Alcumus ISOQAR

# ISO/IEC 42001:2023

## Artificial Intelligence Management Systems Gap Analysis — Controls

isoqar.com

# ISO/IEC 42001:2023 Gap Analysis

## If you're currently implementing an Artificial Intelligence Management System (AIMS) and aiming for ISO/IEC 42001 certification, this Gap Analysis will help you assess your compliance level and pinpoint areas that need further work.

This document is not an exhaustive checklist of everything in ISO/IEC 42001, and marking 'Yes' to all items here does not guarantee certification. However, it serves as an excellent starting point if you're new to ISO/IEC 42001 and can support your internal audits once your system is implemented.

*Please note that this document is for your own internal use only and has no official standing.*

# Implementation guidance for AI controls
# A.2 Policies related to AI

**Objective:** To provide management direction and support for AI systems according to business requirements.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.2.2 | The AI policy should align with the organisation's business strategy, values, risk tolerance, and legal requirements, while considering the broader risk environment and potential impacts on stakeholders.<br><br>It should set guiding principles for all AI activities, include processes for managing deviations, and address specific topics such as AI resources, impact assessments, and development.<br><br>This policy should also reference other relevant policies to ensure cohesive governance over the lifecycle of AI systems. | | | | | | |
| A.2.3 | AI intersects with areas like quality, security, safety, and privacy, so organisations should analyse where current policies overlap with AI needs.<br><br>They should update these policies as necessary or incorporate relevant provisions in the AI policy itself. The AI policy should also reflect guidance set by the governing body, with ISO/IEC 38507 offering support for governing AI systems across their lifecycle. | | | | | | |
| A.2.4 | An appointed, management-approved role should oversee the development, review, and evaluation of the AI policy.The review process should identify improvement opportunities and adapt the policy to changes in the organisational, legal, or technical environment.<br><br>Management review outcomes should also inform the AI policy updates to ensure alignment with organisational goals. | | | | | | |

# A.3 Internal organisation

**Objective:** To establish accountability within the organisation to uphold its responsible approach for the implementation, operation and management of AI systems.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.3.2 | Clearly defining roles and responsibilities across the AI system's lifecycle is essential for organisational accountability.<br><br>Roles should align with AI policies, objectives, and risks, covering key areas like risk management, security, privacy, development, and human oversight.<br><br>Prioritising role assignments ensures all critical functions, from impact assessments to data quality and legal compliance, are managed effectively. | | | | | | |
| A.3.3 | The reporting mechanism should ensure confidentiality or anonymity, be accessible and well-promoted to all employees and contractors, and be managed by qualified staff with investigative authority.<br><br>It must support timely escalation to management, protect against reprisals, and uphold confidentiality standards.<br><br>Additionally, it should provide responses within a reasonable timeframe while adhering to business confidentiality. | | | | | | |

# A.4 Resources for AI Systems

**Objective:** To ensure that the organisation accounts for the resources (including AI system components and assets) of the AI system in order to fully understand and address risks and impacts.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.4.2 | Comprehensive documentation of AI system resources is essential for assessing potential risks and impacts on individuals, groups, and society. This includes detailing components like data, tools, computing systems, and skilled personnel involved throughout the AI lifecycle.<br><br>Resources, which may come from the organisation, customers, or third parties, should be visualised (e.g., with data flow or system architecture diagrams) to inform impact assessments effectively.<br><br>**Other information**<br>Documentation of resources can also help to determine if resources are available and, if they are not available, the organisation should revise the design specification of the AI system or its deployment requirements. | | | | | | |
| A.4.3 | Data documentation should cover its origin, last modification date, data categories (e.g., training, validation), labelling processes, and intended use. It should also include data quality standards, retention and disposal policies, known biases, and preparation steps.<br><br>This thorough documentation ensures data is traceable, reliable, and aligned with AI system requirements. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.4.4 | Tooling resources for AI, especially in machine learning, encompass various components, including algorithms, models, data conditioning tools, optimisation and evaluation methods, and provisioning tools.<br><br>Additionally, they cover essential software and hardware for designing, developing, and deploying AI systems, supporting robust model development and operation. | | | | | | |
| A.4.5 | AI system documentation should detail resource needs, such as processing capabilities, storage, and network requirements, as well as where resources are located (on-premises, cloud, or edge).<br><br>It should also consider hardware impacts, including environmental effects and costs. Different resource requirements may arise at various stages (development, deployment, operation) to support continuous AI improvement. | | | | | | |
| A.4.6 | Organisations should ensure diverse expertise for AI development, covering roles like data scientists, human oversight specialists, and experts in safety, security, and privacy.<br><br>Including specific demographic insights may be essential for training data relevance. Different roles may be required across the AI system lifecycle to ensure a comprehensive and trustworthy approach. | | | | | | |

# A.5 Assessing impacts of AI systems

**Objective:** To assess AI system impacts to individuals or groups of individuals, or both, and societies affected by the AI system throughout its life cycle.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.5.2 | Organisations should assess the potential impacts of AI systems on individuals, groups, and society, focusing on factors like legal status, well-being, human rights, and societal effects.<br><br>This assessment should consider the AI system's purpose, complexity, and data sensitivity. Key steps include identifying risks, analysing consequences, evaluating impact, applying mitigation measures, and documenting findings.<br><br>Impact assessments should inform system design and adapt to changes in system use or technology, with processes tailored to specific fields like privacy, security, and safety.<br><br>In some cases, discipline-specific risk management assessments may need to incorporate AI-related considerations. | | | | | | |
| A.5.3 | Organisations should document AI impact assessments to inform communication with users and stakeholders, updating these records as needed per retention schedules or legal requirements.<br><br>Documentation should cover the system's intended use, potential misuse, positive and negative impacts, anticipated failures and mitigation strategies, relevant demographics, system complexity, human oversight capabilities, and any associated employment or skill requirements. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.5.4 | When assessing AI system impacts, organisations should align with their governance principles and AI policies, considering user expectations around system trustworthiness.<br><br>Special attention should be given to vulnerable groups like children, elderly, and workers. Key impact areas to evaluate include fairness, accountability, transparency, security, privacy, safety, financial implications, accessibility, and human rights, addressing any specific needs or risks for each group.<br><br>**Other information**<br>Where necessary, the organisation should consult experts (e.g. researchers, subject matter experts and users) to obtain a full understanding of potential impacts of the AI system on individuals or groups of individuals, or both, and societies. | | | | | | |
| A.5.5 | AI systems have diverse societal impacts, which can be beneficial (e.g., sustainability, healthcare access) or harmful (e.g., misinformation, societal biases).<br><br>Organisations should consider effects on the environment, economy, governance, health, culture, and societal norms. AI can impact sustainability by either consuming resources or aiding in conservation. AI misuse, such as influencing elections or reinforcing biases in justice, also requires careful oversight.<br><br>Organisations should assess AI's potential for misuse, address historical harms, and ensure systems are aligned with goals for societal benefit. | | | | | | |

# A.6 AI system life cycle
# A.6.1 Management guidance for AI system development

**Objective:** To ensure that the organisation identifies and documents objectives and implements processes for the responsible design and development of AI systems.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.6.1.2 | Organisations should set clear objectives for AI design and development, integrating them into every stage of the process.<br><br>For instance, if "fairness" is a key objective, it should guide requirements, data handling, model training, and validation steps.<br><br>Guidelines and requirements should support these objectives, ensuring tools or methods are used to address issues like bias effectively across the AI lifecycle.<br><br>**Other information**<br>AI techniques can enhance security by predicting, detecting, and preventing threats, protecting both AI and traditional systems.<br><br>Annex C of ISO/IEC 42001 offers examples of risk management objectives, helping organisations set effective goals for secure AI system development. | | | | | | |
| A.6.1.3 | Responsible AI development should address lifecycle stages, testing, and human oversight—particularly where AI impacts individuals.<br><br>Key considerations include setting rules for training data, specifying required expertise, defining release criteria, managing change control, and involving relevant stakeholders.<br><br>These processes should align with the AI system's functionality and chosen technologies, ensuring usability and accountability throughout. | | | | | | |

# A.6.2 AI system life cycle

**Objective:** To define the criteria and requirements for each stage of the AI system life cycle.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.6.2.2 | Organisations should document the purpose and goals behind developing an AI system, including factors like business need, customer demand, or regulatory requirements.<br><br>They should outline how the system will be trained and meet data requirements.<br><br>These requirements should cover the AI lifecycle and be revisited if the system fails to meet objectives or if new information emerges, including financial feasibility concerns. | | | | | | |
| A.6.2.3 | Designing an AI system requires choices in machine learning approach, model type, training methods, and data quality.<br><br>It also involves considerations for hardware, software, security (e.g., preventing data poisoning or model theft), user interaction, and system interoperability.<br><br>Although design and development may undergo multiple iterations, each stage should be documented, with a final system architecture maintained for reference. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.6.2.4 | Verification and validation for AI systems should include testing methods, suitable test data, and clear release criteria.<br><br>Evaluation criteria should address system reliability, safety, impact risks, operational quality, and interpretability of outputs for users. Regular assessments should measure the AI's ability to meet minimum performance levels, with methods to handle potential shortfalls.<br><br>If the AI fails to meet criteria, the organisation should reassess its intended use, adjust performance standards, and mitigate any impacts on individuals or society. | | | | | | |
| A.6.2.5 | AI deployment plans should account for differences between development and deployment environments, like on-premises development versus cloud deployment.<br><br>Organisations should also consider whether components are deployed independently, with clear release criteria covering verification, performance metrics, user testing, and necessary approvals.<br><br>The deployment plan should address the perspectives and potential impacts on relevant stakeholders. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.6.2.6 | AI system operation and monitoring should cover system performance, error handling, updates, security, and compliance with user needs.<br><br>Key aspects include continuous monitoring for errors, data drift, and retraining as necessary, particularly with continuously learning models.<br><br>Systems should be repaired and updated to address functionality changes and user feedback, with defined support procedures in place. AI-specific security risks, such as data poisoning, must be addressed, and performance criteria should align with the AI's intended tasks, with metrics like error rates and processing times set according to expert guidance.<br><br>Regular performance assessments help ensure reliability, using benchmarks like the F1 score or ISO standards to evaluate and improve the system as required. | | | | | | |
| A.6.2.7 | AI system technical documentation should include an overview of the system's purpose, usage instructions, technical requirements, limitations, and monitoring capabilities.<br><br>It should cover all lifecycle stages, with records of design choices, data usage, risk management, validation, and any changes made during operation. Documentation should also detail failure management plans, monitoring processes, operating procedures, and roles responsible for system oversight.<br><br>Updates, operational changes, and internal evaluations should be recorded and shared with users as necessary. Regular updates and management approvals ensure the documentation remains accurate and effective. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.6.2.8 | Organisations should implement automatic event logging for deployed AI systems to track functionality and detect any performance deviations from intended conditions.<br><br>Logs should include details like usage times, data inputs, and outputs outside expected ranges. Event logs must be retained according to organisational data policies and any applicable legal requirements.<br><br>**Other information**<br>Some AI systems, such as biometric identification systems, can have additional logging requirements depending on jurisdiction.<br><br>Organisations should be aware of these requirements. | | | | | | |

# A.7 Data for AI systems

**Objective:** To ensure that the organisation understands the role and impacts of data in AI systems in the application and development, provision or use of AI systems throughout their life cycles.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.7.2 | Data management for AI should address privacy, security risks, and transparency, especially with sensitive data.<br><br>It should ensure data provenance, explainability of outputs, representativeness of training data relative to real-world use, and maintain high standards for data accuracy and integrity. | | | | | | |
| A.7.3 | AI data acquisition should consider the type, quantity, and source of data needed, which can vary based on system scope.<br><br>Important details include data origin (e.g., internal, purchased, or synthetic), data characteristics (e.g., static or streamed), demographics, previous handling, data rights (e.g., privacy compliance), and associated metadata like labelling and provenance. | | | | | | |
| A.7.4 | Data quality is crucial to AI system accuracy, affecting the reliability of outputs. For machine learning, the quality of training, validation, test, and production data should be defined, measured, and improved to meet the system's intended use.<br><br>Organisations should also address biases to enhance system fairness and performance, ensuring data suitability for the AI's application. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.7.5 | Data provenance, as outlined in ISO 8000-2, tracks data creation, updates, validation, and control transfers, including data sharing and transformations.<br><br>Organisations should evaluate if verification measures are needed based on data source, content, and usage context. | | | | | | |
| A.7.6 | Data for AI systems must be prepared to meet specific task requirements, as machine learning models may be sensitive to issues like missing data or inconsistent scales.<br><br>Common preparation steps include data cleaning, imputation, normalization, scaling, labelling, and encoding.<br><br>Organisations should document criteria for selecting these methods to ensure consistency and data quality, minimising errors in the AI system. | | | | | | |

# A.8 Information for interested parties of AI systems

**Objective:** To ensure that relevant interested parties have the necessary information to understand and assess the risks and their impacts (both positive and negative).

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.8.2 | AI system information should include technical details, usage instructions, and notifications that users are interacting with AI, helping users understand the system's purpose, potential impacts, and limitations.<br><br>Key information includes human oversight needs, performance, technical requirements, and updates.<br><br>Information should be accessible and tailored to user needs, with content specific to user roles, from administrators to general users.<br><br>Organisations should document criteria for what information to provide and ensure it's accessible, accurate, and regularly updated. | | | | | | |
| A.8.3 | Organisations should monitor AI system performance and also enable users and external parties to report any adverse impacts, such as issues of unfairness. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.8.4 | Organisations should be prepared to notify users and stakeholders about AI system incidents, including those related to security or privacy, following applicable legal and regulatory requirements.<br><br>This includes identifying which incidents to report, notification timelines, required details, and notifying relevant authorities.<br><br>Incident response for AI can be integrated into broader incident management processes, but unique requirements—like those for privacy breaches in training data—should be addressed specifically. | | | | | | |
| A.8.5 | Organisations may be required to share AI system information with regulators or other authorities, including technical documentation, risk assessments, impact assessment results, and system logs.<br><br>They should understand these obligations and ensure timely, accurate reporting in line with jurisdictional requirements, including any specific needs for law enforcement. | | | | | | |

# A.9 Use of AI systems

**Objective:** To ensure that the organisation uses AI systems responsibly and per organisational policies.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.9.2 | Organisations should establish clear criteria for using an AI system, whether developed internally or by a third party.<br><br>Key considerations include necessary approvals, costs, sourcing standards, and legal compliance. Existing policies for other systems may also be applied to AI systems if relevant. | | | | | | |
| A.9.3 | Organisations should define responsible AI development objectives based on their specific context, such as fairness, accountability, transparency, safety, privacy, and accessibility.<br><br>To meet these goals, they should implement mechanisms to ensure these standards, whether through third-party or internal solutions.<br><br>Human oversight should be integrated at critical stages, with responsibilities for reviewing AI outputs, monitoring performance, and reporting issues.<br><br>Personnel involved in oversight should be trained and well-informed. Annex C offers examples of risk management objectives to guide responsible AI use. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.9.4 | AI systems should be deployed following documented instructions, with necessary resources and human oversight in place.<br><br>Data used by the system must align with its documentation to ensure accuracy, and performance should be continually monitored.<br><br>Concerns about deployment impact or legal compliance should be reported to internal teams or third-party suppliers.<br><br>Event logs and documentation should be maintained to confirm intended use, with retention periods set according to organisational and legal requirements. | | | | | | |

# A.10 Third-party and customer relationships

**Objective:** To ensure that the organisation understands its responsibilities and remains accountable, and risks are appropriately apportioned when third parties are involved at any stage of the AI system life cycle.

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.10.2 | In the AI lifecycle, roles are divided among data providers, model developers, and AI users, with responsibilities clearly documented.<br><br>When supplying AI systems to third parties, organisations should ensure responsible development and provide necessary documentation to all stakeholders.<br><br>For data involving personal information (PII), roles typically split between controllers and processors, with privacy controls aligned with standards like ISO/IEC 29100 and ISO/IEC 27701.<br><br>Organisations may act as PII controllers, processors, or both, depending on their data handling role. | | | | | | |

| Control | Plain English Description | Yes | No | Gap Identified/Corrective Action Required | Owner | Target Date | Date Completed |
|---|---|---|---|---|---|---|---|
| A.10.3 | Organisations using AI systems rely on various suppliers for datasets, algorithms, models, software libraries, or complete AI systems.<br><br>They should assess suppliers based on the risks their components may pose, set clear requirements, and monitor their performance.<br><br>Documentation on how suppliers' components integrate with the organisation's AI should be maintained.<br><br>If a supplier's component fails to meet performance or ethical standards, corrective action should be required, potentially with collaborative efforts to resolve issues. Suppliers should provide complete and appropriate documentation for their AI contributions. | | | | | | |
| A.10.4 | When providing AI products or services, organisations should understand and address customer expectations, whether they are design requirements, contractual obligations, or usage agreements.<br><br>Different customer relationships may have unique needs and responsibilities.<br><br>Organisations must clarify where responsibility lies between the AI provider and the customer, especially concerning usage risks.<br><br>They should also inform customers about limitations, such as domain-specific applicability, so customers can manage associated risks effectively. | | | | | | |

## About Alcumus ISOQAR

We help organisations create better workplaces through a huge range of common and sector-specific standards and compliance assessments, allowing them to demonstrate to their customers, competitors, suppliers and staff, that they are committed to being the best that they can by minimising risk, delivering change, driving improvement and winning more work.

As one of the UK's largest UKAS accredited certification bodies we can audit, certify and train organisations across multiple sectors.

We work worldwide, so we can help businesses gain a competitive edge anywhere they need us.

## About Alcumus

Alcumus is a leading provider of software-led risk management solutions providing clients with advice, expertise and support to help them identify and mitigate risks, navigate compliance and keep people safe. It supports both UK and International clients – many of whom are on the FTSE 100 index - with a wide range of risk management services. This includes products across Supply Chain Management, EHSQ Software, UKAS Accredited Certification and HR and H&S support services.

Our people are at the heart of our business, building strong relationships with our clients to understand their needs, minimise risks and navigate compliance through our in-depth knowledge of your sector, regulations and challenges.

**E: info@alcumus.com**
**T: 0333 920 8824**
**W: isoqar.com**

Alcumus®
Safer, Healthier, Stronger