Alcumus ISOQAR

ISO/IEC 42001:2023

Artificial Intelligence Management Systems Gap Analysis — Clauses

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.

Clause 4 – Context of the Organisation

This clause requires that you determine the relevant external and internal conditions that may affect your organisation's existence and strategy. The 'context' relates to the business environment in which you operate.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
4.1	Identified the external and internal issues that affect the organisation and the AIMS. To understand the organization and its context, it can be helpful for the organization to determine its role relative to the AI system. External and internal issues to be addressed under this clause can vary according to the organization's roles and jurisdiction and their impact on its ability to achieve the intended outcome(s) of its AI management system. *Possibly written down e.g. as a SWOT analysis. If not, must be able to explain your awareness to the Auditor. Don't forget to include 'legal requirements'. You might think this is simple but many companies find it's a very useful exercise to write this down.*						
4.2	Clear understanding of needs and expectations of interested parties, including customers, and other stakeholders. *'Other stakeholders' could include regulators, staff, suppliers, visitors. Remember to include legal and regulatory requirements of your customers. Relevant interested parties can have requirements related to climate change.*						

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
4.3	Scope of the AIMS is clearly determined. The scope of the AI management system shall determine the organization's activities with respect to this document's requirements on the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives. The scope of your AIMS must be written down. It should describe the type of products and services you offer and justify if any requirement of the standard is not applicable to you. Remember, an ISO/IEC 42001 system does NOT have to cover the whole organisation; you can ringfence areas. Take advice from ISOQAR.						
4.4	The AIMS is built and maintained in its entirety. You need to demonstrate an understanding of how you maintain and continually improve your system. (See also 9 and 10). *In the past, ISO was seen as an exercise in writing massive documents. That's not the case now but some documentation and organisation is required.*						

Clause 5 - Leadership and Commitment

Top management cannot delegate overall responsibility for the AIMS. They have to take ultimate responsibility and show real leadership, taking a proactive, hands-on role.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
5.1	Top management able to provide evidence that they take accountability for the AIMS. *Able to answer questions, perhaps show minutes of meetings, have awareness of any improvement actions required. Without top management leadership no initiatives will succeed. Support must be there and the Auditor will expect to have time to interview and discuss the system with them.*						
	AI Policy and objectives are aligned with the organisation's overall strategy and integrated into processes. *The policy is also your statement of intent.*						
	Evidence that top management actively promote the AIMS amongst staff. *Auditors might ask random staff for their comments.*						
	Resources (staff, time, budget etc.) are made available where necessary to support the functioning of the AIMS.						
	Ensuring that the AIMS supports continual improvement. *Evidence from Internal Audits, Management Reviews etc. will help support this.*						
	Supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.						

Clause 5 - Leadership and Commitment

Top management cannot delegate overall responsibility for the AIMS. They have to take ultimate responsibility and show real leadership, taking a proactive, hands-on role.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
5.2	The AI Policy, which contains a framework for setting your objectives, should be relevant to your organisation and what you're trying to achieve. Must contain commitment to continual improvement. Should be documented. *Also align it to any legislative requirements.*						
	The AI Policy is available to all interested parties and communicated to them. *Should be visible to staff on noticeboard/ intranet, for example, and people should be familiar with it.*						
5.3	Responsibilities and levels of authority for individuals relating to the AIMS must be understood. *A good way to check this is by random questioning of staff.*						
	Individual(s) with responsibility for ensuring the AIMS conforms to ISO/IEC 42001 are identified. *The identified individuals must understand their responsibilities. Formal ISO training such as 'Internal Auditing' is recommended. Auditors may question individuals to assess capability.*						
	Individual(s) with responsibility for reporting on the performance of the AIMS have been identified. *Possibly the same people as above. Internal Audit reports can satisfy this. See also 9.*						

Clause 6 – Planning

Risk-based thinking is one of the cornerstones of ISO/IEC 42001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.1	With reference to 4.1 and 4.2, be sure that the AIMS can reduce / prevent undesirable effects and support continual improvement. Make sure you have actions identified to address these risks and opportunities and integrate them into your system. *This is one of the main purposes of an AIMS, supporting the aim of continual improvement.*						
	Systems to evaluate the effectiveness of actions you take. *This is connected to clause 9.*						
6.1.2	Develop an AI Risk Assessment that identifies criteria for risk acceptance and for performing the assessments. *This is one of the key parts of the standard. If you're unsure how to perform this, perhaps consider a consultant.*						
	Can repeat the AI Risk Assessment and get consistent, valid, comparable results.						
	Risks analysed to determine: consequences of risk; likelihood of occurrence; the level of risk.						
	Evaluate the risks, comparing results of analysis with the criteria established and prioritise risks for treatment.						

Clause 6 – Planning

Risk-based thinking is one of the cornerstones of ISO/IEC 42001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.1.3	Develop an AI Risk Treatment process based on results of 6.1.2. This should identify AI controls necessary. Also refer to Annex A of ISO/IEC 42001 to ensure nothing is missed. *You'll need a copy of the ISO/IEC 42001 standard for this.*						
	Publish a Statement of Applicability (SoA) that identifies controls and explains, where applicable, why controls have been omitted. *This can be quite a big piece of work despite being such a short sub-clause! The SoA summarises your position on each of the AI controls in Annex A. In essence, it outlines why you are tackling some risks and accepting other risks.*						
	Develop an AI Risk Treatment Plan. *Again, this can be quite a big piece of work despite this being such a short sub-clause! It summarises each of the identified risks and how you intend to manage them (e.g. avoid risk by ceasing an activity; modify it by changing processes; share the risk such as outsourcing; accept the risk because costs outweigh benefits). Include target dates.*						
	Obtained approval of the plan and any risks from the 'risk owners'. *A 'risk owner' is someone with the authority to resolve the problem.*						

Clause 6 – Planning

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.1.4	**AI system impact assessment** The organization shall define a process for assessing the potential consequences for individuals or groups of individuals, or both, and societies that can result from the development, provision or use of AI systems.						
	The AI system impact assessment shall determine the potential consequences an AI system's deployment, intended use and foreseeable misuse has on individuals or groups of individuals, or both, and societies.						
	The AI system impact assessment shall take into account the specific technical and societal context where the AI system is deployed and applicable jurisdictions.						
	The result of the AI system impact assessment shall be documented. Where appropriate, the result of the system impact assessment can be made available to relevant interested parties as defined by the organization.						
	The organization shall consider the results of the AI system impact assessment in the risk assessment.						
	In some contexts (such as safety or privacy critical AI systems), the organization can require that discipline-specific AI system impact assessments (e.g. safety, privacy or security impact) be performed as part of the overall risk management activities of an organization.						

Clause 6 – Planning

Risk-based thinking is one of the cornerstones of ISO/IEC 42001. This is all about ensuring that the expected results are achieved, and no unwanted incidents occur.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
6.2	Have in place AI objectives relating to relevant functions/ processes that support and continually improve the AIMS which are measurable, monitored, communicated and updated when needed. Should be available as documented information. *In determining the objectives and how to achieve them, consider what resources are needed, responsibilities, target dates and how results will be evaluated.*						
6.3	When changes are identified, are these implemented in a planned manner? *Don't rush into making haphazard changes without proper controls and checks.*						

Clause 7 – Support

The organisation is required to establish and maintain the necessary infrastructure to ensure smooth operation and continual improvement of the AI Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
7.1	Determined and provided the resources (people, budget, infrastructure, tools, IT etc.) to support the ongoing running of the AIMS. *You should be able to explain to the Auditor how you did this.*						
7.2	Individuals are competent and records are kept as evidence. *Relates to skills and experience of individuals. Consider training plans, certificates etc. Keep records.*						
7.3	Individuals are aware of the AIMS, their roles, the benefits of improved AI and the implications of nonconformance. *Individuals should be able to answer questions put by the Auditor.*						
7.4	The organisation must determine what to communicate with regard to the AIMS (internal and external) e.g. what, to whom, how, when. *It may be as simple as a statement on your website but possibly much more detailed.*						

Clause 7 – Support

The organisation is required to establish and maintain the necessary infrastructure to ensure smooth operation and continual improvement of the AI Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
7.5	The level of documented information required for effective running of the AIMS has been considered and created. *Can be electronic. Only needs to be proportionate to size and complexity of your organisation, activities and competence of individuals.*						
	Systems of control (e.g. title, date, author, reference number) and for updating documented information are in place. Must also be adequately protected (especially where confidential), accessible and retained. *Don't forget to include relevant documentation from external sources.*						

Clause 8 – Operation

This is the 'Do' part of the Plan-Do-Check-Act (PDCA) cycle and is the day-to-day part of what your organisation does. This clause is at the very heart of the of the AI Management System.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
8.1	Maintain processes to run the AIMS and implement actions identified in 6.1 and 6.2. *Need to have control of processes and be able to demonstrate this.*						
	Documentation retained as required to demonstrate processes carried out as planned. *So you can provide evidence to the Auditor.*						
	Process for controlling planned changes and to mitigate adverse effects. *Remember this includes outsourced activities.*						
8.2	AI Risk Assessment (6.1.2) performed at planned intervals or when significant changes are proposed. *Keep evidence to show to the Auditor.*						
8.3	Implement the AI Risk Treatment Plan. *This clause is simply telling you that the plan you developed at 6.1.3 must actually be activated! Keep evidence.*						
8.4	AI system impact assessment. The organization shall perform AI system impact assessments according to 6.1.4 at planned intervals or when significant changes are proposed to occur. The organization shall retain documented information of the results of all AI system impact assessments.						

Clause 9 – Performance Evaluation

The organisation is required to determine what needs to be monitored, how to monitor and when to do it.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
9.1	Determined what needs to be monitored and measured, and when.						
	Established methods for monitoring, measuring, analysing, evaluating and when this should be done. *The above is used to evaluate conformity and effectiveness of processes and identify need for improvements in the AIMS. Make sure you identify who will do the monitoring and when analysis and evaluation will be done.*						
9.2	Established and implemented a planned approach to internal audits mindful of the frequency, methods, responsibilities, scope.						
	Results of internal audits are reported to management, appropriate corrective action taken. *You may wish to attend an Internal Auditor training course to learn how to do this.*						

Clause 9 – Performance Evaluation

The organisation is required to determine what needs to be monitored, how to monitor and when to do it.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
9.3	Management review meetings are taking place as planned and documented evidence is available.						
	There is an appropriate agenda for the management review meetings to cover all requirements as stated in 9.3 of the standard.						
	There is documented evidence of the outputs of the reviews, identifying opportunities for improvement, any required changes to the AIMS and how to resource any changes required. *Don’t forget to review the needs and expectations of interested parties.*						

Clause 10 – Performance Evaluation

Underpinning the concept of an AIMS are the principles of corrective action and continual improvement.
The organisation must identify opportunities for improvement as well as introduce necessary actions.

Clause	Plain English Description	Yes	No	Gap Identified/Corrective Action Required	Owner	Target Date	Date Completed
10.1	Overall, an approach to continually improve the suitability and effectiveness of the AIMS. *Much of this will be covered in clause 9.*						
10.2	Evidence that you react to, control and correct nonconformities and deal with the consequences. *You should have a procedure for this.*						
	Have a system for, and be able to provide examples of, reviewing and analysing nonconformities and implementing improvements to the AIMS. *To ensure mistakes and errors are not repeated. This is the essence of continual improvement.*						
	Review the effectiveness of any changes made to the AIMS as a consequence of the above.						

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