ICTQual AB

Qualification Specification

ICTQual ISO/IEC 42001 Artificial Intelligence Management System Lead Auditor Course

Website
www.ictqualab.co.uk

Email:
support@ictqualab.co.uk

ICTQual AB's

ISO/IEC 42001 Artificial Intelligence Management System Lead Auditor Course

Contents

Qualification Specification about

ICTQual ISO/IEC 42001 Artificial Intelligence Management System Lead Auditor Course

About ICTQual AB's

ICTQual AB is a distinguished awarding body based in the United Kingdom, dedicated to fostering excellence in education, training, and skills development. Committed to global standards, ICTQual AB's provides internationally recognized qualifications that empower individuals and organizations to thrive in an increasingly competitive world. Their offerings span diverse industries, including technical fields, health and safety, management, and more, ensuring relevance and adaptability to modern workforce needs.

ICTQual AB's delivers high-quality educational solutions through a network of Approved Training Centres worldwide. Their robust standards and innovative teaching methodologies equip learners with practical knowledge and skills for personal and professional growth. With a mission to inspire lifelong learning and drive positive change, ICTQual AB's continuously evolves its programs to stay ahead of industry trends and technological advancements.

Course Overview

As artificial intelligence (AI) rapidly integrates into business processes, the need to manage it responsibly, ethically, and securely has never been greater. ISO/IEC 42001 is the world's first international standard for Artificial Intelligence Management Systems (AIMS), providing a comprehensive framework for managing the risks and opportunities associated with AI.

The **ICTQual ISO/IEC 42001 Lead Auditor Course** is a specialized training program designed to equip professionals with the expertise required to audit AI management systems. Combining theoretical frameworks with practical auditing techniques, the course empowers you to assess an organization's AI infrastructure, ensuring it adheres to international best practices, ethical guidelines, and regulatory requirements. As global regulatory landscapes tighten, with governments implementing strict oversight and legal mandates regarding algorithmic accountability, compliance is transitioning from a voluntary best practice to a strict legal necessity. Organizations require a structured mechanism to demonstrate that their systems are under continuous monitoring, rigorous risk assessment, and effective control

Aims

The primary aim of this course is to provide participants with the comprehensive knowledge and practical skills needed to perform first-party (internal), second-party (supplier), and third-party (certification) audits of an Artificial Intelligence Management System against the ISO/IEC 42001 standard. Ultimately, the program aims to build digital trust across industries by training auditors who can ensure AI systems are deployed transparently, safely, and accountably.

Objectives

By completing this course, participants will be able to:

- **Comprehend the Framework:** Understand the fundamental principles, core concepts, and specific requirements of the ISO/IEC 42001 standard.
- **Master Auditing Techniques:** Plan, execute, report, and close compliance audits in accordance with globally recognized auditing guidelines (such as ISO 19011 and ISO/IEC 17021-1).
- **Evaluate AI Governance:** Assess an organization's AI risk management, data privacy protocols, and ethical governance structures.
- **Identify Non-Conformities:** Recognize deviations from the standard, accurately document audit findings, and evaluate the effectiveness of corrective actions.

Targeted Audience

This course is highly beneficial for professionals looking to stay ahead of the curve in the rapidly evolving landscape of AI governance. The ideal candidates include:

- **Auditors (Internal and External):** Professionals looking to expand their expertise into the specialized field of AI management systems.
- **Governance, Risk, and Compliance (GRC) Professionals:** Risk managers, compliance officers, and legal advisors responsible for ensuring AI technologies meet regulatory and ethical standards.
- **IT and Tech Leaders:** Chief AI Officers, IT directors, and system architects involved in developing, deploying, or managing organizational AI strategies.
- **Consultants and Advisors:** Expert consultants assisting external organizations with improving their AI management practices and achieving ISO/IEC 42001 certification.

Certification Framework

Qualification title	**ICTQual ISO/IEC 42001 Artificial Intelligence Management System Lead Auditor Course**
Course ID	ISOLAC0023
Total Qualification Time	40 Hours
Guided Learning Hours	20 Hours
Grading Type	Pass / Fail
Competency Evaluation	Coursework / Assignments / Verifiable Experience
Assessment	The assessment and verification process for ICTQual AB's qualifications involves two key stages: **Internal Assessment and Verification:** ✓ Conducted by the staff at the Approved Training Centre (ATC) to ensure learners meet the required standards through continuous assessments. ✓ Internal Quality Assurance (IQA) is carried out by the centre's IQA staff to validate the assessment process. **External Quality Assurance:** ✓ Managed by ICTQual AB's verifiers, who periodically review the centre's assessment and IQA processes. Verifies that assessments are conducted to the required standards and ensures consistency across centres

Entry Requirements

Entry requirements for a ISO/IEC 42001 Artificial Intelligence Management System Lead Auditor Course may vary depending on the institution offering the program. However, typical entry requirements for such a course may include:

- ✓ **Age Requirement:** Learners must be at least 18 years of age at the time of enrolment.
- ✓ **Educational Background:** A minimum of secondary education is required. Diplomas or Certificates in Artificial Intelligence, Information Technology, Data Science, Cyber Security, Risk Management, or ISO Management Systems from the International Organization for Standardization are considered advantageous.
- ✓ **Language Proficiency:** Learners should have a good command of English, including reading, writing, and communication skills.
- ✓ **Work Experience:** Prior experience in AI systems, IT, auditing, compliance, or risk management roles is beneficial but not mandatory

Qualification Structure

This qualification comprises 6 mandatory units, totalling 04 Credits. Candidates must successfully complete all mandatory units to achieve the qualification.

Mandatory Units	
Unit Ref#	**Unit Title**
ISOLAC0023-1	Introduction to AI Management Systems:
ISOLAC0023-2	Overview of ISO/IEC 42001 Standard
ISOLAC0023-3	Auditing Techniques
ISOLAC0023-4	AI Governance and Ethics
ISOLAC0023-5	Risk Management in AI
ISOLAC0023-6	Data Management and Privacy

Centre Requirements

To ensure quality training delivery, centres must adhere to the following standards:

1. Centre Approval

- ✓ Centres must be formally approved by ICTQual AB's before delivering this qualification.
- ✓ Approval involves a review of facilities, policies, and staff qualifications.

2. Qualified Staff

- ✓ **Tutors:** Must hold a Bachelor's Degree (Level 6) or higher in Computer Science, Information Technology, or Risk Management alongside relevant professional experience as a certified Lead Auditor with practical expertise in AI governance and compliance.
- ✓ **Assessors:** Must hold a recognized assessor qualification (e.g., CAVA, AVRA) or equivalent)
- ✓ **Internal Quality Assurers (IQAs):** Must hold a recognized IQA qualification (e.g. Level 4 Award in the IQA and Level 4 Certificate in Leading the IQA) and experience to oversee assessment standards.

3. Learning Facilities

Centre must offer:

- ✓ Private study areas and internet-enabled workspaces (for blended or physical delivery)
- ✓ Academic and pastoral support for learners
- ✓ Administrative support must be available to manage enrolment, tracking, and learner queries efficiently

4. Health and Safety Compliance

- ✓ All training facilities must comply with health and safety regulations.

- ✓ Centres must conduct regular risk assessments for practical activities.

5. Learning Resources

- ✓ **Course Materials:** Approved textbooks, study guides, and digital content must align with the qualification standards.
- ✓ **Assessment Tools:** Templates and guidelines must be provided to ensure standardized evaluation processes.
- ✓ **E-Learning Support:** Centres offering online or blended learning must implement an effective Learning Management System (LMS).

6. Assessment and Quality Assurance

- ✓ Centres must ensure assessments meet ICTQual AB's competency standards.
- ✓ Internal quality assurance (IQA) must be conducted to maintain consistency.
- ✓ External verifiers from ICTQual AB's will review assessment and training practices.

7. Learning Support

- ✓ **Qualification Guidance:** Support for coursework and assignments.
- ✓ **Career Pathway Assistance:** Information on progression opportunities in Computer Science, Information Technology, or Risk Management sectors.
- ✓ **Accessibility Support:** Accommodations for learners with disabilities or language barriers.

8. Policies and Compliance

Centres must uphold the following policies in accordance with ICTQual AB's standards:

- ✓ Equality, Diversity, and Inclusion Policy.
- ✓ Health and Safety Policy.
- ✓ Safeguarding and Learner Protection Policy.
- ✓ Complaints and Appeals Procedure.
- ✓ Data Protection and Confidentiality Policy.

9. Reporting Requirements

- Centres must provide ICTQual AB's with regular reports on learner registrations, progress, and certification outcomes.
- Assessment records must be maintained for external auditing and quality assurance purposes.

Support for Candidates

Centres should ensure that materials developed to support candidates:

- ✓ Facilitate tracking of achievements as candidate's progress through the learning outcomes and assessment criteria.
- ✓ Include information on how and where ICTQual AB's policies and procedures can be accessed.
- ✓ Provide mechanisms for Internal and External Quality Assurance staff to verify and authenticate evidence effectively.

This approach ensures transparency, supports candidates' learning journeys, and upholds quality assurance standards.

Assessment

This qualification is competence-based, requiring candidates to demonstrate high-level strategic proficiency as defined in the qualification units. The assessment evaluates the candidate's skills, knowledge, and understanding against the set standards. Key details include:

Assessment Process:

- Must be conducted by an experienced and qualified assessor.
- Candidates compile a portfolio of evidence that satisfies all learning outcomes and assessment criteria for each unit.

Types of Evidence:

- Assignments, detailed research projects, or strategic reports.
- Professional discussions.
- Candidate-produced strategic work (e.g., policy drafts, financial models).
- Recognition of Prior Learning (RPL).

Learning Outcomes and Assessment Criteria:

- **Learning Outcomes:** Define what candidates should know, understand, or accomplish upon completing the unit.
- **Assessment Criteria:** Detail the standards candidates must meet to demonstrate that the learning outcomes have been achieved.

Unit Descriptors

ISOLAC0023-1- Introduction to AI Management Systems

This unit introduces the foundational concepts of management systems tailored for artificial intelligence technologies. Learners will explore the strategic importance of structural governance, operational controls, and continuous improvement in automated environments. The curriculum addresses organizational alignment, baseline terminology, and the foundational elements necessary to establish, maintain, and review a systematic framework for overseeing intelligent technological applications effectively across modern industries.

Learning Outcome:	Assessment Criteria:
1. Understand the fundamental concepts and principles of AI governance and management systems.	1.1 Explain the core concepts and principles of artificial intelligence governance within an organisational context. 1.2 Evaluate how governance principles apply to different stages of the artificial intelligence lifecycle. 1.3 Outline the primary objectives of a management system designed for continual improvement and regulatory compliance.
2. Identify the key components of AI management systems, including governance structures, roles, and responsibilities.	2.1 Describe the essential elements required to establish a functioning management framework. 2.2 Map out the specific roles and responsibilities needed for effective system implementation and daily monitoring. 2.3 Review a proposed governance structure to ensure clear accountability and logical decision making pathways.
3. Recognize the importance of ethical considerations and risk management in AI development and deployment.	3.1 Identify common ethical dilemmas and potential biases associated with technology deployment. 3.2 Conduct a targeted risk assessment to highlight vulnerabilities in a proposed technological solution. 3.3 Formulate practical strategies to mitigate identified risks and ethical concerns during the development phase.
4. Gain insights into the societal impacts of AI technologies and the need for responsible AI governance.	4.1 Discuss the potential positive and negative impacts of these technologies on society, privacy, and the workforce. 4.2 Analyse a real-world scenario to determine the societal implications of an automated decision-making process.

4.3 Justify the necessity of responsible governance practices to build public trust and ensure long term fairness.

ISOLAC0023-2- Overview of ISO/IEC 42001 Standard

This unit provides a comprehensive analysis of the international standard for artificial intelligence management systems. Participants will examine the core clauses, mandatory requirements, and structural framework that define corporate compliance. The material emphasizes understanding structural expectations, policy development, organizational roles, and compliance documentation needed to successfully align institutional operations with global benchmarks and standardized management criteria within contemporary corporate markets.

Learning Outcome:	Assessment Criteria:
1. **Familiarize yourself with the requirements and principles outlined in the ISO/IEC 42001 standard.**	1.1 Summarise the primary objectives and foundational principles of the standard regarding artificial intelligence management. 1.2 Outline the specific mandatory requirements necessary for establishing, maintaining, and improving the management system. 1.3 Assess an organisation's current baseline policies against the core principles of the standard to identify initial compliance gaps.
2. **Interpret the key clauses and provisions of the standard related to AI governance, ethics, and risk management.**	2.1 Explain the practical intent behind the core clauses of the standard, particularly focusing on leadership, planning, and operation. 2.2 Interpret how specific provisions dictate the approach an organisation must take to conduct impact and risk assessments. 2.3 Audit a sample management system to verify its alignment and compliance with the critical clauses governing ethical deployment.
3. **Understand the role of ISO/IEC 42001 in guiding organizations towards the responsible development and deployment of AI technologies.**	3.1 Describe how the standard's framework facilitates a structured, auditable approach to responsible technological innovation. 3.2 Evaluate the effectiveness of the standard in aligning an organisation's operational objectives with safe development practices. 3.3 Demonstrate how the guidelines can be actively applied to improve system transparency and build stakeholder trust during deployment.

4. **Explore case studies and examples illustrating the application of ISO/IEC 42001 in real-world scenarios.**

4.1 Analyse a real world case study to identify how the standard was successfully implemented to resolve specific governance challenges.

4.2 Extract key lessons learned from industry examples regarding the practical application of specific clauses and operational controls.

4.3 Apply insights gained from documented scenarios to propose targeted solutions during a simulated organisational compliance audit.

ISOLAC0023-3- Auditing Techniques

This unit focuses on the practical methodologies required to plan, execute, report, and follow up on professional compliance audits. Learners will master advanced auditing principles, interviewing strategies, and reporting protocols. The curriculum prepares individuals to lead evaluation teams, identify gaps, gather documentation, verify institutional compliance, and present clear findings to stakeholders while maintaining strict objectivity throughout the entire auditing process.

Learning Outcome:	Assessment Criteria:
1. **Develop proficiency in auditing techniques specific to AI management systems.**	1.1 Explain the specialized auditing methods required to evaluate algorithmic transparency, data sets, and system bias. 1.2 Apply interview techniques effectively to gather information from technical developers and system operators during an audit. 1.3 Evaluate the operational effectiveness of automated logging and tracking tools used within the management framework.
2. **Learn how to plan, conduct, and report on AI management system audits in accordance with ISO/IEC 42001 standards.**	2.1 Prepare a comprehensive audit plan that defines the scope, objectives, resource requirements, and schedules for a system review. 2.2 Execute an audit opening meeting and perform on site verification activities following established international auditing protocols. 2.3 Draft a clear audit report that accurately presents the findings, conclusions, and summary of the management system state.
3. **Acquire the skills to assess compliance, identify non-conformities, and recommend corrective actions.**	3.1 Evaluate operational processes against standard requirements to determine the level of organizational compliance. 3.2 Identify and document formal non conformities by linking observed deficiencies directly to specific clauses of the standard. 3.3 Review and approve proposed corrective action plans to ensure they address the root cause of identified failures.

4. Gain practical experience through simulated audit scenarios and exercises.	4.1 Participate in a simulated audit activity to demonstrate practical application of gathering and verifying information. 4.2 Manage a mock audit team during a practical scenario to ensure all assigned areas of the management system are assessed. 4.3 Deliver a professional closing meeting presentation summarizing audit findings to simulated organizational management.

ISOLAC0023-4- AI Governance and Ethics

This unit explores the critical intersection of ethical accountability, fairness, and governance within automated systems. Participants will analyze transparency challenges, algorithmic bias mitigation, and socio-economic impacts of technology deployment. The course material guides learners in evaluating organizational policies, corporate responsibility guidelines, and international principles to ensure automated processes remain trustworthy, unbiased, and aligned with current global societal values and expectation.

Learning Outcome:	Assessment Criteria:
1. **Explore the ethical implications of AI technologies, including fairness, accountability, transparency, and bias.**	1.1 Define the core ethical terms of fairness, accountability, transparency, and bias as they relate to automated decision-making. 1.2 Analyze an AI system's design documentation during an audit to identify potential areas where data bias could occur. 1.3 Evaluate the methods an organization uses to ensure that automated system outcomes can be clearly explained to end-users.
2. **Understand the role of AI governance frameworks in promoting ethical AI development and deployment.**	2.1 Explain how an AI governance framework turns high-level ethical values into practical, day-to-day business policies. 2.2 Contrast regular corporate governance with the specialized governance requirements outlined in the ISO/IEC 42001 standard. 2.3 Verify during a sample audit that an organization's ethical AI policies are actively supported by senior management and applied to all live projects.
3. **Learn how to integrate ethical considerations into AI governance structures and decision-making processes.**	3.1 Outline the exact steps required to include mandatory ethical checkpoints within an AI project's lifecycle and decision-making path. 3.2 Audit the meeting logs and charter of an organization's AI oversight committee to ensure they have the authority to halt high-risk deployments. 3.3 Review a company's product release process to confirm that sign-offs require a completed ethical and societal impact assessment.

4. **Gain insights into emerging trends and best practices in AI ethics and governance.**

4.1 Identify current global trends, international standards, and changing legal regulations that affect AI governance.

4.2 Assess whether an organization's AI management system has a clear, working process to update its rules when new ethical risks or laws emerge.

4.3 Review an organization's post-deployment monitoring plans to ensure they follow industry best practices for detecting unexpected algorithmic drift or unfair outcomes.

ISOLAC0023-5- Risk Management in AI

This unit addresses the specialized methodologies for identifying, assessing, and mitigating risks unique to advanced computational models. Learners will evaluate systemic vulnerabilities, continuous oversight models, and impact assessment procedures. The focus remains on establishing robust control mechanisms, defining risk tolerance, implementing safety protocols, and managing algorithmic life cycles to protect organizational assets from potential disruption and unforeseen corporate operational failure.

Learning Outcome:	Assessment Criteria:
1. **Understand the principles and methodologies of risk management as applied to AI technologies.**	1.1 Explain how the risk management process in the ISO/IEC 42001 standard applies to the entire lifecycle of an AI system. 1.2 Describe the difference between standard IT security risks and specialized AI risks, such as model drift (how an AI's accuracy changes over time) and data bias. 1.3 Review an organization's risk assessment policy to confirm it outlines clear, logical rules for measuring risk likelihood and impact.
2. **Identify and assess potential risks associated with AI development, implementation, and use.**	2.1 Identify the main sources of operational and ethical risks that can occur during data collection and model training. 2.2 Examine a live AI application during a practical exercise to spot potential risks regarding data privacy, user safety, and lack of explainability. 2.3 Check an organization's AI risk register during an audit to verify that all logged risks have accurate and measurable rating scores.
3. **Learn how to develop risk management strategies and mitigation plans to address identified risks.**	3.1 Explain the standard methods used to treat risks, such as reducing, avoiding, transferring, or accepting the risk. 3.2 Review a sample AI risk treatment plan to ensure it selects the correct protective controls from Annex A of the standard. 3.3 Evaluate whether a company's incident response and escalation procedures are strong enough to handle unexpected AI performance failures or data breaches.

4. **Explore case studies and examples illustrating effective risk management practices in AI projects.**

4.1 Analyze a real-world example of an AI system failure to point out exactly which risk controls were missing or broken.

4.2 Explain how industry best practices, like "human-in-the-loop" monitoring, can successfully prevent automated systems from making unfair decisions.

4.3 Use lessons from documented industry case studies to suggest practical audit improvements for a simulated AI management system.

ISOLAC0023-6- Data Management and Privacy

This unit examines the critical role of data quality, processing pipelines, and privacy compliance in intelligent systems. Participants will analyze data lineage, masking techniques, consent management, and regulatory protection laws. The lessons emphasize auditing security infrastructure, information life cycles, governance controls, and validation techniques to ensure data handling practices remain secure, legally compliant, and systematically verified across all corporate environments.

Learning Outcome:	Assessment Criteria:
1. Gain an understanding of data management practices relevant to AI technologies.	1.1 Explain the data lifecycle stages including collection, storage, processing, and disposal within a management system. 1.2 Evaluate how data quality, relevance, and balance are checked to ensure system accuracy. 1.3 Check an organisation's data inventory records during a practical audit to verify that data sources are properly tracked.
2. Learn about the privacy implications of AI systems and the importance of data protection.	2.1 Describe potential privacy risks that occur when large datasets are used for system training. 2.2 Review an organisation's data protection impact assessments to verify how personal information is safeguarded. 2.3 Evaluate the practical application of data minimization and anonymization techniques within a system.
3. Understand regulatory requirements and compliance considerations related to data privacy in AI projects.	3.1 Outline the primary legal and regulatory requirements governing data privacy and protection applicable to the organisation. 3.2 Audit data consent records to confirm that user permission is obtained and managed legally. 3.3 Identify compliance gaps between actual data sharing workflows and relevant privacy laws.
4. Acquire knowledge of best practices for managing and securing data in AI environments.	4.1 Detail industry best practices for securing training data against unauthorized access, tampering, or corruption. 4.2 Audit the access control logs and encryption methods used to protect sensitive datasets. 4.3 Review a company's data breach response procedure to ensure it includes clear steps for reporting data issues.

ICTQual AB

Yew Tree Avenue, Dagenham,

London East, United Kingdom RM10 7FN

+447441398083

support@ictqualab.co.uk|www.ictqualab.co.uk

VisitOfficialWebpage