Enterprise AI Governance & Assurance Framework

Aligned with ISO/IEC 42001, ISO/IEC 27001, SOC 2, and Azure

- Kumar Sambhav Pandey

Inspired by ISO/IEC 42001 (AI Management System)

Contents

Purpose Statement

This document defines the organization's **AI Management System (AIMS)** in alignment with **ISO/IEC 42001** and demonstrates how AI governance is operationalized through **ISO/IEC 27001 controls**, **SOC 2 trust principles**, and **Azure-native technical enforcement**.

The objective is to ensure that AI systems are **lawful, ethical, secure, transparent, and aligned with business value**, while remaining audit-ready and scalable across the enterprise

Accountability for AI outcomes remains with the organization, regardless of whether AI systems are developed internally or procured from third parties.

Readers may review this document sequentially or navigate directly to implementation, use-case mapping, or evidence sections depending on their role

ISO 42001 Requirements: Clauses and Structure

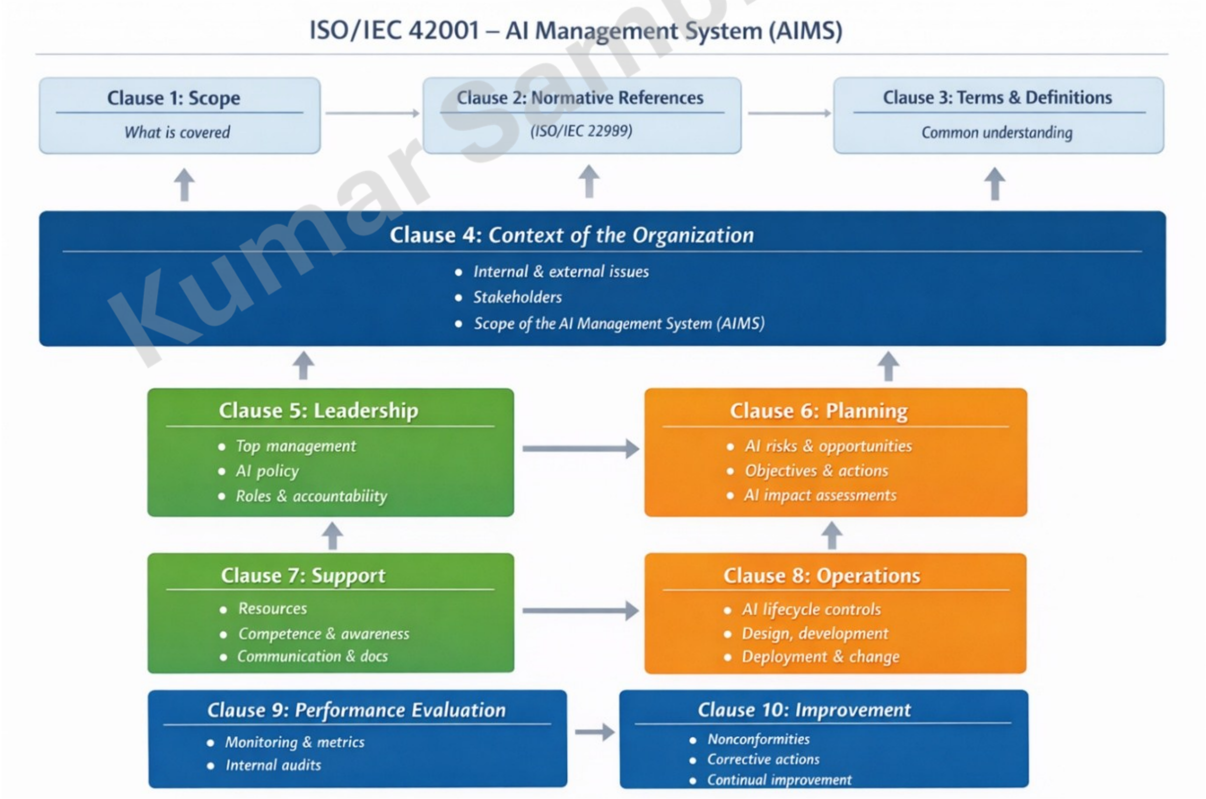
These clauses are designed to ensure that AI systems are managed from a holistic perspective, covering everything from leadership to performance evaluation.

Like with other ISO management standards, the main clauses of ISO 42001 start with clause 4 Context of the organization and end with Clause 10 Improvement; it also has Annex A that provides requirements for AI controls, and Annex B with guidance on how those controls could be implemented.

- **Clause** 1: Scope: What the standard covers.
- **Clause** 2: Normative References: References ISO/IEC 22989.
- **Clause** 3: Terms and Definitions: Defines key terms for consistent understanding.
- **Clause** 4: Context of the Organization: Understand internal/external issues, stakeholders, and scope of the AIMS.
- **Clause** 5: Leadership: Top management commitment, policy, roles, and responsibilities for AI.
- **Clause** 6: Planning: Address AI risks/opportunities, set objectives, and plan actions (including AI Impact Assessments).
- **Clause** 7: Support: Provide resources, competence, awareness, communication, and documented information.

- **Clause** 8: Operations: Plan and control processes for AI system lifecycle, including design, development, and deployment.
- **Clause** 9: Performance Evaluation: Monitor, measure, analyze, and evaluate the AIMS.
- **Clause** 10: Improvement: Address nonconformities and continually improve the AIMS.

Clauses 1 to 3: These clauses are not mandatory, and are not so important when companies want to comply with ISO 42001:



Clause 1: Scope

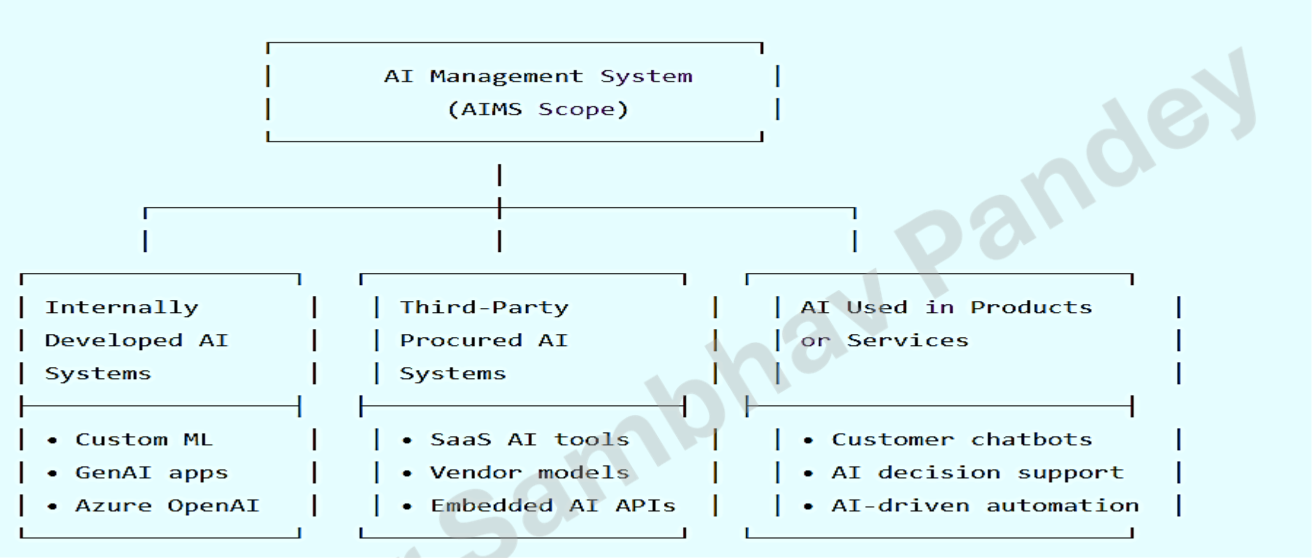
ISO/IEC 42001 establishes a structured management system for governing the lifecycle of artificial intelligence systems. It ensures AI is deployed responsibly, with clear accountability, risk management, and continuous oversight across the organization.

It applies to any organization that **develops, provides, or uses AI systems**, regardless of size or industry.

The scope covers:

- AI systems developed internally

- AI systems procured from third parties
- AI systems used to provide products or services



AI Management System (AIMS Scope)

Internally Developed AI Systems
- Custom ML
- GenAI apps
- Azure OpenAI

Third-Party Procured AI Systems
- SaaS AI tools
- Vendor models
- Embedded AI APIs

AI Used in Products or Services
- Customer chatbots
- AI decision support
- AI-driven automation

The focus is **responsible, trustworthy, and risk-aware use of AI**, not technical model accuracy alone.

Clause 2: Normative References

There are **no mandatory normative references**.
This allows flexibility but assumes alignment with related standards such as ISO 27001, ISO 27701, and risk management frameworks.

Clause 3: Terms and Definitions

Key concepts include:

- **AI system**: A system that infers outputs such as predictions, recommendations, or decisions influencing environments
- **AI risk**: Effect of uncertainty related to AI systems
- **Impact**: Effect of AI on individuals, groups, society, or organizations
- **Interested parties**: Stakeholders affected by AI outcomes
- **Lifecycle**: From design and development to deployment, monitoring, and retirement

Understanding these terms ensures **common language across business, legal, and technical teams**.

Clause 4: Context of the Organization

4.1 Understanding the organization and its context

The organization must understand its internal and external context, including its role in developing or using AI systems, legal and ethical factors, and even climate change, to ensure its AI Management System can achieve its objectives.

Understanding organizational context is foundational to responsible AI. The organization evaluates internal and external factors that influence how AI systems are designed, deployed, and governed, ensuring alignment with strategic objectives, regulatory obligations, and societal expectations.

4.2 Understanding needs and expectations of interested parties

Identify stakeholders such as:

- Customers
- Employees
- Regulator
- Partners
- Affected individuals

Understand their expectations around fairness, transparency, safety, and accountability.

4.3 Determining the scope of the AI Management System

Define:

- Which AI systems are included
- Which business units are in scope
- Lifecycle stages covered

Scope must be **documented and justified**.

4.4 AI Management System

Establish, implement, maintain, and continually improve AIMS using a **process-based approach**.

Clause 5: Leadership

Accountability for AI outcomes rests with top management and cannot be delegated solely to technology teams.

5.1 Leadership and commitment

Top management must:

- Own accountability for AI outcomes
- Ensure AI objectives align with business strategy
- Promote responsible AI culture
- Allocate resources

5.2 AI Policy

The organization must define an AI policy that:

- States commitment to responsible AI
- Includes compliance with laws and ethical principles
- Supports continual improvement
- The policy must be communicated and available.

5.3 Roles, responsibilities, and authorities

Clear assignment of:

- AI governance owners
- Risk owners
- Model owners
- Data owners
- Oversight bodies

Accountability must be explicit.

Clause 6: Planning

6.1 Actions to address risks and opportunities

Organizations must:

- Identify AI-related risks
- Evaluate likelihood and impact
- Define risk acceptance criteria
- Plan mitigation actions

AI risks span technical, ethical, legal, and societal dimensions, including bias, privacy violations, security exposure, misuse, lack of explainability, and unintended societal or downstream impact.

6.2 AI objectives and planning to achieve them

AI objectives must:

- Be measurable where possible
- Align with AI policy

- Be monitored and updated

Plans should define owners, timelines, and evaluation methods.

Clause 7: Support

7.1 Resources

Ensure adequate:

- Skilled personnel
- Tools
- Data infrastructure
- Governance mechanisms

7.2 Competence

Personnel involved in AI must be competent based on:

- Education
- Training
- Experience

Training effectiveness should be evaluated.

7.3 Awareness

Personnel must be aware of:

- AI policy
- Their role in AI governance
- Consequences of non-compliance

7.4 Communication

Define:

- What to communicate
- When
- With whom
- How

This includes internal and external communication.

7.5 Documented Information

Maintain:

- Required documents

- Records as evidence
  Ensure version control, access control, and retention.

Clause 8: Operation

Organizations must:

- Control AI lifecycle processes
- Manage changes to AI systems
- Ensure operational controls align with risk treatment plans

Includes:

- Model development controls
- Deployment approvals
- Monitoring mechanisms
- Decommissioning procedures

Clause 9: Performance Evaluation

9.1 Monitoring, measurement, analysis, and evaluation

Track:

- AI performance
- Risk indicators
- Compliance metrics

9.2 Internal audit

Conduct audits to verify:

- Conformance to AIMS
- Effectiveness of controls

9.3 Management review

Top management must review:

- Audit results
- Risk status
- Improvement opportunities

Clause 10: Improvement

10.1 Nonconformity and corrective action

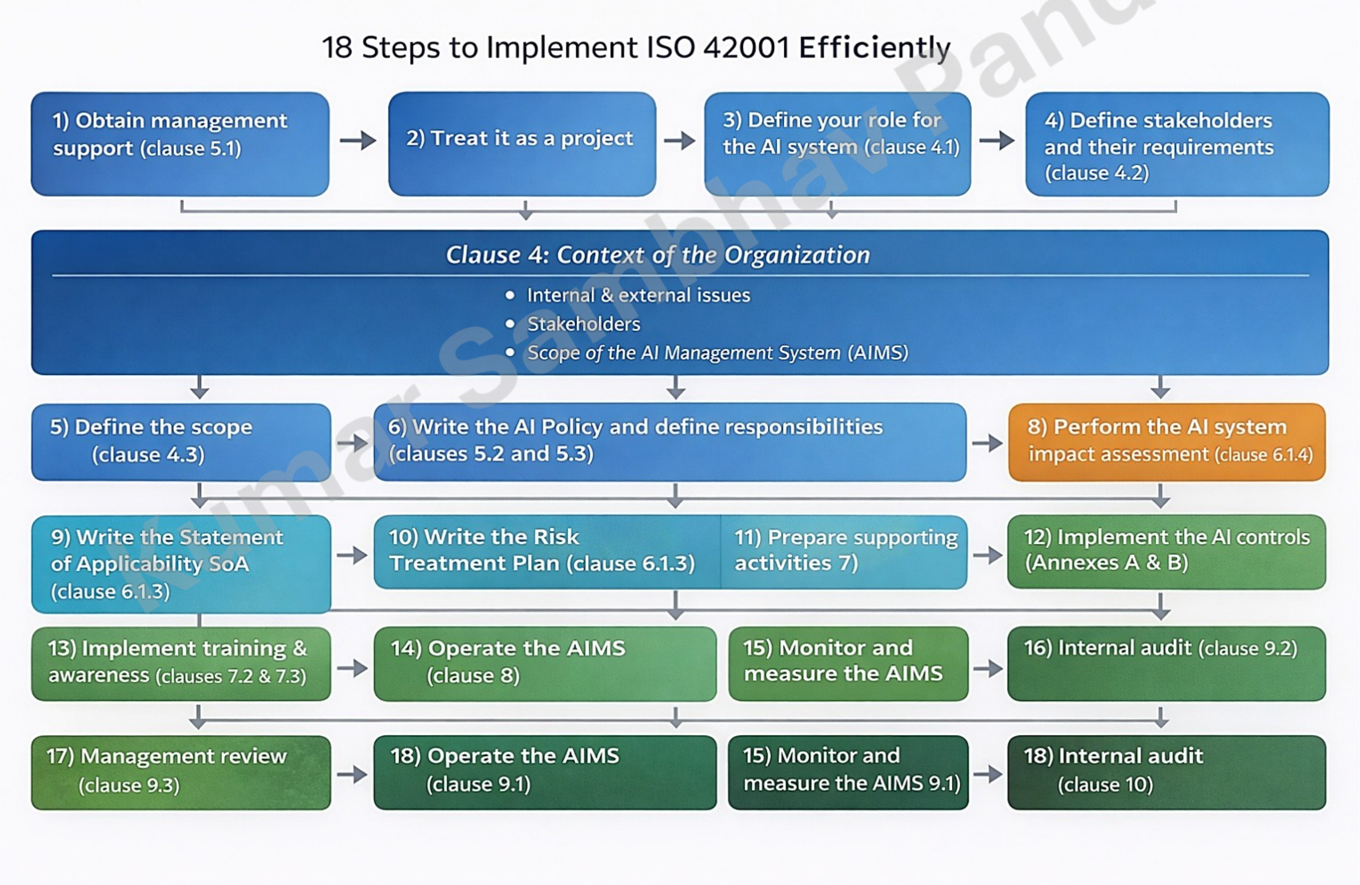
When issues occur:

- Take corrective action
- Address root cause
- Prevent recurrence

10.2 Continual improvement

Improve AIMS based on:

- Monitoring results
- Audits
- Incidents
- Technological and regulatory changes


18 Steps to Implement ISO 42001 Efficiently
1) Obtain management support (clause 5.1)
2) Treat it as a project
3) Define your role for the AI system (clause 4.1)
4) Define stakeholders and their requirements (clause 4.2)
Clause 4: Context of the Organization
Internal & external issues
Stakeholders
Scope of the AI Management System (AIMS)
5) Define the scope (clause 4.3)
6) Write the AI Policy and define responsibilities (clauses 5.2 and 5.3)
8) Perform the AI system impact assessment (clause 6.1.4)
9) Write the Statement of Applicability SoA (clause 6.1.3)
10) Write the Risk Treatment Plan (clause 6.1.3)
11) Prepare supporting activities 7)
12) Implement the AI controls (Annexes A & B)
13) Implement training & awareness (clauses 7.2 & 7.3)
14) Operate the AIMS (clause 8)
15) Monitor and measure the AIMS
16) Internal audit (clause 9.2)
17) Management review (clause 9.3)
18) Operate the AIMS (clause 9.1)
15) Monitor and measure the AIMS 9.1)
18) Internal audit (clause 10)

ISO/IEC 42001 – Implementation Guide (Practical View)

1. AI Management System Overview

AIMS provides a **governance layer over AI systems**, similar to ISMS for security.

It ensures AI is:

- Lawful
- Ethical
- Controlled
- Aligned with business value

2. Governance Model

Typical governance structure includes:

- AI Steering Committee
- Ethics Review Board
- Risk and Compliance function
- Technical Review Panels

Decision rights must be defined clearly.

3. Risk Management

Key AI risk domains:

- Bias and discrimination
- Privacy and data misuse
- Security vulnerabilities
- Model drift
- Explainability failures
- Societal impact

Risk treatment includes avoidance, mitigation, transfer, or acceptance.

4. Operating Model

Defines how AI is:

- Requested
- Designed
- Approved

- Deployed
- Monitored
- Retired

Roles span business, legal, compliance, IT, and data science.

5. Integration with Other Standards

ISO 42001 integrates well with:

- ISO 27001 for security
- ISO 27701 for privacy
- SOC 2 for trust
- GDPR and AI regulations

6. Continuous Improvement

Uses PDCA cycle:

- Plan: Define objectives and risks
- Do: Implement controls
- Check: Monitor and audit
- Act: Improve and update

ISO/IEC 42001 – Controls & Audit Checklist

Clause	Control Intent	What to Implement	Evidence
4.1	**Understand AI context**	Internal and external context analysis	Context document
4.2	**Identify stakeholders**	Stakeholder register	Stakeholder matrix
4.3	**Define AIMS scope**	Scope statement	Approved scope
5.2	**AI policy**	AI policy document	Policy approval
5.3	**Roles defined**	RACI for AI governance	Role definitions
6.1	**AI risk management**	AI risk assessment process	Risk register
6.2	**AI objectives**	Measurable AI objectives	Objective tracking
7.2	**Competence**	AI training programs	Training records
8.1	**Lifecycle controls**	AI lifecycle procedures	SOPs
9.2	**Internal audit**	AI audit program	Audit reports

10.2	**Improvement**	Corrective action process	Action logs

Azure / GenAI Examples Mapped to ISO/IEC 42001

The following examples demonstrate how ISO/IEC 42001 requirements are operationalized using Azure-native services, ensuring governance is enforced technically and not solely through policy.

1. Clause 4 – Context of the Organization

Azure / GenAI Example

Scenario

An enterprise wants to use **Azure OpenAI** to build:

- Internal Copilot for employees
- Customer-facing chatbot
- AI-assisted document analysis

1.1. How Clause 4 is applied

- **Internal context**
  - Data sources include SharePoint, SQL, CRM
  - Varying data quality across business units
  - Limited AI literacy among business users
- **External context**
  - GDPR, upcoming AI regulations
  - Customer expectations around transparency
  - Industry sensitivity (finance, insurance, healthcare)

Azure-specific actions

- Classify data using Microsoft Purview
  - **Discover, classify, and label enterprise data** based on sensitivity, regulatory requirements, and business criticality.
    - *Identify sensitive data such as PII, financial records, health information, and legal documents.*

Purpose: Prevent exposure of sensitive or regulated data to GenAI systems.

- Identify which workloads can use Azure OpenAI

- Each proposed AI workload is assessed against **data classification, business risk, compliance impact, and ethical considerations** to determine suitability for Azure OpenAI integration.
  - *Internal Copilot → Allowed for low to medium sensitivity business content*
  - *Document analysis → Allowed for classified internal documents after applying redaction and masking*
  - *Customer chatbot → Restricted to curated, approved knowledge bases*

Purpose: Ensure GenAI is applied **only where risk is understood and controlled**.

- Exclude high-risk data domains from GenAI initially
  - High-risk data domains such as:
    - *Personally identifiable information (PII)*
    - *Financial transaction data*
    - *Health records*
    - *Legal case data*

      *are **explicitly excluded** during early GenAI adoption phases.*
  - These domains are onboarded **only after additional safeguards**, including:
    - Strong anonymization
    - Human-in-the-loop validation
    - Legal and compliance approval

Purpose: Enable **safe, phased AI adoption** while minimizing regulatory, ethical, and reputational risk.

Output artifacts

- AI context assessment document
- In-scope vs out-of-scope AI use cases

Clause 5 – Leadership & AI Policy

Azure / GenAI Example

AI Policy for Azure OpenAI usage

The policy states:

- Azure OpenAI deployments are restricted to private network access, eliminating public exposure and reducing data exfiltration risk.
- No customer PII allowed in prompts unless approved
- Human oversight is mandatory for customer-facing AI outputs to ensure accountability, accuracy, and regulatory compliance.
- Explainability required for regulated decisions

AI systems are treated as **managed enterprise systems**, not experimental tools.

Leadership accountability

- CIO owns AI strategy
- CISO owns AI security risks
- Legal owns regulatory compliance
- Business owns AI value realization

Azure-specific enforcement

- Azure Policy to restrict public network access
- Managed identities for model access
- RBAC to control who can deploy models

Evidence

- Approved AI policy
- Azure Policy assignments
- Role definitions

Clause 6 – Planning (AI Risks & Objectives)

Azure / GenAI Example

AI Risk Identification

Risk Type	Azure / GenAI Risk
Bias	LLM responses biased due to training data
Privacy	Prompts contain sensitive data
Security	Model endpoints exposed publicly
Hallucination	Incorrect responses used operationally
Misuse	Employees using GenAI beyond intended purpose

AI Risk Treatment

- Private networking for Azure OpenAI
- Prompt filtering and content moderation
- Logging prompts and responses securely
- Human review for high-impact outputs

AI Objectives

- Reduce support ticket resolution time by 30%
- Improve internal productivity without exposing sensitive data
- Maintain regulatory compliance

Evidence

- AI risk register
- Risk treatment plan
- Measurable AI objectives

Clause 7 – Support

Azure / GenAI Example

Competence

- Train developers on:
  - Prompt engineering
  - Responsible AI principles
  - Azure OpenAI security controls
- Train business users on:
  - What GenAI can and cannot do
  - Risks of over-reliance

Azure tools

- Microsoft Responsible AI learning paths
- Azure AI Studio governance controls

Awareness

Employees understand:

- Outputs may be probabilistic
- AI is advisory, not authoritative

Evidence

- Training records
- Awareness communications
- Role-based training plans

Clause 8 – Operation (AI Lifecycle Control)

Azure / GenAI Example

AI Lifecycle Stages

Design

- Define allowed use cases

- Identify required data sources

Development

- Use Azure OpenAI with approved models only
- Use system prompts aligned to policy

Deployment

- Private endpoint enabled
- Monitoring and logging enabled

Operation

- Track prompt volume
- Monitor drift and misuse
- Apply rate limiting

Decommissioning

- Disable endpoints
- Archive logs
- Review data retention

Evidence

- AI lifecycle SOP
- Change management records
- Deployment approvals

Clause 9 – Performance Evaluation

Azure / GenAI Example

Monitoring

- Accuracy and usefulness of responses
- User feedback
- Incident reports
- Prompt misuse patterns

Azure monitoring tools

- Azure Monitor
- Log Analytics
- Application Insights
- Defender for Cloud alerts

Internal Audit

Auditors verify:

- AI usage aligns with policy
- Risk controls are effective
- Logs are retained securely

Evidence

- Monitoring dashboards
- Audit reports
- Management review minutes

Clause 10 – Improvement

Azure / GenAI Example

Continuous improvement actions

- Refine prompts to reduce hallucinations
- Improve content filters
- Update AI policy as regulations evolve
- Add stronger human review for sensitive use cases

Trigger events

- AI incident
- Audit findings
- Regulatory updates
- Business expansion

Evidence

- Corrective action logs
- Policy revisions
- Improvement plans

ISO/IEC 42001 – Clause Mapping to Real Azure / GenAI Use Cases

ISO 42001 Clause	Clause Focus	Real AI / GenAI Use Case	Azure / GenAI Example	Key Risks Addressed	Typical Evidence / Artifacts
Clause 4 Context of the Organization	Define AI scope and environment	Internal employee copilot	Azure OpenAI summarizing internal documents	Data leakage, misuse	AI context analysis, in-scope data list

Clause 4 Context of the Organization	Stakeholder expectations	Customer support chatbot	Azure OpenAI chatbot for customers	Accuracy, trust, compliance	Stakeholder register, risk assessment
Clause 5 Leadership	AI accountability	AI assisted decision support	GenAI recommendations for sales or finance	Over-reliance, liability	AI policy, decision accountability
Clause 5 Leadership	Responsible AI policy	Content generation	GenAI for marketing drafts	Brand risk, legal risk	AI usage guidelines, approval workflow
Clause 6 Planning	AI risk management	Resume screening	ML based candidate shortlisting	Bias, discrimination	AI risk register, bias assessment
Clause 6 Planning	Risk treatment	Fraud detection	ML fraud detection models	False positives, customer impact	Risk treatment plan, model metrics
Clause 7 Support	Competence and skills	AI application development	Developers using Azure OpenAI	Misconfiguration, poor prompts	Training records, secure coding guides
Clause 7 Support	Awareness	Self-service GenAI	Business users using AI Studio	Misuse, data exposure	Awareness training, RBAC settings
Clause 8 Operation	Lifecycle governance	Document intelligence	AI extracting invoice data	Data errors, uncontrolled changes	AI lifecycle SOP, approvals
Clause 8 Operation	Controlled deployment	Knowledge search (RAG)	GenAI answering from internal content	Hallucinations, stale data	Data source approval, monitoring
Clause 9 Performance Evaluation	Monitoring and metrics	AI customer support	GenAI resolving Tier-1 tickets	Accuracy degradation	Dashboards, monitoring reports
Clause 9 Performance Evaluation	Audit and review	Recommendation engine	AI product recommendations	Drift, unfair outcomes	Audit reports, review minutes
Clause 10 Improvement	Incident management	Hallucination incident	AI giving incorrect guidance	Compliance breach	Incident log, corrective action
Clause 10 Improvement	Regulatory adaptation	Compliance updates	AI policy updates for new laws	Non-compliance	Updated policies, reassessments

ISO/IEC 42001 – AI Use Case Mapping (Azure / GenAI) with RACI and Azure Services

Each AI use case is governed through explicit ownership, risk classification, and technical controls, ensuring accountability across business, security, and technology domains.

Context

AI Use Case	Purpose	Key Context Considerations	Azure Services	R	A	C	I
Internal Employee Copilot	Improve employee productivity	Mixed data sensitivity, internal access only	Azure OpenAI, Microsoft Purview, Entra ID	IT AI Team	CIO	Security, Legal	Employees
Customer Support Chatbot	Handle customer queries	External users, accuracy and trust critical	Azure OpenAI, App Service, Azure Monitor	Digital Product Team	Business Head	Legal, Compliance	Support Teams
AI Knowledge Search (RAG)	Answer queries from internal docs	Data freshness, access control	Azure OpenAI, Azure AI Search, Purview	IT Platform Team	CIO	Data Owners	Business Users
AI Document Summarization	Reduce manual effort	Confidential documents, access segregation	Azure OpenAI, Blob Storage, Purview	IT AI Team	CIO	Security	Business Users

GOVERNANCE

AI Use Case	Governance Focus	Key Risks	Azure Services	R	A	C	I
AI Assisted Decision Support	AI advisory not authoritative	Over-reliance, liability	Azure OpenAI, Azure Monitor	Business Analytics Team	Business Owner	Legal, Risk	Leadership
Resume Screening AI	Fair and unbiased hiring	Bias, discrimination	Azure ML, Azure OpenAI, Purview	HR Tech Team	CHRO	Legal, DEI	HR Ops
Fraud Detection AI	Protect customers and revenue	False positives, trust erosion	Azure ML, Defender for Cloud	Risk Analytics Team	CRO	Compliance	Operations
Marketing Content Generation	Brand-safe AI content	Reputation, IP risk	Azure OpenAI, Content Filters	Marketing Ops	CMO	Legal	Marketing Teams
GenAI Policy Enforcement	Responsible AI usage	Policy violations	Azure Policy, Entra ID	Cloud Governance Team	CIO	Security, Legal	All Users

OPERATIONS

AI Use Case	Operational Control	Monitoring & Improvement	Azure Services	R	A	C	I
AI Application Development	Secure GenAI app lifecycle	Prompt misuse, drift	Azure OpenAI, App Insights	Dev Teams	IT Director	Security	Business
Document Intelligence Automation	Controlled extraction accuracy	Errors, change impact	Azure AI Document Intelligence	Automation Team	CIO	Finance	Ops Teams
Customer Chatbot Operations	Response quality & escalation	Hallucinations, CSAT	Azure Monitor, App Insights	Support Tech Team	Customer Head	QA	Customers
AI Model Monitoring	Performance & drift tracking	Accuracy degradation	Azure Monitor, Log Analytics	ML Ops Team	CIO	Risk	Leadership
AI Incident Management	Corrective actions	Compliance failures	Sentinel, Azure Monitor	Security Ops	CISO	Legal	Leadership
AI System Decommissioning	Safe retirement	Data retention risks	Azure Resource Manager	IT Ops	CIO	Compliance	Stakeholders

AI Use Cases mapped to ISO 27001 and SOC 2

Operational control applicability per AI use case

This section maps individual AI use cases to applicable ISO 27001 and SOC 2 controls, highlighting ownership, implementation approach, and audit evidence.

CONTEXT

AI Use Case	ISO 27001 Control Areas	SOC 2 Trust Principles	What This Proves
Internal Employee Copilot	A.5 Information Security Policies, A.8 Asset Management, A.9 Access Control	Security, Confidentiality	AI access is scoped, data classified, and protected
Customer Support Chatbot	A.6 Organization of IS, A.13 Communications Security	Security, Availability	External AI exposure is controlled and monitored
AI Knowledge Search (RAG)	A.8 Asset Management, A.9 Access Control	Confidentiality, Security	Only authorized data sources are used
AI Document Summarization	A.8 Asset Management, A.10 Cryptography	Confidentiality	Sensitive data is identified and protected

GOVERNANCE

AI Use Case	ISO 27001 Control Areas	SOC 2 Trust Principles	What This Proves
AI Assisted Decision Support	A.5 Policies, A.6 Responsibilities	Security, Integrity	AI does not replace human accountability
Resume Screening AI	A.18 Compliance, A.7 Human Resource Security	Confidentiality, Integrity	Bias and regulatory risks are governed
Fraud Detection AI	A.12 Operations Security, A.16 Incident Management	Security, Availability	AI decisions are controlled and auditable
Marketing Content Generation	A.18 Compliance	Integrity	AI output aligns with brand and legal rules
GenAI Policy Enforcement	A.5 Policies, A.9 Access Control	Security	Centralized governance over AI usage

OPERATIONS

AI Use Case	ISO 27001 Control Areas	SOC 2 Trust Principles	What This Proves
AI Application Development	A.14 System Acquisition, Development & Maintenance	Security, Integrity	Secure-by-design AI development
Document Intelligence Automation	A.12 Operations Security	Integrity, Availability	Reliable and controlled AI processing
Customer Chatbot Operations	A.12 Operations Security, A.16 Incident Management	Availability, Security	AI service reliability and escalation
AI Model Monitoring	A.12 Logging and Monitoring	Security, Availability	Continuous oversight and detection
AI Incident Management	A.16 Information Security Incident Management	Security	AI failures are handled like security incidents
AI System Decommissioning	A.11 Physical & Environmental, A.8 Asset Management	Confidentiality	Secure AI retirement and da

Consolidated AI Governance & Assurance Traceability Matrix

(ISO 42001 × ISO 27001 × SOC 2 × Azure Controls: Framework-level alignment across ISO/IEC 42001, ISO/IEC 27001, SOC 2, and Azure)

This consolidated assurance matrix demonstrates traceability from AI governance intent (ISO/IEC 42001) through control enforcement (ISO/IEC 27001), assurance reporting (SOC 2), and technical implementation on Azure.

This prevents parallel governance models and embeds AI risk into the existing enterprise control environment.

What this matrix is all about

- **ISO 42001** explains why AI is governed
- **ISO 27001** explains how controls are enforced
- **SOC 2** explains what assurance is provided
- **Azure controls** explain where this is technically implemented

CONTEXT (ISO 42001 – Clause 4)

AI Use Case	ISO 42001 Focus	ISO 27001 Controls	SOC 2 Principles	Azure Controls & Services
Internal Employee Copilot	Context definition, scope, interested parties	A.5 Policies, A.8 Asset Management, A.9 Access Control	Security, Confidentiality	Azure OpenAI (Private Endpoint), Microsoft Purview (Data Classification), Entra ID (RBAC), Azure Policy
Customer Support Chatbot	External stakeholders, trust expectations	A.6 Organization of IS, A.13 Communications Security	Security, Availability	Azure OpenAI, App Service, Azure Front Door, Azure Monitor
AI Knowledge Search (RAG)	Data source boundaries, scope	A.8 Asset Management, A.9 Access Control	Confidentiality, Security	Azure AI Search, Azure OpenAI, Purview, Entra ID
AI Document Summarization	Data sensitivity context	A.8 Asset Management, A.10 Cryptography	Confidentiality	Azure OpenAI, Blob Storage (Encryption), Purview

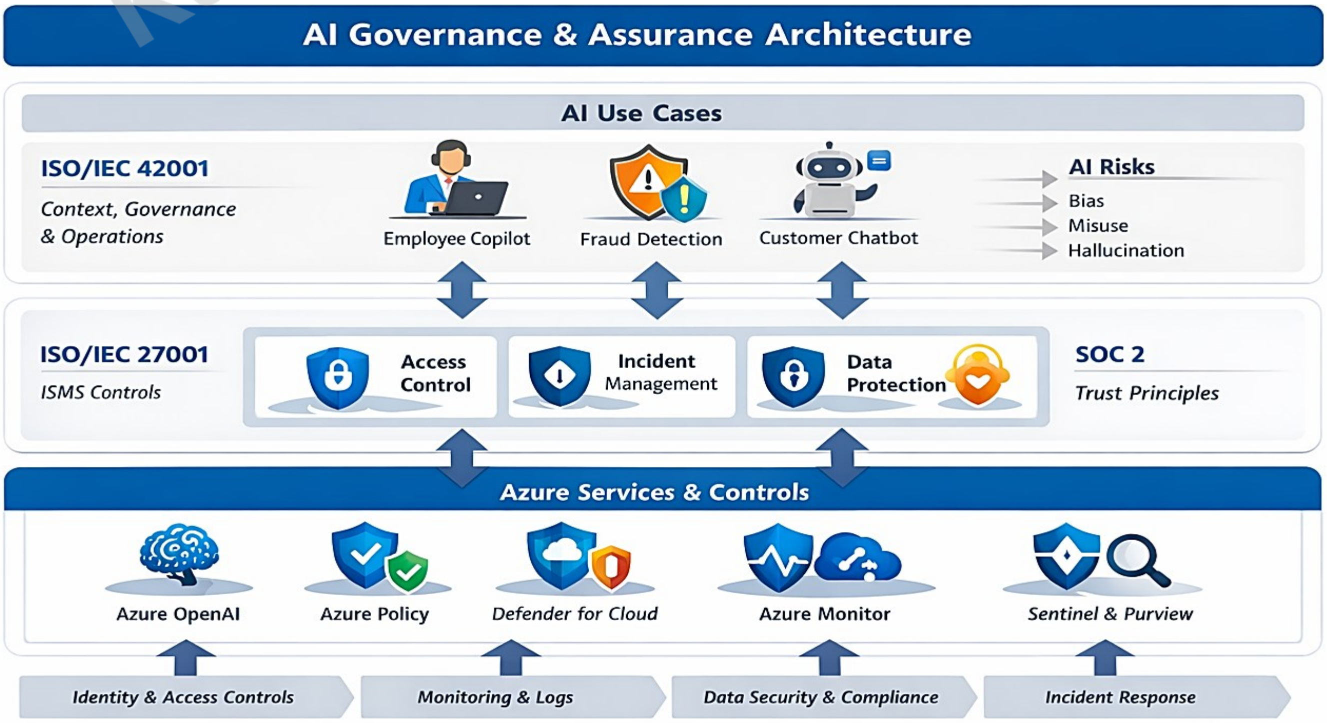
GOVERNANCE (ISO 42001 – Clauses 5 & 6)

AI Use Case	ISO 42001 Focus	ISO 27001 Controls	SOC 2 Principles	Azure Controls & Services
AI Assisted Decision Support	Leadership accountability, AI advisory use	A.5 Policies, A.6 Responsibilities	Integrity, Security	Azure OpenAI, Azure Monitor, Application Insights
Resume Screening AI	AI risk planning, fairness	A.18 Compliance, A.7 HR Security	Confidentiality, Integrity	Azure Machine Learning, Azure OpenAI, Purview
Fraud Detection AI	Risk treatment, impact control	A.12 Operations Security, A.16 Incident Mgmt	Security, Availability	Azure ML, Defender for Cloud, Sentinel
Marketing Content Generation	Responsible AI policy	A.18 Compliance	Integrity	Azure OpenAI, Content Filtering, Azure Policy
GenAI Policy Enforcement	Governance enforcement	A.5 Policies, A.9 Access Control	Security	Azure Policy, Entra ID, Management Groups

OPERATIONS(ISO 42001 – Clauses 7, 8, 9, 10)

AI Use Case	ISO 42001 Focus	ISO 27001 Controls	SOC 2 Principles	Azure Controls & Services
AI Application Development	Competence, secure lifecycle	A.14 Secure Development	Security, Integrity	Azure DevOps, Azure OpenAI, Application Insights
Document Intelligence Automation	Operational control	A.12 Operations Security	Integrity, Availability	Azure AI Document Intelligence, Azure Monitor
Customer Chatbot Operations	Monitoring & escalation	A.12 Operations, A.16 Incidents	Availability, Security	Azure Monitor, App Insights, Azure Logic Apps
AI Model Monitoring	Performance evaluation	A.12 Logging & Monitoring	Security, Availability	Azure Monitor, Log Analytics, Sentinel
AI Incident Management	Corrective action	A.16 Incident Management	Security	Sentinel, Defender for Cloud
AI System Decommissioning	Secure retirement	A.8 Asset Management, A.11 Secure Disposal	Confidentiality	Azure Resource Manager, Key Vault, Storage Lifecycle Policies

Visual governance architecture diagram



AI Governance Evidence Matrix

Evidence is maintained to demonstrate both **design effectiveness** and **operational effectiveness** of AI governance controls.

(Logs, Dashboards, Policies, Records)

CONTEXT – Evidence

Control Area	Evidence Type	Concrete Evidence Example	Azure Location / Tool
AI Scope Definition	Policy / Document	AI use case inventory with in-scope and out-of-scope systems	SharePoint / Confluence
Data Classification	Configuration	Classified datasets tagged as Public, Internal, Confidential	Microsoft Purview
Stakeholder Identification	Document	Stakeholders register for AI systems	SharePoint
Data Boundary Enforcement	Configuration	Only approved data sources indexed for RAG	Azure AI Search
Access Scope	Logs	User access logs showing authorized users only	Entra ID Sign-in Logs

GOVERNANCE – Evidence (ISO 42001 Clauses 5 & 6)

Control Area	Evidence Type	Concrete Evidence Example	Azure Location / Tool
AI Policy	Policy	Approved Responsible AI & GenAI Usage Policy	SharePoint
Leadership Oversight	Records	Steering committee meeting minutes	SharePoint
AI Risk Assessment	Register	AI risk register with bias, privacy, hallucination risks	Excel / GRC Tool
Risk Treatment	Plan	Risk mitigation plan for GenAI use cases	SharePoint
Fairness & Bias	Reports	Bias testing results for hiring or scoring models	Azure ML
Regulatory Compliance	Evidence	DPIA / AI impact assessment	Compliance repository
Access Enforcement	Configuration	Azure Policy restricting public OpenAI endpoints	Azure Policy

OPERATIONS – Evidence (ISO 42001 Clauses 7, 8, 9, 10)

Control Area	Evidence Type	Concrete Evidence Example	Azure Location / Tool
Secure Development	Logs	Pull requests with security checks	Azure DevOps
Model Deployment	Records	Approved deployment tickets	Azure DevOps / ITSM
Change Management	Logs	Model version change history	Azure ML
Prompt Controls	Configuration	System prompts enforcing policy language	Azure OpenAI
Content Filtering	Configuration	Enabled content moderation policies	Azure OpenAI

Monitoring & Detection

Control Area	Evidence Type	Concrete Evidence Example	Azure Location / Tool
AI Usage Monitoring	Dashboard	Prompt volume, token usage, response rates	Azure Monitor
Hallucination Tracking	Logs	Logged user feedback and escalations	App Insights
Drift Detection	Reports	Accuracy drift over time	Azure ML
Security Monitoring	Alerts	Suspicious API access alerts	Defender for Cloud
SIEM Correlation	Logs	AI-related security incidents	Azure Sentinel

Incident & Improvement

Control Area	Evidence Type	Concrete Evidence Example	Azure Location / Tool
AI Incident Records	Incident Log	Hallucination or misuse incidents	ITSM / Sentinel
Root Cause Analysis	Document	RCA for incorrect AI outputs	SharePoint
Corrective Actions	Tracker	Action items and owners	Jira / Azure Boards
Policy Updates	Version History	Updated AI policy after incidents	SharePoint
Management Review	Minutes	Periodic AI governance review	SharePoint

SOC 2 Mapping – Evidence View

SOC 2 Principle	Typical Evidence
Security	Access logs, SIEM alerts, Azure Policy assignments
Availability	Azure Monitor uptime dashboards
Confidentiality	Purview labels, encryption settings
Integrity	Change logs, deployment approvals
Privacy (if applicable)	DPIA, consent handling documentation

Sample Screenshots Auditors Usually Ask For

(AI / GenAI – Azure Environment)

IDENTITY & ACCESS (Very High Priority)

Screenshot	What Auditor Is Verifying	Azure Location
Entra ID Sign-in Logs	Who accessed AI services and when	Entra ID → Monitoring → Sign-in logs
Role Assignments for Azure OpenAI	Least-privilege access enforced	Azure OpenAI → Access control (IAM)
Conditional Access Policy	MFA and access conditions	Entra ID → Conditional Access

Service Principal Permissions	App-to-app access control	Entra ID → App registrations

AI SERVICE CONFIGURATION

Screenshot	What Auditor Is Verifying	Azure Location
Azure OpenAI Resource Overview	Approved AI services in use	Azure Portal → Azure OpenAI
Network Configuration	Private endpoint / no public exposure	Azure OpenAI → Networking
Content Filters Configuration	Responsible AI safeguards enabled	Azure OpenAI → Safety & filters
Model Deployment List	Approved models only	Azure OpenAI → Deployments

DATA GOVERNANCE & PRIVACY

Screenshot	What Auditor Is Verifying	Azure Location
Purview Data Classification	Sensitive data identified	Microsoft Purview → Data map
Data Source Inventory (RAG)	Only approved sources used	Azure AI Search
Storage Encryption Settings	Data at rest protection	Storage Account → Encryption
Access Policies on Data Stores	Data access restricted	Storage / SQL / Blob IAM

LOGGING & MONITORING (SOC 2 Favourite)

Screenshot	What Auditor Is Verifying	Azure Location
Azure Monitor Dashboard	Continuous monitoring	Azure Monitor
Log Analytics Queries	AI access and usage logged	Log Analytics
Application Insights	Prompt usage & failures	App Insights
Token Usage Metrics	Abuse or over-usage detection	Azure OpenAI metrics

SECURITY & INCIDENT MANAGEMENT

Screenshot	What Auditor Is Verifying	Azure Location
Defender for Cloud Alerts	AI resources monitored	Defender for Cloud
Sentinel Incident List	AI incidents tracked	Microsoft Sentinel

Incident Details View	Evidence of investigation	Sentinel → Incidents
Alert Rules	Proactive detection	Sentinel → Analytics rules

CHANGE & LIFECYCLE MANAGEMENT

Screenshot	What Auditor Is Verifying	Azure Location
Azure DevOps PR History	Controlled AI changes	Azure DevOps
Model Version History	Controlled updates	Azure ML / OpenAI
Release Pipelines	Deployment approvals	Azure DevOps
Resource Activity Logs	Who changed what	Azure Activity Log

POLICY & GOVERNANCE ENFORCEMENT

Screenshot	What Auditor Is Verifying	Azure Location
Azure Policy Assignments	Policy-driven governance	Azure Policy
Policy Compliance View	Enforcement status	Azure Policy → Compliance
Management Group Structure	Central governance	Azure Management Groups
Tagging Enforcement	Asset ownership & scope	Azure Policy

BUSINESS & GOVERNANCE EVIDENCE (Non-Technical)

Screenshot / File	What Auditor Is Verifying	Location
AI Usage Policy	Management intent	SharePoint
AI Risk Register	Risks formally assessed	Excel / GRC tool
Steering Committee Minutes	Leadership oversight	SharePoint
Training Records	Staff competence	LMS / HR system
Incident RCA Document	Continuous improvement	SharePoint

SOC 2 Specific "Show Me" Requests

The following evidence artifacts and screenshots are typically requested by auditors to verify that AI governance controls are operating effectively and continuously.

- Last 90 days of sign-in logs
- Monitoring dashboard with timestamps
- Incident closed with root cause
- Policy compliance percentage
- Approved access vs denied access

Suggested Folder Structure for Audits

```
AI-Governance-Evidence/
├──── 01-Identity-and-Access/
├──── 02-AI-Service-Configuration/
├──── 03-Data-Governance/
├──── 04-Monitoring-and-Logs/
├──── 05-Incident-Management/
├──── 06-Change-Management/
├──── 07-Policies-and-Governance/
```

Conclusion

This AI Governance and Assurance framework enables the organization to scale AI adoption with confidence. By embedding ISO/IEC 42001 within existing ISO/IEC 27001 and SOC 2 control structures, AI risks are governed consistently, transparently, and auditable by design.

This approach ensures that AI innovation remains aligned with organizational values, regulatory expectations, and stakeholder trust.