access instructions]	Step [#]
[Checklist/Template]	Template	[File path or URL]	Step [#]
[Add rows as needed]			

9. Quality Controls and Checkpoints

[Define quality checks and validation points throughout the procedure]

Checkpoint	Location (Step)	What to Verify	Acceptance Criteria
[Checkpoint 1]	Step [#]	[What to check]	[Pass/fail criteria]
[Checkpoint 2]	Step [#]	[What to check]	[Pass/fail criteria]
[Checkpoint 3]	Step [#]	[What to check]	[Pass/fail criteria]
[Add rows as needed]			

Quality Assurance:

- • All checkpoints must pass before proceeding to next phase
- • Failed checkpoints require [corrective action process]
- • Quality records maintained in [location]

10. Exception Handling and Troubleshooting

[Address common issues and how to resolve them]

10.1 Common Issues and Resolutions:

Issue/Error	Possible Cause	Resolution
[Issue description]	[Why it occurs]	[How to fix]
[Issue description]	[Why it occurs]	[How to fix]
[Issue description]	[Why it occurs]	[How to fix]
[Add rows as needed]		

10.2 Exception Approval Process:

[Describe how to request and obtain approval for exceptions to this procedure]

Exceptions to this procedure require:

39. 1. Documentation of exception reason and justification
40. 2. Risk assessment of proceeding with exception
41. 3. Approval from [approving authority]
42. 4. Exception logged in [tracking system]

10.3 Escalation:

If issues cannot be resolved using this procedure:

- • Level 1: Contact [first-line support/supervisor]
- • Level 2: Escalate to [process owner/manager]
- • Level 3: Escalate to [department head/governance committee]

Emergency contact: [Name, Title, Phone, Email]

11. Records and Documentation

[Specify what records must be created and retained]

Record Type	Created in Step	Storage Location	Retention Period	Responsible Party
[Record name]	Step [#]	[System/location]	[Duration]	[Role]
[Record name]	Step [#]	[System/location]	[Duration]	[Role]
[Record name]	Step [#]	[System/location]	[Duration]	[Role]
[Add rows as needed]				

Records Management:

- • All records must be stored in designated locations
- • Records must be protected according to data classification
- • Access to records controlled based on need-to-know
- • Records subject to audit and compliance reviews

12. Performance Metrics

[Define how procedure effectiveness and efficiency will be measured]

Metric	Target/Threshold	Measurement Method	Frequency
Cycle time (end-to-end)	[Target duration]	[How measured]	[Monthly/Quarterly]
Error/rework rate	[% target]	[How measured]	[Monthly/Quarterly]
Compliance rate	[% target]	[How measured]	[Monthly/Quarterly]
[Add metrics as needed]			

Continuous Improvement:

- • Metrics reviewed [frequency] by [responsible party]
- • Trends analyzed to identify improvement opportunities
- • Procedure updated based on lessons learned
- • User feedback solicited and incorporated

13. Related Documents

[Reference related policies, procedures, and supporting documents]

13.1 Related Policies:

- • [Policy Name] - [Policy Number]
- • [Policy Name] - [Policy Number]

13.2 Related Procedures:

- • [Procedure Name] - [Procedure Number]
- • [Procedure Name] - [Procedure Number]

13.3 Standards and Guidelines:

- • [Standard Name] - [Reference]
- • [Guideline Name] - [Reference]

13.4 External References:

- • AI RMF 2026 - [Specific sections]
- • ISO/IEC 42001:2023 - [Specific clauses]
- • ISO/IEC 27001:2022 - [Specific clauses]
- • [Other relevant standards or regulations]

14. Approval and Review

14.1 Procedure Approval:

Role	Name/Title	Signature	Date
Procedure Author	[Name, Title]	_____	_____
SME Review	[Name, Title]	_____	_____
Process Owner	[Name, Title]	_____	_____
Final Approval	[Name, Title]	_____	_____

14.2 Review Schedule:

- • Scheduled review: [Annually / Bi-annually]
- • Triggered review: Upon process changes, system updates, policy changes
- • Review responsibility: [Process Owner]

14.3 Revision History:

Version	Date	Author	Description of Changes	Approved By
1.0	[Date]	[Name]	Initial procedure creation	[Name]
[Version]	[Date]	[Name]	[Changes]	[Name]
[Add rows for each revision]				

END OF PROCEDURE

Note to Procedure Developers:
• Remove all bracketed instructional text [like this] before finalizing
• Test procedure with actual users before final approval
• Include actual screenshots or flowcharts where indicated
• Ensure all steps are clear, accurate, and complete
• Obtain all required approvals before publication

Template Information:
Template Version: 1.0
Template Owner: AI Governance Office / Process Management
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001

Template F.6
AI Training and Competency Record

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive system for documenting personnel training, competencies, and qualifications related to AI systems. It ensures that individuals working with AI have the necessary knowledge, skills, and competencies to perform their roles effectively and in compliance with framework requirements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-1.2 (Workforce diversity and expertise), GOVERN-5.1 (Organizational culture and competence), MANAGE-1.2 (Personnel competency)
- **ISO/IEC 42001:** Clause 7.2 (Competence), Clause 7.3 (Awareness), Clause 7.5 (Documented information)
- **ISO/IEC 27001:** Clause 7.2 (Competence), Clause 7.3 (Awareness), Annex A.6.3 (Information security awareness)

Instructions for Use

1. Record Maintenance:

- • Maintain one training record per individual
- • Update records immediately upon training completion
- • Review records during performance evaluations
- • Store securely with restricted access

2. Competency Assessment:

- • Assess competencies before assigning AI-related responsibilities
- • Identify gaps and required training
- • Document assessment results and action plans
- • Re-assess periodically or when roles change

3. Training Tracking:

- • Record all AI-related training completions
- • Track mandatory vs. optional training
- • Monitor training currency and renewal dates
- • Generate reports for compliance verification

4. Privacy and Confidentiality:

- • Training records are confidential personnel information
- • Access limited to HR, supervisors, and authorized personnel
- • Comply with applicable privacy laws and regulations

AI TRAINING AND COMPETENCY RECORD

Section 1: Individual Information

Employee ID:	_____
Full Name:	_____
Job Title:	_____
Department:	_____
Supervisor:	_____
Start Date (Current Role):	_____
Email:	_____
Phone:	_____
Record Created:	_____
Last Updated:	_____

Section 2: AI-Related Role and Responsibilities

2.1 Primary AI Role:

☐ AI System Developer
☐ Data Scientist/ML Engineer
☐ AI Product Manager
☐ AI System Owner/Operator
☐ AI Governance/Compliance
☐ AI Risk/Security Specialist
☐ AI Ethics/Fairness Specialist
☐ Data Engineer/Data Steward
☐ AI Quality Assurance/Testing
☐ Executive/Leadership (AI oversight)
☐ Other: _____

2.2 Key AI-Related Responsibilities:

[Describe specific AI-related duties and responsibilities]

_____
_____
_____
_____

2.3 AI Systems/Projects Involved:
[List AI systems or projects this individual works with]

_____
_____
_____

Section 3: Required Competencies

The following competencies are required for this role. Rate current proficiency level and identify gaps.

Proficiency Rating Scale:

- 1 = None - No knowledge or skill
- 2 = Basic - Fundamental knowledge, requires supervision
- 3 = Intermediate - Solid understanding, works independently
- 4 = Advanced - Expert level, can train others
- 5 = Master - Industry-recognized expertise

3.1 Technical Competencies

Competency	Required Level	Current Level	Gap/Notes
AI/ML Fundamentals	[1-5]	[1-5]	
Programming (Python, R, etc.)	[1-5]	[1-5]	
Machine Learning Algorithms	[1-5]	[1-5]	
Deep Learning/Neural Networks	[1-5]	[1-5]	
Data Engineering/Processing	[1-5]	[1-5]	
Model Development & Training	[1-5]	[1-5]	
Model Validation & Testing	[1-5]	[1-5]	
MLOps/Model Deployment	[1-5]	[1-5]	
AI Security & Privacy	[1-5]	[1-5]	
[Add role-specific competencies]			

3.2 AI Governance and Compliance Competencies

Competency	Required Level	Current Level	Gap/Notes
AI Risk Management	[1-5]	[1-5]	
AI Regulations & Standards	[1-5]	[1-5]	
AI Ethics & Responsible AI	[1-5]	[1-5]	
Bias Detection & Mitigation	[1-5]	[1-5]	
AI Transparency & Explainability	[1-5]	[1-5]	
Data Governance & Privacy	[1-5]	[1-5]	
Documentation & Record-keeping	[1-5]	[1-5]	
[Add role-specific competencies]			

3.3 Business and Soft Skills Competencies

Competency	Required Level	Current Level	Gap/Notes
AI Business Strategy	[1-5]	[1-5]	
Stakeholder Communication	[1-5]	[1-5]	
Cross-functional Collaboration	[1-5]	[1-5]	
Problem-Solving & Critical Thinking	[1-5]	[1-5]	
Project Management	[1-5]	[1-5]	
Change Management	[1-5]	[1-5]	
[Add role-specific competencies]			

3.4 Competency Assessment Summary:

Overall Competency Status: ☐ Meets Requirements ☐ Gaps Identified ☐ Below Requirements

Critical Gaps Requiring Immediate Attention:

_____
_____
_____

Development Plan Summary:

_____
_____
_____

Section 4: Mandatory Training Requirements

The following training courses are mandatory for this role.

Training Course	Required By	Completion Date	Score/Result	Valid Until	Status
AI Fundamentals	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
AI Ethics & Responsible AI	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
AI Risk Management	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
Data Privacy & Security	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
Bias & Fairness in AI	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
AI Governance & Compliance	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
AI Documentation Standards	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
Incident Reporting Procedures	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
[Role-Specific Training]	[Policy/Standard]	[Date]	[Score/%]	[Date/N/A]	☐Complete ☐Pending
[Add rows as needed]					

Mandatory Training Compliance Status:
All Mandatory Training Complete: ☐ Yes ☐ No
If No, Outstanding Requirements:

_____
_____

Section 5: Additional Training and Development

Optional, recommended, and completed additional training.

Training/Course Title	Provider/Source	Completion Date	Duration/Credits	Certificate/Credential
[Course name]	[Provider]	[Date]	[Hours/Credits]	[Yes/No - File location]
[Course name]	[Provider]	[Date]	[Hours/Credits]	[Yes/No - File location]
[Course name]	[Provider]	[Date]	[Hours/Credits]	[Yes/No - File location]
[Course name]	[Provider]	[Date]	[Hours/Credits]	[Yes/No - File location]
[Conference/Workshop]	[Event name]	[Date]	[Duration]	[Certificate if applicable]
[Webinar/Online Course]	[Provider]	[Date]	[Duration]	[Certificate if applicable]
[Add rows as needed]				

Section 6: Professional Certifications

Relevant professional certifications and credentials.

Certification Name	Issuing Organization	Date Obtained	Expiration Date	Certificate Number
[e.g., AWS Certified ML]	[Organization]	[Date]	[Date/No expiry]	[Number]
[e.g., TensorFlow Developer]	[Organization]	[Date]	[Date/No expiry]	[Number]
[e.g., CRISP-ML(Q)]	[Organization]	[Date]	[Date/No expiry]	[Number]
[e.g., ISO 42001 Lead Auditor]	[Organization]	[Date]	[Date/No expiry]	[Number]
[Other certification]	[Organization]	[Date]	[Date/No expiry]	[Number]
[Add rows as needed]				

Section 7: Education and Academic Qualifications

Degree/Qualification	Field of Study	Institution	Year Completed	Relevant Coursework
[e.g., M.S.]	[e.g., Computer Science]	[University name]	[Year]	[Key courses]
[e.g., B.S.]	[Major]	[University name]	[Year]	[Key courses]
[Additional degree/diploma]	[Field]	[Institution]	[Year]	[Relevant coursework]
[Add rows as needed]				

Section 8: Work Experience and Projects

Relevant AI-related work experience and projects.

Project/Role	Organization/Client	Duration	Key Responsibilities/Achievements
[Project name or previous role]	[Organization]	[Start-End dates]	[Brief description]
[Project/Role]	[Organization]	[Duration]	[Description]
[Project/Role]	[Organization]	[Duration]	[Description]
[Add rows as needed]			

Total Years of AI-Related Experience:

_____

Section 9: Training Plan and Development Goals

9.1 Individual Development Plan (IDP):

Development Goal	Action/Training Needed	Target Date	Status	Completion Date
[Competency to develop]	[Training course or activity]	[Date]	☐Not Started ☐In Progress ☐Complete	[Date]
[Goal]	[Action]	[Date]	☐Not Started ☐In Progress ☐Complete	[Date]
[Goal]	[Action]	[Date]	☐Not Started ☐In Progress ☐Complete	[Date]
[Goal]	[Action]	[Date]	☐Not Started ☐In Progress ☐Complete	[Date]
[Add rows as needed]				

9.2 Annual Training Budget Allocated:

$_____

9.3 Career Development Path:

[Describe potential career progression and required competencies]

_____

_____

_____

Section 10: Compliance and Attestations

10.1 Acknowledgment of Training Requirements:

I acknowledge that I have been informed of the training requirements for my role and understand my responsibility to complete all mandatory training.

Employee Signature: _____ Date: _____

10.2 Code of Ethics/Conduct Attestation:

I confirm that I have read, understood, and agree to comply with:
☐ AI Ethics Policy
☐ Responsible AI Guidelines
☐ Code of Conduct for AI Development
☐ Data Privacy and Security Policies

Employee Signature: _____ Date: _____

10.3 Supervisor Review and Approval:

I have reviewed this training and competency record and confirm:
☐ Employee meets all mandatory training requirements
☐ Competency gaps identified and development plan in place
☐ Employee is qualified for current AI-related responsibilities

Supervisor Name: _____
Supervisor Signature: _____ Date: _____

Section 11: Record Maintenance and Review

11.1 Review History:

Review Date	Reviewer	Changes/Updates Made	Next Review Due
[Date]	[Name]	[Description of changes]	[Date]
[Date]	[Name]	[Description]	[Date]
[Date]	[Name]	[Description]	[Date]
[Add rows for each review]			

11.2 Record Retention:

• Retention Period: [Per HR policy - typically 7 years after employment ends]
• Storage Location: [HR Information System / Document Repository]
• Access: Restricted to HR, employee, and direct supervisor

11.3 Record Disposal:

Upon reaching end of retention period:
• Records shall be securely destroyed per data retention policy
• Disposal shall be documented in destruction log
• Certificate of destruction maintained

END OF TRAINING AND COMPETENCY RECORD

Document Control:
Template Version: 1.0
Owner: Human Resources / AI Governance Office
Classification: Confidential - Personnel Record
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001

Template F.7
AI Audit and Assessment Report Template

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a standardized structure for documenting internal and external audits and assessments of AI systems and the AI Management System (AIMS). It ensures consistent reporting of findings, evidence, and recommendations in compliance with framework requirements.

Framework Alignment:

- **AI RMF 2026:** GOVERN-4.1 (Accountability mechanisms), MEASURE-4.1 (Validation), MANAGE-4.1 (Monitoring and review)
- **ISO/IEC 42001:** Clause 9.2 (Internal audit), Clause 9.3 (Management review), Clause 10.1 (Continual improvement)
- **ISO/IEC 27001:** Clause 9.2 (Internal audit), Clause 9.3 (Management review), Clause 10.1 (Nonconformity and corrective action)

Instructions for Use

1. Audit Types:

- • Internal Audit: Conducted by organization personnel or authorized representatives
- • External Audit: Conducted by independent third-party auditors
- • Certification Audit: For ISO/IEC 42001, ISO/IEC 27001, or other certifications
- • Compliance Assessment: Verification of regulatory compliance
- • Technical Assessment: Deep-dive evaluation of AI system performance

2. Report Preparation:

- • Complete all sections thoroughly with evidence-based findings
- • Use objective language and cite specific evidence
- • Classify findings by severity (Critical/Major/Minor)
- • Provide clear, actionable recommendations
- • Include supporting documentation as appendices

3. Finding Classification:

- • Critical: Severe non-compliance with immediate risk, requires urgent action
- • Major: Significant non-compliance or systematic failure, corrective action required

- • Minor: Isolated issue or minor deviation, improvement recommended
- • Observation: Not a non-compliance but opportunity for improvement

4. Report Distribution:

- • Distribute to audit sponsor, auditee, and relevant stakeholders
- • Present findings to governance committee
- • Track corrective actions to closure
- • Maintain audit records per retention policy

AUDIT AND ASSESSMENT REPORT

Report Number:	**[e.g., AUDIT-2024-001]**
Report Date:	[DD/MM/YYYY]
Audit/Assessment Type:	[Internal/External/Certification/Compliance/Technical]
Audit Period:	[Start Date] to [End Date]
Lead Auditor/Assessor:	[Name, Title/Organization]
Audit Team Members:	[Names and roles]
Audit Sponsor:	[Name, Title]
Auditee:	[Department/System/Organization Unit]
Audit Standard/Criteria:	[AI RMF 2026 / ISO 42001 / ISO 27001 / Other]
Previous Audit Date:	[DD/MM/YYYY or N/A]
Report Classification:	[Confidential/Internal/Public]
Report Distribution:	[List recipients]

Section 1: Executive Summary

1.1 Purpose and Scope:
[Briefly state the purpose of this audit/assessment and what was covered]

_____
_____
_____

1.2 Overall Assessment:
[Provide high-level summary of audit outcome]

Overall Rating: ☐ Satisfactory ☐ Satisfactory with Observations ☐ Non-Compliant

1.3 Key Findings Summary:

Finding Category	Count
Critical Findings	[Number]
Major Findings	[Number]
Minor Findings	[Number]
Observations	[Number]

1.4 Critical Issues Requiring Immediate Attention:
[List any critical findings that require urgent action]

_____
_____
_____

1.5 Positive Observations:
[Highlight areas of strong performance or best practices observed]

_____
_____

Section 2: Audit/Assessment Scope and Methodology

2.1 Scope Definition:

Areas Included:
[Specify what was audited/assessed]

- • [Area 1 - e.g., AI governance structure]
- • [Area 2 - e.g., Risk management processes]
- • [Area 3 - e.g., Specific AI systems]
- • [Area 4 - e.g., Documentation and records]

AI Systems Evaluated:

System Name/ID	System Type	Risk Level
[System name]	[Type]	[Critical/High/Medium/Low]
[System name]	[Type]	[Risk level]
[System name]	[Type]	[Risk level]
[Add rows as needed]		

Areas Excluded:
[Specify what was not covered and why]

_____
___
_____
___

2.2 Audit/Assessment Methodology:

Methods Used:
☐ Document Review
☐ Interviews
☐ Process Observation
☐ System Testing/Validation
☐ Evidence Sampling
☐ Technical Analysis
☐ Data Analysis
☐ Other: _____

Sampling Approach:
[Describe sampling methodology if applicable]

_____

_____

2.3 Audit Criteria and Standards:

Standards/Frameworks Applied:
☐ AI RMF 2026 (NIST)
☐ ISO/IEC 42001:2023
☐ ISO/IEC 27001:2022
☐ Industry-specific standards: _____
☐ Regulatory requirements: _____
☐ Organizational policies and procedures

2.4 Timeline and Effort:

Phase	Date(s)	Duration/Effort
Planning and Preparation	[Dates]	[Days/Hours]
Opening Meeting	[Date]	[Duration]
Fieldwork/Evidence Collection	[Dates]	[Days/Hours]
Analysis and Report Writing	[Dates]	[Days/Hours]
Closing Meeting	[Date]	[Duration]

Section 3: Personnel Interviewed

[List all individuals interviewed during the audit/assessment]

Name	Title/Role	Department	Interview Date
[Name]	[Title]	[Department]	[Date]
[Name]	[Title]	[Department]	[Date]
[Name]	[Title]	[Department]	[Date]
[Name]	[Title]	[Department]	[Date]
[Name]	[Title]	[Department]	[Date]
[Name]	[Title]	[Department]	[Date]
[Add rows as needed]			

Section 4: Documents Reviewed

[List key documents reviewed during the audit/assessment]

Document Name	Document Number/Version	Date	Notes
AI Governance Policy	[Number/Version]	[Date]	
Risk Assessment(s)	[Number/Version]	[Date]	
AI System Inventory	[Number/Version]	[Date]	
Training Records	[Number/Version]	[Date]	
Model Documentation	[Number/Version]	[Date]	
Testing/Validation Reports	[Number/Version]	[Date]	
Incident Reports	[Number/Version]	[Date]	
Meeting Minutes	[Number/Version]	[Date]	
Monitoring Reports	[Number/Version]	[Date]	
[Document name]	[Number/Version]	[Date]	
[Add rows as needed]			

Section 5: Detailed Findings

[Document each finding in detail using the template below. Copy template for each finding.]

FINDING #1

Finding Classification:
☐ Critical ☐ Major ☐ Minor ☐ Observation

Framework Reference:
[e.g., AI RMF GOVERN-1.1 / ISO 42001 Clause 5.1 / ISO 27001 Clause 6.1]
_____

Area/Process:
[e.g., AI Risk Management / Data Governance / Model Validation]
_____

Finding Description:
[Clear, objective description of what was found - what is wrong or missing]
_____
_____
_____
_____

Evidence:
[Specific evidence supporting the finding - documents, interviews, observations]
_____
_____
_____

Requirement/Criteria:
[What standard, policy, or requirement was not met]
_____
_____

Impact/Risk:
[Potential consequences if not addressed]
_____
_____
_____

Root Cause Analysis:
[Why did this issue occur - underlying causes]
_____
_____

Recommendation:
[Specific, actionable steps to address the finding]
_____
_____
_____

Management Response:
[To be completed by auditee]
Agree: ☐ Yes ☐ No ☐ Partially
Response: _____
_____
_____

Corrective Action Plan:
Action to be taken: _____
_____
___
Responsible Party: _____
Target Completion Date: _____
Resources Required: _____

[Repeat the above finding template for Finding #2, Finding #3, etc.]

Section 6: Findings Summary by Category

[Organize findings by framework area or process category]

Framework Area/Process	Critical	Major	Minor	Observations
Governance Structure	[#]	[#]	[#]	[#]
Risk Management	[#]	[#]	[#]	[#]
Data Governance	[#]	[#]	[#]	[#]
Model Development	[#]	[#]	[#]	[#]
Testing & Validation	[#]	[#]	[#]	[#]
Security & Privacy	[#]	[#]	[#]	[#]
Monitoring & Maintenance	[#]	[#]	[#]	[#]
Documentation	[#]	[#]	[#]	[#]
TOTAL	[#]	[#]	[#]	[#]

Section 7: Positive Observations and Best Practices

[Document areas of strong performance and best practices observed]

Area/Process	Best Practice Observed
[Area]	[Description of best practice]
[Area]	[Description]
[Area]	[Description]
[Area]	[Description]
[Add rows as needed]	

Section 8: Previous Audit Follow-Up

[Status of findings from previous audit, if applicable]

Previous Finding #	Description	Corrective Action	Status	Verification
[Finding ID]	[Brief description]	[Action taken]	☐Closed ☐Open ☐Partial	[Evidence]
[Finding ID]	[Description]	[Action]	☐Closed ☐Open ☐Partial	[Evidence]
[Finding ID]	[Description]	[Action]	☐Closed ☐Open ☐Partial	[Evidence]
[Finding ID]	[Description]	[Action]	☐Closed ☐Open ☐Partial	[Evidence]
[Add rows as needed]				

Summary:
Total previous findings: _____
Closed: _____ Open: _____ Partially Addressed: _____

Section 9: Overall Conclusions

9.1 Audit Opinion:

Based on the evidence collected, the audit team concludes:

☐ Effective - AI Management System is effective and compliant
☐ Generally Effective - Minor issues noted, overall compliant
☐ Partially Effective - Significant gaps require attention
☐ Not Effective - Major non-compliance, substantial improvement needed

9.2 Key Strengths:
[Highlight main strengths observed]
_____
_____
_____
_____

9.3 Key Areas for Improvement:
[Summarize primary areas needing improvement]
_____
_____
_____
_____

9.4 Strategic Recommendations:
[High-level recommendations for leadership]
1. _____
2. _____
3. _____
4. _____
5. _____

9.5 Certification/Compliance Statement:
[If applicable - statement on certification readiness or compliance status]
_____
_____
_____

Section 10: Action Plan Summary

[Summary of all corrective actions required]

Finding #	Priority	Action Required	Owner	Target Date	Status
#1	[Critical/Major/Minor]	[Brief action]	[Name/Role]	[Date]	☐Not Started ☐In Progress ☐Complete
#2	[Priority]	[Action]	[Owner]	[Date]	☐Not Started ☐In Progress ☐Complete
#3	[Priority]	[Action]	[Owner]	[Date]	☐Not Started ☐In Progress ☐Complete
#4	[Priority]	[Action]	[Owner]	[Date]	☐Not Started ☐In Progress ☐Complete
#5	[Priority]	[Action]	[Owner]	[Date]	☐Not Started ☐In Progress ☐Complete
#6	[Priority]	[Action]	[Owner]	[Date]	☐Not Started ☐In Progress ☐Complete
[Add rows for all findings]					

Follow-Up Audit Planned:
☐ Yes - Date: _____
☐ No - Ongoing monitoring sufficient

Section 11: Report Approval and Sign-Off

11.1 Audit Team Sign-Off:

Name	Role	Signature	Date
[Lead Auditor]	Lead Auditor	_____	_____
[Auditor]	Auditor	_____	_____
[Technical Expert]	Technical Expert	_____	_____

11.2 Auditee Acknowledgment:

I acknowledge receipt of this audit report and commit to implementing the agreed corrective actions.

Name: _____
Title: _____
Signature: _____ Date: _____

11.3 Management Approval:

Name: _____
Title: _____
Signature: _____ Date: _____

Section 12: Appendices

[List and attach supporting documentation]

Appendix A: Audit Program/Checklist
Appendix B: Detailed Evidence
Appendix C: Interview Notes
Appendix D: Sample Records Reviewed
Appendix E: Technical Test Results
Appendix F: Screenshots/Visual Evidence
Appendix G: Framework Compliance Matrix
Appendix H: [Additional supporting materials]

END OF AUDIT AND ASSESSMENT REPORT

Report Information:
Template Version: 1.0
Template Owner: AI Governance Office / Internal Audit
Classification: Confidential - Internal Use Only
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001

Template F.8
AI Incident Response Log

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive system for documenting, tracking, and managing AI-related incidents. It ensures consistent incident handling, root cause analysis, and continuous improvement in compliance with framework requirements.

Framework Alignment:

- **AI RMF 2026:** MEASURE-2.11 (Incident tracking), MANAGE-1.3 (Incident response), MANAGE-4.3 (Post-incident review)
- **ISO/IEC 42001:** Clause 8.1 (Operational control), Clause 10.1 (Nonconformity and corrective action), Clause 10.2 (Continual improvement)
- **ISO/IEC 27001:** Clause 10.1 (Nonconformity and corrective action), Annex A.5.24 (Information security incident management planning)

Instructions for Use

1. Incident Definition:

- An AI incident is any event or occurrence that:
- - Causes or could cause harm to individuals or organizations
- - Results in AI system malfunction or degraded performance
- - Violates policies, regulations, or ethical standards
- - Compromises data security, privacy, or integrity
- - Produces biased, unfair, or discriminatory outcomes

2. Incident Reporting:

- • All AI incidents must be reported immediately upon discovery
- • Use this log to document each incident comprehensively
- • Assign unique incident ID for tracking
- • Classify incident by severity (Critical/High/Medium/Low)

3. Incident Response Process:

- • Immediate: Contain and mitigate (within 1-4 hours for critical)
- • Short-term: Investigate root cause (within 24-48 hours)
- • Medium-term: Implement corrective actions (per severity)
- • Long-term: Review lessons learned and update controls

4. Record Retention:

- • Maintain incident records for minimum 7 years
- • Store securely with restricted access
- • Review incidents quarterly for trending and patterns

AI INCIDENT RESPONSE LOG

Incident Severity Classification

Severity	Impact	Response Time
Critical	Severe harm; major business impact; regulatory breach; system failure	Immediate (1 hour)
High	Significant harm potential; serious business impact; compliance concern	Urgent (4 hours)
Medium	Moderate harm; noticeable business impact; minor compliance gap	Priority (24 hours)
Low	Limited harm; minimal business impact; no compliance concern	Standard (72 hours)

INCIDENT LOG ENTRY

Section 1: Incident Identification

Incident ID:	**[Auto-generated or INC-YYYY-###]**
Date/Time Reported:	[DD/MM/YYYY HH:MM]
Date/Time Discovered:	[DD/MM/YYYY HH:MM]
Date/Time Occurred (est.):	[DD/MM/YYYY HH:MM]
Reported By:	[Name, Title, Contact]
Incident Owner/Coordinator:	[Name, Title - person managing response]
Affected AI System:	[System Name/ID from inventory]
System Owner:	[Name, Title]
Current Status:	☐New ☐Investigating ☐Contained ☐Resolved ☐Closed
Log Entry Updated:	[DD/MM/YYYY - update with each status change]

1.1 Incident Severity:
☐ Critical
☐ High
☐ Medium
☐ Low

1.2 Incident Type (check all that apply):
☐ Performance Degradation/Failure
☐ Accuracy/Prediction Error
☐ Bias/Fairness Issue
☐ Security Breach/Vulnerability
☐ Privacy/Data Protection Violation
☐ Safety Incident (harm to individuals)
☐ Compliance/Regulatory Violation
☐ Ethical Concern
☐ Data Quality/Integrity Issue
☐ Model Drift/Degradation
☐ Adversarial Attack
☐ System Unavailability/Downtime
☐ Human Override/Intervention Required
☐ Other: _____

Section 2: Incident Description

2.1 What Happened:
[Detailed description of the incident - what occurred, when, where]
_____
_____
_____
_____
_____

2.2 How Was It Detected:
☐ Automated monitoring/alerting
☐ User report/complaint
☐ Internal audit/review
☐ External notification
☐ Routine testing
☐ Other: _____

2.3 Affected Users/Stakeholders:
[Who was or could be affected]
Number of users affected: _____
User groups affected: _____
Geographic scope: _____

2.4 Business Impact:
☐ Critical - Severe business disruption or harm
☐ High - Significant impact on operations or reputation
☐ Medium - Moderate impact, workarounds available
☐ Low - Minimal impact

Impact Description:
_____
_____
_____

2.5 Estimated Financial Impact:
$_____ (if quantifiable)

2.6 Regulatory/Compliance Implications:
☐ Potential regulatory reporting required
☐ Compliance violation identified
☐ Legal notification required
☐ No compliance implications

Details: _____
_____

Section 3: Immediate Response and Containment

3.1 Immediate Actions Taken:
[List actions taken to contain the incident]

Action	Taken By	Date/Time	Outcome
[Action description]	[Name]	[Date/Time]	[Result]
[Action]	[Name]	[Date/Time]	[Result]
[Action]	[Name]	[Date/Time]	[Result]
[Action]	[Name]	[Date/Time]	[Result]
[Add rows as needed]			

3.2 System Status After Containment:
☐ System disabled/taken offline
☐ System operating in degraded mode
☐ System operating normally with monitoring
☐ No system changes required

3.3 Stakeholder Notifications:

Stakeholder/Party	Notified By	Date/Time	Method
[e.g., Executive Management]	[Name]	[Date/Time]	[Email/Phone/Meeting]
[e.g., Affected Users]	[Name]	[Date/Time]	[Method]
[e.g., Regulatory Authority]	[Name]	[Date/Time]	[Method]
[Add rows as needed]			

3.4 Evidence Preserved:
☐ Log files captured
☐ System snapshots/backups created
☐ Screenshots/documentation captured
☐ Model state preserved
☐ Data samples preserved
☐ Other evidence: _____

Evidence location: _____

Section 4: Investigation and Root Cause Analysis

4.1 Investigation Team:

Name	Title/Role	Expertise/Responsibility
[Name]	[Title]	[Area of focus]
[Name]	[Title]	[Area of focus]
[Name]	[Title]	[Area of focus]
[Add rows as needed]		

4.2 Investigation Start Date:

_____

4.3 Root Cause Analysis Method:

☐ 5 Whys
☐ Fishbone/Ishikawa Diagram
☐ Fault Tree Analysis
☐ Timeline Analysis
☐ Other: _____

4.4 Root Cause(s) Identified:

[Describe underlying causes - not just symptoms]

Primary Root Cause:

_____
_____
_____

Contributing Factors:
• _____
• _____
• _____
• _____

4.5 Root Cause Category:
☐ Data Quality/Integrity Issue
☐ Model Design/Architecture Flaw
☐ Training Data Bias/Insufficiency
☐ Algorithm/Code Defect
☐ Configuration Error
☐ Insufficient Testing/Validation
☐ Inadequate Monitoring/Alerting
☐ Human Error (operational)
☐ Process/Procedure Gap
☐ Third-Party/Vendor Issue
☐ Infrastructure/Platform Issue
☐ Environmental/External Factor
☐ Security Vulnerability
☐ Other: _____

4.6 Could This Have Been Prevented:

☐ Yes - preventable with existing controls
☐ Yes - would require additional controls
☐ Partially - some aspects preventable
☐ No - unavoidable/unpredictable

Explanation: _____
_____
_____

Section 5: Corrective and Preventive Actions

5.1 Corrective Actions (fix this incident):

Action	Owner	Target Date	Actual Completion	Status	Verification
[Action description]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Add rows as needed]					

5.2 Preventive Actions (prevent recurrence):

Action	Owner	Target Date	Actual Completion	Status	Verification
[Action description]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Action]	[Name]	[Date]	[Date]	☐Not Started ☐In Progress ☐Complete	[How verified]
[Add rows as needed]					

5.3 Process/Policy Updates Required:

☐ Update risk assessment
☐ Update system documentation
☐ Revise policies/procedures
☐ Update training materials
☐ Modify monitoring/alerting
☐ Update testing protocols

☐ Other: _____

Details: _____
_____

Section 6: Lessons Learned

6.1 What Went Well:
[Aspects of response that were effective]
• _____
• _____
• _____

6.2 What Could Be Improved:
[Areas for improvement in detection, response, or recovery]
• _____
• _____
• _____

6.3 Key Takeaways:
[Main lessons for organization]
_____
_____
_____
_____

6.4 Recommendations for Similar Systems:
[Apply lessons to other AI systems]
_____
_____
_____

6.5 Training Needs Identified:
☐ Technical training for staff
☐ Incident response training
☐ User awareness training
☐ No training needs identified

Details: _____
_____

Section 7: Incident Timeline

[Comprehensive chronological record of incident events]

Date/Time	Event/Action	Person/Team	Notes
[DD/MM HH:MM]	Incident occurred (estimated)	[System/Auto]	
[DD/MM HH:MM]	Incident detected	[How/Who]	
[DD/MM HH:MM]	Incident reported	[Name]	
[DD/MM HH:MM]	Initial assessment	[Name]	
[DD/MM HH:MM]	Containment actions initiated	[Name/Team]	
[DD/MM HH:MM]	Stakeholders notified	[Name]	
[DD/MM HH:MM]	Investigation commenced	[Team]	
[DD/MM HH:MM]	Root cause identified	[Team]	
[DD/MM HH:MM]	Corrective actions implemented	[Name/Team]	
[DD/MM HH:MM]	Incident resolved	[Name]	
[Add rows as needed for all events]			

Section 8: Incident Metrics

Metric	Value
Time to Detect (occurrence to detection)	[Duration]
Time to Report (detection to reporting)	[Duration]
Time to Respond (report to initial action)	[Duration]
Time to Contain (report to containment)	[Duration]
Time to Resolve (report to resolution)	[Duration]
Total Incident Duration	[Duration]
System Downtime (if applicable)	[Duration]
Response Team Effort (person-hours)	[Hours]

Section 9: Incident Closure

9.1 Resolution Verification:
[How was resolution verified]

_____
_____

9.2 Post-Resolution Monitoring:
Monitoring Period: _____ days/weeks
Monitoring Frequency: _____
Metrics Monitored: _____
_____

9.3 Similar Incidents Check:
Similar incidents identified in other systems: ☐ Yes ☐ No

If Yes, actions taken:
_____
_____

9.4 Governance Committee Briefing:
Briefed: ☐ Yes ☐ No ☐ Not Required
Date: _____
Key Discussion Points: _____
_____

9.5 Incident Status:
☐ Resolved - No further action required
☐ Resolved - Monitoring continues
☐ Partially Resolved - Actions ongoing
☐ Closed - All actions complete

9.6 Closure Approval:

Incident Owner:
Name: _____
Signature: _____ Date: _____

System Owner:
Name: _____
Signature: _____ Date: _____

Management Approval:
Name: _____
Title: _____

Signature: _____ Date: _____

END OF INCIDENT LOG ENTRY

[Create a new incident log entry for each incident using this template]

Section 10: Incident Summary Dashboard

[Aggregate view of all incidents - update quarterly]

Reporting Period:
[Start Date] to [End Date]

10.1 Incident Statistics

Metric	Count/Value
Total Incidents	[Number]
Critical Incidents	[Number]
High Severity Incidents	[Number]
Medium Severity Incidents	[Number]
Low Severity Incidents	[Number]
Average Time to Resolution	[Duration]
Repeat Incidents (same root cause)	[Number]

10.2 Incidents by Type

Incident Type	Count
Performance/Failure	[Number]
Accuracy/Prediction Error	[Number]
Bias/Fairness	[Number]
Security	[Number]
Privacy	[Number]
Safety	[Number]
Compliance	[Number]
Data Quality	[Number]
System Availability	[Number]
Other	[Number]

10.3 Trends and Patterns

[Narrative description of trends, patterns, or concerning observations]

_____
_____
_____

10.4 Recommendations

[System-wide recommendations based on incident trends]

- _____
- _____
- _____

═══

END OF INCIDENT RESPONSE LOG

Document Information:
Template Version: 1.0
Template Owner: AI Governance Office / Security Operations
Classification: Confidential - Sensitive Incident Information
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001
Retention Period: 7 years minimum

Template F.9
AI Monitoring and Metrics Dashboard

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive framework for monitoring AI system performance, governance effectiveness, and compliance metrics. It enables data-driven decision-making and continuous improvement in alignment with framework requirements.

Framework Alignment:

- **AI RMF 2026:** MEASURE-2.1 through 2.13 (Measurement and monitoring), MANAGE-4.1 (Monitoring systems), GOVERN-4.2 (Performance monitoring)
- **ISO/IEC 42001:** Clause 9.1 (Monitoring, measurement, analysis and evaluation), Clause 9.3 (Management review), Clause 10.2 (Continual improvement)
- **ISO/IEC 27001:** Clause 9.1 (Monitoring, measurement, analysis and evaluation), Annex A.5.25 (Assessment of information security events)

Instructions for Use

1. Dashboard Structure:

- This template contains multiple metric categories:
- - Technical Performance Metrics
- - Fairness and Bias Metrics
- - Security and Privacy Metrics
- - Governance and Compliance Metrics
- - Operational Metrics
- - Business Impact Metrics

2. Metric Selection:

- • Not all metrics apply to every AI system
- • Select metrics based on system risk level and use case
- • High-risk systems require more comprehensive monitoring
- • Establish baseline values before deployment

3. Data Collection:

- • Automate metric collection where possible
- • Define clear measurement methods for each metric
- • Establish data quality controls

- • Document data sources and calculation methods

4. Threshold Setting:

- • Set target values based on requirements and benchmarks
- • Define warning thresholds (yellow) and critical thresholds (red)
- • Review and adjust thresholds based on actual performance
- • Establish escalation procedures for threshold breaches

5. Reporting Frequency:

- • Critical metrics: Real-time or daily monitoring
- • Important metrics: Weekly or bi-weekly review
- • Standard metrics: Monthly or quarterly review
- • Generate executive summary reports quarterly

6. Continuous Improvement:

- • Analyze trends over time
- • Investigate anomalies and threshold breaches
- • Use metrics to drive improvement initiatives
- • Review metric relevance and effectiveness periodically

AI MONITORING AND METRICS DASHBOARD

AI System Name/ID:	**[System name from inventory]**
Reporting Period:	[Start Date] to [End Date]
Report Generated:	[DD/MM/YYYY]
Report Frequency:	☐Daily ☐Weekly ☐Monthly ☐Quarterly
System Owner:	[Name, Title]
Report Prepared By:	[Name, Title]
Overall Health Status:	☐Green (Healthy) ☐Yellow (Warning) ☐Red (Critical)
Distribution:	[List recipients]

Section 1: Executive Summary

1.1 Overall System Health:
[Brief narrative summary of system health and performance]
_____
_____
_____

1.2 Key Highlights:
• [Notable achievement or positive trend]
• [Important finding or improvement]
• [Significant metric change]

1.3 Critical Issues Requiring Attention:
• [Issue 1 - if any]
• [Issue 2 - if any]
☐ No critical issues identified

1.4 Actions Recommended:
• [Recommended action 1]
• [Recommended action 2]
☐ No immediate actions required

Section 2: Technical Performance Metrics

Metrics measuring AI model and system performance.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
Model Accuracy	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Precision	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Recall	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
F1 Score	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
AUC-ROC	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Mean Absolute Error (MAE)	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
False Positive Rate	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
False Negative Rate	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Latency (avg)	[ms]	[ms]	[Target ms]	[Warning ms]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Throughput (predictions/sec)	[#]	[#]	[Target #]	[Warning #]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Data Drift Score	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Drift Score	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
System Uptime	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓

[Add custom metrics as needed]						

Analysis and Commentary:
[Explain significant changes, trends, or concerns in technical performance]

_____
_____
_____

Section 3: Fairness and Bias Metrics

Metrics measuring fairness across protected characteristics.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
Demographic Parity Ratio	[Value]	[Value]	[0.8-1.2 typical]	[Warning value]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Equal Opportunity Difference	[Value]	[Value]	[<0.1 typical]	[Warning value]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Disparate Impact Ratio	[Value]	[Value]	[0.8-1.25 typical]	[Warning value]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Statistical Parity Difference	[Value]	[Value]	[<0.1 typical]	[Warning value]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Average Odds Difference	[Value]	[Value]	[<0.1 typical]	[Warning value]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Error Rate Parity	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
False Positive Rate Parity	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
False Negative Rate Parity	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Bias Audit Score (overall)	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
[Add custom metrics as needed]						

Protected Characteristics Monitored:
☐ Age
☐ Gender
☐ Race/Ethnicity
☐ Disability Status
☐ Geographic Location
☐ Other: _____

Analysis and Commentary:
[Explain fairness findings, disparities identified, or improvements observed]
_____
_____
_____

Section 4: Security and Privacy Metrics

Metrics measuring security posture and privacy protection.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
Security Incidents	[Count]	[Count]	[0 target]	[>0 warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Adversarial Attack Attempts	[Count]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Robustness Score	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Unauthorized Access Attempts	[Count]	[Count]	[0 target]	[>threshold warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Data Encryption Coverage	[%]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Privacy Policy Compliance	[%]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Data Minimization Score	[Value]	[Value]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Privacy Incidents	[Count]	[Count]	[0 target]	[>0 warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Data Breach Incidents	[Count]	[Count]	[0 target]	[>0 critical]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Access Control Violations	[Count]	[Count]	[0 target]	[>threshold warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Vulnerability Remediation Time (avg)	[Days]	[Days]	[Target days]	[Warning days]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
[Add custom metrics as needed]						

Analysis and Commentary:
[Explain security posture, privacy compliance status, or concerns]

_____

_____

Section 5: Governance and Compliance Metrics

Metrics measuring governance effectiveness and regulatory compliance.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
Policy Compliance Rate	[%]	[%]	[100% target]	[<95% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Documentation Completeness	[%]	[%]	[100% target]	[<95% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Risk Assessment Currency	[Days since update]	[Days]	[<90 days target]	[>90 days warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Training Compliance Rate	[%]	[%]	[100% target]	[<90% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Audit Findings (open)	[Count]	[Count]	[0 target]	[>threshold warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Corrective Action Completion	[%]	[%]	[100% target]	[<80% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Governance Meeting Attendance	[%]	[%]	[>80% target]	[<75% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Review Cycle Compliance	[%]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Validation Status	[% validated]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Ethical Review Completion	[% complete]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Regulatory Compliance Score	[%]	[%]	[100% target]	[<95% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Incident Response Time (avg)	[Hours]	[Hours]	[Target hours]	[Warning hours]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Change Management Compliance	[%]	[%]	[100% target]	[<95% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓

Third-Party Assessments Current	[% current]	[%]	[100% target]	[<100% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
[Add custom metrics as needed]						

Analysis and Commentary:
[Explain governance effectiveness, compliance status, or improvement areas]
_____
_____
_____

Section 6: Operational Metrics

Metrics measuring day-to-day operations and system usage.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
Total Predictions/Transactions	[Count]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Active Users	[Count]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
User Satisfaction Score	[1-5 or %]	[Score]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Human Override Rate	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
User-Reported Issues	[Count]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Support Ticket Volume	[Count]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Issue Resolution Time (avg)	[Hours/Days]	[Time]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Model Retraining Frequency	[Per period]	[Count]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Deployment Success Rate	[%]	[%]	[>95% target]	[<90% warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Rollback Incidents	[Count]	[Count]	[0 target]	[>0 warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Infrastructure Cost Efficiency	[$/prediction]	[Cost]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
[Add custom metrics as needed]						

Analysis and Commentary:
[Explain operational trends, user feedback, or efficiency improvements]

_____
_____
_____

Section 7: Business Impact Metrics

Metrics measuring business value and strategic alignment.

Metric	Current Value	Previous Period	Target	Threshold (Warning)	Status	Trend
ROI (Return on Investment)	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Cost Savings Achieved	[$]	[$]	[Target $]	[Warning $]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Revenue Impact	[$]	[$]	[Target $]	[Warning $]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Process Efficiency Gain	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Time Saved (hours)	[Hours]	[Hours]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Customer Retention Impact	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Decision Quality Improvement	[%]	[%]	[Target %]	[Warning %]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Strategic Objective Alignment	[Score 1-5]	[Score]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
Stakeholder Satisfaction	[Score/%]	[Score]	[Target]	[Warning]	☐Green ☐Yellow ☐Red	☐↑ ☐→ ☐↓
[Add custom metrics as needed]						

Analysis and Commentary:
[Explain business value delivered, ROI trends, or strategic alignment]

_____
_____
_____

Section 8: Actions and Recommendations

8.1 Immediate Actions Required:

Issue/Metric	Action Required	Owner	Target Date
[Metric/issue]	[Specific action]	[Name/Role]	[Date]
[Metric/issue]	[Action]	[Owner]	[Date]
[Metric/issue]	[Action]	[Owner]	[Date]
☐ **No immediate actions required**			

8.2 Recommendations for Improvement:

- [Recommendation 1]
- [Recommendation 2]
- [Recommendation 3]

8.3 Resource Requirements:

[Identify resources needed to address issues or implement improvements]

_____

_____

Section 9: Report Approval and Distribution

Report Prepared By:

Name: _____

Title: _____

Date: _____

Signature: _____

Reviewed By:
Name: _____
Title: _____
Date: _____
Signature: _____

Approved By (System Owner):
Name: _____
Title: _____
Date: _____
Signature: _____

END OF MONITORING AND METRICS DASHBOARD

Document Information:
Template Version: 1.0
Template Owner: AI Governance Office / System Operations
Update Frequency: [Per system requirements]
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001

Note: This dashboard template should be adapted to specific system needs. Not all metrics will apply to every AI system. Select and customize metrics based on system risk level, use case, and organizational requirements.

Template F.10
AI Model Card and Documentation Template

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive structure for documenting AI models, following model card best practices and framework requirements. It ensures transparency, reproducibility, and accountability for AI systems throughout their lifecycle.

Framework Alignment:

- **AI RMF 2026:** GOVERN-2.1 (Transparency and documentation), MAP-1.1 (System documentation), MEASURE-3.1 (Documentation of methods)
- **ISO/IEC 42001:** Clause 7.5 (Documented information), Clause 8.1.2 (AI system development), Annex A (Controls for documentation)
- **ISO/IEC 27001:** Clause 7.5 (Documented information), Annex A.8.1 (User endpoint devices - documentation)

Instructions for Use

1. When to Create:

- • For every AI model developed or procured
- • Before model deployment to production
- • When model undergoes significant changes/retraining
- • As part of model validation process

2. Completion Guidelines:

- • Complete all applicable sections thoroughly
- • Use clear, non-technical language where possible
- • Include technical details in appropriate sections
- • Provide references to supporting documentation
- • Update model card with each model version

3. Audience:

- Model cards serve multiple audiences:
- - Technical teams (developers, data scientists)
- - Business stakeholders and decision-makers
- - Governance and compliance teams
- - End users and affected individuals
- - Auditors and regulators

4. Transparency Levels:

- • Public: Information appropriate for external disclosure
- • Internal: Detailed technical information for organization
- • Confidential: Proprietary or sensitive details
- Clearly mark sections with appropriate classification

5. Version Control:

- • Maintain version history for all model cards
- • Document changes between versions
- • Archive previous versions

AI MODEL CARD

Model Name:	**[Descriptive model name]**
Model ID/Version:	[Unique identifier and version number]
Model Card Version:	[Card version - e.g., 1.0]
Model Card Date:	[DD/MM/YYYY]
Model Development Date:	[Date model was developed/trained]
Model Owner:	[Name, Title, Department]
Development Team:	[Team name or key members]
Model Status:	☐Development ☐Testing ☐Production ☐Deprecated
Model Type:	[Classification/Regression/NLP/Computer Vision/etc.]
Risk Classification:	☐Critical ☐High ☐Medium ☐Low
Document Classification:	☐Public ☐Internal ☐Confidential
Contact Information:	[Email/phone for questions]

Section 1: Model Overview

1.1 Model Summary:
[Brief, non-technical description of what the model does]

_____
_____
_____

1.2 Model Purpose and Use Case:
[Why was this model developed? What business problem does it solve?]

_____
_____
_____

1.3 Key Features:
• [Key capability 1]
• [Key capability 2]
• [Key capability 3]

1.4 Model Lineage:
☐ Developed in-house from scratch
☐ Based on open-source model: _____
☐ Fine-tuned from pre-trained model: _____
☐ Commercial/third-party model: _____
☐ Transfer learning from: _____

Section 2: Intended Use

2.1 Primary Intended Use(s):
[Describe the specific intended applications]

_____
_____
_____

2.2 Primary Intended Users:
[Who will use this model? Internal/external users?]

_____
_____

2.3 Out-of-Scope Uses:
[Important: What should this model NOT be used for?]

- _____
- _____
- _____

2.4 Use Case Restrictions:
[Any regulatory, ethical, or practical limitations on use]

_____
_____
_____

2.5 Geographic Scope:
☐ Global
☐ Regional: _____
☐ Country-specific: _____
Geographic limitations: _____

Section 3: Model Architecture and Technical Details

3.1 Model Architecture:
Algorithm/Approach: _____
Framework/Library: _____
Model Type: _____

Architecture Details:
[Describe model architecture - layers, components, structure]
_____
_____
_____
_____

3.2 Model Parameters:

Parameter	Value/Description
Total Parameters	[Number]
Trainable Parameters	[Number]
Model Size	[MB/GB]
Input Dimensions	[Dimensions/format]
Output Dimensions	[Dimensions/format]
Number of Classes (if applicable)	[Number]
[Other relevant parameters]	

3.3 Hyperparameters:

Hyperparameter	Value
Learning Rate	[Value]
Batch Size	[Value]
Number of Epochs	[Value]
Optimizer	[Type and parameters]
Loss Function	[Type]
Regularization	[Type and parameters]
[Other hyperparameters]	

3.4 Software and Hardware Environment:

Development Environment:
• Programming Language: _____
• Framework Version: _____
• Key Libraries: _____
• Development Tools: _____

Hardware Used for Training:
• CPU/GPU: _____
• Memory: _____
• Training Time: _____

Production Environment:
• Deployment Platform: _____
• Infrastructure: _____
• Inference Hardware: _____

Section 4: Training Data

4.1 Dataset Overview:
Dataset Name: _____
Dataset Source: _____
Dataset Version: _____
Data Collection Period: _____

4.2 Dataset Characteristics:

Characteristic	Value/Description
Total Records	[Number]
Training Set Size	[Number and %]
Validation Set Size	[Number and %]
Test Set Size	[Number and %]
Number of Features	[Number]
Data Modality	[Structured/Unstructured/Images/Text/etc.]
Class Balance	[Balanced/Imbalanced - provide ratios]
Missing Data	[% missing, handling approach]

4.3 Data Sources and Collection:
[How and where was data collected?]
_____
___
_____
___
_____
___

4.4 Data Preprocessing and Feature Engineering:
[Describe preprocessing steps, transformations, feature creation]
• _____
• _____
• _____
• _____

4.5 Data Quality Assessment:
Data Quality Issues Identified: _____
_____

Data Quality Assurance Measures: _____
_____

4.6 Data Sensitivity and Privacy:
☐ Contains Personal Data (PII)
☐ Contains Sensitive Personal Data
☐ Anonymized/Pseudonymized
☐ Publicly Available Data
☐ Proprietary/Licensed Data

Privacy Protection Measures: _____
_____

4.7 Data Representativeness:
[Does the training data represent the target population?]
_____
_____

Known Limitations or Biases in Data: _____
_____

Section 5: Model Performance

5.1 Evaluation Methodology:

Evaluation Approach: _____
Cross-validation Strategy: _____
Evaluation Metrics Used: _____

5.2 Overall Performance Metrics:

Metric	Training Set	Test Set
Accuracy	[%]	[%]
Precision	[Value]	[Value]
Recall	[Value]	[Value]
F1 Score	[Value]	[Value]
AUC-ROC	[Value]	[Value]
Mean Absolute Error (MAE)	[Value]	[Value]
Root Mean Squared Error (RMSE)	[Value]	[Value]
R-squared (R^2)	[Value]	[Value]
False Positive Rate	[%]	[%]
False Negative Rate	[%]	[%]
[Other relevant metrics]		

5.3 Performance by Subgroup:

[Performance metrics broken down by demographic or other relevant subgroups]

Subgroup	Sample Size	Accuracy	Other Key Metric
[Group 1]	[N]	[%]	[Value]
[Group 2]	[N]	[%]	[Value]
[Group 3]	[N]	[%]	[Value]
[Group 4]	[N]	[%]	[Value]
[Add rows as needed]			

5.4 Benchmark Comparisons:
[How does this model compare to baselines or industry benchmarks?]
_____
_____

5.5 Error Analysis:
[Common failure modes, error patterns, edge cases]
_____
_____
_____

Section 6: Fairness and Bias Assessment

6.1 Fairness Evaluation Conducted:
☐ Yes ☐ No ☐ Partially

6.2 Protected Characteristics Evaluated:
☐ Age
☐ Gender
☐ Race/Ethnicity
☐ Disability Status
☐ Geographic Location
☐ Socioeconomic Status
☐ Other: _____

6.3 Fairness Metrics:

Fairness Metric	Value	Acceptable Range
Demographic Parity Ratio	[Value]	[0.8-1.2 typical]
Equal Opportunity Difference	[Value]	[<0.1 typical]
Disparate Impact Ratio	[Value]	[0.8-1.25 typical]
Statistical Parity Difference	[Value]	[<0.1 typical]
Average Odds Difference	[Value]	[<0.1 typical]
[Other fairness metrics]		

6.4 Bias Identified:
[Describe any biases identified in the model]
_____
_____
_____

6.5 Bias Mitigation Measures:
[Actions taken to address identified biases]
• _____
• _____
• _____

6.6 Residual Fairness Concerns:
[Remaining fairness issues or limitations]
_____
_____

Section 7: Explainability and Interpretability

7.1 Model Interpretability:
Model Type: ☐ Inherently Interpretable ☐ Black Box ☐ Partially Interpretable

7.2 Explainability Methods Used:
☐ Feature Importance (e.g., SHAP, LIME)
☐ Attention Mechanisms
☐ Decision Trees/Rules
☐ Counterfactual Explanations
☐ Saliency Maps
☐ Prototype/Example-Based Explanations
☐ Other: _____

7.3 Feature Importance:
[Top features contributing to model predictions]

Feature Name	Importance Score/Rank
[Feature 1]	[Score/Rank]
[Feature 2]	[Score/Rank]
[Feature 3]	[Score/Rank]
[Feature 4]	[Score/Rank]
[Feature 5]	[Score/Rank]
[Feature 6]	[Score/Rank]
[Feature 7]	[Score/Rank]
[Feature 8]	[Score/Rank]
[Feature 9]	[Score/Rank]
[Feature 10]	[Score/Rank]

7.4 Explanation Format for End Users:
[How are predictions explained to users?]

_____
_____

7.5 Interpretability Limitations:
[Known limitations in model explainability]

_____
_____

Section 8: Limitations and Risks

8.1 Known Limitations:
[Technical, performance, or applicability limitations]
- _____
- _____
- _____
- _____

8.2 Model Constraints:
Input Requirements/Constraints: _____
_____
Operational Constraints: _____
_____

8.3 Risk Assessment Summary:

Risk Category	Risk Level	Mitigation Measures
Performance Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Bias/Fairness Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Security Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Privacy Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Safety Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Operational Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]
Compliance Risk	☐Critical ☐High ☐Medium ☐Low	[Mitigations]

8.4 Failure Modes:
[How might the model fail? What are the consequences?]
_____
_____
_____

8.5 Recommended Human Oversight:
☐ Human-in-the-loop (human approval required)
☐ Human-on-the-loop (human monitoring, can intervene)
☐ Human-in-command (human sets parameters, oversees)
☐ Fully automated (no human oversight)

Oversight Requirements: _____
_____

Section 9: Ethical Considerations

9.1 Ethical Review Conducted:
☐ Yes ☐ No ☐ Not Required

Review Date: _____
Reviewed By: _____

9.2 Ethical Concerns Identified:
[Ethical issues or concerns related to this model]

_____
_____
_____

9.3 Potential Social Impact:
[Positive and negative impacts on individuals, communities, society]

_____
_____
_____

9.4 Stakeholder Considerations:
[Impact on different stakeholder groups]

_____
_____

9.5 Value Alignment:
[How does this model align with organizational values and principles?]
_____
_____

Section 10: Deployment and Monitoring

10.1 Deployment Information:
Deployment Date: _____
Deployment Environment: _____
Deployment Method: _____
Integration Points: _____

10.2 Monitoring Plan:

Metric/Indicator	Monitoring Frequency	Alert Threshold
Model Accuracy	[Daily/Weekly/Monthly]	[Threshold]
Data Drift	[Frequency]	[Threshold]
Model Drift	[Frequency]	[Threshold]
Fairness Metrics	[Frequency]	[Threshold]
Latency/Performance	[Frequency]	[Threshold]
Error Rates	[Frequency]	[Threshold]
[Other metrics]		

10.3 Model Maintenance Schedule:
Retraining Frequency: _____
Performance Review Frequency: _____
Update Process: _____

10.4 Incident Response:
Incident Response Plan: _____
Escalation Path: _____
Model Rollback Criteria: _____

Section 11: Compliance and Governance

11.1 Regulatory Compliance:

[Applicable regulations and compliance status]

Regulation/Standard	Compliance Status
AI RMF 2026	☐Compliant ☐Partial ☐N/A
ISO/IEC 42001	☐Compliant ☐Partial ☐N/A
ISO/IEC 27001	☐Compliant ☐Partial ☐N/A
[Other applicable regulations]	☐Compliant ☐Partial ☐N/A
[Add rows as needed]	

11.2 Data Protection and Privacy:

GDPR/Privacy Law Compliance: ☐Yes ☐No ☐N/A

Data Protection Impact Assessment (DPIA): ☐Completed ☐Not Required

Legal Basis for Processing: _____

11.3 Intellectual Property:

Model Ownership: _____

Third-Party Components: _____

Licensing: _____

11.4 Approvals and Sign-Offs:

Role	Name	Date	Signature
Model Developer	[Name]	[Date]	_____
Data Scientist/ML Lead	[Name]	[Date]	_____
Model Validator	[Name]	[Date]	_____
Model Owner	[Name]	[Date]	_____
Governance Approval	[Name]	[Date]	_____

Section 12: References and Additional Resources

12.1 Technical Documentation:
• Technical Specification: _____
• Source Code Repository: _____
• API Documentation: _____
• Architecture Diagrams: _____

12.2 Supporting Documents:
• Risk Assessment Report: _____
• Validation Report: _____
• Test Results: _____
• User Documentation: _____
• Training Materials: _____

12.3 Related Publications:
[Academic papers, technical reports, or other publications related to this model]
_____
_____

12.4 Contact Information:
Technical Questions: _____
Ethical Concerns: _____
General Inquiries: _____

Section 13: Version History

Model Version	Card Version	Date	Changes	Author
1.0	1.0	[Date]	Initial model card	[Name]
[Version]	[Version]	[Date]	[Description of changes]	[Name]
[Version]	[Version]	[Date]	[Description]	[Name]
[Add rows for each version]				

END OF MODEL CARD

Document Information:
Template Version: 1.0
Template Owner: AI Governance Office / ML Operations
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001
Based on: Model Cards for Model Reporting (Mitchell et al., 2019)

Template F.11
AI Third-Party Vendor Assessment Template

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive framework for evaluating third-party AI vendors, service providers, and technology suppliers. It ensures thorough due diligence and ongoing oversight in compliance with framework requirements.
Framework Alignment:

- **AI RMF 2026:** GOVERN-3.1 (Third-party risk), MAP-5.1 (External dependencies), MANAGE-2.2 (Third-party oversight)
- **ISO/IEC 42001:** Clause 8.1 (Operational control), Clause 6.1.2 (Risk assessment), Annex A (Third-party controls)
- **ISO/IEC 27001:** Clause 6.1.2 (Risk assessment), Annex A.5.19-5.23 (Supplier relationships), Annex A.15 (Supplier relationships)

Instructions for Use

1. When to Use:

- • Before engaging any third-party AI vendor or service provider
- • During procurement/vendor selection process
- • For annual vendor risk reassessment
- • When vendor relationship or service changes significantly

2. Assessment Types:

- • Initial Assessment: Full evaluation before engagement
- • Annual Review: Periodic reassessment of existing vendors
- • Change Assessment: Evaluation when services change
- • Incident-Triggered: Assessment after vendor incident

3. Risk-Based Approach:

- • Critical vendors: Full assessment, annual reviews, continuous monitoring
- • High-risk vendors: Full assessment, annual reviews
- • Medium-risk vendors: Standard assessment, biennial reviews
- • Low-risk vendors: Basic assessment, reviews as needed

4. Documentation Requirements:

- • Collect vendor certifications, policies, and documentation
- • Request SOC 2, ISO certifications, security assessments
- • Review contracts and SLAs carefully
- • Maintain evidence of vendor compliance

5. Decision Criteria:

- • Approved: Vendor meets all requirements, low risk
- • Conditional: Vendor approved with conditions or mitigations
- • Rejected: Vendor does not meet requirements, unacceptable risk
- • Pending: Additional information or assessment needed

THIRD-PARTY VENDOR ASSESSMENT

Assessment ID:	**[VA-YYYY-###]**
Assessment Date:	[DD/MM/YYYY]
Assessment Type:	☐Initial ☐Annual Review ☐Change ☐Incident-Triggered
Vendor Name:	[Full legal name]
Vendor Contact:	[Name, Title, Email, Phone]
Service/Product:	[Description of AI service/product]
Assessor Name:	[Name, Title]
Assessment Team:	[Additional team members]
Business Owner:	[Internal stakeholder requesting vendor]
Contract Value:	[$_____ annually]
Contract Duration:	[Start Date] to [End Date]
Previous Assessment:	[Date of last assessment or N/A]
Next Review Due:	[DD/MM/YYYY]

Section 1: Vendor Profile and Background

1.1 Company Information:

Legal Entity Name:	_____
Headquarters Location:	_____
Year Established:	_____
Number of Employees:	_____
Annual Revenue:	_____
Public/Private:	☐Public ☐Private ☐Government
Website:	_____
Primary Industry:	_____
Key Executives:	_____
Parent Company (if applicable):	_____

1.2 Financial Stability:

☐ Publicly traded - ticker: _____
☐ Privately held - funding rounds: _____
☐ Venture-backed - investors: _____
☐ Bootstrapped/Self-funded

Financial Health Assessment: ☐Strong ☐Stable ☐Concerns Identified
Notes: _____
_____

1.3 Reputation and References:
Industry Reputation: ☐Excellent ☐Good ☐Fair ☐Unknown
Notable Clients: _____
_____

References Checked: ☐Yes ☐No
Reference Feedback Summary: _____
_____

1.4 Legal and Regulatory Status:
☐ No known legal issues
☐ Pending litigation: _____
☐ Regulatory actions: _____
☐ Bankruptcy/financial distress: _____

Section 2: Service/Product Description

2.1 AI Service/Product Overview:
[Detailed description of the AI service or product being procured]
_____
_____
_____
_____

2.2 Service Type:
☐ AI Model/Algorithm (pre-trained)
☐ AI Platform/Infrastructure
☐ AI Development Tools/Framework
☐ AI-as-a-Service (SaaS)
☐ Data Processing/Annotation Services
☐ AI Consulting/Professional Services
☐ Model Training Services
☐ Other: _____

2.3 Data Handling:
Vendor handles our data: ☐Yes ☐No

If Yes, data types:
☐ Personal Data (PII)
☐ Sensitive Personal Data
☐ Proprietary Business Data
☐ Training Data
☐ Transaction Data
☐ Other: _____

Data residency/location: _____
Data retention period: _____

2.4 Integration Requirements:
Integration method: _____
APIs provided: ☐Yes ☐No
Customization required: ☐Yes ☐No
Technical dependencies: _____
_____
___

2.5 Service Criticality:
☐ Critical - Essential to operations, no alternatives
☐ High - Important, limited alternatives
☐ Medium - Important, alternatives available
☐ Low - Nice-to-have, easily replaceable

Section 3: AI Capabilities and Technical Assessment

3.1 Model/Algorithm Information:
Model type: _____
Model architecture: _____
Pre-trained model base: _____
Training data description: _____
_____

3.2 Performance Metrics:

Metric	Claimed Performance	Verified/Evidence
Accuracy	[Vendor claim]	☐Verified ☐Unverified
Precision/Recall	[Vendor claim]	☐Verified ☐Unverified
Latency/Response Time	[Vendor claim]	☐Verified ☐Unverified
Throughput	[Vendor claim]	☐Verified ☐Unverified
Uptime/Availability	[Vendor claim]	☐Verified ☐Unverified
Scalability	[Vendor claim]	☐Verified ☐Unverified

[Other metrics]		

3.3 Model Documentation:

Model card provided: ☐Yes ☐No ☐Partial
Technical documentation quality: ☐Excellent ☐Good ☐Fair ☐Poor
Training data disclosed: ☐Yes ☐No ☐Partial
Limitations documented: ☐Yes ☐No ☐Partial
Performance benchmarks provided: ☐Yes ☐No

3.4 Testing and Validation:
Vendor testing methodology: _____
_____

Independent validation conducted: ☐Yes ☐No ☐Planned
Pilot/POC results: _____
_____

3.5 Explainability and Interpretability:
Model interpretability: ☐High ☐Medium ☐Low ☐Black Box
Explanation methods available: _____
Explainability adequate for use case: ☐Yes ☐No ☐Partial

Section 4: Fairness, Bias, and Ethics Assessment

4.1 Bias Testing and Mitigation:

Bias testing conducted by vendor: ☐Yes ☐No ☐Unknown
Bias testing results provided: ☐Yes ☐No ☐N/A
Bias mitigation measures: _____
_____
___

4.2 Fairness Assessment:

Protected Characteristic	Tested by Vendor	Results/Findings
Age	☐Yes ☐No ☐Unknown	[Results if available]
Gender	☐Yes ☐No ☐Unknown	[Results if available]
Race/Ethnicity	☐Yes ☐No ☐Unknown	[Results if available]
Disability	☐Yes ☐No ☐Unknown	[Results if available]
[Other characteristics]		

4.3 Ethical AI Practices:

AI ethics policy/principles: ☐Published ☐Internal ☐None ☐Unknown
Ethics review board: ☐Yes ☐No ☐Unknown
Responsible AI certification: _____
Human rights impact assessment: ☐Conducted ☐Not Conducted ☐Unknown

4.4 Transparency Commitments:

Model changes communicated to customers: ☐Yes ☐No ☐Sometimes
Incident notification policy: ☐Yes ☐No ☐Unknown
Transparency reports published: ☐Yes ☐No

Section 5: Security Assessment

5.1 Security Certifications:

Certification/Standard	Status	Valid Until
SOC 2 Type II	☐Yes ☐No ☐In Progress	[Date]
ISO/IEC 27001	☐Yes ☐No ☐In Progress	[Date]
ISO/IEC 42001	☐Yes ☐No ☐In Progress	[Date]
FedRAMP (if applicable)	☐Yes ☐No ☐In Progress	[Date]
PCI DSS (if applicable)	☐Yes ☐No ☐In Progress	[Date]
HIPAA (if applicable)	☐Yes ☐No ☐In Progress	[Date]
[Other certifications]		

5.2 Security Controls:

Security Control	Implementation	Assessment
Data Encryption (at rest)	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Data Encryption (in transit)	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Access Controls (MFA, RBAC)	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Network Security	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Vulnerability Management	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Penetration Testing	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Security Monitoring/SIEM	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Incident Response Plan	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Disaster Recovery/BCP	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Security Training Program	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Model Security (adversarial)	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate
Supply Chain Security	☐Yes ☐No ☐Partial	☐Adequate ☐Inadequate

5.3 Security Incidents:
Known security breaches (last 3 years): ☐None ☐Yes - describe below
_____
_____

Incident notification SLA: _____
Public breach disclosures: ☐None found ☐Found - details: _____

Section 6: Privacy and Data Protection

6.1 Privacy Compliance:

Regulation/Standard	Compliance Status
GDPR	☐Compliant ☐Partial ☐N/A ☐Unknown
CCPA/CPRA	☐Compliant ☐Partial ☐N/A ☐Unknown
HIPAA (if applicable)	☐Compliant ☐Partial ☐N/A ☐Unknown
PIPEDA (Canada)	☐Compliant ☐Partial ☐N/A ☐Unknown
Other regional laws	☐Compliant ☐Partial ☐N/A ☐Unknown
[Specify applicable laws]	

6.2 Data Processing Terms:
Data Processing Agreement (DPA): ☐Yes ☐No ☐In negotiation
Standard Contractual Clauses (SCCs): ☐Yes ☐No ☐N/A
Data processing role: ☐Processor ☐Controller ☐Sub-processor
Data subject rights support: ☐Yes ☐No ☐Partial

6.3 Data Handling Practices:
Data minimization: ☐Practiced ☐Not Practiced ☐Unknown
Purpose limitation: ☐Enforced ☐Not Enforced ☐Unknown
Data retention policy: ☐Documented ☐Undocumented
Retention period: _____

Data deletion upon request: ☐Yes ☐No ☐With limitations
Data portability support: ☐Yes ☐No ☐N/A

6.4 Cross-Border Data Transfers:
Data stored in: _____
Data processed in: _____
Adequate jurisdiction: ☐Yes ☐No ☐With safeguards
Transfer mechanisms: _____

6.5 Sub-processors:
Uses sub-processors: ☐Yes ☐No
Sub-processor list provided: ☐Yes ☐No ☐N/A
Sub-processor changes notification: ☐Yes ☐No ☐N/A

Key sub-processors: _____
_____

Section 7: Governance and Compliance

7.1 AI Governance Framework:
Documented AI governance: ☐Yes ☐No ☐Partial
AI governance committee/board: ☐Yes ☐No ☐Unknown
AI risk management process: ☐Yes ☐No ☐Unknown
Model validation process: ☐Yes ☐No ☐Unknown

7.2 Regulatory Compliance:

Applicable Regulation	Compliance Status
EU AI Act (if applicable)	☐Compliant ☐Preparing ☐N/A
Industry-specific regulations	[Specify and status]
Export control compliance	☐Compliant ☐N/A
Accessibility requirements	☐Compliant ☐N/A
[Other regulations]	

7.3 Quality Management:
Quality management system: ☐ISO 9001 ☐Other ☐None
Continuous improvement process: ☐Yes ☐No
Customer feedback mechanism: ☐Yes ☐No

7.4 Audit Rights:
Customer audit rights: ☐Yes ☐Limited ☐No
Third-party audit frequency: _____
Audit reports shared: ☐Yes ☐Summary only ☐No

7.5 Insurance Coverage:
Professional liability insurance: ☐Yes ☐No
Cyber insurance: ☐Yes ☐No
Coverage amount: $_____
Certificate of insurance provided: ☐Yes ☐No ☐Requested

Section 8: Contractual and Legal Assessment

8.1 Contract Terms Review:

Contract Element	Status/Assessment
Service Level Agreement (SLA)	☐Acceptable ☐Needs Negotiation ☐Missing
Performance Guarantees	☐Acceptable ☐Needs Negotiation ☐Missing
Liability and Indemnification	☐Acceptable ☐Needs Negotiation ☐Missing
Data Ownership	☐Clear ☐Ambiguous ☐Unacceptable
IP Rights	☐Acceptable ☐Needs Negotiation ☐Missing
Termination Rights	☐Acceptable ☐Needs Negotiation ☐Missing
Data Return/Deletion	☐Acceptable ☐Needs Negotiation ☐Missing
Dispute Resolution	☐Acceptable ☐Needs Negotiation ☐Missing
Change Management Process	☐Acceptable ☐Needs Negotiation ☐Missing

8.2 Service Level Agreement (SLA):

SLA Metric	Committed Level	Penalty/Remedy
Availability/Uptime	[e.g., 99.9%]	[Credit/refund]
Response Time	[Time]	[Remedy]
Support Response	[Time by severity]	[Remedy]
Incident Resolution	[Time by severity]	[Remedy]
[Other SLA metrics]		

8.3 Liability and Insurance:

Liability cap: $_____

Uncapped liability for: _____

Indemnification scope: ☐Adequate ☐Limited ☐Inadequate

8.4 Exit Strategy:

Termination notice period: _____

Data transition assistance: ☐Yes ☐No ☐For fee

Transition period: _____

Alternative vendors identified: ☐Yes ☐No

Section 9: Operational and Support Assessment

9.1 Support and Service:

Support Element	Details
Support Hours	[24/7, business hours, etc.]
Support Channels	[Phone, email, portal, chat]
Dedicated Support	☐Yes ☐No ☐For premium tier
Technical Account Manager	☐Yes ☐No ☐For enterprise tier
Escalation Process	[Documented: ☐Yes ☐No]

9.2 Change Management:

Model update notification: ☐Advance notice ☐Post-deployment ☐None
Notice period for updates: _____
Customer approval for major changes: ☐Yes ☐No
Rollback capability: ☐Yes ☐No ☐Limited

9.3 Monitoring and Reporting:

Performance dashboards provided: ☐Yes ☐No
Regular reports: ☐Yes ☐No - Frequency: _____
Custom reporting available: ☐Yes ☐No ☐For fee
Audit logs accessible: ☐Yes ☐No ☐Limited

9.4 Business Continuity:

Disaster recovery plan: ☐Yes ☐No ☐Unknown
Recovery Time Objective (RTO): _____
Recovery Point Objective (RPO): _____
Backup frequency: _____
Redundancy/failover: ☐Yes ☐No ☐Partial

9.5 Vendor Viability and Dependencies:

Key person dependencies: ☐Low ☐Medium ☐High
Technology dependencies: _____
_____
___
Vendor lock-in risk: ☐Low ☐Medium ☐High
Exit/migration difficulty: ☐Easy ☐Moderate ☐Difficult

Section 10: Risk Assessment and Scoring

10.1 Risk Category Scores:

Risk Category	Score (1-5)	Weight	Weighted Score
Technical Performance	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Security Posture	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Privacy Compliance	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Fairness & Bias Controls	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Governance & Compliance	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Vendor Stability	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Contractual Terms	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Support & Service	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
Transparency & Documentation	[1=Poor, 5=Excellent]	[%]	[Auto-calc]
TOTAL SCORE		100%	[Sum]

10.2 Overall Risk Rating:

[Based on total weighted score and qualitative factors]

☐ Low Risk (Score > 4.0)
☐ Medium Risk (Score 3.0-4.0)
☐ High Risk (Score 2.0-2.9)
☐ Critical Risk (Score < 2.0)

10.3 Key Risk Factors:
[List top 3-5 risk factors identified]
- _____
- _____
- _____
- _____

10.4 Risk Mitigation Plan:

Risk	Mitigation Strategy	Responsibility
[Risk 1]	[Mitigation approach]	[Vendor/Us/Shared]
[Risk 2]	[Mitigation approach]	[Responsibility]
[Risk 3]	[Mitigation approach]	[Responsibility]
[Add rows as needed]		

Section 11: Recommendation and Decision

11.1 Assessment Summary:
[Brief summary of key findings - strengths and concerns]
_____
___
_____
___
_____
___
_____
___

11.2 Recommendation:
☐ Approve - Vendor meets all requirements
☐ Conditional Approval - Approve with conditions/mitigations specified below
☐ Reject - Vendor does not meet requirements
☐ Pending - Additional information/assessment required

11.3 Conditions/Requirements (if conditional approval):
• _____
• _____
• _____

11.4 Ongoing Monitoring Requirements:

Review frequency: ☐Quarterly ☐Semi-annually ☐Annually ☐As needed
Performance metrics to monitor: _____
_____
Audit schedule: _____
Escalation triggers: _____

11.5 Approval Required From:

☐ IT/Technology Leadership
☐ Information Security
☐ Legal/Compliance
☐ Privacy Office
☐ AI Governance Committee
☐ Procurement
☐ Executive Management

Section 12: Approvals and Sign-Off

Role	Name	Decision	Date/Signature
Assessor	[Name]	[Recommendation]	_____/_____
Business Owner	[Name]	☐Approve ☐Reject	_____/_____
IT/Technology	[Name]	☐Approve ☐Reject	_____/_____
Information Security	[Name]	☐Approve ☐Reject	_____/_____
Legal/Compliance	[Name]	☐Approve ☐Reject	_____/_____
AI Governance	[Name]	☐Approve ☐Reject	_____/_____
Final Approval	[Name/Title]	☐Approve ☐Reject	_____/_____

END OF VENDOR ASSESSMENT

Document Information:
Template Version: 1.0
Template Owner: AI Governance Office / Procurement / Information Security
Classification: Internal - Vendor Evaluation
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001
Retention: 7 years after vendor relationship ends

Template F.12
AI Data Management Plan

Integrated AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001 Framework

Purpose and Scope

Purpose: This template provides a comprehensive framework for managing data throughout the AI system lifecycle. It ensures data quality, security, privacy, and compliance with framework requirements from collection through disposal.
Framework Alignment:

- **AI RMF 2026:** MAP-2.1 through MAP-2.3 (Data quality and management), MEASURE-2.1 through 2.4 (Data measurement), MANAGE-3.2 (Data management)
- **ISO/IEC 42001:** Clause 7.4 (Communication), Clause 8.1 (Operational planning and control), Annex A (Data management controls)
- **ISO/IEC 27001:** Clause 8.1 (Operational planning), Annex A.5.10 (Information management), Annex A.8.3 (Information backup)

Instructions for Use

1. When to Create:

- • At the beginning of every AI project
- • Before data collection or acquisition
- • As part of AI system design documentation
- • When data sources or usage changes significantly

2. Plan Maintenance:

- • Review and update quarterly or when changes occur
- • Document all changes in revision history
- • Obtain approval for significant changes
- • Maintain version control

3. Data Lifecycle Coverage:

- This plan covers all phases:
- - Planning and requirements
- - Collection and acquisition
- - Preprocessing and transformation
- - Storage and security
- - Usage and access
- - Quality assurance and validation
- - Retention and archival
- - Disposal and deletion

4. Stakeholder Involvement:

- • Involve data owners, privacy office, legal, security
- • Consult subject matter experts
- • Include business stakeholders
- • Engage compliance and governance teams

5. Compliance Requirements:

- • Ensure alignment with privacy laws (GDPR, CCPA, etc.)
- • Address industry-specific regulations
- • Follow organizational data policies
- • Document all compliance considerations

AI DATA MANAGEMENT PLAN

Plan ID:	**[DMP-YYYY-###]**
Plan Version:	[1.0]
Plan Date:	[DD/MM/YYYY]
AI System/Project:	[System name and ID]
Data Owner:	[Name, Title, Department]
Data Steward:	[Name, Title, Department]
Plan Author:	[Name, Title]
Project Manager:	[Name, Title]
Review Frequency:	☐Quarterly ☐Semi-annually ☐Annually ☐As needed
Next Review Date:	[DD/MM/YYYY]
Plan Status:	☐Draft ☐Approved ☐Active ☐Archived

Section 1: Executive Summary

1.1 Purpose of Data Management Plan:
[Brief description of why this plan exists and what it governs]

_____
_____
_____

1.2 AI System Context:
[Brief description of the AI system that will use this data]

_____
___
_____
___

1.3 Data Overview:
Types of data: _____
Volume of data: _____
Data sources: _____
Data sensitivity: ☐Public ☐Internal ☐Confidential ☐Highly Sensitive

1.4 Key Stakeholders:

Role	Name/Department	Responsibility
Data Owner	[Name]	Overall accountability
Data Steward	[Name]	Day-to-day management
Data Custodian	[Name/Team]	Technical administration
Privacy Officer	[Name]	Privacy compliance
Security Officer	[Name]	Data security
[Other stakeholders]		

Section 2: Data Inventory and Classification

2.1 Data Asset Inventory:

[List all datasets used by the AI system]

Dataset Name	Description	Source	Format	Volume	Classification
[Dataset 1]	[Description]	[Source]	[CSV/JSON/DB/etc.]	[Size/Records]	[Classification]
[Dataset 2]	[Description]	[Source]	[Format]	[Volume]	[Classification]
[Dataset 3]	[Description]	[Source]	[Format]	[Volume]	[Classification]
[Dataset 4]	[Description]	[Source]	[Format]	[Volume]	[Classification]
[Add rows as needed]					

2.2 Data Classification Framework:

Classification Level	Definition	Applies To
Public	No restrictions on disclosure	☐Yes ☐No
Internal	Organization use only	☐Yes ☐No
Confidential	Sensitive business data	☐Yes ☐No
Highly Sensitive	Personal data, trade secrets	☐Yes ☐No

2.3 Data Sensitivity Assessment:

Contains Personal Data (PII): ☐Yes ☐No
Contains Sensitive Personal Data: ☐Yes ☐No
Contains Protected Health Information (PHI): ☐Yes ☐No
Contains Financial Information: ☐Yes ☐No
Contains Proprietary/Trade Secret Data: ☐Yes ☐No
Contains Biometric Data: ☐Yes ☐No
Other sensitive categories: _____

2.4 Data Elements and Schema:

[List key data fields/features and their characteristics]

Field/Feature Name	Data Type	Sensitivity	Purpose	Required/Optional
[Field 1]	[String/Int/Float/etc.]	[High/Med/Low]	[Purpose]	☐Required ☐Optional

[Field 2]	[Type]	[Sensitivity]	[Purpose]	☐Required ☐Optional
[Field 3]	[Type]	[Sensitivity]	[Purpose]	☐Required ☐Optional
[Field 4]	[Type]	[Sensitivity]	[Purpose]	☐Required ☐Optional
[Add rows as needed - attach detailed schema separately if extensive]				

Section 3: Data Collection and Acquisition

3.1 Data Sources:

Source	Type	Collection Method	Frequency	Authorization
[Source 1]	☐Internal ☐External ☐Third-party	[API/Manual/Automated/etc.]	[Real-time/Daily/etc.]	☐Yes ☐No ☐N/A
[Source 2]	☐Internal ☐External ☐Third-party	[Method]	[Frequency]	☐Yes ☐No ☐N/A
[Source 3]	☐Internal ☐External ☐Third-party	[Method]	[Frequency]	☐Yes ☐No ☐N/A
[Source 4]	☐Internal ☐External ☐Third-party	[Method]	[Frequency]	☐Yes ☐No ☐N/A
[Add rows as needed]				

3.2 Data Collection Methods:

[Describe how data is collected or acquired]

_____
_____
_____

3.3 Legal Basis for Data Collection:
☐ Consent
☐ Contractual necessity
☐ Legal obligation
☐ Legitimate interest
☐ Public interest
☐ Other: _____

Documentation of legal basis: _____
_____

3.4 Third-Party Data Providers:

Provider Name	Data Provided	Contract/Agreement	DPA in Place
[Provider 1]	[Description]	☐Yes - Ref: _____	☐Yes ☐No ☐N/A
[Provider 2]	[Description]	☐Yes - Ref: _____	☐Yes ☐No ☐N/A
[Provider 3]	[Description]	☐Yes - Ref: _____	☐Yes ☐No ☐N/A
☐ **N/A - No third-party providers**			

3.5 Data Lineage and Provenance:
[Document the origin and chain of custody for data]
_____
_____
_____

3.6 Consent and Transparency:
User consent obtained: ☐Yes ☐No ☐N/A
Consent mechanism: _____
Privacy notice provided: ☐Yes ☐No ☐N/A
Data subjects informed of AI use: ☐Yes ☐No ☐N/A

Section 4: Data Quality Management

4.1 Data Quality Objectives:

Quality Dimension	Target/Requirement	Measurement Method
Accuracy	[Target %]	[How measured]
Completeness	[Target %]	[How measured]
Consistency	[Requirement]	[How measured]
Timeliness	[Requirement]	[How measured]
Validity	[Requirement]	[How measured]
Uniqueness	[Requirement]	[How measured]
Representativeness	[Requirement]	[How measured]

4.2 Data Quality Assessment Process:

Assessment frequency: ☐Continuous ☐Daily ☐Weekly ☐Monthly ☐Quarterly
Assessment method: _____
Responsible party: _____
Documentation location: _____

4.3 Data Validation Rules:

[Define validation rules and constraints]

- _____
- _____
- _____
- _____

4.4 Data Quality Issues and Remediation:
Issue detection method: _____
Issue tracking system: _____
Remediation process: _____
_____
Escalation criteria: _____

4.5 Data Profiling and Monitoring:
Profiling tools: _____
Monitoring dashboard: ☐Yes ☐No ☐Planned
Alerting configured: ☐Yes ☐No
Alert recipients: _____

Section 5: Data Preprocessing and Transformation

5.1 Data Preprocessing Steps:
[Document all preprocessing and transformation steps]

Step	Description	Tool/Method	Rationale
1. [e.g., Data Cleaning]	[Description]	[Tool/Script]	[Why]
2. [e.g., Normalization]	[Description]	[Tool/Script]	[Why]
3. [e.g., Feature Engineering]	[Description]	[Tool/Script]	[Why]
4. [Step]	[Description]	[Tool/Script]	[Why]
[Add rows as needed]			

5.2 Data Anonymization/Pseudonymization:
Anonymization required: ☐Yes ☐No ☐N/A
Anonymization technique: _____
Pseudonymization used: ☐Yes ☐No ☐N/A
Re-identification risk assessed: ☐Yes ☐No ☐N/A
Risk level: ☐Low ☐Medium ☐High

5.3 Data Augmentation:
Data augmentation used: ☐Yes ☐No
Augmentation techniques: _____
_____
Augmentation rationale: _____

5.4 Feature Engineering:
[Document derived features and transformations]
_____
_____
_____

5.5 Data Splitting Strategy:
Training set: _____% (_____records)
Validation set: _____% (_____records)
Test set: _____% (_____records)
Splitting method: ☐Random ☐Stratified ☐Time-based ☐Other: _____
Random seed (if applicable): _____

5.6 Preprocessing Pipeline Documentation:
Pipeline code location: _____
Pipeline version control: ☐Yes ☐No
Pipeline testing: ☐Yes ☐No
Pipeline reproducibility verified: ☐Yes ☐No

Section 6: Data Storage and Security

6.1 Storage Infrastructure:

Data Type	Storage System	Location	Backup
Raw Data	[Database/S3/etc.]	[Region/DC]	☐Yes ☐No
Processed Data	[System]	[Location]	☐Yes ☐No
Training Data	[System]	[Location]	☐Yes ☐No
Production Data	[System]	[Location]	☐Yes ☐No

6.2 Data Security Controls:

Security Control	Implementation
Encryption at Rest	☐Yes - Method: _____ ☐No
Encryption in Transit	☐Yes - Protocol: _____ ☐No
Access Controls	☐RBAC ☐ABAC ☐Other: _____
Authentication	☐MFA ☐SSO ☐Password ☐Other
Network Security	☐Firewall ☐VPN ☐Private Network
Data Masking	☐Yes - Fields: _____ ☐No
Audit Logging	☐Yes ☐No
Intrusion Detection	☐Yes ☐No
Data Loss Prevention (DLP)	☐Yes ☐No

6.3 Access Management:

Role/Group	Access Level	Justification
[Role 1]	☐Read ☐Write ☐Admin	[Justification]
[Role 2]	☐Read ☐Write ☐Admin	[Justification]
[Role 3]	☐Read ☐Write ☐Admin	[Justification]
[Role 4]	☐Read ☐Write ☐Admin	[Justification]
[Add rows as needed]		

6.4 Backup and Recovery:
Backup frequency: _____
Backup retention period: _____
Backup location: _____
Backup encryption: ☐Yes ☐No
Recovery Time Objective (RTO): _____
Recovery Point Objective (RPO): _____
Recovery testing frequency: _____
Last recovery test date: _____

6.5 Data Residency and Sovereignty:
Data storage location(s): _____
Cross-border transfers: ☐Yes ☐No
If yes, transfer mechanism: _____
Compliance with data localization laws: ☐Yes ☐No ☐N/A

Section 7: Data Governance and Compliance

7.1 Applicable Regulations and Standards:

Regulation/Standard	Applicable	Compliance Measures
GDPR	☐Yes ☐No	[Measures implemented]
CCPA/CPRA	☐Yes ☐No	[Measures]
HIPAA	☐Yes ☐No	[Measures]
PCI DSS	☐Yes ☐No	[Measures]
Industry-specific regulations	☐Yes ☐No	[Specify and measures]
Organizational data policies	☐Yes ☐No	[Policies followed]
[Other applicable regulations]		

7.2 Data Subject Rights:

[How will data subject rights be honored?]

Right	Implementation
Right to Access	[Process to provide access]
Right to Rectification	[Process to correct data]
Right to Erasure	[Process to delete data]
Right to Restriction	[Process to restrict processing]
Right to Portability	[Process to export data]
Right to Object	[Process to object to processing]
Right to Opt-out (CCPA)	[Process to opt-out]
Request handling SLA: _____	

7.3 Data Protection Impact Assessment (DPIA):

DPIA required: ☐Yes ☐No

DPIA completed: ☐Yes ☐No ☐Not Required

DPIA date: _____

DPIA reference: _____

High privacy risk identified: ☐Yes ☐No

Mitigations implemented: _____

7.4 Data Ethics Considerations:

[Ethical considerations for data use]

_____

_____

_____

7.5 Data Sharing and Disclosure:

Data shared with third parties: ☐Yes ☐No
If yes, recipients: _____
Data sharing agreements in place: ☐Yes ☐No ☐N/A
Purpose of sharing: _____
Legal basis for sharing: _____

Section 8: Data Retention and Disposal

8.1 Data Retention Policy:

Data Type	Retention Period	Retention Rationale	Legal/Regulatory Basis
Raw Data	[Period]	[Rationale]	[Basis]
Training Data	[Period]	[Rationale]	[Basis]
Model Output/Predictions	[Period]	[Rationale]	[Basis]
Logs and Audit Trails	[Period]	[Rationale]	[Basis]
[Other data types]			

8.2 Retention Review Process:

Review frequency: ☐Annually ☐Bi-annually ☐Other: _____
Review responsibility: _____
Retention policy location: _____

8.3 Data Disposal Procedures:

Disposal method for electronic data: _____
Disposal method for physical media: _____
Secure deletion verification: ☐Yes ☐No
Disposal certification: ☐Required ☐Not Required
Disposal logging: ☐Yes ☐No

8.4 Archival Strategy:
Data archival required: ☐Yes ☐No
Archival criteria: _____
Archival location: _____
Archival format: _____
Archive access process: _____

8.5 Legal Hold and Litigation Support:
Legal hold process: _____
Responsible party: _____
e-Discovery support: ☐Planned ☐Not Planned

Section 9: Data Documentation and Metadata

9.1 Data Documentation:
Data dictionary: ☐Yes ☐No ☐In Progress
Data dictionary location: _____
Schema documentation: ☐Yes ☐No ☐In Progress
Data lineage diagrams: ☐Yes ☐No ☐In Progress
Documentation format: _____

9.2 Metadata Management:
Metadata captured: ☐Yes ☐No ☐Partial
Metadata standards used: _____

Key metadata fields:
☐ Data source
☐ Collection date/time
☐ Data owner
☐ Data classification
☐ Data quality metrics
☐ Versioning information
☐ Transformation history
☐ Usage statistics

9.3 Version Control:
Data versioning: ☐Yes ☐No
Versioning system: _____
Version naming convention: _____
Change tracking: ☐Yes ☐No

9.4 Data Catalog:
Centralized data catalog: ☐Yes ☐No ☐In Progress
Catalog tool: _____
Catalog accessibility: _____

Section 10: Monitoring and Continuous Improvement

10.1 Data Monitoring Plan:

What to Monitor	Frequency	Responsible Party	Action if Issue Found
Data Quality Metrics	[Frequency]	[Name/Role]	[Action]
Data Drift	[Frequency]	[Name/Role]	[Action]
Access Patterns	[Frequency]	[Name/Role]	[Action]
Security Events	[Frequency]	[Name/Role]	[Action]
Compliance Status	[Frequency]	[Name/Role]	[Action]
[Other monitoring]			

10.2 Performance Metrics:

[Define KPIs for data management]

- _____
- _____
- _____

10.3 Continuous Improvement Process:

Review meetings: ☐Monthly ☐Quarterly ☐Annually
Improvement tracking: _____
Lessons learned documentation: ☐Yes ☐No

10.4 Incident Management:

Data incident definition: _____
Incident reporting process: _____
Incident response plan reference: _____

Section 11: Roles and Responsibilities

Role	Name/Department	Responsibilities
Data Owner	[Name]	Overall accountability, approve policies
Data Steward	[Name]	Day-to-day management, quality oversight
Data Custodian	[Name/Team]	Technical implementation, storage, backup
Data Engineer	[Name/Team]	Pipeline development, ETL processes
Data Scientist	[Name/Team]	Data analysis, feature engineering
Privacy Officer	[Name]	Privacy compliance, DPIA oversight
Security Officer	[Name]	Security controls, access management
Compliance Officer	[Name]	Regulatory compliance oversight
Legal Counsel	[Name]	Legal review, contracts, rights requests
[Other roles]		

Section 12: Plan Approval and Maintenance

12.1 Approval Signatures:

Role	Name	Date/Signature
Plan Author	[Name]	_____/_____
Data Owner	[Name]	_____/_____
Privacy Officer	[Name]	_____/_____
Security Officer	[Name]	_____/_____
Legal/Compliance	[Name]	_____/_____
AI Governance	[Name]	_____/_____

12.2 Revision History:

Version	Date	Changes Made	Author
1.0	[Date]	Initial plan	[Name]
[Version]	[Date]	[Description of changes]	[Name]
[Version]	[Date]	[Description]	[Name]
[Add rows for each revision]			

END OF DATA MANAGEMENT PLAN

Document Information:
Template Version: 1.0
Template Owner: AI Governance Office / Data Governance / Information Security
Classification: Internal - Data Management
Framework Alignment: AI RMF 2026, ISO/IEC 42001, ISO/IEC 27001
Review and update plan quarterly or when significant changes occur

Appendix G

Glossary - Unified Terminology

AI RMF 2026, ISO/IEC 42001, and ISO/IEC 27001
Version 1.0 | January 2026

Introduction

This unified glossary harmonizes terminology across AI Risk Management Framework, ISO/IEC 42001:2023, and ISO/IEC 27001:2022. Terms are presented with their source standard(s) and unified definitions for consistent implementation.

Notation

Code	Source
[N]	AI Risk Management Framework
[42]	ISO/IEC 42001:2023 (AI Management Systems)
[27]	ISO/IEC 27001:2022 (Information Security Management)
[U]	Unified definition harmonizing all applicable standards

Terms and Definitions

A

Accountability
[N][42] The property of being responsible for decisions and actions to affected parties or stakeholders. In AI systems, includes clear assignment of roles, responsibilities, and authority for AI governance, risk management, and system performance.

Adversarial Attack
[N][27] Deliberate attempt to compromise AI system integrity through input manipulation, model poisoning, or exploitation of system vulnerabilities. May target confidentiality, integrity, or availability.

AI Actor
[N] Individual or organization involved in at least one stage of the AI system lifecycle. Includes developers, deployers, operators, evaluators, policy makers, and end users.

AI Impact Assessment
[42][U] Systematic evaluation of potential AI system impacts on individuals, groups, communities, organizations, and society. Addresses technical, ethical, social, legal, and human rights considerations throughout the AI lifecycle.

AI Management System (AIMS)
[42] Management system specifically for artificial intelligence, consisting of policies, procedures, processes, and resources for establishing, implementing, maintaining, and continually improving AI governance and trustworthiness.

AI Model
[N][42] Component of an AI system implementing machine learning, logic and knowledge-based approaches, or statistical methods to generate outputs from inputs. May be trained, manually engineered, or combinations thereof.

AI System
[N][42][U] Engineered or machine-based system that generates outputs such as predictions, recommendations, decisions, or content for a given set of objectives. Includes the AI model plus supporting components (data, infrastructure, interfaces, human oversight mechanisms).

AI System Lifecycle
[N][42] Stages through which an AI system progresses from initial conception through decommissioning. Typically includes: planning and design, data collection and processing, model development, verification and validation, deployment, operation and monitoring, and retirement.

Asset
[27][42] Anything of value to the organization. In AI context, includes data, AI models, algorithms, training infrastructure, documentation, intellectual property, and supporting IT systems.

B

Bias (AI)
[N][U] Systematic and repeatable errors in AI systems that create unfair outcomes. May arise from data, algorithms, human decisions, or feedback loops. Distinguished from statistical bias (variance from true value).

C

Competence
[42][27] Ability to apply knowledge and skills to achieve intended results. In AI context, includes technical expertise, understanding of AI risks, awareness of ethical considerations, and capability to perform assigned AI management roles.

Conformity Assessment
[42] Demonstration that specified requirements relating to an AI system, process, or management system are fulfilled. May include testing, inspection, certification, or validation activities.

Continual Improvement
[42][27] Recurring activity to enhance performance and effectiveness. Applied to AI systems, processes, and management systems through monitoring, measurement, corrective actions, and incorporation of lessons learned.

Control
[27][42][U] Measure that modifies risk. In information security, maintains or improves confidentiality, integrity, and availability. In AI management, addresses trustworthiness characteristics and manages AI-specific risks throughout the lifecycle.

D

Data Governance
[N][42][27] System of decision rights and accountabilities for data-related processes. Ensures data quality, availability, usability, integrity, and security throughout the AI lifecycle.

Data Quality
[N][42] Degree to which data meets requirements for its intended use. Dimensions include accuracy, completeness, consistency, timeliness, validity, representativeness, and relevance for AI system objectives.

Deployment
[N][42] Process of integrating an AI system into production environment and making it available for intended use. Includes installation, configuration, testing, and transition to operational state.

Documented Information
[42][27] Information required to be controlled and maintained by the organization, and the medium on which it is contained. Includes policies, procedures, plans, records, and evidence of activities performed.

E

Effectiveness
[42][27] Extent to which planned activities are realized and planned results achieved. Measured through performance indicators, audit results, and achievement of AI management objectives.

Equity
[N] Just and impartial treatment across demographic groups. In AI context, addresses both equal treatment (procedural fairness) and equal outcomes (distributive fairness).

Explainability
[N][U] Property of an AI system whereby humans can understand its decision-making process. Includes technical explanations (how the system works) and outcome explanations (why specific outputs were produced).

F

Fairness
[N][42] Property of an AI system whereby it does not discriminate against or systematically disadvantage individuals or groups. Encompasses both individual fairness (similar individuals treated similarly) and group fairness (equitable outcomes across demographic groups).

G

Governance
[N][42][27] System of structures, policies, processes, and practices by which an organization directs and controls its activities. AI governance specifically addresses responsible development, deployment, and use of AI systems.

H

Hallucination
[N] AI system output that appears plausible but is factually incorrect or nonsensical. Common in generative AI systems, particularly large language models.

Harm
[N][42] Physical, psychological, financial, social, or other adverse impact on individuals, groups, communities, organizations, or society. May be direct or indirect, immediate, or delayed.

Human Oversight
[N][42][U] Governance mechanism ensuring appropriate human involvement in AI system decision-making. Includes human-in-the-loop (active involvement), human-on-the-loop (monitoring with intervention capability), and human-in-command (high-level governance).

I

Impact
[N][42][27] Consequence of an event or action affecting objectives. May be positive (benefits) or negative (harms). Evaluated across multiple dimensions: individuals, organizations, society, environment.

Incident
[27][42][N] Single or series of events that has caused or could cause harm, service disruption, or other adverse consequences. In AI context, includes performance failures, security breaches, fairness issues, and safety events.

Information Security
[27][42] Preservation of confidentiality, integrity, and availability of information. Extended for AI systems to include model confidentiality, training data protection, and inference integrity.

Interested Party (Stakeholder)
[42][27] Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. In AI context, includes developers, deployers, end users, impacted individuals, regulators, and civil society.

Interpretability
[N] Degree to which a human can understand the cause of a decision made by an AI system. Related to but distinct from explainability; focuses on model transparency and feature importance.

L

Lifecycle
[N][42] See AI System Lifecycle.

M

Management System
[42][27] Set of interrelated elements to establish policies, objectives, processes, and procedures to achieve objectives. AI Management Systems integrate with or extend existing Information Security Management Systems.

Monitoring
[N][42][27] Determining the status of a system, process, or activity. For AI systems, includes performance tracking, data quality assessment, fairness evaluation, and detection of distribution shifts or concept drift.

N

Nonconformity
[42][27] Non-fulfillment of a requirement. Identified through audits, assessments, monitoring, or incident investigation. Requires corrective action to prevent recurrence.

O

Objective
[42][27] Result to be achieved. AI management objectives are consistent with AI policy and contribute to organizational goals.

P

Performance
[42][27][N] Measurable result. For AI systems, encompasses technical metrics (accuracy, precision, recall), trustworthiness characteristics (fairness, robustness), and operational effectiveness.

Privacy
[N][27] Right of individuals to control collection, use, and disclosure of their personal information. AI-specific considerations include data minimization, purpose limitation, and protection against re-identification.

R

Reliability
[N] Ability of an AI system to consistently perform its intended function under specified conditions. Related to but distinct from robustness; focuses on consistency over time.

Resilience
[N][42] Ability of an AI system to withstand, adapt to, and recover from adverse conditions, attacks, or failures. Includes technical resilience (system recovery) and operational resilience (business continuity).

Risk
[N][42][27][U] Effect of uncertainty on objectives. Characterized by likelihood and impact. AI risks may affect individuals, organizations, society, or the environment across multiple dimensions (technical, ethical, legal, social).

Risk Assessment
[42][27][N] Overall process of risk identification, risk analysis, and risk evaluation. For AI systems, considers technical risks, trustworthiness concerns, and broader societal impacts.

Risk Treatment
[42][27] Process of selecting and implementing measures to modify risk. Options include: avoid (eliminate activity), reduce (implement controls), transfer (share with third parties), accept (informed decision to retain risk).

Robustness
[N][42] Ability of an AI system to maintain performance under varying conditions, including distributional shifts, adversarial inputs, and edge cases. Includes both technical robustness and adversarial robustness.

S

Safety
[N][42] Condition where AI systems do not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered. Encompasses both physical safety and broader societal safety.

Security (AI)
[N][42][27] Protection of AI systems, models, and data from unauthorized access, disclosure, manipulation, or destruction. Includes model security, data security, and infrastructure security against AI-specific attacks.

Stakeholder
[N][42][27] See Interested Party.

T

Third Party
[42][27] Person or body that is independent of the organization and interested parties. In AI context, includes external auditors, certification bodies, AI system vendors, and data processors.

Threat
[27][42] Potential cause of an unwanted incident, which may result in harm. AI-specific threats include adversarial attacks, data poisoning, model theft, and exploitation of algorithmic vulnerabilities.

Traceability
[N][42] Ability to trace the history, application, or location of an object or activity. For AI systems, includes data lineage, model provenance, decision trails, and change history.

Training Data
[N][42] Data used to train a machine learning model. Quality, representativeness, and governance of training data are critical factors in AI system trustworthiness.

Transparency
[N][42][U] Property of an AI system whereby information about the system, its capabilities, limitations, and decision-making processes is made available to stakeholders. Includes documentation, disclosure, and explainability mechanisms.

Trustworthiness
[N][42] Degree to which an AI system demonstrates characteristics warranting trust. AI RMF identifies seven characteristics: valid and reliable, safe, secure, and resilient, accountable, and transparent, explainable, and interpretable, privacy-enhanced, and fair (with harmful bias managed).

V

Validation
[N][42][27] Confirmation through provision of objective evidence that requirements for a specific intended use or application have been fulfilled. For AI systems, demonstrates fitness for purpose in operational environment.

Verification
[N][42][27] Confirmation through provision of objective evidence that specified requirements have been fulfilled. For AI systems, confirms correct implementation and technical specification compliance.

Vulnerability
[27][N] Weakness that can be exploited by threats to cause harm. AI-specific vulnerabilities include adversarial susceptibility, data distribution assumptions, and model architecture limitations.

Document Control

Document Information	Details
Document Title	Appendix G: Unified Glossary
Version	1.0
Date	January 2026
Author	AI RMF 2026 Integration Project
Classification	Public
Purpose	Harmonize terminology across AI RMF 2026, ISO 42001, and ISO 27001

End of Appendix H

Appendix I

Evidence Repository Structure

For ISO 42001 and ISO 27001 Certification Audits
Version 1.0 | January 2026

Introduction

This appendix provides a recommended structure for organizing audit evidence to support ISO/IEC 42001 and ISO/IEC 27001 certification. A well-organized evidence repository streamlines the audit process, reduces audit time, and demonstrates management system maturity.

Key Principles

- **Logical Organization**: Evidence grouped by ISO clause and control category
- **Version Control:** All documents versioned with change tracking
- **Access Control:** Role-based access aligned with confidentiality requirements
- **Auditability:** Clear audit trails for all evidence creation and modification
- **Retention:** Evidence retained per policy requirements (minimum 3 years for certification)

Recommended Repository Structure

Level 1: Management System Foundation

Folder	Contents
01_Policies	AI Management System Policy (ISO 42001 5.2) Information Security Policy (ISO 27001 5.2) Supporting policies: Data Governance, Risk Management, Ethics
02_Context	AIMS Scope document (ISO 42001 4.3, 4.4) ISMS Scope document (ISO 27001 4.3) Stakeholder analysis and needs assessment External and internal issues register
03_Leadership	Leadership commitment evidence (meeting minutes, directives) RACI matrix: Roles, Responsibilities, Authorities (ISO 42001 5.3) Organizational structure charts Job descriptions for key AI/security roles

Level 2: Planning and Risk Management

Folder	Contents
04_Risk_Management	Risk assessment methodology (ISO 42001 6.1.2, ISO 27001 6.1.2) AI risk register with AI RMF 2026 mappings Information security risk register AI impact assessments (ISO 42001 6.1.3) Risk treatment plans Statement of Applicability (SoA) - ISO 27001 Annex A controls
05_Objectives	AI management objectives (ISO 42001 6.2) Information security objectives (ISO 27001 6.2) Plans to achieve objectives Progress tracking and measurement

Level 3: Support and Resources

Folder	Contents
06_Competence	Competency framework and requirements Training programs and materials Training records and attendance Certifications and qualifications Awareness program evidence
07_Documentation	Document control procedure (ISO 42001/27001 7.5) Document register and master list Records retention schedule Communication plan and evidence

Level 4: Operational Implementation

Folder	Contents
08_AI_Systems	AI system inventory/register (ISO 42001 8.1) System documentation by lifecycle stage Data quality and governance records Model cards and technical documentation Validation and testing reports Deployment records and approvals
09_Controls	ISO 42001 Annex A control implementation evidence ISO 27001 Annex A control implementation evidence Control testing results Control effectiveness reviews
10_Third_Parties	Supplier and vendor assessment records Third-party contracts with AI/security clauses External service monitoring Vendor audit reports

Level 5: Performance and Improvement

Folder	Contents
11_Monitoring	Performance metrics and KPIs Monitoring reports and dashboards AI system performance tracking Risk monitoring results Compliance monitoring evidence
12_Audits	Internal audit program and schedule Internal audit reports Corrective action tracking Previous certification audit reports Surveillance audit evidence
13_Management_Review	Management review agenda and schedule Management review meeting minutes Management review action items Strategic decisions and direction
14_Incidents	Incident response procedure Incident logs and reports Post-incident reviews Lessons learned
15_Improvement	Nonconformity and corrective action register Root cause analysis Improvement initiatives Effectiveness verification

Evidence Quality Criteria

All evidence in the repository should meet these quality criteria:

Criterion	Description
Authenticity	Evidence can be verified as genuine, with clear authorship and dates
Relevance	Evidence directly demonstrates compliance with specific requirement
Currency	Evidence is current and reflects present state of implementation
Completeness	Evidence fully addresses the requirement without gaps
Consistency	Evidence aligns with other documents and does not contradict

Audit Preparation Checklist

Before certification audit, verify:

- All folders populated with required evidence
- Documents are current versions with approval signatures
- Cross-references between documents are accurate
- Evidence covers entire audit scope period (typically 3+ months operational evidence)
- Access permissions configured for auditor review
- Index or roadmap provided to guide auditors through repository

Document Control

Document Information	Details
Document Title	Appendix H: Evidence Repository Structure
Version	1.0
Date	January 2026
Author	AI RMF Integration Project
Classification	Public
Purpose	Guide evidence organization for certification audits

End of Appendix I

Appendix J

Certification Body Selection Guide

ISO/IEC 42001 and ISO/IEC 27001
Version 1.0 | January 2026

Introduction

Selecting the right certification body (CB) is critical for successful ISO 42001 and ISO 27001 certification. This guide provides criteria and evaluation methods to select a qualified, experienced CB that meets organizational needs.

Accreditation Requirements

Requirement	Details
ISO/IEC 17021-1	CB must be accredited under ISO/IEC 17021-1 for management system certification
ISO 42001 Scope	CB accreditation must include ISO/IEC 42001 in scope (verify with national accreditation body)
ISO 27001 Scope	CB accreditation must include ISO/IEC 27001 in scope
IAF MLA	Verify CB’s accreditation body is signatory to IAF Multilateral Recognition Arrangement for international recognition

Selection Criteria

1. Technical Competence

- AI expertise: Auditors with demonstrated AI/ML knowledge
- Industry experience: Relevant sector-specific expertise
- ISO 42001 experience: Track record with AI management system audits
- ISO 27001 experience: Proven information security audit capability

2. Operational Considerations

- Geographic coverage: Ability to audit all locations in scope
- Language capabilities: Native or fluent auditors for all required languages
- Scheduling flexibility: Availability aligned with organizational timeline
- Remote audit capability: Virtual audit options if needed

3. Service Quality

- References: Positive testimonials from similar organizations
- Report quality: Sample audit reports demonstrate thoroughness and clarity
- Support services: Pre-audit consultation, training, or readiness assessments
- Communication: Responsive, professional, transparent processes

4. Commercial Terms

- Pricing: Competitive and transparent fee structure
- Audit duration: Reasonable person-days based on scope
- Contract terms: Fair terms for surveillance audits and recertification
- Payment terms: Acceptable payment schedule

Evaluation Process

Step 1: Initial Research

- Identify accredited CBs through national accreditation body websites (ANAB, UKAS, Dack's, etc.)
- Verify ISO 42001 and ISO 27001 are in CB accreditation scope
- Create shortlist of 3-5 qualified CBs

Step 2: Request for Information

Send RFI to shortlisted CBs requesting:

- Accreditation certificates and scope
- Auditor qualifications and CVs
- Reference clients (similar size/industry)
- Sample audit report (redacted)
- Pricing estimate based on preliminary scope

Step 3: Proposal Evaluation

Score each CB on weighted criteria:

Criterion	Weight	Score (1-5)
Accreditation and recognition	25%	
Technical competence (AI/ML expertise)	25%	
Industry and organizational fit	20%	
Service quality and reputation	15%	
Price and value	15%	

Step 4: Reference Checks

Contact 2-3 reference clients to inquire about:

- Auditor professionalism and knowledge
- Audit process efficiency and thoroughness
- Value-add insights provided
- Any challenges or issues encountered
- Whether they would use the CB again

Step 5: Final Selection

- Calculate weighted scores
- Conduct finalist interviews/presentations
- Negotiate final terms
- Execute certification agreement

Red Flags to Avoid

- **No accreditation or accreditation not in good standing**

Verify current status with accreditation body

- **ISO 42001/27001 not in accreditation scope**

Must be explicitly listed; general management system accreditation is insufficient

- **Promises guaranteed certification**

Legitimate CBs cannot guarantee outcomes; certification depends on conformity

- **Offers consulting and certification from same entity**

Violates ISO/IEC 17021-1 impartiality requirements

- **Unusually low pricing**

May indicate inadequate audit time or inexperienced auditors

- **Lack of AI expertise among audit team**

ISO 42001 requires specialized AI/ML knowledge

- **Poor communication or unprofessionalism**

Indicative of audit experience quality

Key Questions to Ask Certification Bodies

About Accreditation

- Which accreditation body accredits you?
- Is your accreditation body an IAF MLA signatory?
- Can you provide your current accreditation certificate showing ISO 42001 and ISO 27001 in scope?

About Experience

- How many ISO 42001 certifications have you issued?
- How many ISO 27001 certifications have you issued in our industry?
- Can you provide CVs of proposed audit team members?
- What specific AI/ML qualifications do your auditors have?

About Process

- What is your typical audit timeline from application to certification?
- How many person-days do you estimate for our scope?
- What happens if nonconformities are identified?
- What is your surveillance audit schedule?

Common Certification Body Types

Type	Advantages	Considerations
Global CBs	International recognition, multi-site capability, extensive resources	Higher cost, may be less flexible
Regional CBs	Local expertise, personalized service, competitive pricing	Limited multi-national capability
Specialized CBs	Deep AI expertise, industry-specific knowledge	May have limited ISO 42001 track record

Document Control

Document Information	Details
Document Title	Appendix I: Certification Body Selection Guide
Version	1.0
Date	January 2026
Author	AI RMF 2026 Integration Project
Classification	Public
Purpose	Guide selection of qualified certification bodies

End of Appendix J

Appendix K

Common Audit Findings and Remediation

ISO/IEC 42001 and ISO/IEC 27001 Certification
Version 1.0 | January 2026

Introduction

This appendix documents common nonconformities identified during ISO 42001 and ISO 27001 certification audits, organized by severity and management system clause. For each finding, recommended remediation actions are provided to achieve and maintain compliance.

Finding Categories

Severity	Description
Major NC	Absence of or complete failure to implement a requirement; prevents certification
Minor NC	Isolated or partial failure to meet a requirement; must be corrected before certification
Observation	Area for improvement that could become a nonconformity; advisory only

Context of the Organization (Clause 4)

Finding J-01: Incomplete Scope Definition

Severity: Major NC
Description: AIMS scope document does not clearly define boundaries, including which AI systems, organizational units, locations, or processes are in/out of scope.

Remediation:
- Create formal scope document explicitly listing included/excluded elements
- Define physical and logical boundaries (sites, networks, systems)
- Justify any exclusions with documented rationale
- Ensure scope is appropriate for organization’s AI activities
- Obtain management approval of final scope

Finding J-02: Inadequate Stakeholder Analysis

Severity: Minor NC
Description: Organization has not systematically identified and documented needs and expectations of relevant interested parties.

Remediation:
- Conduct stakeholder identification workshop
- Document stakeholder register including: customers, employees, regulators, partners, affected communities
- Analyze and document each stakeholder’s requirements and expectations
- Link stakeholder needs to AIMS objectives and requirements
- Establish process for ongoing stakeholder engagement

Leadership (Clause 5)

Finding J-03: No AI Policy or Inadequate Policy

Severity: Major NC
Description: Organization lacks documented AI management system policy, or policy does not meet ISO 42001 requirements (appropriate to purpose, framework for objectives, commitment to requirements, commitment to improvement).

Remediation:
- Draft comprehensive AI policy using Template 1 in Appendix F
- Ensure policy addresses: purpose and scope, governance principles, risk management commitment, compliance commitment, continuous improvement
- Obtain executive/board approval with documented authorization
- Communicate policy to all relevant personnel and stakeholders
- Make policy available to interested parties (website publication recommended)

Finding J-04: Unclear Roles and Responsibilities

Severity: Minor NC
Description: Roles, responsibilities, and authorities for the AIMS are not clearly defined, documented, or communicated.

Remediation:
- Create RACI matrix for all key AIMS activities and processes
- Define and document job descriptions for critical AI roles (AI Risk Officer, Data Governance Lead, etc.)
- Establish governance committee structure with clear terms of reference
- Communicate assignments to affected personnel with acknowledgment
- Update organizational charts to reflect AIMS governance structure

Planning (Clause 6)

Finding J-05: No Formal Risk Assessment

Severity: Major NC
Description: Organization has not conducted systematic risk assessment of AI systems or risk assessment does not follow established methodology.

Remediation:
- Establish and document risk assessment methodology aligned with AI RMF 2026
- Conduct comprehensive risk assessment for all in-scope AI systems
- Document risks in risk register with likelihood, impact, and risk level ratings
- Address all key risk categories: technical, fairness, security, privacy, safety, operational, legal
- Obtain management review and acceptance of residual risks

Finding J-06: Missing AI Impact Assessments

Severity: Major NC
Description: AI impact assessments have not been conducted for AI systems, particularly those affecting individuals or high-risk applications.

Remediation:
- Develop AI impact assessment template addressing: fairness, privacy, transparency, accountability, safety, human rights
- Conduct assessments for all AI systems, prioritizing high-risk systems
- Document mitigation measures for identified negative impacts
- Obtain stakeholder input on potential impacts where appropriate
- Establish process for ongoing impact monitoring and reassessment

Finding J-07: No Risk Treatment Plans

Severity: Minor NC
Description: Identified risks lack documented treatment plans specifying controls, responsibilities, and timelines.

Remediation:
- For each identified risk, document treatment option: avoid, reduce, transfer, or accept
- Specify controls to be implemented with clear ownership
- Assign implementation timelines and milestones
- Allocate resources for control implementation
- Track treatment plan execution and verify effectiveness

Support (Clause 7)

Finding J-08: Insufficient Training Records

Severity: Minor NC
Description: Organization cannot demonstrate that personnel have received required competency training for their AIMS roles.

Remediation:
- Define competency requirements for all AI-related roles
- Develop and deliver training programs addressing: AI fundamentals, responsible AI principles, AIMS requirements, role-specific skills
- Maintain training records including: attendee names, dates, topics covered, trainer credentials
- Conduct competency assessments to verify knowledge transfer
- Establish process for ongoing training and competency maintenance

Finding J-09: Poor Document Control

Severity: Minor NC
Description: Documents lack version control, approval evidence, or controlled distribution. Obsolete documents in use.

Remediation:
- Establish document control procedure (ISO 42001/27001 7.5)
- Implement version numbering and change tracking system
- Require approval signatures for all controlled documents
- Create master document register with current versions
- Remove or clearly mark obsolete documents
- Implement document repository with access controls

Operation (Clause 8)

Finding J-10: No AI System Inventory

Severity: Major NC
Description: Organization does not maintain comprehensive inventory or register of AI systems within AIMS scope.

Remediation:
- Create AI system register documenting: system name/ID, purpose and capabilities, risk classification, lifecycle stage, ownership, data sources, integration points
- Conduct discovery process to identify all AI systems
- Link each system to applicable controls and documentation
- Establish process for adding new systems to register
- Review and update register quarterly

Finding J-11: Inadequate Data Governance

Severity: Minor NC
Description: Training data quality, lineage, and governance not documented. No evidence of data quality checks or validation.

Remediation:
- Establish data governance framework with clear roles and responsibilities
- Document data lineage for all AI training and operational data
- Implement data quality metrics and monitoring: accuracy, completeness, consistency, timeliness, representativeness
- Conduct data validation checks and document results
- Address identified bias in datasets with remediation plans

Finding J-12: Missing Validation Evidence

Severity: Major NC
Description: AI systems deployed without documented validation showing fitness for intended purpose.

Remediation:
- Define validation requirements for each AI system based on intended use
- Conduct validation testing in representative environments
- Document validation results with performance metrics
- Test for trustworthiness characteristics: fairness, robustness, safety, security
- Obtain validation approval before production deployment
- Establish revalidation triggers (model updates, data drift, etc.)

Performance Evaluation (Clause 9)

Finding J-13: No Performance Monitoring

Severity: Minor NC
Description: Organization is not systematically monitoring AI system performance, trustworthiness, or AIMS effectiveness.

Remediation:
- Define KPIs for AI system performance and AIMS effectiveness
- Implement monitoring infrastructure and dashboards
- Establish monitoring frequency based on system risk level
- Monitor for: accuracy degradation, fairness metrics, data drift, security incidents, user feedback
- Document monitoring results and trend analysis
- Define thresholds and alerts for out-of-bounds performance

Finding J-14: No Internal Audit Program

Severity: Major NC
Description: Organization has not established internal audit program for the AIMS, or audits not conducted at planned intervals.

Remediation:
- Develop internal audit program covering all AIMS clauses
- Create annual audit schedule ensuring full AIMS coverage
- Train internal auditors on ISO 42001 and ISO 27001 requirements
- Conduct audits per schedule using standardized checklist
- Document audit findings and track corrective actions
- Report audit results to management

Finding J-15: No Management Review

Severity: Major NC
Description: Top management has not conducted systematic review of the AIMS at planned intervals.

Remediation:
- Establish management review schedule (minimum annually)
- Define management review inputs per ISO 42001 9.3: audit results, stakeholder feedback, AI system performance, risk status, incidents, opportunities for improvement
- Conduct formal management review meetings with executive participation
- Document meeting minutes including decisions and action items
- Communicate outcomes to relevant stakeholders
- Track implementation of management review decisions

Improvement (Clause 10)

Finding J-16: No Incident Response Procedure

Severity: Major NC
Description: Organization lacks documented process for responding to AI system incidents, failures, or security events.

Remediation:
- Develop incident response procedure addressing: incident detection and reporting, triage and severity assessment, containment and remediation, investigation and root cause analysis, communication and escalation, post-incident review
- Establish incident response team with defined roles
- Create incident classification matrix based on impact
- Train personnel on incident reporting and response
- Test procedure through tabletop exercises

Finding J-17: Corrective Actions Not Tracked

Severity: Minor NC
Description: Nonconformities identified but corrective actions not documented, implemented, or verified for effectiveness.

Remediation:
- Establish corrective action procedure (ISO 42001/27001 10.1)
- Create corrective action register tracking: issue description, root cause, corrective action plan, responsible party, target date, verification method
- Assign owners for each corrective action
- Implement corrective actions and document evidence
- Verify effectiveness after implementation
- Review open corrective actions in management review

ISO 27001 Annex A Controls

Finding J-18: Missing Statement of Applicability

Severity: Major NC
Description: Organization has not created Statement of Applicability (SoA) documenting which ISO 27001 Annex A controls are applicable and their implementation status.

Remediation:
- Review all 93 ISO 27001:2022 Annex A controls
- For each control, document: applicability (yes/no), justification for exclusions, implementation status, reference to implementation evidence
- Link controls to identified information security risks
- Obtain management approval of SoA
- Update SoA when changes occur

Finding J-19: Weak Access Controls

Severity: Minor NC
Description: Access to AI systems, models, or training data not adequately controlled. Excessive permissions observed.

Remediation:
- Implement principle of least privilege for all AI system access
- Conduct access review identifying excessive permissions
- Revoke unnecessary access rights
- Implement role-based access control (RBAC) where possible
- Establish process for provisioning/deprovisioning access
- Conduct quarterly access reviews

Finding J-20: No Vendor Security Assessment

Severity: Minor NC
Description: Third-party AI services or vendors used without documented security assessment or contractual security requirements.

Remediation:
- Develop supplier security assessment questionnaire
- Assess all AI vendors and service providers
- Include security requirements in contracts: data handling, access controls, incident notification, audit rights, compliance attestations
- Monitor vendor compliance through periodic reviews
- Maintain vendor risk register

Summary and Best Practices

Prevention Strategies

- Conduct gap assessment using Appendix F audit checklist before certification audit
- Engage experienced implementation consultants for complex areas
- Implement AIMS progressively with documentation at each step
- Establish document templates early to ensure consistency
- Allow 3-6 months operational evidence before certification audit
- Conduct internal audits to identify gaps proactively
- Consider pre-assessment or readiness review from certification body

During Audit

- Have evidence organized and readily accessible per Appendix H structure
- Assign knowledgeable representatives to guide auditors
- Document all auditor questions and requests for future reference
- Ask for clarification if findings are unclear
- Begin corrective action planning during audit if possible

Post-Audit

- Address major nonconformities immediately
- Develop comprehensive corrective action plans with root cause analysis
- Provide clear evidence of corrective action implementation
- Verify effectiveness of corrections before resubmission
- Learn from findings to improve overall AIMS

Document Control

Document Information	Details
Document Title	Appendix J: Common Audit Findings and Remediation
Version	1.0
Date	January 2026
Author	AI RMF 2026 Integration Project
Classification	Public
Purpose	Guide remediation of common certification audit findings

End of Appendix K