GSDC
Global Skill Development Council

ISO 42001 LEAD AUDITOR

Clause-wise Audit Checklist

www.gsdcouncil.org

Introduction

1	**Purpose** Provide a structured, clause-by-clause checklist for ISO 42001 audits to ensure comprehensive evaluation
2	**Scope** Covers all key clauses of ISO/IEC 42001:2023 Artificial Intelligence Management System (AIMS)
3	**Usage** Designed for lead auditors to verify compliance, evidence, and effectiveness systematically
4	**Format** Consistent checklist style with audit questions, evidence requirements, and compliance notes

This checklist serves as a comprehensive tool for auditors conducting ISO 42001 assessments, ensuring thorough coverage of all requirements while maintaining consistency across audit activities. Each section follows a standardized format to facilitate efficient auditing and clear documentation of findings.

Clause 4: Context of the Organization

Audit Questions

- Has the organization identified internal and external issues relevant to AI management?
- Are the needs and expectations of interested parties documented and reviewed?
- Is the scope of the AI Management System clearly defined and justified?
- Does the organization understand the regulatory environment affecting AI operations?
- Are technological trends and competitive factors considered in context analysis?
- Have stakeholder groups been identified including customers, regulators, employees, and affected communities?
- Is there a process to regularly review and update context analysis?
- Are AI-specific risks and opportunities identified based on organizational context?
- Does the scope statement clearly define boundaries, applicability, and exclusions?
- Are interfaces with other management systems documented?
- Is the context analysis aligned with organizational strategic objectives?
- Have ethical considerations specific to the organization's AI use been identified?

Evidence to Verify

- Context analysis documents
- Stakeholder registers
- Scope statements

Compliance Notes

Context must be current and reflect AI-specific risks and opportunities. Organizations should demonstrate understanding of their unique AI landscape and stakeholder expectations.

Regular updates ensure alignment with evolving AI technologies and regulatory environments.

Clause 5: Leadership and Commitment

Audit Questions

- Does top management demonstrate leadership and commitment to AI governance through active participation and resource allocation?
- Are roles, responsibilities, and authorities for AI management clearly assigned and communicated across the organization?
- Is there a policy for responsible AI aligned with organizational objectives and ethical standards?
- Has top management established an AI governance framework with clear accountability?
- Does leadership actively promote ethical AI culture throughout the organization?
- Are adequate resources allocated for AI management system implementation and maintenance?
- Is the AI policy communicated to all relevant stakeholders?
- Does management ensure the AI management system achieves its intended outcomes?
- Are AI objectives integrated into organizational strategic planning?
- Does leadership ensure compliance with applicable legal and regulatory requirements?
- Is there evidence of management commitment in meeting minutes and decisions?
- Are conflicts of interest in AI decision-making identified and managed?
- Does leadership ensure competence of personnel involved in AI activities?
- Is there a process for escalating AI-related issues to top management?

Evidence to Verify

- Signed AI governance policy
- Organizational charts with AI roles
- Meeting minutes showing leadership involvement
- Resource allocation documents

> Leadership must actively promote ethical AI and risk management culture throughout the organization, demonstrating commitment beyond policy statements.

Clause 6: Planning

Audit Questions

- Has the organization identified AI-related risks and opportunities specific to their operations and industry context?
- Are objectives for AI management established, measurable, monitored, and communicated throughout the organization?
- Is there a documented plan to address risks and opportunities, including comprehensive risk treatment strategies?
- Are AI risks assessed for likelihood and impact including bias, fairness, privacy, and security concerns?
- Have risk treatment options been evaluated and selected based on organizational risk appetite?
- Are AI objectives SMART (Specific, Measurable, Achievable, Relevant, Time-bound)?
- Is there a process to identify legal and regulatory requirements applicable to AI systems?
- Are ethical risks including discrimination, transparency, and accountability addressed in planning?
- Have opportunities for AI innovation and competitive advantage been identified?
- Are resources and responsibilities assigned for achieving AI objectives?
- Is there a process to monitor progress toward AI objectives?
- Are risk treatment plans reviewed and updated regularly?
- Have contingency plans been developed for high-risk AI scenarios?
- Is planning integrated with organizational change management processes?
- Are stakeholder concerns incorporated into planning activities?

Evidence to Verify

Risk assessment reports, AI management objectives documentation, risk treatment plans, and evidence of planning integration across organizational functions.

> Planning must integrate AI-specific ethical, legal, and operational risks. Consider bias, fairness, transparency, data privacy, security vulnerabilities, and societal impact in comprehensive risk assessments.

Clause 7: Support

Audit Questions

- Are resources adequate for AI management system implementation, including personnel, technology, and budget?
- Is competence ensured for personnel managing AI systems through training and qualification verification?
- Are communication processes established internally and externally regarding AI governance and transparency?
- Is documented information controlled, maintained, and accessible to relevant stakeholders?
- Have infrastructure requirements for AI systems been identified and provided?
- Are organizational knowledge requirements for AI management identified and maintained?
- Is there a competency framework defining required skills for AI roles?
- Are training needs identified and training programs implemented for AI personnel?
- Is awareness of AI policy and objectives promoted throughout the organization?
- Are internal communication channels effective for AI-related information sharing?
- Is there a process for external communication with stakeholders about AI systems?
- Are documents created, updated, and controlled according to documented procedures?
- Is documented information protected from unauthorized access and modification?
- Are records retained according to legal and organizational requirements?
- Is there a process to ensure availability of documented information when needed?
- Are external documents of external origin identified and controlled?

Evidence to Verify

- Training records and competency assessments
- Resource allocation plans
- Communication logs and protocols
- Document control procedures

> Competence must include AI ethics, bias mitigation, and technical understanding to ensure effective AI management system operation.

Clause 8: Operation

Audit Questions

- Are AI lifecycle processes (design, development, deployment, monitoring) controlled with documented procedures and validation points?
- Is there evidence of bias testing, explainability mechanisms, and human oversight throughout AI operations?
- Are operational controls in place for data management, AI model validation, and performance monitoring?
- Are third-party AI components, libraries, and services assessed and managed for compliance and risk?
- Are AI system requirements clearly defined and documented before development?
- Is there a process for AI model selection, training, and validation?
- Are data quality checks performed before using data for AI training or inference?
- Is model performance continuously monitored against defined metrics?
- Are mechanisms in place to detect and address model drift and degradation?
- Is there a process for managing AI system updates and version control?
- Are human-in-the-loop controls implemented for high-risk AI decisions?
- Is explainability of AI decisions documented and communicated to stakeholders?
- Are bias and fairness assessments conducted throughout the AI lifecycle?
- Is there a process for decommissioning AI systems when no longer needed?
- Are operational procedures documented and accessible to relevant personnel?
- Is there a process for managing AI system incidents and failures?
- Are security controls implemented to protect AI systems from threats?

Evidence to Verify

- AI model documentation and specifications
- Bias test results and mitigation plans
- Human-in-the-loop procedures
- Third-party vendor assessments
- Validation and verification records

Compliance Notes

Operations must ensure transparency, fairness, and traceability of AI outputs. Documentation should demonstrate continuous monitoring and improvement of AI system performance.

Clause 9: Performance Evaluation

Audit Questions:

- Are monitoring and measurement activities defined and implemented for AI performance metrics?
- Is internal audit conducted regularly to assess AI management system conformity and effectiveness?
- Are management reviews held with documented inputs and outputs related to AI governance?
- Have key performance indicators (KPIs) been established for AI system performance?
- Is there a process to collect and analyze data on AI system effectiveness?
- Are monitoring results used to identify trends and improvement opportunities?
- Is the internal audit program planned based on risk and previous audit results?
- Are internal auditors independent and competent in AI management system requirements?
- Are audit findings documented and communicated to relevant management?
- Is there a process to verify closure of audit findings?
- Are management reviews conducted at planned intervals?
- Do management reviews consider changes in internal and external issues affecting AI?
- Are management review inputs comprehensive including audit results, performance data, and stakeholder feedback?
- Do management reviews result in decisions on improvement opportunities and resource needs?
- Are customer and stakeholder satisfaction with AI systems measured?
- Is compliance with legal and regulatory requirements evaluated regularly?

Evidence to Verify

- Internal audit reports and schedules
- Performance metrics dashboards
- Management review minutes and action items
- KPI tracking documentation
- Audit findings and closure records

Evaluation must focus on AI risk controls effectiveness and continual improvement. Reviews should address both technical performance and ethical compliance aspects of AI systems.

Clause 10: Improvement

The improvement process ensures that the AI Management System remains effective, responsive to emerging risks, and aligned with organizational objectives through systematic identification and resolution of issues.

Audit Questions

- Are nonconformities related to AI management identified promptly and corrective actions taken?
- Is there a process for continual improvement of the AI Management System?
- Are root causes analyzed to prevent recurrence?
- Are improvement opportunities identified proactively?
- Is there a documented procedure for handling nonconformities and corrective actions?
- Are corrective actions evaluated for effectiveness after implementation?
- Is there a process to identify and implement preventive actions?
- Are lessons learned from incidents and audits captured and shared?
- Is there evidence of continual improvement in AI system performance and governance?
- Are improvement initiatives prioritized based on risk and impact?
- Is innovation in AI management practices encouraged and supported?
- Are best practices from industry and research incorporated into the management system?
- Is there a process to review and update AI policies and procedures regularly?
- Are stakeholder suggestions for improvement considered and acted upon?
- Is the effectiveness of the AI management system evaluated and improved over time?

Evidence to Verify

- Corrective action records
- Improvement plans and initiatives
- Lessons learned documentation
- Root cause analysis reports

Annex A: AI Governance and Ethical Requirements

Audit Questions

- Does the organization have documented AI ethics guidelines aligned with ISO 42001 principles?
- Are governance structures in place to oversee AI ethical compliance and accountability?
- Are ethical principles such as fairness, transparency, and accountability embedded in AI development?
- Is there a process to assess ethical implications of AI systems before deployment?
- Are diverse perspectives included in ethical decision-making about AI?
- Is there an ethics committee or board responsible for AI governance?
- Are ethical guidelines communicated to all personnel involved in AI activities?
- Is there a process to address ethical dilemmas and conflicts in AI use?
- Are human rights considerations integrated into AI system design and operation?
- Is there a mechanism for stakeholders to raise ethical concerns about AI systems?
- Are ethical risks assessed and mitigated throughout the AI lifecycle?
- Is there evidence of ethical review for high-risk AI applications?
- Are AI systems designed to avoid discrimination and promote inclusivity?
- Is there a process to ensure AI systems respect privacy and data protection rights?
- Are societal impacts of AI systems considered and addressed?

Evidence to Verify

- Ethics policy documents
- Governance committee charters
- Ethical risk assessments
- Decision-making frameworks
- Stakeholder consultation records

> Governance must ensure accountability and transparency in AI decision-making. Ethics frameworks should address fairness, non-discrimination, privacy, and societal impact considerations throughout the AI lifecycle.

Annex A: Risk Identification and Impact Assessment

Audit Questions:

- Are AI risks identified systematically, including bias, privacy violations, security vulnerabilities, and societal impact concerns?
- Is impact assessment performed before AI deployment to evaluate potential consequences and mitigation requirements?
- Are risk assessments regularly updated to reflect changes in AI systems, data, and operating environments?
- Have risk identification methods been defined and applied consistently?
- Are both technical and non-technical risks (ethical, legal, reputational) identified?
- Is there a risk register documenting all identified AI-related risks?
- Are risks assessed for likelihood, impact, and detectability?
- Is impact assessment conducted for affected stakeholders and communities?
- Are cumulative and systemic risks from multiple AI systems considered?
- Is there a process to identify emerging risks from new AI technologies?
- Are risk assessments documented with clear rationale and assumptions?
- Is risk ownership assigned with clear accountability?
- Are risk assessment results communicated to relevant stakeholders?
- Is there a process to validate risk assessment accuracy through monitoring?
- Are lessons learned from incidents incorporated into risk identification?
- Is the risk assessment methodology reviewed and improved regularly?

Evidence to Verify

Risk registers with comprehensive AI-specific risks, impact assessment reports covering ethical and operational dimensions, mitigation plans with clear ownership, and update schedules demonstrating ongoing review.

> Risk assessments must be dynamic and updated with AI system changes, emerging threats, and evolving regulatory landscapes to maintain effective risk management.

Annex A: Data Management Controls

Audit Questions:

- Are data quality, integrity, and ethical use controls implemented throughout data lifecycle?
- Is data provenance and lineage documented for AI training and inference data?
- Are privacy laws and data protection requirements integrated into data handling?
- Is there a data governance framework defining roles, responsibilities, and policies?
- Are data sources evaluated for quality, bias, and representativeness?
- Is there a process for data collection, storage, and processing that ensures compliance?
- Are data quality metrics defined and monitored regularly?
- Is personal data processed in accordance with consent and legal basis requirements?
- Are data minimization principles applied to AI systems?
- Is there a process to ensure data accuracy and completeness?
- Are data retention and deletion policies defined and implemented?
- Is data security ensured through encryption, access controls, and monitoring?
- Are data breaches detected and responded to promptly?
- Is there a process to manage data from third-party sources?
- Are synthetic or augmented data generation processes controlled and validated?
- Is data lineage traceable from source to AI model output?
- Are data processing activities documented in records of processing activities?

Evidence to Verify

- Data management policies and procedures
- Data audit trails and lineage tracking
- Data quality reports and metrics
- Privacy impact assessments
- Data governance frameworks

Compliance Notes

Data controls must prevent bias and ensure compliance with privacy laws including GDPR, CCPA, and sector-specific regulations.

Documentation should demonstrate data quality validation and ethical sourcing throughout the AI lifecycle.

Annex A: Transparency and Explainability

Transparency and explainability are fundamental to building trust and ensuring accountability in AI systems. Organizations must demonstrate clear mechanisms for explaining AI decisions to various stakeholder groups.

Audit Questions:

- Are AI models designed to provide explainable outputs with interpretable decision factors?
- Is documentation available to explain AI decision logic to stakeholders at appropriate technical levels?
- Are tools and methods available to help users understand and challenge AI decisions?
- Is there a transparency policy defining what information about AI systems is disclosed?
- Are stakeholders informed about when they are interacting with AI systems?
- Is the purpose and intended use of AI systems clearly communicated?
- Are limitations and potential errors of AI systems disclosed to users?
- Is there documentation explaining how AI models make decisions?
- Are explainability techniques appropriate for the complexity and risk level of AI systems?
- Is there a process to provide explanations for individual AI decisions when requested?
- Are model architectures and algorithms documented in accessible language?
- Is training data characteristics and sources disclosed appropriately?
- Are performance metrics and accuracy rates communicated to stakeholders?
- Is there a process to handle requests for information about AI systems?
- Are transparency requirements balanced with intellectual property protection?

Evidence to Verify

- Explainability reports
- User guides and documentation
- Model interpretability tools
- Decision explanation logs

Transparency is critical for trust and regulatory compliance. Organizations must balance explainability with intellectual property protection and system security.

Annex A: Human Oversight and Intervention

Audit Questions:

- Are human-in-the-loop controls established for critical AI decisions requiring human judgment?
- Is there continuous monitoring of AI outputs with automated alerts for anomalies or questionable decisions?
- Are clear escalation and intervention processes defined when AI outputs require human review or override?
- Is complete documentation maintained of oversight activities, interventions, and rationale for decisions?
- Are thresholds defined for when human intervention is required in AI processes?
- Do oversight personnel have appropriate authority and competence to intervene?
- Is there a process to ensure human oversight is meaningful and not merely procedural?
- Are human oversight mechanisms tested regularly for effectiveness?
- Is there training for personnel responsible for AI oversight?
- Are override capabilities available and accessible when needed?
- Is there a process to review and learn from human interventions?
- Are oversight activities proportionate to the risk level of AI systems?
- Is there independence between AI system operators and oversight personnel where appropriate?
- Are oversight findings used to improve AI system design and operation?
- Is there a process to prevent automation bias in human oversight?

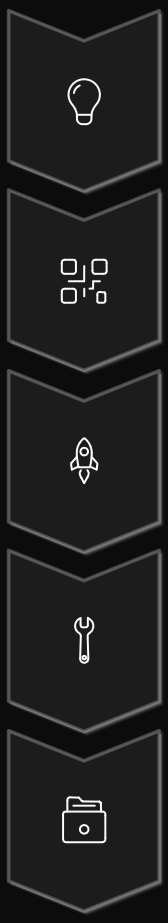
Evidence to Verify

- Oversight procedures and protocols
- Incident logs with human interventions
- Escalation protocols and decision trees
- Training records for oversight personnel

Compliance Notes

Human oversight must be proactive and documented. Organizations should define clear thresholds for when human intervention is required and ensure oversight personnel have appropriate authority and competence.

Annex A: Lifecycle Traceability



Design

Initial concept and requirements documentation

Development

Build, test, and validation phases

Deployment

Production release and monitoring

Maintenance

Updates and improvements

Decommission

Retirement and data handling

Audit Questions

- Is the AI system lifecycle fully documented from design to decommissioning with clear phase transitions?
- Are changes and updates tracked with impact analysis and stakeholder notification?
- Is version control maintained with rollback capabilities?

Evidence to Verify

- Lifecycle documentation for each phase
- Change logs with impact assessments
- Version control records
- Decommissioning procedures

Traceability supports accountability and audit readiness. Complete lifecycle documentation enables effective governance and facilitates compliance demonstration.

Annex A: Third-Party AI Components and Supply Chain

Component Vetting

Are third-party AI models and components vetted for compliance, security, and risk before integration?

Supplier Management

Is there a process to manage supplier risks, contractual obligations, and service level agreements?

Ongoing Monitoring

Are third-party components continuously monitored for updates, vulnerabilities, and compliance changes?

Evidence to Verify

- Vendor assessments and due diligence reports
- Contracts with AI suppliers including SLAs
- Risk mitigation plans for supply chain
- Third-party audit certificates
- Vendor performance reviews

Compliance Notes

Third-party risks must be integrated into the AI Management System with clear accountability. Organizations remain responsible for AI system compliance regardless of vendor involvement.

Annex A: Incident Management and Response

Effective incident management ensures rapid identification and resolution of AI-related issues while capturing valuable lessons to prevent future occurrences and strengthen the management system.

Audit Questions

- Is there a documented process for AI-related incident detection, reporting, and response?
- Are incident severity levels defined with corresponding response procedures?
- Are lessons learned from incidents incorporated into system improvements?
- Is incident response tested regularly through simulations?

Evidence to Verify

- Incident reports and logs
- Response plans and procedures
- Post-incident review documents
- Root cause analysis reports
- Corrective action implementation records

Incident management must be timely and effective to maintain trust. Organizations should establish clear escalation paths, communication protocols, and stakeholder notification procedures for AI-related incidents.

Annex A: Training and Awareness

AI Ethics Training

Are personnel trained on AI ethics principles, fairness, and responsible AI practices?

Risk Management

Do employees understand AI-specific risks, controls, and their role in risk mitigation?

Operational Controls

Are staff competent in implementing and monitoring operational controls for AI systems?

Effectiveness Evaluation

Is training effectiveness evaluated through assessments and updated regularly based on feedback?

Evidence to Verify

- Training records with attendance logs
- Competency assessments and test results
- Training materials and curricula
- Training effectiveness evaluations
- Continuous education plans

Compliance Notes

Continuous education is essential for maintaining compliance as AI technology and regulations evolve. Training programs should be tailored to roles and regularly refreshed.

Annex A: Documentation and Record Keeping

Document Control

Are all AI management system documents controlled, versioned, and accessible to authorized personnel?

Regular Reviews

Are documents reviewed regularly for accuracy, relevance, and compliance with current requirements?

Audit Trails

Are audit trails maintained for critical AI decisions, changes, and approvals?

Retention Policies

Are retention periods defined and implemented for different document types?

Evidence to Verify

- Document control procedures
- Audit trail logs and histories
- Document review records
- Access control matrices
- Retention schedules

Documentation must support transparency and auditability. Complete, accurate records demonstrate organizational commitment to AI governance and enable effective oversight and continuous improvement.

Conclusion and Auditor Recommendations

10	10	100%
Core Clauses	**Annex Controls**	**Coverage**
Mandatory requirements covering context through improvement	Specific AI management and ethical requirements	Complete ISO 42001 compliance framework

Summary Approach

Auditors should summarize compliance status clause-wise, providing a comprehensive overview of the organization's conformity to ISO 42001 requirements. This includes identifying strengths, weaknesses, and areas requiring immediate attention.

01

Identify Nonconformities

Highlight major nonconformities, minor findings, and opportunities for improvement discovered during the audit

02

Recommend Actions

Recommend specific, actionable corrective actions with timelines and responsible parties for resolution

03

Drive Improvement

Propose continuous improvement steps to enhance AI management system effectiveness and maturity

04

Maintain Alignment

Encourage periodic internal audits and management reviews to sustain certification readiness

Emphasize the importance of maintaining the AI Management System aligned with evolving AI risks, emerging technologies, and changing regulatory landscapes. Continuous monitoring and adaptation are essential for long-term compliance and organizational success in AI governance.

GSDC
Global Skill Development Council

CERTIFIED ISO 42001:2023 LEAD AUDITOR

ABOUT GSDC CERTIFICATION

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING OBJECTIVE

- Gain insights into autonomous decision-making processes
- Apply knowledge using ready-to-implement templates
- Demonstrate ability to work with Agentic AI models
- Validate your skills wit

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org