# ISO 42001
# Compliance checklist

# Contents

# Use our checklist and find out if you are sufficiently prepared for certification.

This ISO 42001 compliance checklist is a valuable tool to help you assess your Artificial Intelligence Management System (AIMS) and identify any areas that may require attention before your certification or transition audit.

Structured around the core clauses of ISO 42001, this checklist will help you evaluate whether your AIMS is aligned with the standard's requirements and key AI governance principles. It covers:

- The context of your organisation
- Leadership and governance
- Risk identification and impact assessment
- Operational and data management controls
- Lifecycle, transparency and third-party relationships

By using this checklist, you can review each requirement and input your responses directly. This will support a more comprehensive understanding of your AI-related risks and responsibilities and help you move forward with confidence.

# Clause 4 – Context of the organisation



Understanding your organisation’s purpose, internal and external context and the expectations of interested parties is essential to establishing an effective AIMS. This sets the foundation for scope, objectives and governance of AI systems.

- [ ] Have you identified internal and external issues relevant to your AI systems?
- [ ] Have you determined the needs and expectations of interested parties?
- [ ] Is the scope of your AIMS clearly defined?
- [ ] Is your AIMS established, implemented, maintained and continually improved?

Comments

# Clause 5 – Leadership



Leadership plays a critical role in establishing and supporting the AI Management System. Top management must demonstrate commitment, align the AIMS with the organisation’s strategic direction and assign clear responsibilities.

- [ ] Has top management demonstrated leadership and commitment to the AIMS?
- [ ] Is there an established AI policy aligned with the organisation’s strategic direction?
- [ ] Are roles, responsibilities and authorities for AI management assigned and communicated?

Comments

# Clause 6 – Planning



Effective planning ensures that AI-related risks and opportunities are managed proactively. This includes setting objectives and defining how your organisation will meet the requirements of ISO 42001.

- [ ] Have actions to address risks and opportunities been determined?
- [ ] Is there a process for AI risk assessment and treatment?
- [ ] Are AI system impact assessments conducted?
- [ ] Is the AI risk assessment informed and aligned with the AI policy and AI objectives?
- [ ] Are appropriate risk treatment options selected?
- [ ] Are AI objectives established and plans to achieve them in place?

Comments

# Clause 7 – Support



Support covers the resources, competence, communication and documentation needed to operate and improve the AIMS. Ensuring your teams are informed, equipped and supported is essential for consistent implementation.

- [ ] Are necessary resources for the AIMS provided?
- [ ] Is there a process to ensure personnel are competent on the basis of education, training, or experience?
- [ ] Are persons doing work under the organisation’s control aware of the AI policy and relevant procedures?
- [ ] Is internal and external communication determined and implemented?
- [ ] Is documented information required by the AIMS and ISO 42001 controlled?

Comments

# Clause 8 – Operation



Operational planning ensures that your AI systems are developed and used in line with defined processes. This includes managing change, assessing impacts and applying risk treatments throughout the system lifecycle.

- [ ] Are processes needed for the operation of AI systems planned, implemented and controlled?
- [ ] Are AI risk assessments and treatments integrated into operational processes?
- [ ] Are AI system impact assessments maintained and updated as necessary?

Comments

# Clause 9 – Performance Evaluation



Evaluating your AIMS performance helps confirm whether processes are effective and outcomes are being achieved. Internal audits and management reviews are essential tools for driving continual improvement.

- [ ] Are monitoring, measurement, analysis and evaluation of the AIMS conducted?
- [ ] Are internal audits performed at planned intervals?
- [ ] Does management review the organisation’s AIMS at planned intervals?

Comments

# Clause 10 – Improvement



Nonconformities and incidents can occur – what matters is how your organisation identifies, corrects and learns from them. A robust improvement process ensures sustained trust and effectiveness of your AIMS.

- [ ] Are opportunities for improvement determined and implemented?
- [ ] Are nonconformities and corrective actions managed effectively?

Comments

# Annex A Controls (Expanded)
# A.2 – Policies related to AI

To provide clear direction and establish the foundation for responsible AI use, your organisation should define a policy that guides the development, deployment and oversight of AI systems. This policy should be reviewed regularly and align with your business goals, risk appetite and legal obligations.

- [ ] A formal AI policy has been documented and approved by top management.
- [ ] The policy includes principles for responsible AI use and continual improvement.
- [ ] The policy is reviewed regularly for suitability and effectiveness.
- [ ] The AI policy aligns with and references other relevant organisational policies.

Comments

# A.3 – Internal organisation



To ensure accountability and clarity across your AI management system, your organisation must define and communicate roles, responsibilities and escalation processes that support responsible AI usage across the life cycle.

- [ ] Roles and responsibilities for AI systems are clearly defined and allocated.
- [ ] There is a process in place to report concerns related to AI use or development.
- [ ] Concerns can be escalated confidentially, with protections against reprisals.
- [ ] The reporting mechanism includes appropriate investigation and resolution steps.

Comments

# A.4 – Resources for AI systems



Understanding the full range of resources used to support your AI systems is essential to manage risk. This includes technical infrastructure, data sets, tooling and human capabilities needed at each stage of the system life cycle.

- [ ] A register of all AI-related resources has been created, including data, tools, systems and people.
- [ ] Tooling and computing resources are documented and matched to system requirements.
- [ ] Competency and capability of human resources involved in AI development and oversight are assessed and recorded.
- [ ] Environmental or operational impacts of infrastructure are considered where applicable.

Comments

# A.5 – Assessing impacts of AI systems



To safeguard individuals and society, your organisation must assess and document the potential impacts of your AI systems. These assessments should be conducted at key points throughout the life cycle and should guide design and risk treatment decisions.

- [ ] Impact assessments are performed to evaluate effects on individuals, groups, or society.
- [ ] The process for conducting impact assessments is documented and repeatable.
- [ ] AI system impact assessments are updated after significant changes or at planned intervals.
- [ ] Findings from assessments inform design, controls and stakeholder communication.

Comments

# A.6 – AI system life cycle



The entire AI system life cycle, from design to decommissioning, must be supported by clearly defined requirements, specifications, validation and monitoring processes. These help ensure ongoing reliability and alignment with intended use.

- [ ] Objectives for responsible development are defined and documented.
- [ ] Verification and validation processes are specified and linked to organisational objectives.
- [ ] Technical documentation is available for users, partners and regulators.
- [ ] Event logs are recorded and maintained, especially during system use.

Comments

# A.7 – Data for AI systems



High-quality, ethically sourced and properly documented data is foundational to safe, effective AI systems. Your organisation should define criteria for selecting, preparing and evaluating data at every stage of the AI life cycle.

- [ ] There is a documented data management process for AI development.
- [ ] Data sources are clearly identified, with provenance and intended use recorded.
- [ ] Data quality requirements are defined and reviewed regularly.
- [ ] Methods for data preparation are documented and justified.

Comments

# A.8 – Information for interested parties



Interested parties – including system users and regulators – must be equipped with the information needed to understand, use and assess the AI systems you manage. This supports transparency, accountability and trust.

- [ ] Users and other interested parties are provided with necessary system documentation.
- [ ] There is a process in place for reporting and escalating AI-related incidents.
- [ ] Incident communication plans are documented and periodically reviewed.
- [ ] Requirements to inform stakeholders are defined and followed.

Comments

# A.9 – Use of AI systems



Your organisation must ensure that AI systems are used in ways that align with your policies, objectives and ethical commitments. This includes clarifying usage boundaries, responsibilities and intended outcomes.

- [ ] There is a defined process for the responsible use of AI systems.
- [ ] Objectives have been set to ensure AI systems are used ethically and appropriately.
- [ ] Usage is in line with intended purpose and documented procedures.
- [ ] Misuse or unintended consequences are monitored and addressed.

Comments

# A.10 – Third-party and customer relationships



When third parties are involved in any stage of the AI system life cycle, clear roles, shared responsibilities and aligned expectations must be established to ensure ongoing accountability and compliance.

- [ ] Responsibilities across the AI life cycle are clearly defined with third parties.
- [ ] There is a process for selecting and managing suppliers involved in AI systems.
- [ ] Customer expectations are captured and considered in system design and operation.
- [ ] Third-party roles are reviewed as part of ongoing system governance.

Comments

# Our ISO 42001 services



### Training

Build your knowledge of ISO 42001 with a range of courses designed for different experience levels – delivered via multiple learning styles.

View available courses

### Gap analysis

An optional service where one of our expert auditors will help you identify any critical, high-risk or weak areas of your system prior to certification.

### Certification

We assess your AIMS in line with the requirements of ISO 42001 – with a particular focus on Annex A controls and how they impact your system.

### Integrated assessments

If you've implemented multiple management systems, you could benefit from an integrated audit and surveillance programme – a more efficient and cost-effective way to manage risk.

# Why work with us?



At LRQA, we help organisations develop robust, future-ready risk management programmes that enable the safe, responsible and effective adoption of AI and technology.

From ensuring compliance with evolving AI regulations to strengthening data security and embedding best practices in governance, we provide the assurance needed to drive innovation with confidence – helping businesses integrate AI and technology while managing risks proactively.

### On the ground expertise

Our solutions are delivered by a global team of experts specialising in cybersecurity, compliance and supply chain risk management, helping you navigate AI-related risks, meet evolving regulatory requirements and integrate responsible AI practices into your operations.

### Continuous assurance

AI-driven risks require continuous oversight. Our approach to real-time risk management enables proactive issue resolution, reducing business disruption and enhancing resilience. Our connected portfolio of risk management solutions helps businesses go beyond regulatory requirements and embed AI risk management into day-to-day operations.

### Solution-based partnerships

We don’t just certify – we work alongside you to integrate AI governance into your wider risk and compliance strategy. Our tailored approach ensures AI and technology help drive sustainable growth while meeting evolving legal and ethical expectations.

### Data-driven decision-making

We leverage digital platforms and analytics to provide deeper insights into AI risks across your business. Our human intelligence, enhanced by data-driven tools, helps organisations identify vulnerabilities, predict future risks and make informed decisions with confidence.

## About LRQA

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

## Get in touch

Visit **lrqa.com** for more information or email **enquiries@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom