

August 2026

No. 1

AI Conformity Assessment Use Case

Use of AI to Support Management
System Certification Decisions



Artificial
Intelligence
Quality
Infrastructure

Introduction

Use Case Purpose and Scope

This use case is provided as an illustrative example to support discussion on how AI *could* be used to support specific conformity assessment activities. It is not a playbook, implementation guide, or prescriptive guidance, and should not be read as instructions for designing, deploying, or operating AI systems.

The purpose is to give Conformity Assessment Bodies (CABs) considering AI use context on potential applications, risks, and control considerations, rather than “how-to” direction. Following the guidance in this document is not evidence of conformity, compliance, or suitability under any standard, accreditation scheme, or regulatory framework.

Intended Audience

This use case is intended for CAB leadership, technical and operational management, including those without specialist AI expertise. AI concepts are therefore presented at a high level, focusing on implications for conformity assessment activities rather than technical detail.

Responsibility and Applicability

Any consideration of AI use remains the responsibility of the individual CAB. CABs must assess suitability and allowability in line with their own:

- Accreditation body requirements including those at local, regional or global level, such as IAF MD4
- Applicable standards and regulations such as the EU AI Act (including data protection and AI regulation where relevant)
- Sector-specific and contractual obligations
- Internal governance, competence, and risk management arrangements

What may be appropriate in one context may not be appropriate or permissible in another.

How This Use Case Should Be Used

This use case should be read as:

- An example scenario, not a recommended solution
- A basis for risk-based discussion and internal consideration
- A way to explore where AI support may add value, and where it may introduce unacceptable risk

Use Case Overview

- a. **Conformity Assessment Type:** - Management System Certification (ISO/IEC 17021-1)
- b. **Conformity Assessment Process Step:** - Review and Decision / Attestation
- c. **Use Case Description:** - AI is used to support certification decision-making by analysing outputs from the conformity assessment process, including audit reports, nonconformities, and corrective actions. The system provides structured insights to highlight key risks, inconsistencies, and potential gaps in information. The objective is to support more consistent and informed decision-making, while ensuring that final certification decisions remain the responsibility of competent personnel.
- d. **Potential AI Technologies:** - Large Language Models (LLMs), Natural Language Processing (NLP), Machine Learning, Predictive Analytics, Rule-Based Expert Systems

Data Inputs & Processing

- a. **Typical data inputs are likely to include:**
 - Current and historic audit reports
 - Nonconformity reports and classifications
 - Corrective action plans and closure evidence
 - Internal decision criteria or guidance
 - Relevant standard requirements, potentially utilising SMART standards
 - Historical certification decisions
 - Client submitted information and data
 - Auditor notes including audio or video
- b. **The AI system processes the input data to:**
 - Check completeness of decision inputs
 - Analyse nonconformities (severity, recurrence, patterns)
 - Compare the case against defined decision criteria
 - Identify inconsistencies or unusual patterns

Data Outputs

- a. **Typical outputs of such a system could include:**
 - A structured decision support summary
 - Flagging for missing, inconsistent or incomplete information
 - A risk or complexity indicator (e.g. low / medium / high)

- Suggested areas for decision-maker attention

Potential Benefits

- Improved consistency of certification decisions
- Reduced risk of overlooking critical issues
- Increased efficiency in reviewing complex cases
- Enhanced ability to identify systemic patterns across decisions

Explainability Considerations

- a. The ability to explain how an AI system reaches its outputs is an important consideration for conformity assessment activities, particularly where AI is used to support review or decision-making processes.
- b. Different AI technologies provide different levels of explainability. For example:
 - Rule-based and expert systems typically provide a clear rationale for outputs and can often show which rules were applied.
 - Machine learning models may identify patterns within data but provide limited visibility of how specific conclusions were reached.
 - Large Language Models (LLMs) can provide explanations for their outputs, but these explanations may not always accurately reflect the underlying reasoning of the model.
- c. When selecting and designing AI systems, CABs should consider whether the level of explainability provided is appropriate for the intended use case and sufficient to support:
 - effective human review and challenge of outputs;
 - investigation of unexpected outcomes;
 - demonstration of competence, impartiality and consistency;
 - explanation of decisions to customers, regulators and accreditation bodies where required.
- d. For higher-risk use cases, it may be more appropriate to favour AI approaches that provide greater transparency or incorporate additional controls to improve explainability and traceability.

Risks and Considerations

The following are potential risks and other considerations relevant to this use case that should be considered for AI system design, training and the implementation of control measures. This list is not exhaustive.

Data Risks

- Use of unstructured, inconsistent or unclear data in training data set
- Use of client, personal or commercially sensitive data creating confidentiality concerns
- Collection and use of data outside of existing contractual consent boundaries
- Use of external data sources not subject to CAB control – e.g. training data for public LLMs
- Bias or inconsistency in historical decision data.

Technical / AI Risks

- The clarity of explainability of AI decisions and outputs to end users and other stakeholders in natural language, understandable to both
 - internally (e.g. to support internal auditing)
 - externally (e.g. for responding to complaints or legal challenges)
- Potential for incorrect interpretation of context
- Performance variability depending on input quality

Conformity Assessment Risks

- Automation bias, where decision-makers rely too heavily on AI outputs
- Provision of falsely confident responses on incomplete or poor-quality audit inputs.
- Reduced critical assessment by decision-makers
- Edge cases where decision is borderline AI output may give false sense of certainty
- Niche cases where the training data has insufficient data to train the AI system on sector/standard context and requirements

Regulatory / Accreditation Risks

- Misalignment with ISO/IEC and/or Accreditation Body requirements
- Lack of transparency or explainability in AI decisions/outcomes

Potential Control Measures:

The following are potential control measures related to the risks and other considerations relevant to this use case that could be deployed to help remove, manage or mitigate risks. This list is not exhaustive.

Governance & Oversight

- Define AI system with CAB processes as a decision-support tool only
- Prohibit autonomous decision-making by AI
- Clearly document scope and limitations of the AI system – communicate these to relevant stakeholders
- Consider a RACI (Responsible, Accountable, Consulted, Informed) matrix to manage governance actions
- Include 'Human-in-the-loop' measures at critical decision-making points
 - *(Note: It should be recognised that experience and seniority of resources does not fully mitigate the potential for automation bias)*

Design, Validation & Performance

- Validate outputs across range of decision complexity and technical sectors, including edge cases before operational use
- Periodically review AI performance, consistency and potential bias through benchmarking against human review outcomes and representative datasets.
- Design the AI system to flag uncertainty rather than try resolve it
- Introduce indicators to identify low confidence, or inconsistent data
- Review historical decision data for consistency and potential bias before using it to train or validate AI systems.

Data Management

- Control use of client data
- Ensure AI service providers are subject to appropriate contractual and information security controls
- Seek permission from clients prior to using their data
- Ensure data confidentiality is maintained
- Define clear rules for data usage
- Consider data minimisation techniques (e.g. anonymisation, redaction or removal of unnecessary client information)

- Consider how potential AI providers retain, process and use submitted data, including whether data may be used for model training or service improvement
- Where highly sensitive information is involved, consider deployment options that provide greater control over data handling and retention.

Process Integration

- Require escalation/deeper human review of borderline or complex cases
- Avoid use of AI-generated recommendations in edge cases
- Require explicit human validation of process changes
- Maintain auditable records of AI-supported decisions, including relevant inputs, outputs, human review activities and the rationale for final decisions.

Competence

- Train staff to:
 - understand AI systems limitations
 - critically assess AI system outputs
- Train staff to identify automation bias and build in processes to manage and reduce the risks of automation bias
- Continue to maintain independent human decision-making capability

Transparency

- Document use of AI within the management system
- Inform customers and stakeholders of AI use

AI Systems Drift & Change Management:

- Periodically review AI system output against data sets with known outcomes
- Implement change management procedures requiring revalidation of AI systems across range of scenarios following change, either to system design, operational processes or conformity assessment requirements.
- Establish procedures to identify and assess changes made by third-party AI providers to their models and systems and determine whether revalidation is required before continued operational use.

Where This Use Case Is Lower or Higher Risk

Situations and scenarios where such a use of an AI system would present higher or lower risk to the CAB.

a. Lower risk when:

- High volumes of certification decisions are conducted
- Well-defined decision criteria exist
- Sufficient high-quality data, structured data is available to train the AI system
- Explainability of AI decisions is clear and transparent

b. Higher Risk when: Less suitable when:

- Decisions are highly bespoke or context-dependent
- Potential training data is limited or inconsistent
- Existing processes are not standardised or well defined
- Where certification outcomes have significant legal or safety implications
- Explainability of AI decisions are unclear
- Where regulatory or accreditation requirements restrict automation or use of ICT



Artificial
Intelligence
Quality
Infrastructure

Learn more about our work at www.aiqi.org