100 Common Non-Conformities in ISO 42001 Audits

A Practical Guide to Identifying, Understanding, and Fixing the Most Frequent ISO 42001 Audit Issues in Artificial Intelligence Management Systems (AIMS)

Objectives of This Guide:

Achieving ISO 42001 compliance strengthens an organization’s **Artificial Intelligence Management System (AIMS)** and builds trust with users, regulators, and stakeholders.

However, many organizations struggle with **common audit non-conformities** that can delay certification and expose AI systems to ethical, operational, and legal risks.

This guide highlights **100 frequent ISO 42001 audit non-conformities**, complete with practical insights on how to fix them.

✓ Identify and address recurring ISO 42001 non-conformities before your audit

✓ Provide real-world scenarios that reveal critical AI governance failures

✓ Deliver actionable solutions for compliance across ethics, risk, and transparency

✓ Promote best practices in responsible AI development, deployment, and oversight

✓ Support continuous improvement for AIMS teams, data scientists, and auditors

This guide is ideal for:

- AI governance leads, compliance officers, and risk managers preparing for ISO 42001 audits
- AI/ML development teams seeking to align with responsible AI standards
- Consultants and lead auditors supporting ISO 42001 implementation
- Business leaders looking to ensure ethical, scalable, and trustworthy AI

Use this resource to take a proactive approach to AI compliance, streamline audit readiness, and build a responsible, resilient AI governance framework.

1. No Formal AI Risk Assessment Framework

📌 Clause: 6.1 – Addressing Risks & Opportunities

Scenario:
An AI startup builds models using public datasets but has no documented risk assessments. The team cannot identify ethical or technical risks like bias or explainability failures.

What's Missing:
A structured, repeatable AI risk management framework integrated into the development lifecycle.

How to Fix:
✓ Build an AI risk register
✓ Conduct regular impact assessments (bias, misuse, performance)
✓ Involve legal, ethics, and technical teams in evaluation
✓ Update the risk framework with each major system change

2. Weak Documentation of Risk Treatment

📌 Clause: 6.1.3 – Risk Treatment Plan

Scenario:
The company acknowledges AI-related risks but treats them informally—mostly through team meetings with no written plans or mitigation actions.

What's Missing:
A documented Risk Treatment Plan (RTP) linked to the AI risk register.

How to Fix:
✓ Create an RTP outlining risks, mitigation steps, owners, and deadlines

✓ Track progress with version-controlled documentation

✓ Use tools to monitor and report on mitigation progress

3. No Internal Audits or Management Reviews of AI Systems

📌 Clauses: 9.2 & 9.3 – Internal Audit & Management Review

Scenario:
AI systems are deployed without audit checkpoints. Leadership is unaware of AI compliance risks or performance metrics.

What's Missing:
A schedule for internal audits and structured review meetings to evaluate AI governance.

How to Fix:

✓ Conduct internal audits annually, covering development, deployment, and post-launch monitoring

✓ Document all findings and corrective actions

✓ Include AIMS in executive-level management reviews

4. Poorly Defined Scope of Applicability (SoA) for AI Controls

📌 Clause: 6.1.3(d) – Statement of Applicability

Scenario:
The organization lists general security controls but doesn't align them with AI-specific risks. Several AI functions have no justification for excluded safeguards.

What’s Missing:
A clear, AI-focused Statement of Applicability showing which controls apply, and why.

How to Fix:
✓ Map SoA to AI-specific controls like model explainability, fairness, and human oversight
✓ Provide written justification for exclusions
✓ Update the SoA with each risk treatment revision

5. No KPIs for AI Governance Performance

📌 **Clause: 9.1 – Monitoring and Evaluation**

Scenario:
AI projects are launched, but there's no mechanism to measure their ethical, legal, or operational performance.

What’s Missing:
Defined performance indicators to monitor AI system effectiveness and compliance.

How to Fix:
✓ Create AI-specific KPIs (e.g., bias detection rate, accuracy drift, audit closure times)
✓ Review KPIs quarterly and align with business objectives
✓ Automate performance tracking using dashboards

6. Lack of AI Incident Management Process

📌 **Clause: 8.5 – Incident Response and Improvement**

Scenario:
A chatbot misinforms users, causing reputational harm. The issue is resolved ad-hoc with no root cause analysis or formal report.

What's Missing:
A formal AI incident response process tied to the AIMS.

How to Fix:
✓ Define AI incident types (e.g., model failures, fairness breaches)
✓ Set clear roles, escalation paths, and documentation standards
✓ Conduct post-incident reviews and feed insights into risk updates

7. Insufficient Access Controls for AI Systems

📌 **Clause: 8.4 – Access Control**

Scenario:
Developers and non-technical staff have full access to AI training data, posing risks to privacy and model integrity.

What's Missing:
Granular access control aligned with the principle of least privilege.

How to Fix:
✓ Use role-based access control (RBAC) for AI-related assets
✓ Log access to sensitive datasets and model parameters
✓ Conduct quarterly access reviews and remove excess privileges

8. No Security Oversight of AI Supply Chain or Third-Party Models

📌 **Clause: 8.2 – Control of Externally Provided Processes**

Scenario:
A pre-trained model from an external vendor is used in a customer-facing product, but its risks (bias, poisoning) are never assessed.

What's Missing:
Due diligence for third-party models and AI tools.

How to Fix:

✓ Vet all third-party tools with a supplier security checklist

✓ Require assurance documentation (e.g., bias testing, license reviews)

✓ Include third-party models in AI risk assessments and contracts

9. No AI-Specific Training for Employees

📌 **Clause: 7.2 – Competence and Awareness**

Scenario:
Employees involved in AI development are unaware of emerging ethical frameworks and ISO 42001 clauses.

What's Missing:
Targeted training on responsible AI, regulatory obligations, and organizational AI governance.

How to Fix:

✓ Conduct mandatory AI governance training

✓ Include topics like transparency, fairness, privacy, and accountability

✓ Track participation and issue refresher courses annually

10. No Inventory of AI Assets or Models

📌 Clause: 8.1 – Operational Planning and Control

Scenario:
The organization runs multiple AI systems but has no central inventory. Some models in production are unmonitored and undocumented.

What's Missing:
A complete and up-to-date registry of AI models and assets.

How to Fix:

✓ Build an AI model registry with metadata like purpose, owner, dataset, and risk level

✓ Assign ownership for each AI asset

✓ Conduct biannual reviews of the inventory

11. No AI Ethics Review Board or Oversight Mechanism

📌 Clause: 5.1 – Leadership and Commitment

Scenario:
The organization has deployed AI systems that impact hiring decisions, but no ethical oversight exists to evaluate potential discrimination or bias.

What’s Missing:
Formal ethical governance to assess, review, and approve AI systems with societal or individual impact.

How to Fix:
✓ Establish an AI Ethics Review Board with cross-functional members (legal, compliance, technical, HR)
✓ Mandate reviews for high-impact or high-risk AI use cases
✓ Document findings and decisions as part of the AIMS governance record

12. Lack of Model Lifecycle Management

📌 Clause: 8.1 – Operational Planning and Control

Scenario:
Multiple AI models are in production, but there's no formal process to track versions, updates, or retirement timelines.

What’s Missing:
A structured AI lifecycle management process from development to decommissioning.

How to Fix:
✓ Create a model lifecycle framework with defined stages (build, test, deploy, monitor, retire)
✓ Maintain logs for all model changes
✓ Link each model to a unique identifier in the asset inventory

13. No Human-in-the-Loop (HITL) Safeguards for Critical AI Systems

📌 **Clause: 8.6 – Human Oversight**

Scenario:
A predictive algorithm automates loan approvals with no human validation, even in high-stakes decisions.

What's Missing:
Mechanisms for human intervention or override in AI-driven decisions that affect individuals or rights.

How to Fix:

✓ Introduce human review for high-risk decisions

✓ Set thresholds for manual override or escalation

✓ Train staff on when and how to intervene

14. Poor Documentation of AI Model Purpose and Limitations

📌 **Clause: 7.5 – Documented Information**

Scenario:
Auditors request an explanation of an AI model's intended use and known limitations, but no documentation exists.

What's Missing:
Formal documentation of model objectives, intended audience, assumptions, and risks.

How to Fix:

✓ Document every model's purpose, limitations, and expected behavior

✓ Include transparency statements for internal and external stakeholders

✓ Keep documentation updated after retraining or changes

15. No Post-Deployment Monitoring of AI Fairness

📌 Clause: 9.1 – Monitoring, Measurement, and Evaluation

Scenario:
An AI model initially passed fairness testing but later showed bias due to data drift. No monitoring system was in place to catch it.

What's Missing:
Ongoing evaluation of model fairness, accuracy, and drift post-deployment.

How to Fix:

✓ Define fairness metrics appropriate for your context (e.g., demographic parity)

✓ Set thresholds for acceptable variation and retrain when breached

✓ Use automated monitoring tools for real-time alerts

16. No Bias Testing Framework in Model Development

📌 Clause: 6.1 – Risk and Opportunity Assessment

Scenario:
Developers assume their dataset is representative but fail to test for underrepresentation of specific groups.

What's Missing:
A structured bias testing protocol during training and validation phases.

How to Fix:

✓ Mandate bias testing before deployment

✓ Use tools to analyze representation and outcome fairness

✓ Include bias test results in model documentation

17. Unsecured Access to Training Data and Models

📌 Clause: 8.4 – Access Control

Scenario:

Sensitive training datasets are stored in open cloud buckets with no access restrictions or logging.

What's Missing:

Access controls and audit trails to protect sensitive AI-related assets.

How to Fix:

✓ Restrict access using RBAC or ABAC policies

✓ Encrypt training data in storage and transit

✓ Implement logging to track who accessed what and when

18. No Traceability Between Data, Models, and Decisions

📌 Clause: 8.7 – Traceability and Record Keeping

Scenario:

The organization can't explain why a model produced a specific decision because data lineage isn't maintained.

What's Missing:
Traceability from input data to model output and final decision.

How to Fix:

✓ Maintain data lineage logs

✓ Record which dataset and model version were used for each deployment

✓ Use explainability tools to connect features with decisions

19. Lack of Explainability for End-Users

📌 Clause: 7.4 – Communication and Awareness

Scenario:
Users affected by automated decisions don't receive an explanation of how or why the decision was made.

What's Missing:
Clear, accessible communication of how AI systems make decisions—especially for external stakeholders.

How to Fix:

✓ Generate user-friendly summaries of decision logic

✓ Provide justification or rationale for decisions where legally or ethically required

✓ Offer recourse or appeal mechanisms when needed

20. No Contingency Plan for AI System Failures

📌 **Clause: 8.9 – Emergency Preparedness and Response**

Scenario:
An AI-powered recommendation engine crashes during peak traffic, with no fallback mechanism in place.

What's Missing:
A documented contingency plan for AI outages or failures.

How to Fix:
✓ Create fallback procedures or manual overrides
✓ Establish service-level objectives (SLOs) for critical AI systems
✓ Simulate AI failure scenarios and update your response plan

21. No Third-Party AI Risk Assessment Process

📌 **Clause: 8.2 – Control of Externally Provided Processes**

Scenario:
An organization integrates a third-party AI analytics tool into its system without assessing its risks. Later, a privacy breach occurs due to lack of transparency in the third-party's data practices.

What's Missing:
A structured process for evaluating third-party AI risks before onboarding.

How to Fix:
✓ Vet vendors using a formal AI risk checklist
✓ Require security, bias, and compliance disclosures from all AI partners
✓ Incorporate vendor performance and risk into your own AIMS reviews

22. No Policy for Responsible AI Deployment

📌 Clause: 5.2 – AI Policy and Objectives

Scenario:
AI systems are launched without internal policies governing acceptable use, risk thresholds, or social impact considerations.

What's Missing:
An overarching Responsible AI policy aligned with ISO 42001 principles.

How to Fix:
✓ Define acceptable use cases, prohibited applications, and ethical boundaries
✓ Align the policy with ISO 42001 and your organizational values
✓ Communicate and train employees on the policy regularly

23. Lack of Defined AI Roles and Responsibilities

📌 Clause: 5.3 – Roles and Responsibilities

Scenario:
During an audit, no one can clearly identify who owns the model, data pipeline, or risk assessments for deployed AI systems.

What's Missing:
Clearly defined roles for every stage of the AI lifecycle and AIMS accountability.

How to Fix:

✓ Assign ownership for model development, governance, ethics, and compliance

✓ Map roles in a RACI chart and integrate with org structure

✓ Review role responsibilities annually or when teams shift

24. No Change Management Process for AI Model Updates

📌 Clause: 8.8 – Change Management

Scenario:
A deployed model is retrained with new data but performs unpredictably. The update wasn't documented or risk-reviewed.

What's Missing:
A formal process to control and document changes to AI systems.

How to Fix:

✓ Create a change request system for model updates

✓ Evaluate risks and run validations before production deployment

✓ Maintain version control and change logs

25. No Testing of AI Business Continuity or Failure Scenarios

📌 Clause: 8.9 – Emergency Preparedness and Response

Scenario:
When an AI-driven logistics system fails, the company has no backup process. Deliveries are delayed for days.

What’s Missing:
Business continuity and failure response testing specific to AI systems.

How to Fix:
✓ Conduct tabletop exercises and technical failover simulations
✓ Document expected behaviors under failure conditions
✓ Define who takes over in case of AI disruption and how

26. No Data Provenance Documentation

📌 **Clause: 8.3 – Data Management**

Scenario:
A model uses customer data from various internal sources, but the organization cannot trace where the data originated or how it was processed.

What’s Missing:
Data provenance tracking and documentation to ensure compliance, explainability, and fairness.

How to Fix:
✓ Implement data lineage tools or maintain manual documentation
✓ Link each dataset to its source, transformation, and consent mechanism
✓ Include data provenance in model training logs

27. Lack of Stakeholder Engagement in AI Design

📌 Clause: 4.2 – Needs and Expectations of Interested Parties

Scenario:
A predictive policing algorithm is deployed without consulting affected community groups, leading to public backlash.

What's Missing:
Structured stakeholder engagement during AI system planning and development.

How to Fix:
✓ Identify internal and external stakeholders early
✓ Use surveys, focus groups, or ethics panels to gather input
✓ Document how feedback influences design choices

28. No Explainability Standards in AI Model Design

📌 Clause: 8.7 – Explainability and Transparency

Scenario:
A decision-support AI model produces outputs that even developers struggle to interpret.

What's Missing:
Design-phase explainability standards to ensure outputs can be understood and justified.

How to Fix:
✓ Select inherently interpretable models when possible
✓ Integrate XAI (Explainable AI) tools for complex models

✓ Provide explanations appropriate to the audience (technical vs non-technical)

29. Inconsistent Version Control for AI Models

📌 Clause: 7.5 – Documented Information

Scenario:
Multiple versions of the same AI model are in circulation, with no clear documentation of which one is in production.

What's Missing:
Robust version control to track models, datasets, and configuration settings.

How to Fix:
✓ Use MLOps tools to manage and version models
✓ Tag and store metadata (e.g., training data, code version, hyperparameters)
✓ Archive deprecated versions and prevent accidental redeployment

30. No Communication Strategy for AI System Failures

📌 Clause: 7.4 – Communication

Scenario:
An AI-powered customer service bot goes offline for 12 hours, but customers receive no updates, damaging trust.

What’s Missing:
A defined process for internal and external communication during AI outages or incidents.

How to Fix:
✓ Draft communication templates for AI failure scenarios
✓ Define who communicates what, when, and through which channel
✓ Include escalation steps and status update timelines

31. No Procedure for Decommissioning AI Models

📌 Clause: 8.1 – Operational Planning and Control

Scenario:
An outdated AI model is still active in production, even though a new version was deployed six months ago. Users receive inconsistent outputs.

What’s Missing:
A structured decommissioning process to retire outdated or underperforming AI models.

How to Fix:
✓ Define decommissioning criteria (e.g., low accuracy, regulatory changes)
✓ Archive old models and clearly mark them as inactive
✓ Communicate model retirement to impacted teams or users

32. AI Training Data Stored Without Retention or Deletion Policy

📌 **Clause: 8.3 – Data Management**

Scenario:
The organization retains all AI training data indefinitely—including outdated personal information—without any deletion schedule.

What's Missing:
A formal data retention and disposal policy tied to AI datasets.

How to Fix:
✓ Set retention periods based on data type and purpose
✓ Securely delete training data that's no longer needed
✓ Document deletion logs and align with privacy regulations (e.g., GDPR)

33. No Review of AI System Impact on Human Rights

📌 **Clause: 4.2 – Needs and Expectations of Interested Parties**

Scenario:
An AI surveillance system is deployed without considering its implications for privacy, discrimination, or freedom of movement.

What's Missing:
An ethical impact assessment addressing AI's effect on fundamental rights.

How to Fix:
✓ Conduct Human Rights Impact Assessments (HRIAs) for high-risk systems
✓ Involve external advisors or civil society where applicable
✓ Include mitigation strategies for identified risks

34. Inadequate Logging of AI System Activities

📌 Clause: 9.1 – Monitoring and Evaluation

Scenario:
After a system failure, the root cause cannot be determined because logs were incomplete or missing.

What's Missing:
Comprehensive logging of AI activities, decisions, and data interactions.

How to Fix:

✓ Log inputs, outputs, errors, access events, and overrides

✓ Use centralized log management tools

✓ Regularly review logs to identify anomalies or system drift

35. No Periodic Review of AI Risk Assessments

📌 Clause: 6.1.2 – Risk Identification and Evaluation

Scenario:
The AI risk register hasn't been updated in over a year, even though new systems and datasets have been introduced.

What's Missing:
A cadence for reviewing and updating AI risk assessments.

How to Fix:

✓ Schedule quarterly or biannual risk assessment reviews

✓ Update the register after model updates, incidents, or policy changes

✓ Link risk changes to controls and mitigation plans

36. No Consent Mechanism for AI Data Collection

📌 **Clause: 8.3 – Data Management**

Scenario:
User data is collected and used to train personalization algorithms without transparent consent.

What's Missing:
A mechanism to ensure informed user consent for data used in AI.

How to Fix:

✓ Implement clear opt-in/opt-out options for data usage

✓ Document consent logs and integrate with your AIMS

✓ Allow users to revoke consent and update models accordingly

37. Inadequate Testing for Adversarial Attacks

📌 **Clause: 8.6 – AI System Security**

Scenario:
The AI vision system is fooled by simple adversarial examples (e.g., manipulated images), but this vulnerability was never tested.

What's Missing:
Security testing for adversarial robustness in AI models.

How to Fix:

✓ Conduct adversarial testing as part of model validation

✓ Use AI-specific penetration testing tools

✓ Build model hardening strategies based on findings

38. Lack of Policy for Shadow AI Detection

📌 Clause: 8.1 – Operational Planning and Control

Scenario:
An internal team builds and deploys a generative AI tool without oversight, violating company AI governance rules.

What's Missing:
Controls to detect and manage "shadow AI" systems developed without approval.

How to Fix:

✓ Implement a centralized AI system registration process

✓ Use internal audits to identify unauthorized AI deployments

✓ Enforce disciplinary or corrective measures for policy violations

39. AI Development Not Integrated into the SDLC

📌 Clause: 8.8 – Change Management and Development

Scenario:
AI is treated as an isolated research project with no formal process for testing, staging, or integration into DevOps pipelines.

What's Missing:
Integration of AI development into the secure software development lifecycle (SDLC).

How to Fix:
✓ Extend DevSecOps practices to cover AI lifecycle activities
✓ Introduce gates for ethics, bias, and explainability checks
✓ Align AI deployment with existing release and rollback workflows

40. No Mechanism to Monitor and Mitigate Model Drift

📌 Clause: 9.1 – Performance Monitoring

Scenario:

A fraud detection model becomes ineffective as new fraud patterns emerge, but no monitoring alerts were triggered.

What's Missing:
A process to detect model drift and automatically trigger review or retraining.

How to Fix:
✓ Set drift detection thresholds (e.g., accuracy, input distribution)

✓ Use real-time monitoring and alerts for critical models

✓ Define triggers for retraining or rollback procedures

41. No Defined Criteria for AI Model Performance Evaluation

📌 **Clause: 9.1 – Monitoring, Measurement, Analysis, and Evaluation**

Scenario:
Deployed AI models are reviewed periodically, but there are no clear benchmarks to determine whether they are performing acceptably.

What's Missing:
Defined performance indicators and thresholds for success/failure.

How to Fix:

✓ Establish quantitative KPIs (e.g., precision, recall, latency, false positive rate)

✓ Include qualitative metrics (e.g., user satisfaction, ethical alignment)

✓ Regularly assess performance and link findings to improvement plans

42. No Policy for Responsible Use of Generative AI

📌 **Clause: 5.2 – AI Policy and Objectives**

Scenario:
Employees begin using ChatGPT-like tools in business operations without any rules governing output validation or data input risks.

What's Missing:
Governance over the use of generative AI, including prompt safety, copyright concerns, and hallucination risks.

How to Fix:
✓ Define acceptable use cases for generative AI
✓ Train employees on risks and output validation
✓ Implement approval processes and disclosure guidelines for public-facing use

43. Inconsistent Application of AI Controls Across Business Units

📌 **Clause: 4.3 – Determining the Scope of the AIMS**

Scenario:

One department has robust AI governance, while another uses AI tools with no oversight, resulting in uneven compliance.

What's Missing:
A harmonized AIMS that applies consistently across the entire organization.

How to Fix:
✓ Clearly define the AIMS scope to include all business units using or developing AI
✓ Standardize governance tools, documentation, and training
✓ Conduct cross-functional reviews to ensure consistent application

44. AI Systems Operate Without User Feedback Loops

📌 Clause: 9.1 – Monitoring and Continuous Improvement

Scenario:
End users receive AI-generated recommendations, but there’s no channel to report issues, inaccuracies, or unintended consequences.

What’s Missing:
Structured feedback mechanisms to gather user input and improve system performance.

How to Fix:
✓ Implement user feedback forms or in-app reporting features
✓ Assign responsibility for reviewing and acting on feedback
✓ Use feedback trends to refine models or retrain where needed

45. No Structured Method for Documenting AI Model Assumptions

📌 Clause: 7.5 – Documented Information

Scenario:
During an audit, developers cannot recall the assumptions or constraints applied during model training.

What’s Missing:
Documentation of underlying assumptions, use limitations, and design trade-offs.

How to Fix:
✓ Require a “Model Card” or equivalent artifact for each system
✓ Include assumptions, known limitations, data bias concerns, and

expected use cases

✓ Review and update documentation with every major model change

46. No Formal Process for AI Model Validation Before Deployment

📌 Clause: 8.1 – Operational Planning and Control

Scenario:

AI models are deployed after basic performance checks, but without formal testing against adversarial cases or edge scenarios.

What's Missing:

A rigorous validation protocol to verify AI model reliability before deployment.

How to Fix:

✓ Establish a checklist of validation steps (fairness, security, stability)

✓ Use benchmark datasets and scenario testing

✓ Require sign-off by compliance and technical leads

47. Lack of Regulatory Mapping for AI Use Cases

📌 Clause: 4.2 – Needs and Expectations of Interested Parties

Scenario:

An AI tool processes biometric data, but the organization is unaware of applicable data protection laws in multiple regions.

What’s Missing:
Mapping of AI use cases to legal and regulatory requirements (e.g., GDPR, HIPAA, EU AI Act).

How to Fix:
✓ Conduct legal reviews for every high-risk AI use case
✓ Maintain a compliance matrix aligned with jurisdictions and AI functionalities
✓ Involve legal counsel early in AI product development

48. No Controls Around AI System Retraining Frequency

📌 Clause: 8.1 – Operational Planning and Model Maintenance

Scenario:
An AI model trained on seasonal data hasn’t been retrained in over a year, resulting in degraded performance and errors.

What’s Missing:
Retraining schedule and triggers based on data changes or performance drift.

How to Fix:
✓ Define retraining intervals based on use case (e.g., quarterly, post-drift)
✓ Use automation to flag models for review when thresholds are breached
✓ Log retraining activities and version changes

49. Absence of AI-Specific Threat Modeling in Development

📌 Clause: 6.1 – Risk Management

Scenario:
Security reviews cover infrastructure, but not AI-specific threats like data poisoning, adversarial attacks, or model inversion.

What's Missing:
AI-tailored threat modeling as part of the secure development lifecycle.

How to Fix:

✓ Integrate threat modeling sessions into AI development planning

✓ Include risks like inference attacks, training data leakage, model theft

✓ Use frameworks like MITRE ATLAS for AI threat identification

50. No External Disclosure of AI System Usage to Users

📌 Clause: 7.4 – Communication and Transparency

Scenario:
Users interact with an AI-driven decision tool on a website without being informed that the system is automated.

What's Missing:
Transparency about AI involvement in decision-making, as required by ethical and legal standards.

How to Fix:

✓ Clearly disclose when users are interacting with or being influenced by AI

✓ Include disclaimers or AI usage statements on digital interfaces

✓ Provide contact info or appeal options for automated decisions

51. No Monitoring of Environmental Impact of AI Systems

📌 **Clause: 4.1 – Understanding the Organization and Its Context**

Scenario:
A large-scale AI model is trained using significant compute resources, but the environmental impact (energy use, emissions) is never measured or reported.

What's Missing:
Consideration of sustainability and environmental risks as part of AI system planning.

How to Fix:

✓ Assess energy consumption and carbon footprint of AI infrastructure

✓ Choose efficient model architectures and green data centers

✓ Document environmental considerations in AI risk assessments

52. No Backup or Rollback Plan for AI System Updates

📌 **Clause: 8.9 – Emergency Preparedness and Response**

Scenario:
An updated recommendation engine introduces serious errors, but the organization lacks a backup model or rollback plan.

What’s Missing:
A recovery plan in case of faulty AI system deployments.

How to Fix:
✓ Implement rollback capabilities in deployment pipelines
✓ Maintain backup versions of previously validated models
✓ Test rollback procedures as part of regular drills

53. No Integration of AI Governance with Enterprise Risk Management (ERM)

📌 **Clause: 6.1 – Risk-Based Thinking**

Scenario:
AI-related risks are managed separately from broader enterprise risks, leading to duplication and oversight gaps.

What’s Missing:
Alignment between AI risk processes and the organization's ERM framework.

How to Fix:
✓ Integrate AI risks into the corporate risk register
✓ Involve AI governance teams in enterprise risk reviews
✓ Report AI-related risks to executive risk committees

54. Incomplete Asset Inventory of AI-Related Components

📌 Clause: 8.1 – Operational Control

Scenario:
An audit reveals that the organization cannot produce a complete list of AI tools, APIs, datasets, and models in use.

What's Missing:
A central, current inventory of all AI-related assets.

How to Fix:
✓ Build a structured AI asset registry (models, training datasets, APIs, platforms)
✓ Assign asset owners and update records quarterly
✓ Use automated discovery tools where possible

55. No Assessment of Social Impact for AI Applications

📌 Clause: 4.2 – Needs and Expectations of Interested Parties

Scenario:
An AI tool used in public housing decisions is launched without evaluating its effect on vulnerable populations.

What's Missing:
Social impact assessments for high-impact AI deployments.

How to Fix:
✓ Evaluate societal effects (inclusion, bias, accessibility) during planning
✓ Include community stakeholders in the assessment process
✓ Use findings to refine model goals and governance controls

56. No Pre-Deployment Review of Legal and Ethical Risks

📌 Clause: 6.1 – Risk Identification and Mitigation

Scenario:
An AI product is launched without reviewing legal requirements for data protection, discrimination, or consumer rights.

What's Missing:
A mandatory checkpoint for legal and ethical risks before go-live.

How to Fix:

✓ Include legal/ethics leads in AI go/no-go decisions

✓ Maintain a pre-launch checklist of legal, regulatory, and ethical requirements

✓ Delay deployment until all risks are reviewed and documented

57. AI Training Data Collected Without Purpose Limitation

📌 Clause: 8.3 – Data Management

Scenario:
Data gathered for customer support is later used to train sentiment analysis models—without notifying users or reassessing consent.

What's Missing:
Adherence to purpose limitation principles for data reuse.

How to Fix:

✓ Clearly define intended use when collecting data

✓ If repurposing data, assess legal, ethical, and consent implications

✓ Update privacy notices and get new consent if required

58. Lack of Procedures for Auditing AI Ethics Compliance

📌 **Clause: 9.2 – Internal Audit**

Scenario:
Internal audits focus on IT security and regulatory compliance but never evaluate fairness, transparency, or explainability.

What's Missing:
AI ethics checkpoints within the audit process.

How to Fix:

✓ Include ethical impact criteria in internal audit scope

✓ Train auditors to review bias mitigation, transparency, and oversight

✓ Use AI-specific audit templates and checklists

59. No Mechanism for Users to Challenge or Appeal AI Decisions

📌 **Clause: 7.4 – Communication with Stakeholders**

Scenario:
An automated system denies users access to a service, and there's no clear way to dispute or appeal the outcome.

What's Missing:
Appeal mechanisms for decisions made (or influenced) by AI.

How to Fix:

✓ Create a documented process for users to challenge outcomes

✓ Assign human reviewers to evaluate appeals

✓ Communicate the option to appeal in user-facing interfaces

60. AI Documentation Lacks Version History and Change Logs

📌 Clause: 7.5 – Documented Information

Scenario:

Auditors find that documentation for an AI model has been updated multiple times, but changes aren't tracked.

What's Missing:

Version control and change history for critical AI documentation.

How to Fix:

✓ Use version control systems (e.g., Git) for model documentation

✓ Maintain changelogs for key documents (model cards, risk registers, SoA)

✓ Require approval and sign-off for major document revisions

61. No Integration of AI Controls into Vendor Contracts

📌 Clause: 8.2 – Control of Externally Provided Processes

Scenario:

A vendor provides AI tools and services, but there are no contract clauses requiring ethical AI practices, bias testing, or transparency.

What's Missing:
Contractual controls to extend your AIMS to third-party AI vendors.

How to Fix:
✓ Include AI governance requirements in all contracts and SLAs
✓ Require vendors to adhere to ISO 42001-aligned practices
✓ Mandate reporting of incidents, audits, or material changes in their systems

62. AI Systems Built Without Stakeholder Risk Workshops

📌 **Clause: 4.2 – Needs and Expectations of Interested Parties**

Scenario:
The risk register reflects only technical inputs—there's no consultation with impacted departments or end users.

What's Missing:
Stakeholder-driven risk identification during early planning phases.

How to Fix:
✓ Conduct cross-functional risk workshops involving HR, legal, product, and affected teams
✓ Document concerns from all parties and address them in the AI risk register
✓ Update risk mitigation strategies based on stakeholder insights

63. No Defined Roles for AI Model Review and Sign-Off

📌 Clause: 5.3 – Roles, Responsibilities, and Authorities

Scenario:
An AI model is deployed without formal review or approval. No one is accountable for vetting its performance or risk posture.

What's Missing:
Assigned accountability for final review and sign-off before launch.

How to Fix:
✓ Assign clear model sign-off authority (AI governance lead, ethics officer, risk manager)
✓ Require documented approval for every production deployment
✓ Link sign-off to validation, testing, and compliance checklists

64. No Policy for Handling Public Data in AI Training

📌 Clause: 8.3 – Data Management

Scenario:
The organization scrapes public forums for training data, but doesn't assess legal or ethical implications of using public content.

What's Missing:
Guidelines for sourcing and validating publicly available training data.

How to Fix:
✓ Define acceptable sources and criteria for public data use
✓ Assess IP, copyright, consent, and bias implications
✓ Apply filters or remove sensitive information from public datasets

65. AI System Lifecycle Not Linked to Business Objectives

📌 **Clause: 6.2 – Objectives of the AIMS**

Scenario:
AI projects are launched with technical success metrics only—there's no alignment with company strategy or values.

What's Missing:
Business-aligned objectives driving AI development and use.

How to Fix:

✓ Link AI outcomes (e.g., automation, accuracy, fairness) to business KPIs

✓ Include strategic objectives in model documentation

✓ Involve business leaders in the AI design and review phases

66. No Audit Trail for AI Model Retraining Activities

📌 **Clause: 7.5 – Documented Information**

Scenario:
Auditors request evidence of retraining activity after a major data shift—but logs are missing or inconsistent.

What's Missing:
Retraining documentation and traceability of when and how models evolve.

How to Fix:

✓ Document every retraining instance with dates, data used, reasons, and performance metrics

✓ Store logs in a centralized, secure location

✓ Include retraining audits in your AIMS review process

67. AI Performance Not Benchmarked Against Alternatives

📌 Clause: 9.1 – Evaluation and Effectiveness

Scenario:
An AI-driven customer support system is underperforming, but there's no baseline comparison against manual or rule-based methods.

What's Missing:
Benchmarking to validate AI effectiveness versus traditional approaches.

How to Fix:

✓ Define benchmark scenarios and KPIs for comparison

✓ Measure AI vs. manual process accuracy, cost, speed, and fairness

✓ Use findings to support deployment decisions or revert when needed

68. No Consideration of Cultural Sensitivity in AI Outputs

📌 Clause: 4.2 – Needs and Expectations of Interested Parties

Scenario:
A language model generates responses that unintentionally offend users from certain regions due to cultural nuances.

What's Missing:
Cultural sensitivity and localization reviews during AI design.

How to Fix:

✓ Involve linguists and cultural experts in high-impact AI projects

✓ Test outputs in multilingual and multicultural contexts

✓ Set redlines for cultural content and offensive output filtering

69. No Escalation Process for AI Ethics Concerns

📌 **Clause: 8.6 – Human Oversight**

Scenario:
Team members identify ethical concerns during development but have no formal route to report or escalate them.

What's Missing:
An ethics escalation channel within your AI governance framework.

How to Fix:

✓ Create an internal hotline or reporting form for ethical concerns

✓ Assign a designated reviewer (e.g., Ethics Officer)

✓ Track cases and resolutions to improve future practices

70. Lack of Integration Between AI and Data Privacy Teams

📌 **Clause: 5.1 – Leadership and Coordination**

Scenario:
AI and privacy teams operate in silos. Personal data is used in model training without DPO (Data Protection Officer) involvement.

What's Missing:
Cross-team coordination to ensure privacy is embedded in AI design.

How to Fix:

✓ Involve the DPO in all high-risk AI development and reviews

✓ Establish joint workflows between AI, compliance, and legal

✓ Embed privacy impact assessments (PIAs) into the AI lifecycle

71. No Periodic Testing of AI System Explainability

📌 **Clause: 8.7 – Explainability and Transparency**

Scenario:
The organization claims its AI models are explainable, but regular testing of explanation clarity and relevance isn't performed.

What's Missing:
Ongoing validation that AI decisions remain interpretable over time.

How to Fix:

✓ Test explanation quality with technical and non-technical users

✓ Use updated examples after retraining or data shifts

✓ Document improvements and user feedback on explainability

72. Lack of Monitoring for AI Hallucinations in Generative Systems

📌 **Clause: 9.1 – Monitoring, Measurement, and Evaluation**

Scenario:
A generative AI tool produces fabricated information, but there's no monitoring or control to detect hallucinated outputs.

What’s Missing:
A strategy to identify, log, and respond to generative hallucinations.

How to Fix:
✓ Flag high-risk outputs with uncertainty scoring or disclaimers
✓ Monitor for hallucinations using prompt tracking and content reviews
✓ Fine-tune or constrain models based on problem areas

73. AI System Not Reviewed Following Regulatory Updates

📌 Clause: 6.1 – Risk and Compliance Management

Scenario:
A new regional law requires disclosure of automated decision-making, but deployed AI systems were never reviewed or updated.

What’s Missing:
Regulatory change tracking tied to AI system reviews.

How to Fix:
✓ Monitor global AI and data regulations continuously
✓ Maintain a log of system reviews triggered by legal changes
✓ Assign responsibility to legal/compliance teams for alerting relevant stakeholders

74. No Controls for AI Use in Sensitive Functions (e.g., Hiring, Healthcare)

📌 **Clause: 8.1 – Operational Planning and Control**

Scenario:
An AI tool is used in recruitment decisions without additional controls for fairness, explainability, or human review.

What's Missing:
Stricter governance for AI used in high-impact domains.

How to Fix:
✓ Apply heightened controls and audits to high-risk applications
✓ Require bias testing, ethical reviews, and human-in-the-loop mechanisms
✓ Flag these systems as "critical" in your AIMS asset register

75. No Internal Training on ISO 42001 or AIMS Requirements

📌 **Clause: 7.2 – Competence and Awareness**

Scenario:
Staff involved in AI development are unaware of ISO 42001 or the organization's Artificial Intelligence Management System.

What's Missing:
Awareness and education on ISO 42001 principles and internal policies.

How to Fix:
✓ Run training sessions for relevant teams (AI, risk, compliance, execs)
✓ Include ISO 42001 basics, governance roles, and non-conformity risks
✓ Refresh annually and track participation

76. No Audit Trail for AI-Driven Decisions

📌 Clause: 9.1 – Monitoring and Traceability

Scenario:
A user is negatively impacted by an AI-driven decision, but the organization cannot reconstruct how the output was generated.

What's Missing:
Traceability logs linking input data, model version, and decision outcome.

How to Fix:
✓ Log all decision-making steps: input, process, output, timestamp, model version
✓ Secure and retain logs for a defined period
✓ Review logs during incidents, audits, and retraining

77. AI Risk Assessments Do Not Include Edge Cases or Adversarial Scenarios

📌 Clause: 6.1.2 – AI Risk Identification

Scenario:
The risk register only considers expected behaviors, ignoring what happens when inputs are manipulated or edge cases occur.

What's Missing:
Consideration of adversarial inputs and failure modes.

How to Fix:

✓ Run scenario analysis using edge case inputs

✓ Simulate adversarial attacks to test model robustness

✓ Document failure handling strategies and update controls accordingly

78. No Role-Based Access Control (RBAC) for Model and Data Pipelines

📌 **Clause: 8.4 – Access Control**

Scenario:
Multiple staff have unrestricted access to live AI pipelines and sensitive training data without clear justification.

What's Missing:
Access control by role and least-privilege principles.

How to Fix:

✓ Implement RBAC policies for AI systems and data assets

✓ Review access rights quarterly

✓ Revoke access when roles change or projects conclude

79. No Guidelines for the Use of Synthetic Data in AI Training

📌 **Clause: 8.3 – Data Management**

Scenario:
Synthetic data is used in training, but there are no internal criteria to ensure its quality, utility, or ethical implications.

What's Missing:
Policy and procedures for generating and validating synthetic data.

How to Fix:

✓ Define acceptable use cases for synthetic data

✓ Validate synthetic datasets for realism, bias, and privacy

✓ Document generation methods and link to model documentation

80. AI Systems Lack End-of-Life Planning

📌 Clause: 8.1 – Lifecycle Management

Scenario:
AI systems remain operational long after their usefulness or support has ended, creating unmanaged risks.

What's Missing:
Defined criteria and processes for system decommissioning.

How to Fix:

✓ Include "end-of-life" as a required step in AI lifecycle management

✓ Document when and how systems will be retired

✓ Archive related data, logs, and models securely

81. No Process to Assess the Ethical Use of AI in Marketing

📌 **Clause: 4.2 – Needs and Expectations of Interested Parties**

Scenario:
An AI tool personalizes ads based on user behavior, but there's no ethical review of targeting practices or manipulation risks.

What's Missing:
Ethical assessment for AI-driven persuasion or behavioral targeting.

How to Fix:
✓ Review marketing use cases for manipulation, profiling, or discrimination
✓ Establish red lines (e.g., no targeting based on sensitive attributes)
✓ Involve ethics officers or external advisors in high-risk reviews

82. AI Training Pipelines Lack Data Quality Validation Steps

📌 **Clause: 8.3 – Data Management**

Scenario:
Models are trained using datasets with missing values and labeling errors, leading to unpredictable behavior.

What's Missing:
Data quality checks during pipeline design and ingestion.

How to Fix:
✓ Validate training data for accuracy, completeness, and consistency
✓ Implement automated checks for outliers, duplicates, and label issues
✓ Document quality metrics as part of model development artifacts

83. Lack of User Education on AI Limitations and Risks

📌 Clause: 7.4 – Communication

Scenario:
Users trust AI-generated results as fact, unaware of limitations like bias, inaccuracy, or hallucinations.

What’s Missing:
User awareness of system boundaries and potential risks.

How to Fix:
✓ Provide clear disclaimers or explanations with AI outputs
✓ Offer user guides or tutorials for interacting with AI responsibly
✓ Communicate fallback options or when to consult a human

84. No Controls for Prompt Injection or Manipulation in AI Interfaces

📌 Clause: 8.6 – AI System Security

Scenario:
A generative AI assistant is vulnerable to prompt injection, allowing users to manipulate it into unsafe behavior.

What’s Missing:
Defensive mechanisms against input manipulation in user-facing AI.

How to Fix:
✓ Sanitize and validate all user inputs
✓ Implement safeguards like token limits, response filtering, and context resets
✓ Continuously test for jailbreaks and injection vulnerabilities

85. AI Performance Metrics Are Not Aligned with Stakeholder Expectations

📌 Clause: 6.2 – AIMS Objectives

Scenario:
The development team tracks technical metrics like accuracy, but stakeholders care about fairness and user satisfaction.

What's Missing:
Business and user-aligned performance evaluation.

How to Fix:
✓ Define KPIs with stakeholder input
✓ Balance precision/recall with ethical and experiential goals
✓ Recalibrate metrics as feedback and expectations evolve

86. No Evaluation of AI Use in Internal HR or Employee Monitoring Systems

📌 Clause: 4.2 – Needs and Expectations of Interested Parties

Scenario:
An AI system monitors productivity and flags "underperformers," but there's no ethical or legal assessment of its impact on employees.

What's Missing:
Human-centered review of AI use in HR and workforce analytics.

How to Fix:

✓ Conduct risk and fairness assessments before deploying HR-related AI

✓ Consult legal and HR stakeholders

✓ Document oversight and ensure transparency with affected employees

87. AI-Driven Systems Lack Localization or Regional Adaptation

📌 **Clause: 4.1 – Understanding Context**

Scenario:
An AI assistant built for global rollout performs poorly in non-English markets due to cultural and language mismatches.

What's Missing:
Localization planning and testing for diverse user groups.

How to Fix:

✓ Adapt AI outputs, tone, and logic to regional needs

✓ Test systems in local languages with local users

✓ Include cultural advisors in product and testing phases

88. No Regular Review of AI Documentation for Accuracy and Relevance

📌 **Clause: 7.5 – Documented Information**

Scenario:
Auditors find outdated or incomplete documentation describing model purpose, data, and ownership.

What’s Missing:
Periodic documentation reviews to ensure reliability.

How to Fix:
✓ Set a documentation review schedule (e.g., quarterly or post-deployment)
✓ Use version control to track updates
✓ Assign responsibility for maintaining documentation accuracy

89. Inadequate Consideration of AI Risks in Mergers & Acquisitions (M&A)

📌 **Clause: 6.1 – Risk Identification and Evaluation**

Scenario:
An acquired company brings AI models with undocumented risks and no governance history.

What’s Missing:
Due diligence process for AI assets during M&A.

How to Fix:
✓ Assess AI models for data lineage, risk, IP status, and compliance gaps
✓ Integrate acquired AI assets into your AIMS immediately
✓ Revalidate models under your organization’s governance controls

90. No Assessment of Long-Term Societal Impact of AI Technologies

📌 Clause: 4.1 – Context of the Organization

Scenario:
The company launches an AI-driven content recommender that contributes to echo chambers, but long-term societal effects were never considered.

What's Missing:
Forward-looking analysis of systemic AI impact.

How to Fix:

✓ Include societal impact in AI ethics and governance reviews

✓ Evaluate feedback loops, content amplification, and behavioral change risks

✓ Consult external ethics advisors for critical systems

91. No Process to Phase Out Unsustainable AI Practices

📌 Clause: 4.1 – Understanding Context and Sustainability

Scenario:
High-resource models are continuously trained with no review of environmental cost or sustainable alternatives.

What's Missing:
Governance for identifying and replacing environmentally unsustainable practices.

How to Fix:

✓ Track compute usage and emissions of AI workloads

✓ Phase out inefficient models or processes

✓ Evaluate trade-offs between performance and sustainability

92. No Policy for Dual-Use or High-Risk AI Research

📌 Clause: 6.1 – Risk Assessment

Scenario:
A research team develops an advanced generative model that could be misused (e.g., for misinformation) without governance review.

What's Missing:
Dual-use and misuse prevention protocols.

How to Fix:
✓ Identify dual-use risks in early research stages

✓ Apply ethics review and usage restrictions

✓ Restrict open deployment and model weights sharing when warranted

93. Lack of Procedures to Retire AI Features That Cause Harm

📌 Clause: 10.1 – Nonconformity and Corrective Action

Scenario:
A chatbot feature generates offensive content, but the organization delays removal due to business pressure.

What's Missing:
A clear path to sunset harmful features quickly and transparently.

How to Fix:
✓ Build deactivation into your incident response process

✓ Monitor for harm and escalate rapidly

✓ Communicate deprecations clearly to users and internal teams

94. No Post-Mortem Analysis for AI Incidents

📌 **Clause: 10.2 – Continual Improvement**

Scenario:
An AI malfunction affects customer experience, but there's no structured debrief to prevent recurrence.

What's Missing:
Post-incident learning and preventive process enhancement.

How to Fix:

✓ Conduct structured post-mortems for every significant AI issue

✓ Include root cause, contributing factors, and corrective actions

✓ Feed insights into training, documentation, and governance updates

95. Infrequent Review of the Artificial Intelligence Management System (AIMS)

📌 **Clause: 9.3 – Management Review**

Scenario:
The AIMS has not been updated in over 18 months, despite several new tools and regulatory changes.

What's Missing:
Regular strategic review of the overall AI governance system.

How to Fix:

✓ Schedule biannual AIMS reviews with leadership

✓ Evaluate effectiveness, scope, resource needs, and compliance alignment

✓ Capture new risks, stakeholder needs, and audit findings

96. No Independent Oversight of High-Risk AI Projects

📌 **Clause: 5.1 – Leadership and Oversight**

Scenario:
All decisions for a controversial AI deployment are made within the same team, without independent review or dissenting input.

What's Missing:
Neutral, cross-functional oversight for projects with elevated societal impact.

How to Fix:

✓ Mandate external review boards or independent internal committees

✓ Rotate reviewers and include ethical or public-interest representatives

✓ Document dissenting opinions and how they were addressed

97. Failure to Track and Learn from Industry AI Failures

📌 **Clause: 10.2 – Continual Improvement**

Scenario:
Despite widely publicized failures in similar AI systems (e.g., bias lawsuits, compliance fines), the organization doesn't apply those lessons internally.

What’s Missing:
External learning and adaptive governance.

How to Fix:
✓ Track AI-related news, legal cases, and regulator updates
✓ Add a “Lessons Learned” section to your AIMS documentation
✓ Review external incidents quarterly and apply improvements

98. No Process for Transparent Communication of AI Capabilities and Limitations

📌 **Clause: 7.4 – Stakeholder Communication**

Scenario:
Marketing materials overstate the precision of an AI tool, leading to unrealistic user expectations.

What’s Missing:
Fact-checking and transparency in how AI is positioned externally.

How to Fix:
✓ Review public-facing materials for AI claims
✓ Disclose capabilities, known limitations, and boundaries of use
✓ Involve compliance, legal, and ethics teams in review

99. No Real-Time Monitoring of Mission-Critical AI Systems

📌 **Clause: 9.1 – Monitoring and Evaluation**

Scenario:
An AI system that controls industrial machinery fails, causing costly downtime, because real-time alerts weren’t in place.

What’s Missing:
Live monitoring and proactive alerts for critical AI applications.

How to Fix:
✓ Set up monitoring dashboards with anomaly detection
✓ Define alert thresholds and escalation paths
✓ Integrate alerts with operational response teams

100. AI System Improvement Suggestions from Users Are Not Captured or Reviewed

📌 **Clause: 10.2 – Continual Improvement**

Scenario:
Users regularly share feedback on improving an AI product, but it's not collected, tracked, or acted on.

What’s Missing:
A feedback loop from users into AI system design and updates.

How to Fix:
✓ Implement a feedback capture system (e.g., forms, tickets, NPS prompts)
✓ Review feedback regularly during governance meetings
✓ Prioritize common suggestions for system improvement

Advancing Your ISO 42001 Compliance Journey

Achieving ISO 42001 certification is more than a milestone — it's a commitment to building AI systems that are ethical, transparent, and accountable.

By addressing these 100 common non-conformities, you're not just preparing for an audit. You're establishing a foundation for trustworthy AI governance, reducing reputational and operational risk, and aligning with the future of responsible innovation.

🔄 AI Governance Requires Momentum

AI is constantly evolving — and so are its risks. Continuous monitoring, bias reviews, retraining, stakeholder engagement, and ethical oversight must be **woven into your AIMS lifecycle** to ensure long-term compliance and resilience.

📃 Transparency and Traceability Are Non-Negotiable

Documenting decisions, managing model lifecycles, and maintaining audit trails aren't just technical tasks — they are essential for **demonstrating accountability**, building stakeholder trust, and withstanding regulatory scrutiny.

🏆 Compliance as a Competitive Differentiator

Organizations that treat AI governance as a strategic advantage — not a checkbox — will lead the next wave of innovation. A well-executed ISO 42001 framework will **set your organization apart**, unlock global partnerships, and future-proof your AI strategy.

Use this guide as your survival kit — a field-tested resource to identify blind spots, correct course, and mature your AI Management System into a vehicle for sustainable, responsible growth.

GSDC
Global Skill Development Council
ISO
42001:2023
Lead Auditor
CERTIFIED