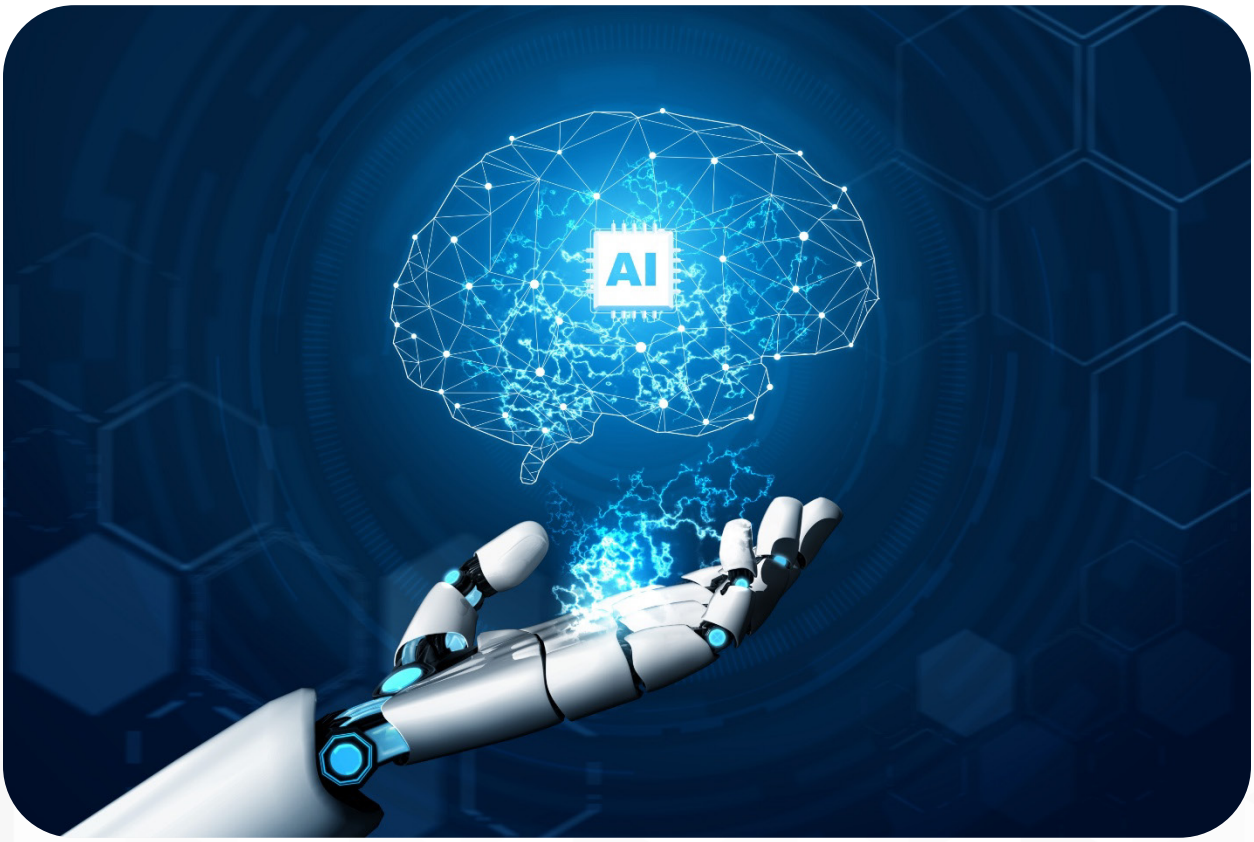
ISO 42001 INTERNATIONAL STANDARD

FOR ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEMS (AIMS)

SkillWeed

CONTENTS

1. INTRODUCTION TO ISO 42001



1.1 WHAT IS ISO 42001?

ISO/IEC 42001:2023 is the **first international standard for Artificial Intelligence Management Systems (AIMS)**.

- Developed jointly by **ISO (International Organization for Standardization)** and **IEC (International Electrotechnical Commission)**.
- Published in **December 2023** to address the rapid global adoption of AI.
- Provides organizations with a **management framework** to ensure AI is developed, deployed, and used in a **safe, trustworthy, and responsible manner**.

1.2 WHY WAS ISO 42001 DEVELOPED?

Artificial Intelligence (AI) is transforming industries, but it brings **unique risks and challenges**:

- **Bias and fairness** → AI decisions may unintentionally discriminate.
- **Transparency and explainability** → AI models often act as "black boxes."
- **Data privacy and security** → Sensitive personal or organizational data is at risk.
- **Accountability and governance** → Who is responsible for AI outcomes?

ISO 42001 was created to:

- Provide a **standardized governance structure** for AI.
- Help organizations **balance innovation with compliance and ethics**.
- Promote **trust** in AI systems across industries and borders.

1.3 SCOPE OF THE STANDARD

ISO 42001 applies to **any organization** that:

- **Develops AI systems** (e.g., tech companies, startups, R&D centers).
- **Deploys AI solutions** (e.g., banks using AI for credit scoring, hospitals using AI diagnostics).
- **Uses AI in operations** (e.g., retailers applying AI for logistics and customer insights).

It is **industry-neutral** and **technology-agnostic**—whether using machine learning, natural language processing, robotics, or computer vision, the principles apply.

1.4 KEY FOCUS AREAS OF ISO 42001

- Establishing an **AI management framework** similar to ISO 9001 (quality) and ISO 27001 (security).
- Embedding **risk-based thinking** specific to AI risks.
- Ensuring **transparency, accountability, and ethics** in AI decision-making.
- Continuous improvement of AI systems and organizational practices.

1.5 WHO BENEFITS FROM ISO 42001?

- **Organizations** → Build trust with clients, reduce risks, and demonstrate compliance.
- **Regulators** → Gain confidence that AI is being responsibly managed.
- **Customers & Public** → Assurance that AI systems are safe, ethical, and transparent.
- **Employees & Developers** → Clear roles, responsibilities, and guidance in building AI responsibly.

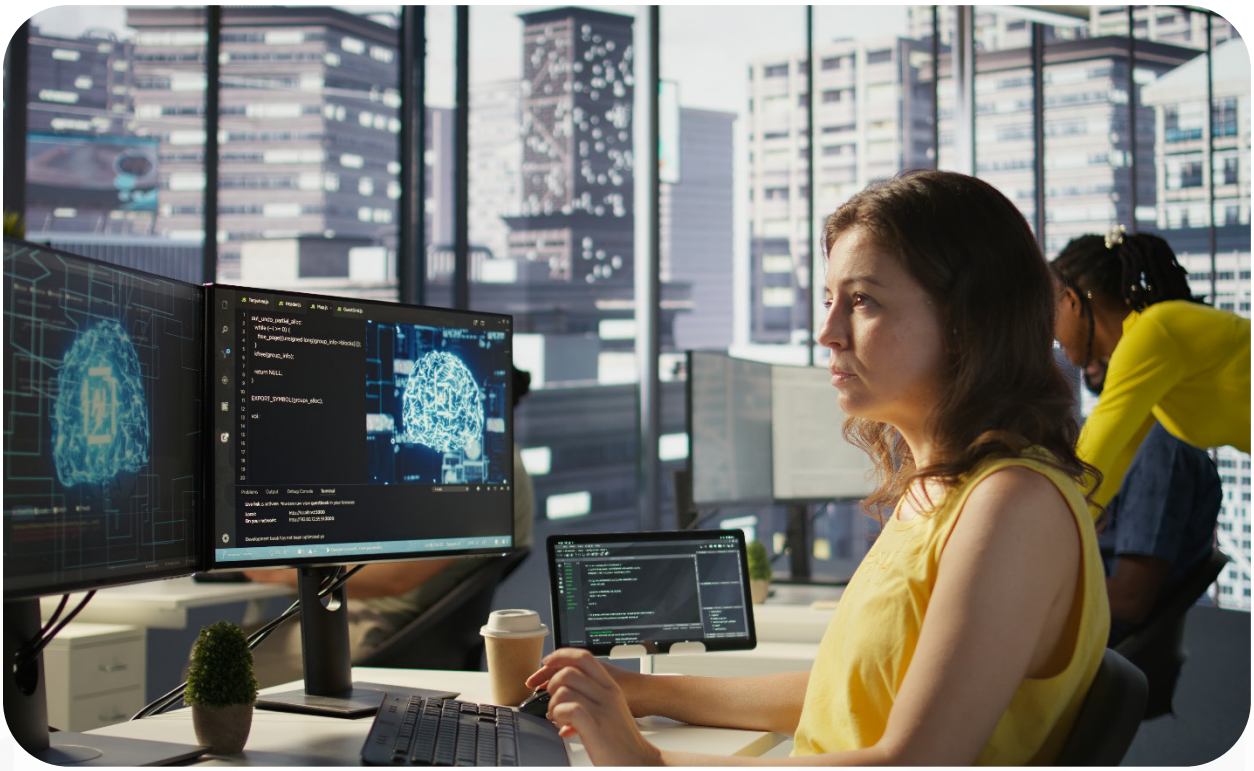
1.6 RELATION TO OTHER STANDARDS

ISO 42001 is **complementary** to other management system standards:

- **ISO 9001** (Quality Management)
- **ISO 27001** (Information Security Management)
- **ISO 27701** (Privacy Management)
- **NIST AI Risk Management Framework** (guidance from the U.S.)
- **EU AI Act** (upcoming regulation)

Together, these frameworks create a **comprehensive compliance and governance ecosystem** for AI.

2. OBJECTIVES OF ISO 42001



2.1 PROMOTE TRUSTWORTHY AND RESPONSIBLE AI

- Establishes a **structured governance system** for AI development and deployment.
- Ensures AI systems are **transparent, reliable, and fair**.
- Builds **trust** among customers, regulators, employees, and society.

2.2 ENSURE ETHICAL AND LEGAL COMPLIANCE

- Helps organizations align with **ethical guidelines** for fairness, human-centric design, and accountability.
- Supports compliance with **global and local regulations**, such as GDPR (privacy) and the EU AI Act.
- Encourages organizations to **proactively manage risks** related to misuse or unintended consequences of AI.

2.3 MANAGE AI RISKS EFFECTIVELY

- Provides a **risk-based framework** for addressing:
  - **Bias and discrimination** in datasets and algorithms.
  - **Data privacy and protection** across AI lifecycle.
  - **Security threats** to AI systems and data integrity.
  - **Explainability gaps** in complex AI models.
- Promotes **early detection and mitigation** of risks before they cause harm.

2.4 INTEGRATE AI INTO ORGANIZATIONAL STRATEGY

- Aligns AI adoption with **business goals and values**.
- Helps leadership **define AI objectives and performance indicators**.
- Ensures AI supports **sustainability, innovation, and long-term competitiveness**.

2.5 ENABLE CONTINUOUS IMPROVEMENT

- Encourages **monitoring, auditing, and feedback loops** to refine AI practices.
- Drives **ongoing learning and adaptation** as AI technologies evolve.
- Embeds a **culture of continuous improvement** in AI governance.

2.6 PROVIDE A GLOBAL BENCHMARK

- Creates an **internationally recognized standard** for managing AI responsibly.
- Allows organizations to **demonstrate conformance or pursue certification**, gaining competitive advantage.
- Facilitates **cross-border trust and collaboration** in AI initiatives.

3. KEY COMPONENTS OF ISO 42001

ISO 42001 follows the **Annex SL High-Level Structure (HLS)** used in other ISO management system standards (like ISO 9001, ISO 27001). This makes it easier to integrate with existing systems.

3.1 CONTEXT OF THE ORGANIZATION

- Define the **scope** of the Artificial Intelligence Management System (AIMS).
- Understand **internal and external issues** that influence AI adoption.
- Identify **stakeholders** (regulators, customers, employees, suppliers, public) and their requirements.
- Map **AI opportunities and risks** across business areas.

3.2 LEADERSHIP & GOVERNANCE

- Demonstrate **top management commitment** to responsible AI.
- Define **AI roles and responsibilities** (including ethics officers, governance committees).
- Establish an **AI policy** reflecting organizational values, compliance, and transparency.
- Promote a **culture of accountability** across the AI lifecycle.

3.3 PLANNING

- Conduct **AI risk assessments** to address bias, privacy, explainability, and misuse.
- Set **AI objectives** aligned with strategic goals.
- Define **controls and mitigation plans** to manage AI-specific risks.
- Prepare for **emerging regulatory requirements**.

3.4 SUPPORT

- Ensure **competence and training** of employees working with AI.
- Drive **awareness campaigns** on responsible AI within the organization.
- Maintain **documented information** on AI systems, processes, and policies.
- Provide **resources and technology infrastructure** to support compliance.

3.5 OPERATION

- Implement processes to **design, develop, test, and deploy AI systems** responsibly.
- Manage **data quality, security, and fairness** throughout the AI lifecycle.
- Ensure **explainability and traceability** in AI decisions.
- Establish safeguards for **human oversight** and escalation mechanisms.

3.6 PERFORMANCE EVALUATION

- Monitor and measure **AI performance and risk indicators**.
- Collect **user feedback** and stakeholder insights.
- Conduct **internal audits** of AI governance and technical processes.
- Perform **management reviews** to assess the AIMS' effectiveness.

3.7 IMPROVEMENT

- Identify **nonconformities or failures** in AI processes.
- Take **corrective actions** to address incidents, ethical breaches, or compliance gaps.
- Foster **continuous improvement** in AI governance, policies, and outcomes.
- Encourage **innovation balanced with responsibility**.

4. RELATIONSHIP WITH OTHER STANDARDS & FRAMEWORKS

4.1 ALIGNMENT WITH ISO MANAGEMENT SYSTEM STANDARDS

ISO 42001 is built on the **Annex SL High-Level Structure (HLS)**, the same framework used by other ISO standards. This allows organizations to **integrate AI governance with existing management systems**:

- **ISO 9001 (Quality Management)** → Ensures AI aligns with quality objectives and continuous improvement.
- **ISO 27001 (Information Security)** → Addresses confidentiality, integrity, and availability of data used in AI.
- **ISO 27701 (Privacy Management)** → Extends ISO 27001 to cover AI's handling of personal data.
- **ISO 31000 (Risk Management)** → Provides the broader enterprise risk management context for AI-related risks.

4.2 COMPLEMENTING AI-SPECIFIC FRAMEWORKS

- **NIST AI Risk Management Framework (AI RMF)**: Offers practical guidelines for identifying and mitigating AI risks. ISO 42001 complements it by embedding those practices into a formal management system.
- **IEEE Standards on AI Ethics**: Focuses on responsible design and ethical guidelines, while ISO 42001 provides a governance structure to apply them.
- **OECD AI Principles**: High-level principles for trustworthy AI (transparency, fairness, human oversight) that ISO 42001 operationalizes.

4.3 REGULATORY ALIGNMENT

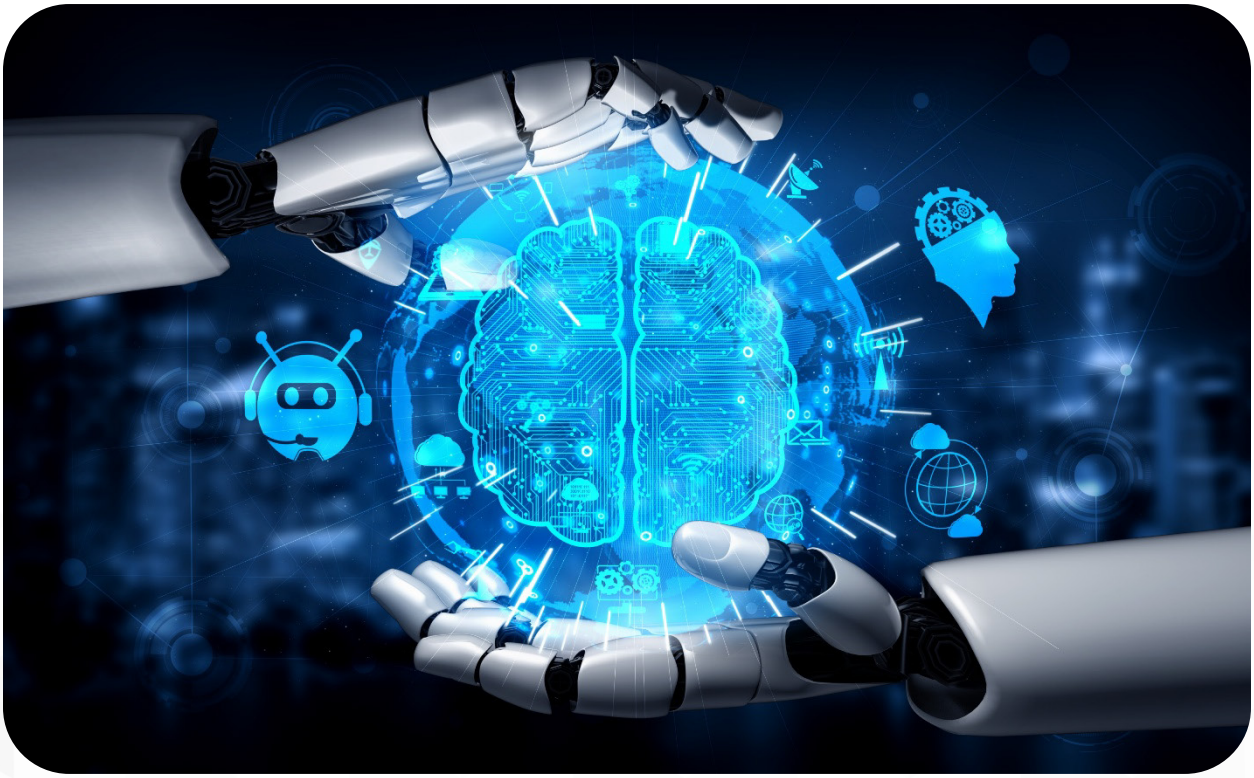
ISO 42001 helps organizations prepare for and demonstrate compliance with:

- **EU AI Act** → Especially relevant for organizations deploying "high-risk AI systems."
- **GDPR (General Data Protection Regulation)** → Protecting personal data processed by AI models.
- **U.S. Executive Orders on AI & Federal Guidance** → Encourages trustworthy and secure AI adoption.
- **National AI Strategies (e.g., Canada, UK, Singapore, UAE)** → ISO 42001 provides a practical compliance and governance layer for policy-driven adoption.

4.4 INTEGRATION BENEFITS

- **Consistency** → Organizations can unify AI, privacy, security, and quality processes under one framework.
- **Efficiency** → Shared audits, documentation, and governance structures reduce duplication.
- **Trust** → Stakeholders gain confidence when AI systems align with internationally recognized standards.
- **Scalability** → Easier adoption of future AI standards and regulations.

5. BENEFITS OF IMPLEMENTING ISO 42001



5.1 BUILD TRUST AND REPUTATION

- Demonstrates **commitment to responsible AI** practices.
- Builds confidence among customers, regulators, investors, and partners.
- Positions the organization as a **leader in ethical and trustworthy AI adoption**.

5.2 STRENGTHEN GOVERNANCE AND ACCOUNTABILITY

- Provides a **clear governance structure** for managing AI activities.
- Defines **roles, responsibilities, and oversight mechanisms**.
- Enhances **transparency and accountability** across the AI lifecycle.

5.3 IMPROVE RISK MANAGEMENT

- Identifies and mitigates AI-specific risks such as:
  - Bias and discrimination
  - Privacy violations
  - Security threats
  - Lack of explainability
- Reduces exposure to **financial, reputational, and legal risks**.

5.4 ENSURE REGULATORY AND ETHICAL COMPLIANCE

- Supports compliance with **global AI laws and regulations** (EU AI Act, GDPR, national AI frameworks).
- Aligns with **international ethical guidelines** (OECD, IEEE).
- Reduces risk of fines, lawsuits, and non-compliance penalties.

5.5 ENHANCE OPERATIONAL EFFICIENCY

- Standardized processes reduce duplication and inefficiencies.
- Integrated audits with **ISO 9001, 27001, 27701** streamline compliance.
- Provides **consistent quality** across AI projects and business units.

5.6 DRIVE CONTINUOUS IMPROVEMENT AND INNOVATION

- Encourages ongoing monitoring, learning, and adaptation as AI evolves.
- Promotes a **culture of responsible innovation**.
- Supports the balance between **rapid AI adoption and responsible safeguards**.

5.7 COMPETITIVE ADVANTAGE

- ISO 42001 certification can serve as a **market differentiator**.
- Attracts customers and partners who prioritize **trustworthy AI**.
- Improves chances of **winning contracts and funding** in regulated industries (healthcare, finance, government).

6. CHALLENGES IN ADOPTION OF ISO 42001

6.1 DEFINING THE SCOPE OF AI USE

- Difficulty in **clearly identifying all AI activities** across the organization.
- AI is often embedded in systems without being labeled as “AI.”
- Risk of **overlooking shadow AI projects** or third-party tools.

6.2 BALANCING INNOVATION WITH COMPLIANCE

- Organizations fear **compliance slowing down AI innovation**.
- Tension between **speed-to-market** and implementing responsible safeguards.
- Possible perception that governance adds **bureaucratic overhead**.

6.3 RESOURCE AND COST IMPLICATIONS

- Requires **investment in skills, training, and governance structures**.
- Small and medium enterprises (SMEs) may face **budgetary and staffing constraints**.
- Need for **dedicated teams** to oversee AIMS implementation.

6.4 COMPLEXITY OF RISK MANAGEMENT

- AI risks are **multidimensional** (bias, explainability, security, privacy).
- Risk assessment methods for AI are still **evolving and not standardized**.
- Ensuring **ongoing monitoring and mitigation** can be resource-intensive.

6.5 CULTURAL AND ORGANIZATIONAL BARRIERS

- Resistance from teams who view ISO 42001 as **compliance-heavy**.
- Lack of **awareness or buy-in from leadership** on AI governance.
- Employees may lack **clarity on roles and responsibilities** in AI oversight.

6.6 RAPIDLY EVOLVING AI LANDSCAPE

- Standards may **lag behind emerging technologies** like generative AI.
- Organizations must adapt ISO 42001 processes to **new risks and use cases**.
- Continuous improvement can be challenging in **fast-moving AI environments**.

6.7 INTEGRATION WITH EXISTING SYSTEMS

- Aligning ISO 42001 with **ISO 9001, 27001, 27701** and other frameworks may be complex.
- Requires **harmonization across departments** (IT, compliance, risk, operations).
- Organizations must avoid **duplication of controls** while maintaining consistency.

7. IMPLEMENTATION ROADMAP (HIGH-LEVEL)

STEP 1: CONDUCT A GAP ASSESSMENT

- Review existing policies, controls, and AI practices.
- Compare current state with **ISO 42001 requirements**.
- Identify strengths, weaknesses, and areas for improvement.
- Output: **Gap Analysis Report**.

STEP 2: DEFINE SCOPE AND GOVERNANCE STRUCTURE

- Determine which AI systems, business units, and geographies are in scope.
- Establish an **AI Governance Committee** or assign responsibility to existing risk/governance teams.
- Define **roles, responsibilities, and accountability** (e.g., Chief AI Officer, Ethics Board).
- Output: **AIMS Charter & Scope Document**.

STEP 3: DEVELOP AI POLICY AND OBJECTIVES

- Draft an **AI Policy** aligned with organizational values and strategy.
- Define **AI objectives**: transparency, fairness, privacy, explainability.
- Ensure objectives are **measurable and aligned** with business outcomes.
- Output: **AI Policy Statement** and **Strategic Objectives**.

STEP 4: ESTABLISH RISK MANAGEMENT FRAMEWORK

- Conduct **AI risk assessments** (bias, data quality, security, explainability).
- Map risks against organizational risk appetite and regulatory requirements.
- Define **controls and safeguards** for high-risk AI use cases.
- Output: **AI Risk Register** and **Mitigation Plan**.

STEP 5: BUILD COMPETENCE AND AWARENESS

- Train staff on AI governance, ethics, and compliance.
- Create awareness programs for developers, business leaders, and end-users.
- Promote a culture of **responsible innovation**.
- Output: **Training Records & Awareness Campaigns**.

STEP 6: IMPLEMENT OPERATIONAL PROCESSES

- Apply ISO 42001 to **AI lifecycle processes**: design, data preparation, testing, deployment, monitoring.
- Establish **documentation, traceability, and explainability** requirements.
- Ensure **human oversight** mechanisms are in place.
- Output: **Operational Procedures & AI Lifecycle Controls**.

STEP 7: MONITOR, MEASURE, AND AUDIT

- Define **key performance indicators (KPIs)** for AI systems.
- Conduct **internal audits** of the AIMS.
- Gather feedback from stakeholders (customers, regulators, employees).
- Output: **Audit Reports & Performance Dashboards**.

STEP 8: MANAGEMENT REVIEW

- Senior leadership reviews **audit results, risk status, and performance outcomes**.
- Adjust objectives and policies where needed.
- Ensure **continuous alignment with strategy and regulations**.
- Output: **Management Review Reports**.

STEP 9: CONTINUOUS IMPROVEMENT

- Address nonconformities and implement **corrective actions**.
- Adapt to **emerging technologies** (e.g., generative AI).
- Foster a loop of **learning, feedback, and innovation**.
- Output: **Improvement Log & Lessons Learned Repository**.

STEP 10 (OPTIONAL): CERTIFICATION

- If desired, pursue **third-party certification** to ISO 42001.
- Benefits: external validation, competitive advantage, regulatory confidence.
- Output: **ISO 42001 Certification**.

8. USE CASES OF ISO 42001

8.1 HEALTHCARE – SAFE AND TRANSPARENT DIAGNOSTICS

- **Challenge**: AI diagnostic tools (e.g., radiology image analysis, symptom checkers) risk bias and errors that affect patient safety.
- **Application**:
  - ISO 42001 ensures **risk assessments** for patient safety.
  - Embeds **explainability requirements** so doctors can interpret AI results.
  - Requires **data governance controls** for sensitive health data.
- **Benefit**: Improves patient trust and regulatory compliance (HIPAA, GDPR).

8.2 FINANCIAL SERVICES – FAIR CREDIT SCORING AND FRAUD DETECTION

- **Challenge**: AI models used in loan approvals and fraud monitoring risk discrimination against certain groups.
- **Application**:
  - ISO 42001 mandates **bias testing** and fairness reviews.
  - Requires **documentation and traceability** of AI decision-making.
  - Aligns with financial regulations (e.g., Basel III, GDPR, OCC guidance).
- **Benefit**: Builds customer trust and reduces legal risk from biased outcomes.

8.3 PUBLIC SECTOR – ETHICAL AI IN CITIZEN SERVICES

- **Challenge**: Governments use AI for citizen services (welfare eligibility, tax fraud detection), which must be transparent and fair.
- **Application**:
  - ISO 42001 requires **stakeholder engagement** in defining fairness.
  - Establishes **accountability and oversight mechanisms**.
  - Standardizes **risk evaluation** across government AI projects.
- **Benefit**: Enhances public trust in digital government initiatives.

8.4 MANUFACTURING – AI IN PREDICTIVE MAINTENANCE AND ROBOTICS

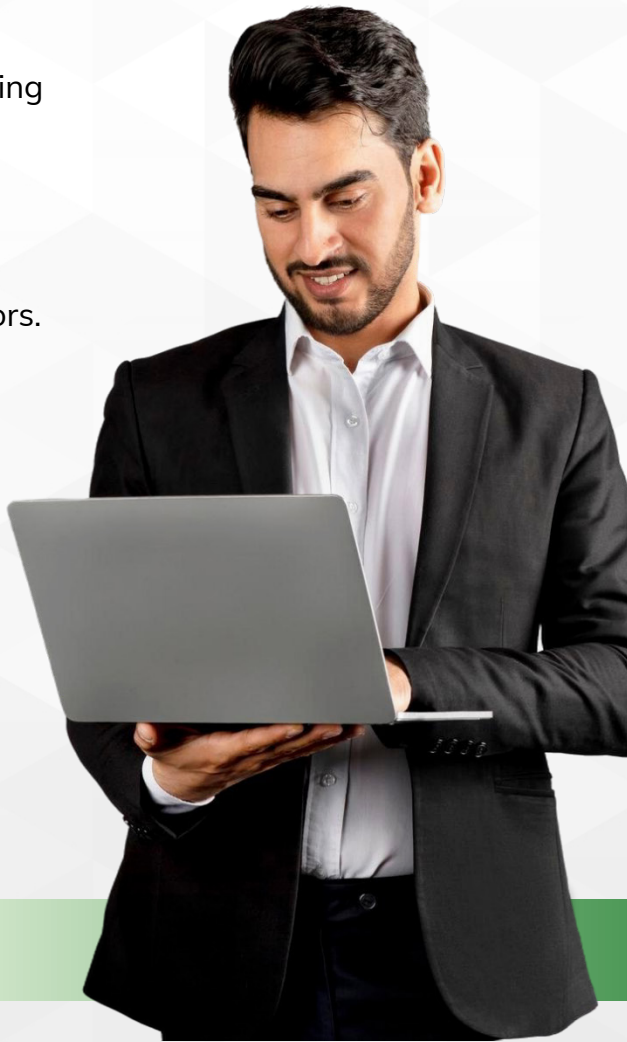
- **Challenge**: AI-driven automation and robotics introduce safety risks and operational dependency.
- **Application**:
  - ISO 42001 requires **risk management** for safety and reliability.
  - Mandates **monitoring KPIs** to evaluate performance.
  - Ensures **continuous improvement** for production AI models.
- **Benefit**: Improves efficiency while maintaining worker safety and compliance.

8.5 RETAIL – PERSONALIZED RECOMMENDATIONS AND CUSTOMER ANALYTICS

- **Challenge**: AI-powered recommendations may overuse personal data and cause privacy concerns.
- **Application**:
  - ISO 42001 integrates with **ISO 27701** for privacy controls.
  - Requires **data minimization** and transparency in data usage.
  - Embeds **continuous monitoring** for accuracy and fairness of AI outputs.
- **Benefit**: Increases customer loyalty and avoids reputational risks.

8.6 EDUCATION – ADAPTIVE LEARNING PLATFORMS

- **Challenge**: AI-driven learning platforms risk reinforcing inequality if not monitored.
- **Application**:
  - ISO 42001 requires **bias detection** in training data.
  - Promotes **human oversight** in student performance assessments.
  - Encourages **responsible data use** for minors.
- **Benefit**: Supports equitable learning while maintaining trust with parents and regulators.



9. KEY TAKEAWAYS FOR PRACTITIONERS

9.1 ISO 42001 IS ABOUT MANAGEMENT, NOT TECHNOLOGY

- Focuses on **how AI is governed, monitored, and improved**, not on coding or model architecture.
- Practitioners should think in terms of **processes, policies, and controls** rather than algorithms alone.

9.2 AI REQUIRES GOVERNANCE LIKE ANY OTHER BUSINESS PROCESS

- Treat AI systems like finance, security, or quality processes.
- Embed **roles, responsibilities, and accountability** across the AI lifecycle.
- Leadership buy-in is essential for success.

9.3 RISK-BASED THINKING IS CENTRAL

- Identify, assess, and mitigate **AI-specific risks** (bias, privacy, explainability, misuse).
- Use ISO 42001 to ensure risks are **aligned with organizational risk appetite and compliance obligations**.
- Maintain **continuous monitoring**—AI risks evolve rapidly.

9.4 INTEGRATION IS KEY

- ISO 42001 aligns with **ISO 9001, ISO 27001, ISO 27701, and ISO 31000**.
- Practitioners should leverage existing management systems to **avoid duplication and reduce complexity**.
- Builds efficiency through **shared governance, audits, and documentation**.

9.5 CONTINUOUS IMPROVEMENT IS NON-NEGOTIABLE

- AI evolves fast; governance must **adapt and improve continuously**.
- Use audits, feedback, and lessons learned to update controls and policies.
- Encourage a **culture of responsible innovation**.

9.6 CERTIFICATION PROVIDES COMPETITIVE ADVANTAGE

- While certification is optional, pursuing it shows **external validation** of responsible AI practices.
- Helps in **winning contracts, building trust, and meeting regulatory expectations**.

ISO 42001 WORKPLAN FOR ARTIFICIAL INTELLIGENCE MANAGEMENT SYSTEMS (AIMS) CONTROLS

1. GOVERNANCE & LEADERSHIP

Control: Establish AI governance structure (roles, policies, oversight).

Risk: Lack of accountability → biased/unethical AI decisions.

BEST PRACTICE:

- Create an **AI Ethics & Governance Committee**.
- Assign **Chief AI Officer / AI Risk Owner**.
- Define AI policy aligned with ISO 42001, NIST AI RMF, and NIST CSF.

TESTING STEPS:

- Verify governance documents exist.
- Interview stakeholders to confirm roles/responsibilities.
- Check alignment of AI policies with enterprise risk appetite.

ARTIFACTS REQUIRED:

- AI Policy Statement
- Governance Charter
- Organizational Chart with AI roles

REMEDIATION PLAN:

- If gaps exist, establish interim governance structure.
- Provide leadership training on AI risk.

REFERENCE:

- NIST AI RMF Core Function: *Govern*
- NIST CSF v2.0: *Govern (GV)*

2. RISK MANAGEMENT & PLANNING

Control: Conduct AI-specific risk assessments.

Risk: AI systems may introduce bias, privacy violations, or security vulnerabilities.

BEST PRACTICE:

- Use **NIST AI RMF Risk Profiles** to assess AI harms.
- Integrate AI risks into **enterprise risk register**.
- Define clear **risk tolerance and mitigation measures**.

TESTING STEPS:

- Review risk assessments for AI use cases.
- Validate inclusion of AI bias, explainability, privacy, and misuse risks.
- Confirm management review and approval.

ARTIFACTS REQUIRED:

- AI Risk Register
- Risk Assessment Reports
- Mitigation Plans

REMEDIATION PLAN:

- Reassess risks with updated models/data.
- Implement missing mitigation controls (bias testing, data quality checks).

REFERENCE:

- NIST AI RMF Core Function: *Map & Measure*
- NIST CSF v2.0: *Identify (ID)*

3. DATA MANAGEMENT & SECURITY

Control: Ensure data quality, security, and compliance.

Risk: Poor data governance → biased or insecure models.

BEST PRACTICE:

- Apply **data minimization & anonymization**.
- Enforce **access controls** (least privilege).
- Continuously monitor for **data drift and anomalies**.

TESTING STEPS:

- Inspect data pipelines for governance controls.
- Check audit trails for access management.
- Review encryption & anonymization settings.

ARTIFACTS REQUIRED:

- Data Governance Policy
- Data Quality Reports
- Data Access Logs

REMEDIATION PLAN:

- Implement data cleansing and anonymization.
- Strengthen IAM for AI datasets.

REFERENCE:

- NIST AI RMF: *Manage*
- NIST CSF: *Protect (PR)*, *Detect (DE)*

4. AI LIFECYCLE OPERATIONS

Control: Standardize design, development, deployment, and monitoring of AI.

Risk: Uncontrolled lifecycle → inconsistent AI behavior or ethical breaches.

BEST PRACTICE:

- Define AI lifecycle stages with **control gates**.
- Require **model documentation & traceability**.
- Enable **human-in-the-loop** decision escalation.

TESTING STEPS:

- Review AI project documentation for lifecycle adherence.
- Confirm explainability requirements are documented.
- Validate post-deployment monitoring logs.

ARTIFACTS REQUIRED:

- AI Development Lifecycle Document
- Model Cards / Datasheets
- Deployment Logs

REMEDIATION PLAN:

- Introduce missing lifecycle stages (e.g., model retirement).
- Enhance monitoring dashboards with bias detection.

REFERENCE:

- NIST AI RMF: *Measure & Manage*
- NIST CSF: *Respond (RS)*, *Recover (RC)*

5. PERFORMANCE EVALUATION & CONTINUOUS IMPROVEMENT

Control: Monitor AI systems against defined KPIs.

Risk: AI performance degrades over time (model drift, fairness issues).

BEST PRACTICE:

- Define **AI KPIs** (accuracy, fairness, explainability, robustness).
- Conduct **internal audits** of AI models.
- Capture **feedback loops** from users.

TESTING STEPS:

- Review monitoring dashboards for defined KPIs.
- Validate audit reports and remediation follow-ups.
- Confirm incident tracking for AI issues.

ARTIFACTS REQUIRED:

- AI KPI Dashboard
- Internal Audit Reports
- Nonconformity & Corrective Action Log

REMEDIATION PLAN:

- Update AI models with new data.
- Adjust controls based on incident root cause analysis.

REFERENCE:

- NIST AI RMF: *Manage*
- NIST CSF: *Detect (DE)*, *Recover (RC)*

6. AWARENESS, TRAINING & CULTURE

Control: Build organizational competence in responsible AI.

Risk: Lack of training → unintentional misuse of AI.

BEST PRACTICE:

- Conduct **AI ethics and governance training** for all staff.
- Tailor programs for **developers, risk managers, leadership**.
- Promote **responsible innovation culture**.

TESTING STEPS:

- Review training records and attendance.
- Interview staff for awareness.
- Validate refresher training schedules.

ARTIFACTS REQUIRED:

- Training Materials
- Attendance Logs
- AI Awareness Campaign Evidence

REMEDIATION PLAN:

- Roll out mandatory training for all AI stakeholders.
- Embed AI awareness in onboarding programs.

REFERENCE:

- NIST AI RMF: *Govern*
- NIST CSF: *Govern (GV)*, *Protect (PR)*

SUMMARY – WORKPLAN FLOW

1. **Governance** → Leadership, accountability, AI policy.
2. **Risk Management** → Identify, assess, and mitigate AI-specific risks.
3. **Data Management** → Secure, high-quality, privacy-compliant data.
4. **AI Lifecycle Operations** → Standardized, explainable, monitored AI.
5. **Performance Evaluation** → KPIs, audits, continuous improvement.
6. **Awareness & Training** → Building competence and ethical culture.

Domain	Control	Risk	Best Practice	Testing Steps	Artifacts Required	Remediation Plan	Reference (NIST AI RMF / NIST CSF)
Governance & Leadership	Establish AI governance structure (roles, policies, oversight)	Lack of accountability → biased/unethical AI decisions	Create AI Ethics & Governance Committee, assign AI Risk Owner, define AI Policy	Verify governance documents, interview stakeholders, check policy alignment with risk appetite	AI Policy, Governance Charter, Org Chart with AI roles	Establish interim governance structure, leadership training	NIST AI RMF: **Govern**, NIST CSF: **GV**
Risk Management & Planning	Conduct AI-specific risk assessments	Bias, privacy, or security risks overlooked	Use NIST AI RMF risk profiles, integrate AI risks into enterprise risk register, define mitigation plans	Review risk assessments, validate inclusion of AI-specific risks, confirm	AI Risk Register, Risk Reports, Mitigation Plans	Reassess risks, implement bias testing & data quality checks	NIST AI RMF: **Map & Measure**, NIST CSF: **ID**

Domain	Control	Risk	Best Practice	Testing Steps	Artifacts Required	Remediation Plan	Reference (NIST AI RMF / NIST CSF)
				management approval			
Data Management & Security	Ensure data quality, security, and compliance	Poor data governance → bias, insecurity, or privacy violations	Apply data minimization, enforce IAM, monitor data drift	Inspect pipelines, check audit trails, review encryption settings	Data Governance Policy, Data Quality Reports, Access Logs	Implement anonymization, improve IAM controls	NIST AI RMF: **Manage**, NIST CSF: **PR, DE**
AI Lifecycle Operations	Standardize AI design, development, deployment & monitoring	Uncontrolled lifecycle → inconsistent, unsafe, or unethical AI	Define lifecycle stages with control gates, require documentation & traceability, ensure human oversight	Review AI lifecycle docs, confirm explainability, validate monitoring logs	AI Lifecycle Doc, Model Cards, Deployment Logs	Add missing lifecycle stages, enhance monitoring dashboards	NIST AI RMF: **Measure & Manage**, NIST CSF: **RS, RC**
Performance Evaluation & Continuous Improvement	Monitor AI systems & conduct audits	Model drift, fairness issues, lack of continuous oversight	Define AI KPIs (accuracy, fairness, robustness), conduct internal audits, use feedback loops	Review KPI dashboards, validate audit reports, check corrective action tracking	KPI Dashboard, Audit Reports, Nonconformity Log	Update AI models, adjust controls, root cause analysis	NIST AI RMF: **Manage**, NIST CSF: **DE, RC**
Awareness, Training & Culture	Build organizational competence in AI governance	Lack of training → misuse or unawareness of risks	Conduct AI ethics training, tailor for developers/leadership, promote responsible AI culture	Review training records, interview staff, check refresher schedules	Training Materials, Attendance Logs, Awareness Campaigns	Roll out mandatory training, embed AI awareness in onboarding	NIST AI RMF: **Govern**, NIST CSF: **GV, PR**

Domain	Control	Risk	Best Practice	Testing Steps	Artifacts Required	Remediation Plan	Reference (NIST AI RMF / NIST CSF)
Governance & Leadership	Establish AI governance structure (roles, policies, oversight)	Lack of accountability → biased/unethical AI decisions	Create AI Ethics & Governance Committee, assign AI Risk Owner, define AI Policy	Verify governance documents, interview stakeholders, check policy alignment with risk appetite	AI Policy, Governance Charter, Org Chart with AI roles	Establish interim governance structure, leadership training	NIST AI RMF: **Govern**, NIST CSF: **GV**
Risk Management & Planning	Conduct AI-specific risk assessments	Bias, privacy, or security risks overlooked	Use NIST AI RMF risk profiles, integrate AI risks into enterprise risk register, define mitigation plans	Review risk assessments, validate inclusion of AI-specific risks, confirm management approval	AI Risk Register, Risk Reports, Mitigation Plans	Reassess risks, implement bias testing & data quality checks	NIST AI RMF: **Map & Measure**, NIST CSF: **ID**
Data Management & Security	Ensure data quality, security, and compliance	Poor data governance → bias, insecurity, or privacy violations	Apply data minimization, enforce IAM, monitor data drift	Inspect pipelines, check audit trails, review encryption settings	Data Governance Policy, Data Quality Reports, Access Logs	Implement anonymization, improve IAM controls	NIST AI RMF: **Manage**, NIST CSF: **PR, DE**
AI Lifecycle Operations	Standardize AI design, development, deployment & monitoring	Uncontrolled lifecycle → inconsistent, unsafe, or unethical AI	Define lifecycle stages with control gates, require documentation & traceability, ensure human oversight	Review AI lifecycle docs, confirm explainability, validate monitoring logs	AI Lifecycle Doc, Model Cards, Deployment Logs	Add missing lifecycle stages, enhance monitoring dashboards	NIST AI RMF: **Measure & Manage**, NIST CSF: **RS, RC**

Domain	Control	Risk	Best Practice	Testing Steps	Artifacts Required	Remediation Plan	Reference (NIST AI RMF / NIST CSF)
Performance Evaluation & Continuous Improvement	Monitor AI systems & conduct audits	Model drift, fairness issues, lack of continuous oversight	Define AI KPIs (accuracy, fairness, robustness), conduct internal audits, use feedback loops	Review KPI dashboards, validate audit reports, check corrective action tracking	KPI Dashboard, Audit Reports, Nonconformity Log	Update AI models, adjust controls, root cause analysis	NIST AI RMF: **Manage**, NIST CSF: **DE, RC**
Awareness, Training & Culture	Build organizational competence in AI governance	Lack of training → misuse or unawareness of risks	Conduct AI ethics training, tailor for developers/leadership, promote responsible AI culture	Review training records, interview staff, check refresher schedules	Training Materials, Attendance Logs, Awareness Campaigns	Roll out mandatory training, embed AI awareness in onboarding	NIST AI RMF: **Govern**, NIST CSF: **GV, PR**


SkillWeed