GSDC
Global Skill Development Council

ISO 42001

Audit Questionnaire

ISO 42001 Audit Questionnaire with 100+ Checklist

Evaluate Readiness, Identify Gaps, and Strengthen Your AI Management System

The Growing Need for Structured ISO 42001 Audits

As artificial intelligence (AI) becomes increasingly integrated into core business functions and public-facing systems, the call for standardized, ethical, and auditable AI management practices has grown louder.

To address this demand, ISO introduced ISO 42001, a management system standard that guides organizations in developing, deploying, and maintaining AI systems responsibly.

Organizations aiming to align with ISO 42001 whether for internal governance, industry trust, or certification must undergo rigorous self-assessment to understand their current maturity and compliance levels. This is where the ISO 42001 Audit Questionnaire becomes indispensable.

The ISO 42001 Audit Questionnaire, developed as an exclusive resource by the Global Skills Development Council (GSDC), serves as a comprehensive internal audit tool.

With over 100 targeted checklist items, it enables organizations to:

- Evaluate their conformance to ISO 42001 across all relevant clauses.
- Identify compliance gaps and governance deficiencies.
- Document existing policies, practices, and outcomes.
- Formulate data-driven action plans for remediation and certification readiness.

This tool is structured to provide a practical, detailed, and scalable audit framework that aligns with the real-world demands of AI deployment in sectors such as finance, healthcare, education, retail, government, and beyond.

How to Use the ISO 42001 Audit Questionnaire

The ISO 42001 Audit Questionnaire is divided into thematic sections based on the structure of the standard. Each section contains specific, clause-aligned questions intended to help organizations assess the presence, effectiveness, and documentation of their AI management system components.

Step 1: Clause Mapping and Customization

Begin by reviewing the scope of ISO 42001 and identifying which clauses are applicable to your organization. This ensures the audit is tailored to your operational model, sector, and AI system use cases.

Customize the checklist accordingly:

- Mark non-applicable items.
- Add supplementary items if your organizational context demands it (e.g., domain-specific regulatory requirements).

Step 2: Assign Responsibilities

For each section or domain (e.g., risk assessment, model explainability, data governance), assign the audit to a relevant subject matter expert or team:

- Legal or Compliance for policy-based questions.
- Data Science or AI teams for technical governance checks.
- IT and Security teams for infrastructure, access, and monitoring items.
- HR or Training for awareness and competency questions.

This promotes accuracy and encourages cross-functional collaboration.

Step 3: Conduct the Audit with Evidence Collection

For each checklist item, the audit team should:

- Answer whether the requirement is met: **Yes**, **No**, or **Partially**.
- Provide supporting evidence such as policies, logs, reports, or observations.
- Assess the maturity or robustness of the control (optional scoring fields can be used).
- Indicate the criticality or priority: **High**, **Medium**, or **Low**.

Sample Item:

Checklist Question: Is there a documented process for identifying and evaluating the ethical implications of AI models before deployment?
Response: Partially
Evidence: Draft AI Ethics Policy (under revision), Risk Committee Minutes
Priority: High

Repeat this process for each item in the checklist.

Step 4: Analyze Results and Identify Gaps

Once the audit is complete, compile the findings and categorize items into:

- Fully compliant areas
- Partially implemented areas
- Non-compliant or missing areas

This becomes your **gap register**, which forms the foundation for creating an ISO 42001 implementation or remediation roadmap.

Use filters or dashboards if available to:

- Prioritize issues by risk or business impact

- Identify quick wins versus long-term process changes
- Track progress in subsequent audits

Step 5: Document Action Plans and Review Cycles

For all non-compliant or partially compliant checklist items, document a corresponding action plan that includes:

- Task owner
- Description of remediation steps
- Target dates
- Required resources
- Review checkpoints

Ensure that the audit and action plan are reviewed periodically—typically quarterly or in sync with key project phases—to promote continual improvement and audit readiness.

ISO 42001 Audit Checklist

1. **Has the organization determined external and internal issues relevant to its purpose and AI management system?**
   (Clause 4.1 – Context of the Organization)
2. **Has the organization identified stakeholders relevant to the AI system and understood their expectations?**
   (Clause 4.2 – Context of the Organization)
3. **Is the scope of the AI management system clearly defined, documented, and communicated?**
   (Clause 4.3 – Context of the Organization)
4. **Is there evidence of top management commitment to the AI management system?**
   (Clause 5.1 – Leadership)
5. **Has the organization established an AI policy appropriate to its purpose and aligned with ISO 42001 principles?**
   (Clause 5.2 – Leadership)
6. **Have roles and responsibilities for the AI management system been clearly assigned and communicated?**
   (Clause 5.3 – Leadership)
7. **Has the organization identified risks and opportunities related to AI systems that need to be addressed?**
   (Clause 6.1 – Planning)
8. **Are there established objectives for the AI management system, and are they measurable and aligned with the policy?**
   (Clause 6.2 – Planning)

9. **Are resources adequately provided to establish, implement, and maintain the AI management system?**
   (Clause 7.1 – Support)
10. **Has the organization ensured necessary competence of personnel involved in AI system development and oversight?**
    (Clause 7.2 – Support)
11. **Has the organization identified training needs and ensured that relevant personnel receive appropriate awareness and education related to AI systems?**
    (Clause 7.2 – Support)
12. **Are there processes in place to ensure that AI-related communication is clear, timely, and consistent across all relevant stakeholders?**
    (Clause 7.4 – Support)
13. **Has the organization established and maintained documented information required for the effective implementation of the AI management system?**
    (Clause 7.5 – Support)
14. **Is documented information appropriately controlled to ensure availability, confidentiality, integrity, and accessibility when needed?**
    (Clause 7.5.3 – Support)
15. **Are AI system requirements, including ethical and legal constraints, considered during operational planning?**
    (Clause 8.1 – Operation)
16. **Are responsibilities and authorities clearly assigned for managing AI system changes and lifecycle stages?**
    (Clause 8.2 – Operation)
17. **Does the organization have procedures to evaluate and approve AI models before deployment?**
    (Clause 8.3 – Operation)

18. **Are safeguards implemented to mitigate the risks of unintended consequences from AI model outputs?**
    (Clause 8.3 – Operation)
19. **Is there a mechanism to review AI system performance against expected outcomes on a regular basis?**
    (Clause 8.4 – Monitoring and Evaluation)
20. **Does the organization maintain traceability and transparency for AI decision-making processes?**
    (Clause 8.5 – Transparency and Accountability)
21. **Is user feedback related to AI system behavior or outcomes collected and analyzed for improvements?**
    (Clause 8.6 – Feedback and Continual Improvement)
22. **Are AI models retrained, recalibrated, or revised when they no longer meet performance expectations or ethical guidelines?**
    (Clause 8.6 – Feedback and Continual Improvement)
23. **Has the organization established protocols for incident reporting and handling AI system failures or breaches?**
    (Clause 8.7 – Incident Management)
24. **Are data inputs and outputs of AI systems continuously monitored for accuracy, bias, and compliance?**
    (Clause 8.8 – Data Management)
25. **Is there a formal review process to assess compliance of AI systems with applicable legal, regulatory, and contractual obligations?**
    (Clause 8.9 – Legal and Regulatory Compliance)
26. **Has the organization defined criteria for data quality, relevance, and representativeness before using datasets in AI systems?**
    (Clause 8.9 – Data Management)

27. **Are data sources and acquisition methods documented, including licensing, consent, and provenance?**
    (Clause 8.9 – Data Governance)
28. **Is there a formal data retention and deletion policy specific to AI training and operational data?**
    (Clause 8.9 – Data Lifecycle Management)
29. **Does the organization assess and mitigate potential biases in datasets used to train AI systems?**
    (Clause 8.9 – Bias and Fairness)
30. **Are pre-processing, augmentation, or transformation steps on training data validated and documented?**
    (Clause 8.9 – Data Processing)
31. **Is there a procedure to ensure continuous validation of AI system behavior post-deployment?**
    (Clause 8.10 – Model Monitoring and Governance)
32. **Are explainability and interpretability standards defined for AI models, particularly for high-risk use cases?**
    (Clause 8.10 – Explainability and Interpretability)
33. **Has the organization identified specific ethical principles or frameworks guiding AI design and use?**
    (Clause 8.11 – Ethical Considerations)
34. **Is there a designated ethics committee or review board involved in oversight of AI initiatives?**
    (Clause 8.11 – Governance Oversight)
35. **Are users informed when they are interacting with an AI system, especially in cases of automated decisions?**
    (Clause 8.12 – Human-Centered Design)

36. **Is human oversight built into the AI lifecycle where necessary, including override or intervention capabilities?**
    (Clause 8.12 – Human-in-the-Loop)
37. **Are risk assessments performed before AI system deployment, including ethical, operational, and technical risks?**
    (Clause 8.13 – Risk Management)
38. **Are mitigation plans in place for foreseeable high-impact or safety-related failures of AI systems?**
    (Clause 8.13 – Risk Mitigation)
39. **Is there documentation of roles and responsibilities for all personnel managing or interacting with AI systems?**
    (Clause 9.1 – Documentation and Roles)
40. **Are internal audits conducted at planned intervals to verify conformity with ISO 42001 requirements?**
    (Clause 9.2 – Internal Audit Planning)
41. **Are audit results, findings, and follow-up actions documented and communicated to relevant management levels?**
    (Clause 9.2 – Internal Audit Reporting)
42. **Are nonconformities identified during audits analyzed for root causes and corrected effectively?**
    (Clause 9.2 – Nonconformity Management)
43. **Is a formal management review conducted at planned intervals to assess the suitability, adequacy, and effectiveness of the AI management system?**
    (Clause 9.3 – Management Review)
44. **Does the management review consider changes in internal/external issues, stakeholder feedback, performance data, and risk assessments?**
    (Clause 9.3 – Inputs to Management Review)

45. **Are decisions and actions arising from the management review documented and followed up systematically?**
    (Clause 9.3 – Outputs of Management Review)
46. **Are all incidents related to AI system failures, inaccuracies, or ethical breaches formally recorded and reviewed?**
    (Clause 10.1 – Incident Reporting)
47. **Is there a structured process to analyze incidents for root causes and implement corrective actions?**
    (Clause 10.1 – Incident Analysis)
48. **Are recurring or systemic issues identified and prioritized for organizational-level improvement?**
    (Clause 10.2 – Trend Analysis and Improvement)
49. **Is a continual improvement plan in place for the AI management system, and is it reviewed regularly?**
    (Clause 10.2 – Continual Improvement)
50. **Are stakeholders consulted or informed during key updates or revisions to AI systems and policies?**
    (Clause 10.3 – Stakeholder Communication)
51. **Is there a formal version control process for AI-related documents, models, and policies?**
    (Clause 10.4 – Documentation Control)
52. **Are obsolete or outdated documents securely archived or removed from operational environments?**
    (Clause 10.4 – Document Retention and Access)
53. **Are controls in place to ensure only authorized individuals can modify AI systems or their training parameters?**
    (Clause 10.5 – Change Management)

54. **Are third-party AI tools, APIs, or data sources evaluated for compliance with organizational standards and ISO 42001 principles?**
(Clause 10.6 – Third-Party and Supply Chain Management)
55. **Are AI systems regularly assessed for alignment with organizational values, policies, and legal obligations?**
(Clause 10.7 – Governance Alignment and Review)
56. **Does the organization have a lifecycle approach in place for managing AI systems, from design to decommissioning?**
(Clause 10.8 – AI Lifecycle Management)
57. **Are AI system updates and iterations governed through formal change control procedures?**
(Clause 10.8 – Version and Update Control)
58. **Is testing and validation conducted before and after AI system deployment to ensure continued performance?**
(Clause 10.9 – Validation and Verification)
59. **Are third-party suppliers required to comply with ethical AI policies or equivalent ISO 42001-aligned standards?**
(Clause 10.10 – Supplier and Partner Accountability)
60. **Is due diligence performed on external vendors providing AI tools, models, or datasets?**
(Clause 10.10 – Third-Party Risk Management)
61. **Is there a framework for transparency in AI system decisions, including the ability to explain results to non-technical stakeholders?**
(Clause 11.1 – Transparency and Disclosure)
62. **Are end users notified when AI systems are used in decisions that significantly affect their rights or interests?**
(Clause 11.2 – User Awareness and Consent)

63. **Are disclaimers or explanatory messages provided alongside AI-generated content or recommendations?**
    (Clause 11.2 – Communication Practices)
64. **Has the organization assessed and documented the potential social or ethical impacts of deployed AI systems?**
    (Clause 11.3 – Social Responsibility Assessment)
65. **Are mechanisms in place to reduce discriminatory or unfair outcomes in automated decision-making processes?**
    (Clause 11.4 – Fairness and Equity Management)
66. **Is the organization prepared to provide documentation or explanations to regulatory bodies upon request?**
    (Clause 11.5 – Legal Accountability and Transparency)
67. **Is there a clear channel for users, employees, or partners to report concerns related to AI system behavior or ethics?**
    (Clause 11.6 – Whistleblowing and Feedback Management)
68. **Are AI systems designed to preserve human dignity, safety, and autonomy in line with international human rights standards?**
    (Clause 11.7 – Human-Centric Design)
69. **Is the organization able to demonstrate how AI governance supports its broader sustainability or ESG goals?**
    (Clause 11.8 – Strategic Alignment and Reporting)
70. **Are independent audits or third-party reviews of AI systems conducted periodically to ensure impartial oversight?**
    (Clause 11.9 – External Assurance and Auditing)
71. **Has the organization implemented a regular schedule for independent model audits or validations by experts not involved in development?**
    (Clause 11.9 – Independent Oversight and Assurance)

72. **Are records of AI system testing, validation, and auditing maintained and accessible for inspection?**
(Clause 11.9 – Documentation and Audit Trails)
73. **Are the principles of human rights, equity, and privacy explicitly embedded in AI policies or charters?**
(Clause 12.1 – Ethical Governance and Commitment)
74. **Has the organization implemented a human rights impact assessment (HRIA) related to its use of AI technologies?**
(Clause 12.1 – Human Rights Assessment)
75. **Are AI systems regularly reviewed to ensure compliance with international labor, civil, and consumer protection laws?**
(Clause 12.2 – Legal and Ethical Conformity)
76. **Is the organization actively training its staff on AI ethics, risk awareness, and responsible development practices?**
(Clause 12.3 – Education and Capacity Building)
77. **Are lessons learned from past AI projects integrated into training programs and process improvements?**
(Clause 12.3 – Organizational Learning)
78. **Does the organization maintain a knowledge base or repository for AI governance materials and past risk cases?**
(Clause 12.4 – Knowledge Management)
79. **Are AI-related cybersecurity risks addressed through threat modeling and regular vulnerability assessments?**
(Clause 13.1 – Information Security and AI Risk)
80. **Is access to sensitive AI models, datasets, and source code restricted based on role and need?**
(Clause 13.1 – Access and Data Control)

81. **Are tamper detection and anomaly tracking tools used to monitor AI system behavior in real time?**
    (Clause 13.2 – System Surveillance and Logging)
82. **Does the organization have incident response plans specific to AI-driven disruptions or misuse?**
    (Clause 13.2 – AI-Specific Security Incidents)
83. **Is stakeholder feedback, including from civil society and end-users, solicited during AI system design or improvement cycles?**
    (Clause 14.1 – Participatory Governance)
84. **Does the organization provide channels for public consultation or engagement on high-impact AI initiatives?**
    (Clause 14.2 – Public Dialogue and Transparency)
85. **Are external experts, such as ethicists or legal scholars, engaged in periodic reviews of AI policy or implementations?**
    (Clause 14.3 – Multi-Stakeholder Involvement)
86. **Is the organization equipped to monitor long-term social and economic impacts of deployed AI systems?**
    (Clause 14.4 – Long-Term Impact Monitoring)
87. **Are post-deployment evaluations conducted to assess whether AI systems meet original goals and public expectations?**
    (Clause 14.4 – Outcome Validation)
88. **Is there a documented procedure for decommissioning AI systems that are no longer ethical, effective, or compliant?**
    (Clause 14.5 – System Retirement and Deactivation)
89. **Does the organization archive data, models, and decisions related to decommissioned systems for future reference or audits?**
    (Clause 14.5 – Data Retention Post-Retirement)

90. **Are all applicable national and international AI-related legal, regulatory, and contractual requirements continuously monitored for compliance?**
(Clause 14.6 – Ongoing Legal Compliance)
91. **Is there a register of all active AI systems in use, along with their risk classification, purpose, and governance status?**
(Clause 14.7 – AI System Inventory)
92. **Are internal and external accountability mechanisms in place to address misuse, harm, or non-conformity in AI system operation?**
(Clause 14.8 – Ethics and Responsibility Enforcement)
93. **Has the organization defined escalation procedures for ethical violations or unresolved governance issues in AI systems?**
(Clause 14.8 – Escalation and Redress Mechanisms)
94. **Are communication materials regarding AI systems clear, accurate, and designed to inform lay audiences, including non-technical stakeholders?**
(Clause 14.9 – Public-Facing Communication)
95. **Is the organization able to demonstrate proactive adjustments in response to emerging AI risks or societal shifts?**
(Clause 14.10 – Agility and Responsiveness)
96. **Does the organization conduct regular internal readiness reviews for ISO 42001 certification or recertification?**
(Clause 15.1 – Certification Preparedness)
97. **Are corrective actions from previous audits or assessments fully implemented and verified?**
(Clause 15.2 – Corrective Action Closure)
98. **Has the AI governance team reviewed the entire management system for alignment with strategic business objectives?**
(Clause 15.3 – Strategic Alignment Review)

99. **Are third-party auditors or certifiers granted appropriate access to records, models, and documentation during certification assessments?** *(Clause 15.4 – External Certification Access)*

100. **Is there a central authority or designated individual responsible for the ISO 42001 implementation and ongoing compliance efforts?** *(Clause 15.5 – Compliance Leadership and Ownership)*

Maximizing the Impact of Your ISO 42001 Audit

The ISO 42001 Audit Questionnaire with its extensive checklist is not merely a compliance tool; it is a strategic instrument that supports responsible innovation. By using this exclusive GSDC resource, organizations can build a culture of transparency, accountability, and trust in their AI systems.

Essential Considerations for Effective Use:

- **Consistency and Accuracy:** Ensure that all checklist items are answered truthfully, with documented evidence and stakeholder input.
- **Customization:** Adapt the questionnaire to reflect organizational size, industry, and AI system complexity.
- **Internal Alignment:** Promote participation across departments to ensure a holistic view of AI governance.
- **Continuous Monitoring:** Use the checklist as a recurring audit tool to track improvements and adjust to evolving standards.
- **Certification Preparation:** Treat this questionnaire as your pre-certification audit baseline. It prepares you not just for external audits but for internal readiness and reputation risk management.

As AI becomes more embedded in the fabric of organizational decision-making, the importance of standards like ISO 42001 will continue to grow. Having a rigorous, structured, and credible internal audit tool—such as this one—is not only prudent but essential.

DISCLAIMER

The templates, articles, and information provided by GSDC on this website are for reference only.

While we strive to keep the information up to date and accurate, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website.

Any reliance you place on such information is therefore strictly at your own risk.

About GSDC

What's the main key point to stand at the top of your career ladder as an IT professional? It is investing in acquiring new skills continuously and getting upskilled in them at a regular interval. If you put an end to learning new technologies in this ever-evolving world, your career scopes won't broaden at all.

Wondering where can you get your certification done from?

The Global Skill Development Council (GSDC) is an independent, vendor-neutral, international credentialing and certification organization for emerging technologies like Blockchain, Six Sigma, DevOps, Cloud, AI-ML, ISO, Agile, and L&D professionals.

- *GSDC's Advisory board members and SMEs are from around the world, drawn from different specializations.*
- *GSDC is supported by the world's most esteemed thought leaders, deans, chairs, professors, and academic affiliates from such prestigious universities as Yale, MIT, Stanford, Wharton, and Harvard.*
- *GSDC has a wide range of certifications curated and handpicked by world-renowned experts that triggers you to board on the knowledge ride of tech explorations.*
- *GSDC Council is a membership organization dedicated to growing, enhancing & certifying the skill within the tech Community*