



Comprehensive Guide to ISO 42001

Table of Contents

1. The basics of ISO 42001	3
2. What is AI governance?	7
3. ISO 42001 requirements: Clauses and structure	11
4. List of ISO 42001 mandatory documents.....	16
5. ISO 42001 checklist of implementation steps.....	20
6. Organizing ISO 42001 training and awareness.....	26
7. ISO 42001 certification	30
8. ISO 42001 vs. ISO 27001: Similarities and differences	34
9. Thirteen key AI concepts important for AI governance	38

1. The basics of ISO 42001

1.1. Essential facts

The full name of this standard is “ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system,” but for reasons of simplicity it is often called “ISO/IEC 42001” or simply “ISO 42001.”

The number “2023” in its name indicates the year when it was published — actually, it was published in December 2023, a year after the AI hype started with the launch of ChatGPT in November 2022.

ISO 42001 was published by ISO, which stands for International Standardization Organization — this is an international organization founded by governments around the world, and each standard needs to be approved by representatives from many countries. In effect, each standard that is published by ISO is accepted by each country in the world.

1.2. Which companies can implement ISO 42001?

ISO 42001 is written in such a way that any type of organization, for profit or non-profit, large or small, from any industry, can comply with ISO 42001 requirements.

Basically, ISO 42001 is intended for companies that create or use AI systems — since AI is becoming more and more dominant in the business world, it is expected that this standard will become one of the most widely implemented standards, like ISO 9001, ISO 14001, or ISO 27001.

1.3. Is ISO 42001 mandatory?

For now, ISO 42001 is not mandatory because no country has yet prescribed that companies must implement this standard.

However, more and more countries are publishing their AI regulations, like the EU AI Act — some of those upcoming regulations might require ISO 42001 implementation.

In any case, companies that do implement ISO 42001 will find compliance with AI regulations much easier.

Learn more here: [What is the EU AI Act?](#)

1.4. Why is ISO 42001 important?

AI is a new technology that brings huge benefits, but also significant risks — which is the reason many companies are skeptical about its use. This is why ISO 42001 is important — it describes how to manage AI systems in a systematic way, in order to decrease those risks.

For example, a company that uses an AI chatbot for customer support might have several risks: providing incorrect or misleading information, leakage of personal data during conversations, or system downtime. To counter those problems, the company might use the following controls: a response validation control where AI answers are checked against a proprietary knowledge base before sending to users, cybersecurity and privacy controls to prevent leakage of personal data, and a fallback mechanism in which a human agent takes over if needed.

ISO 42001 describes how to assess those risks, and how to introduce the right AI controls — in other words, it describes how to use AI governance to build trustworthy AI systems.

1.5. Relationship between AI governance and ISO 42001

The word “governance” means a framework with a set of processes, structures, rules, and roles, and ISO 42001 is a framework that contains exactly this — it also defines how all of those things need to be done in the context of AI systems.

Since ISO 42001 is a leading international standard for managing AI, it has the potential to become the leading worldwide framework for AI governance — like the way ISO 27001 became the leading framework for cybersecurity governance.

1.6. Artificial Intelligence Management System (AIMS)

Actually, ISO 42001 does not use the phrase “AI governance,” but another phrase for the systematic governance of AI systems: Artificial Intelligence Management System, or AIMS.

Why is this so? Because ISO 42001 and other similar standards describe management systems — e.g., ISO 27001 describes Information Security Management Systems (ISMS), and ISO 9001 defines Quality Management Systems (QMS).

In any case, AIMS and AI governance basically have the same meaning.

But why is such systematic governance of AI systems needed in the first place? This is because a company might have not only, e.g., an AI chatbot for customer support, but it might also use AI systems internally for marketing materials, translation, the hiring process, training, and many other processes. And on top of this, a company might develop AI systems like large language models that could have a big impact on its customers or societies in general.

And without a systematic approach to managing all those AI systems, it would be very easy to miss some of the major risks — this is why a system that defines, e.g., how to perform the risk assessment, what kind of controls need to be used, how to control the whole system, etc., is crucial. And ISO 42001 provides the know-how for exactly such an AI Management System.



1.7. How does ISO 42001 work?

As mentioned earlier, the key concept in ISO 42001 is to assess the risks related to AI systems (i.e., to think through what could go wrong), and then define AI controls with which to decrease those risks (i.e., use various methods to prevent those problems).

ISO 42001 defines several requirements on how this risk assessment needs to be performed — for example, it specifies that companies must assess AI risks for the company, but also for individual users, and for societies, and that they need to assess how big the consequences could be, and also how likely it is that those problems could happen.

It also provides a list of 38 AI controls in its Annex A, which can be used to decrease those risks.

1.8. Supporting standards for ISO 42001

There are several other standards that can help you learn more about AI governance. Here are some of the most useful.

ISO 22989 explains artificial intelligence concepts and terminology, and is very useful for beginners in AI governance because it explains the basics.

ISO 23894 is guidance on AI risk management, and it is useful for professionals who want to learn more on how to assess and treat AI risks.

ISO 42005 is guidance on the AI system impact assessment, and it is useful for professionals who want to learn the details on how this assessment needs to be performed.

There are also numerous other standards that go into more depth for particular areas of AI — for example, ISO 24028 speaks about trustworthiness in AI.

Also worth mentioning is the AI Risk Management Framework developed by the U.S. National Institute of Standards and Technology (NIST) — it provides voluntary guidance for trustworthy AI, emphasizing risk-based approaches and stakeholder trust.

1.9. EU AI Act vs. ISO 42001

Even though the EU AI Act does not mention ISO 42001, this standard is recommended as an implementation method for the Act, since it provides an internationally accepted framework on how to systematically assess risks and control AI systems. Essentially, ISO 42001 is as important for the EU AI Act as ISO 27001 is for NIS2 or DORA.

	EU AI Act	ISO 42001
Type	Regulation published by the European Union	Industry standard published by the International Organization for Standardization
Focus	Requirements for high-risk AI systems, general-purpose AI models, and transparency rules	Framework that defines AI governance
Applies to	Companies that use, develop, or sell AI systems in the European Union	Any company that uses or develops AI systems
Mandatory	Yes	No
Companies can certify	No	Yes

2. What is AI governance?

AI technology is developing very quickly; however, its adoption in companies is still rather slow. One of the reasons seems to be lack of trust in AI systems because of hallucinations, privacy, and other issues — and, very often, AI governance is mentioned as a solution to those problems.

But what exactly is AI governance?

2.1. The basics of AI governance

AI governance basically means that a company sets clear rules on how AI systems are developed and used throughout the life cycle of those AI systems.

These rules are typically defined through various technical controls (e.g., guardrails), data management (e.g., ensuring quality of training data), documentation (e.g., policies and procedures, roles and responsibilities), etc.

But how do you know what these rules need to define? How should controls be configured? And how should you handle training data?

2.2. How AI governance works

The core concept of AI governance is that you have to assess the potential risks that could happen when AI systems are used, and then, based on those risks, define what kinds of controls you need to implement to decrease those risks.

There are numerous risks — here are some examples:

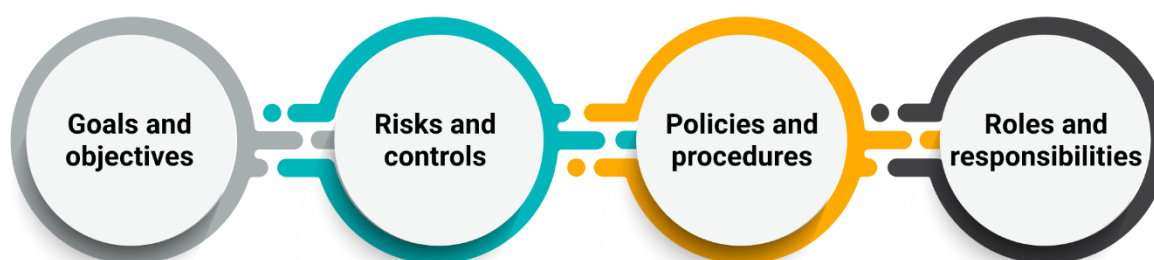
- Bias – This is when an AI system systematically treats certain individuals or groups of people differently from others. An example could be an AI system for hiring new employees that prefers men over women.
- Data leakage – For example, this could happen if an AI system uses the data a user has entered for training its large language model, and then this same data could be displayed as a response to some other user.
- Hallucinations – This is a response generated by AI that contains false or misleading information, which is presented as fact.

And here are some examples of controls that could be applied to decrease those risks:

- Bias – For example, you might check the quality of training data, or you might have human oversight over the output.

- Data leakage – E.g., using an in-house small language model rather than an external large language model; if using external large language models, then you might anonymize the data sent to the LLM, or delete parts of the data that are the most sensitive.
- Hallucination – E.g., use input data checks, but also output validity checks.

AI Governance



2.3. Typical goals and objectives for AI governance

Ultimately, the goals of implementing all of those controls as part of AI governance should be safe, responsible, and ethical AI systems. Or if you want to simplify this, then you can say that the goal should be trustworthiness, which ultimately summarizes all of those previously mentioned goals.

Of course, besides trustworthiness, many companies also want to achieve compliance with AI laws and regulations, and even market visibility if they can prove to their customers that they implemented appropriate AI governance.

Besides these general goals, there are many other objectives that are important for AI governance — here are some examples:

- Accountability
- Environmental impact
- Fairness
- Maintainability
- Privacy and security
- Robustness

- Safety
- Transparency and explainability
- Human oversight
- etc.

2.4. Typical policies and procedures

To be able to handle all of those controls, companies will need to write various internal documents — otherwise, it would be impossible to make sure all of these controls really work.

For example, you might have the following documents as part of your AI governance:

- Top-level AI policy — defines the strategic direction of the company for AI, and general roles and responsibilities
- AI risk management methodology — defines how the risks are assessed and treated
- AI data management policy — defines how the training data is sourced, checked, and prepared for AI systems
- AI design and development policy — describes how AI systems are specified, developed, and tested
- AI operating procedures — defines how the AI systems are handled when in production
- AI acceptable use policy — prescribes for end users which activities are allowed, and which are not
- Etc.

2.5. Typical roles and responsibilities

For AI governance to work, you'll need to include different roles and, ultimately, all of your employees. Below are some typical roles with regard to AI governance.

Senior management needs to set the overall direction for AI in general, and for AI governance — how they need to support the company strategy, which strategic objectives need to be achieved, etc. They also need to provide the resources needed for AI governance.

An **AI officer**, or someone else who is in charge of AI governance (e.g., CIO, CTO, or similar), must coordinate activities related to the management of AI systems, report to senior management, etc.

Middle management should participate in the creation of AI policies and procedures, especially if they are involved in privacy, cybersecurity, legal, data, or similar areas; they also need to make sure that all of those rules are implemented in practice and complied with on a day-to-day basis.

All employees need to comply with whatever AI rules the company has defined.



2.6. Where to start?

All of these risks, controls, documents, roles, and responsibilities sound like a lot, especially if you have several AI systems to work with.

This is why you should use a framework for handling AI governance — and one such framework is [ISO 42001](#), an international standard that defines how to manage AI Management Systems — in other words, how to manage AI governance.

ISO 42001 defines how to perform risk assessment, which documents to write, what the roles and responsibilities will be, etc.; it also provides a list of 38 controls that you can implement. In other words, it clarifies how the whole AI governance needs to be implemented.

3. ISO 42001 requirements: Clauses and structure

You're probably wondering what exactly the text of the ISO 42001 standard says — actually, the standard is written in language that is hard to read, so here you'll find the most important points from each ISO 42001 clause summarized in an easy-to-understand way.

ISO 42001 is aligned with the high-level structure (HLS) set by the International Organization for Standardization (ISO), which means that it has the same structure and roughly the same clause names as other standards, including ISO 27001, ISO 9001, ISO 14001, and ISO 22301.

Below you'll see all clauses from ISO 42001.

3.1. Clauses 1 to 3

These clauses are not mandatory, and are not so important when companies want to comply with ISO 42001:

- Clause 1 Scope — Defines what this standard is focused on and that all kinds of companies can implement it.
- Clause 2 Normative references — Refers to ISO 22989 as a source for describing AI terms and concepts.
- Clause 3 Terms and definitions — Describes some key terms like interested parties, risk, process, etc.

The remaining clauses listed in this article are mandatory.

3.2. Clause 4 Context of the organization

Clause 4, called "Context of the organization," requires analyzing internal and external factors or issues, identifying stakeholder expectations, and defining the scope of the AIMS.

It has four sub-clauses:

- 4.1 Understanding the organization and its context — The organization must understand its internal and external context, including its role in developing or using AI systems, legal and ethical factors, and even climate change, to ensure its AI Management System can achieve its objectives.
- 4.2 Understanding the needs and expectations of interested parties — The organization must identify all stakeholders relevant to its AI Management System, understand their needs, and decide which ones it will address through the AIMS.
- 4.3 Determining the scope of the AI management system — The organization must define and document what parts of its activities the AI Management System covers, based on internal and external factors and relevant requirements.

- 4.4 AI management system — The organization must create, run, improve, and document an AI Management System that meets ISO 42001 requirements and clearly defines how all its processes work together.

3.3. Clause 5 Leadership

Clause 5, called “Leadership,” specifies what the senior management must do, as well as how to define roles and responsibilities and how to create the AI Policy that will provide direction for the AI efforts.

It has three sub-clauses:

- 5.1 Leadership and commitment — Senior management must actively lead the AI Management System by aligning it with the organization’s strategy, providing resources, promoting good AI practices, and driving continual improvement.
- 5.2 AI policy — Senior management must approve an AI Policy that fits the organization’s purpose, guides AI objectives, ensures compliance, promotes continual improvement, and is clearly communicated.
- 5.3 Roles, responsibilities and authorities — Senior management must clearly assign and communicate who is responsible for managing the AI Management System and for reporting its performance.



3.4. Clause 6 Planning

Clause 6, called “Planning,” focuses on managing risks, defining AI objectives, and managing change because of AI.

Sub-clause 6.1, called “Actions to address risks and opportunities,” is quite lengthy, and it has another four subclauses:

- 6.1.1 General — The organization must identify and manage AI-related risks and opportunities to ensure its AI Management System works effectively, prevents problems, improves over time, and keeps records of all actions taken.
- 6.1.2 AI risk assessment — The organization must have a clear and consistent process for assessing AI risks and to keep records of the results: identifying what could go wrong, how serious it could be, how likely it is to happen, and which risks need action.
- 6.1.3 AI risk treatment — The organization must create and document a clear plan for handling AI risks, which includes choosing suitable controls, checking them against a list of controls from Annex A, adding any missing ones, and getting management approval for how significant risks will be managed.
- 6.1.4 AI system impact assessment — The organization must assess and document how its AI system could affect people and society, considering its use or misuse, and use those insights to improve its AI risk management.

Here are the remaining sub-clauses of clause 6:

- 6.2 AI objectives and planning to achieve them — The organization must set clear, measurable AI objectives that align with its AI Policy, plan how to achieve them, assign responsibilities, track progress, and keep records of the results.
- 6.3 Planning of changes — The organization must make any changes to its AI Management System carefully and in a planned way.

3.5. Clause 7 Support

Clause 7, called “Support,” covers resources, competence, training, awareness, communication, and management of documents and records.

It has five sub-clauses:

- 7.1 Resources — The organization must ensure it has all the necessary people, tools, and resources to set up, run, maintain, and continually improve its AI Management System.
- 7.2 Competence — The organization must ensure that everyone involved in its AI work has the right knowledge, skills, and experience — and keep records proving their competence.
- 7.3 Awareness — Everyone involved in the organization’s AI activities must understand the AI Policy, know how their work supports the system’s success, and be aware of the consequences of not following its rules.
- 7.4 Communication — The organization must define what, when, how, and with whom it will communicate about its AI Management System.
- 7.5 Documented information — The organization must create, manage, and protect all documents and records needed for its AI Management System, making sure they’re accurate, up to date, properly approved, and accessible when needed.



3.6. Clause 8 Operation

Clause 8, called “Operation,” specifies requirements for operational planning and control over the AI system lifecycle.

It has four sub-clauses:

- 8.1 Operational planning and control — The organization must plan and control all processes needed to run its AI Management System, apply and monitor AI-related controls, fix problems when results fall short, manage any changes carefully, and control any externally provided processes.
- 8.2 AI risk assessment — The organization must regularly assess risks related to its AI systems, particularly in cases of major changes, and keep records of those assessments.
- 8.3 AI risk treatment — The organization must carry out and regularly check its AI Risk Treatment Plan, update it if new or unresolved risks appear, and keep records of all actions taken.
- 8.4 AI system impact assessment — The organization must regularly assess how its AI system impacts people and the organization (especially after major changes) and keep records of those assessments.

3.7. Clause 9 Performance evaluation

Clause 9, called “Performance evaluation,” sets requirements for monitoring, measuring, analyzing, and evaluating AI systems’ performance, conducting internal audits, and performing management reviews.

It has three sub-clauses:

- 9.1 Monitoring, measurement, analysis and evaluation — The organization must regularly measure and analyze how well its AI Management System performs, using reliable methods and keeping records of the results.
- 9.2 Internal audit — The organization must regularly perform internal audits to check if its AI Management System follows the rules, works effectively, and is properly maintained, while keeping clear records of how audits are planned, done, and reported.
- 9.3 Management review — Senior management must regularly review how well the AI Management System is working, consider any changes or problems, decide on improvements, and keep records of these reviews.

3.8. Clause 10 Improvement

Clause 10, called “Improvement,” covers corrective action and continual improvement of the AIMS.

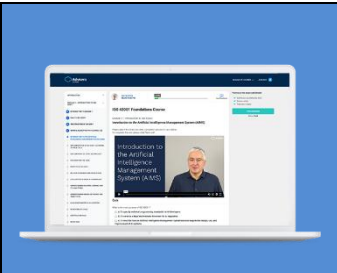
It has two sub-clauses:

- 10.1 Continual improvement — The organization must keep making its AI Management System better over time so it stays effective and fit for its purpose.
- 10.2 Nonconformity and corrective action — When something goes wrong in the AI Management System, the organization must fix the problem, find out why it happened, make sure it won’t happen again, check that the fix works, and keep records of everything done.

3.9. Annexes A to D

There are four annexes in this standard:

- Annex A Reference control objectives and controls — Lists 38 controls organized into nine sections that describe how to reduce AI risks.
- Annex B Implementation guidance for AI controls — Provides detailed guidance for each control from Annex A.
- Annex C Potential AI-related organizational objectives and risk sources — Provides a list of suggested AI objectives (that could be useful for setting the company’s objectives) and risk sources (that could be useful when identifying risks).
- Annex D Use of the AI management system across domains or sectors — Describes how the AIMS can be used across different industries and how it can be integrated with other ISO management standards.



ISO 42001 Online Courses

Free online courses to learn how to comply with ISO 42001

[Enroll for free](#)

4. List of ISO 42001 mandatory documents

Unfortunately, ISO 42001 requires more documentation when compared to some other standards like ISO 27001 or ISO 9001. So if you don't know where to start, here you will see a breakdown of documents and records mapped with particular clauses and controls of the standard.

The criteria for the list below on what must be documented was when a standard uses phrases like “shall retain documented information,” “shall be available as documented information,” or “shall be documented.”

4.1. ISO 42001 mandatory documents and records for the main clauses of the standard

In the table below, you'll find an analysis of which clauses from the main part of ISO 42001 (i.e., from clauses 4 to 10) must be documented.

What must be documented	ISO 42001 clause	Usually documented through
Scope of the AIMS	Clause 4.3	AIMS Scope Document
AI policy	Clause 5.2	AI Policy
Actions taken to identify and address AI risks and opportunities	Clause 6.1.1	AI Risk Register; AI Risk Assessment & Treatment Report
AI risk assessment process	Clause 6.1.2	AI Risk Management Methodology
AI risk treatment process	Clause 6.1.3	AI Risk Management Methodology
Statement of applicability	Clause 6.1.3	Statement of Applicability
AI risk treatment plan	Clause 6.1.3	AI Risk Treatment Plan
Results of the AI system impact assessment	Clause 6.1.4	AI System Impact Assessment Report
AI objectives	Clause 6.2	AIMS Objectives
Evidence of competence	Clause 7.2	CVs, training certificates, etc.
Results of the AI risk assessment	Clause 8.2	AI Risk Register; AI Risk Assessment & Treatment Report
Results of the AI risk treatment	Clause 8.3	AI Risk Register; AI Risk Assessment & Treatment Report
Results of the AI system impact assessment	Clause 8.4	AI System Impact Assessment Report
Results of monitoring and measurement	Clause 9.1	Various automatic reports and dashboards created by AI systems; Monitoring & Measurement Report
Internal audit program	Clause 9.2	Internal Audit Program
Internal audit results	Clause 9.2	Internal Audit Report

Results of management reviews	Clause 9.3	Management Review Minutes
Evidence of nonconformities, actions taken, and results of corrective action	Clause 10.2	Corrective Action Form

4.2. List of mandatory documents and records for ISO 42001 Annex A

Unlike other standards, such as ISO 27001, ISO 42001 requires all controls to be documented. Therefore, the table below lists all 38 controls, with suggested ways to document them. The idea here was to reduce the number of documents by covering several controls with a particular document.

Note: If a company excludes a particular control by marking it as not applicable in the Statement of Applicability, then the document does not need to be written for that control.

What must be documented	ISO 42001 control	Usually documented through
Policy for the design and development of AI systems	Control A.2.2	AI Systems Design and Development Policy
Policy for the use of AI systems	Control A.2.2	AI Systems Acceptable Use Policy
Other policies affected by AI systems	Control A.2.3	AI Policy
Review AI policy at planned intervals	Control A.2.4	AI Policy
Define roles and responsibilities	Control A.3.2	AI Policy
Process to report concerns about AI systems	Control A.3.3	AI Policy
Required resources	Control A.4.2	AI Policy; Register of AI Resources
Utilized data resources	Control A.4.3	Register of AI Resources
Utilized tooling resources	Control A.4.4	Register of AI Resources
Utilized computing resources	Control A.4.5	Register of AI Resources
Utilized human resources	Control A.4.6	Register of AI Resources
Establish a process for AI system impact assessment	Control A.5.2	AI System Impact Assessment Methodology
Document the results of AI system impact assessments	Control A.5.3	AI System Impact Assessment Report
Potential impacts of AI systems on individuals	Control A.5.4	AI System Impact Assessment Report
Potential societal impacts of AI systems	Control A.5.5	AI System Impact Assessment Report

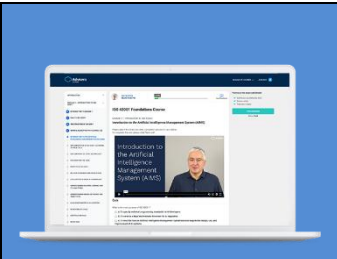
Objectives for responsible development of AI systems	Control A.6.1.2	AI Systems Design and Development Policy
Processes for the design and development of AI systems	Control A.6.1.3	AI Systems Design and Development Policy
Requirements for AI systems	Control A.6.2.2	AI Systems Design and Development Policy; Functional Requirements for AI System
AI system design and development	Control A.6.2.3	AI Systems Design and Development Policy
AI system verification and validation measures	Control A.6.2.4	AI Systems Design and Development Policy
AI system deployment plan	Control A.6.2.5	AI Systems Operating Procedures
Necessary elements for the ongoing operation of the AI system	Control A.6.2.6	AI Systems Operating Procedures
AI system technical documentation	Control A.6.2.7	AI Systems Operating Procedures
AI system event logs	Control A.6.2.8	AI Systems Operating Procedures; various logs from AI systems
Data management processes for the development of AI systems	Control A.7.2	AI Systems Data Management Policy
Details about the acquisition and selection of the data	Control A.7.3	AI Systems Data Management Policy; Register of AI Resources
Requirements for data quality	Control A.7.4	AI Systems Data Management Policy; Register of AI Resources
Process for recording the provenance of data	Control A.7.5	AI Systems Data Management Policy
Criteria for selecting data preparations and data preparation methods to be used	Control A.7.6	AI Systems Data Management Policy
Provide necessary information to users of the AI system	Control A.8.2	Policy for Handling AI Suppliers and Customers
Provide capabilities for interested parties to report adverse impacts	Control A.8.3	Policy for Handling AI Suppliers and Customers
Plan for communicating incidents to users	Control A.8.4	Policy for Handling AI Suppliers and Customers
Obligations for reporting information towards interested parties	Control A.8.5	Policy for Handling AI Suppliers and Customers
Processes for the responsible use of AI systems	Control A.9.2	AI Systems Acceptable Use Policy

Objectives for responsible use of AI systems	Control A.9.3	AI Systems Acceptable Use Policy
Ensure that the AI system is used according to its intended use	Control A.9.4	AI Systems Acceptable Use Policy
Responsibilities within the AI system life cycle are allocated between the company and third parties	Control A.10.2	Policy for Handling AI Suppliers and Customers
Ensure that usage of services and products from suppliers is aligned with responsible development and use of AI systems	Control A.10.3	Policy for Handling AI Suppliers and Customers
Consider customer expectations and needs when developing and using AI systems	Control A.10.4	Policy for Handling AI Suppliers and Customers

4.3. Non-mandatory documents

Here are a few documents that are not mandatory according to ISO 42001; however, they could still be useful:

- Procedure for Document and Record Control (clause 7.5) — this is not directly related to AI governance; however, it is still very helpful to avoid any confusion with managing documents.
- Procedure for Monitoring of AI Systems (clause 9.1) — this is useful to set clear rules and responsibilities for continuous monitoring and measurement.
- Procedure for Internal Audit (clause 9.2) — this is also not directly related to AI governance; however, it's also useful to set clear rules for the internal audit.
- Procedure for Corrective Action (clause 10.2) — again, this document is not directly related to AI governance; however, it is useful for setting clear rules for nonconformities and corrective actions.
- Various cybersecurity and privacy documents — they are not directly required by ISO 42001; however, this is where [ISO 27001](#) and [GDPR documents](#) can be used.



ISO 42001 Online Courses

Free online courses to learn how to comply with ISO 42001

[Enroll for free](#)

5. ISO 42001 checklist of implementation steps

If you're considering how to implement ISO 42001, below you'll find 18 steps that will show you the optimal way to fully comply with this AI governance standard and go for the certification audit.

1) Obtain management support (clause 5.1)

It sounds obvious, but lack of senior management commitment is the number one reason Artificial Intelligence Management System (AIMS) projects stall. You'll need people, time, and budget — and also management's input about how AI fits into the company strategy.

For that purpose, you'll need to present to the management the benefits of AIMS implementation — you'll have to explain that the AIMS is, in fact, about AI governance, and AI governance is crucial for making the AI systems trustworthy.

2) Treat it as a project

Implementing an AIMS touches many teams (data, product, legal, IT, security) and usually runs for months.

Define the project manager, deliverables, milestones, and the project sponsor just as you would for any other strategic initiative. Make the AIMS plan visible, and track progress weekly.

3) Define your role for the AI system (clause 4.1)

As part of understanding the context of your company, you should define whether your company is an AI provider, AI producer, AI customer, AI partner, or AI subject — this role is important because it helps you with defining your approach to governing your AI systems.

To learn what each of these roles means, sign up for this [free ISO 42001 Foundations Course](#).

4) Define stakeholders and their requirements (clause 4.2)

There are various groups of people who have an interest in your AI systems — besides customers, these could also be your employees, regulatory agencies, and even society as a whole. What is important is that you collect their expectations related to AI, because this will drive how you manage your AI systems.

5) Define the scope (clause 4.3)

Don't try to do too much at first. Decide which AI systems, products, and departments are in the AIMS scope so that you can focus on those and avoid doing too much.

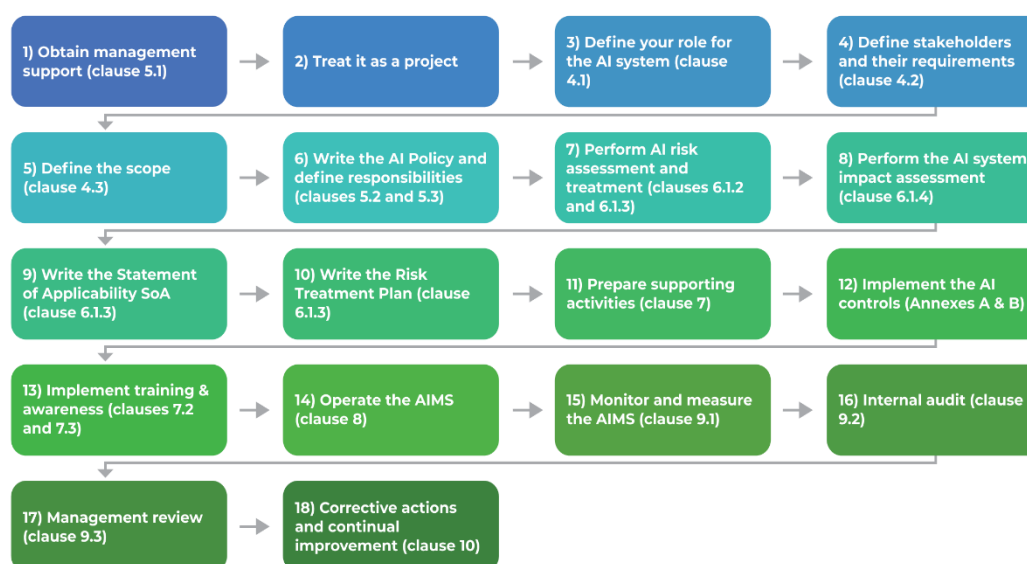
For example, an e-commerce company could focus only on customer support chatbots, while a bank might focus only on an AI system for credit scoring; alternatively, companies might focus only on AI systems deployed in the EU because of the EU AI Act.

6) Write the AI Policy and define responsibilities (clauses 5.2 and 5.3)

This is your highest-level internal document for AI, and it needs to provide your company's direction for AI governance.

Keep it short, but clear: Specify principles (e.g., fairness, safety), how AI objectives will be defined, main roles and responsibilities, commitments to legal compliance and continual improvement, etc. Make sure you communicate it to everyone.

18 steps to implement ISO 42001 efficiently



7) Perform AI risk assessment and treatment (clauses 6.1.2 and 6.1.3)

This is the step that is probably the most complicated. Therefore, before you start doing risk assessment and treatment, you need simple, repeatable rules for identifying, analyzing, and evaluating AI risks: what's "acceptable," how likelihood/impact are assessed, etc. Write those rules in the Risk Management Methodology.

Once you have the methodology, you can start listing all the risks from your AI systems for your company, for individuals, and for society — for each, you have to define the risk level and what kind of AI controls you have to use to decrease those risks. You need to record everything in a Risk Register or some other similar document.

8) Perform the AI system impact assessment (clause 6.1.4)

ISO 42001 requires you to perform an additional, in-depth assessment, called the AI system impact assessment, where you will focus exclusively on what could happen as a consequence of everyday use (or misuse) of your AI systems.

Here you should focus on consequences to individuals and societies, and feed those results into your risk assessment. You should document these results again in the Risk Register, or in a separate document for this particular type of assessment.

9) Write the Statement of Applicability SoA (clause 6.1.3)

In this document, you list all the controls you need and those you're excluding, with justification and how they'll be implemented. Use controls from Annex A as your starting point, and add any additional ones your risks demand.

This document basically summarizes your AI governance activities — in one document, you'll have exactly what you'll do for managing AI and why you're doing this.

10) Write the Risk Treatment Plan (clause 6.1.3)

This is where you turn the SoA into an actionable plan: You need to specify who implements which controls, by when, with what budget, and with which resources.

This is also where you need to get the sign-off from your senior management — not just for this plan, but also for approving the residual AI risks.

11) Prepare supporting activities (clause 7)

For your project to succeed, you'll need to define how the resources are approved and provided — these resources could include money, technology, data, and human resources.

You'll also need to define how the AI governance is communicated throughout the company, but also towards the external stakeholders — who is in charge, and through which means the communication is performed.

Finally, you need to define how you're going to control documents and records — where they will be published, how they're protected, etc.



12) Implement the AI controls (Annexes A & B)

This is the step where you'll spend most of the time and resources, because you need to implement all the controls according to your Risk Treatment Plan.

Typically, these controls are implemented by writing various policies and procedures, but also by purchasing new technologies and performing various other tasks.

As mentioned before, the controls are listed in Annex A; however, in Annex B you have helpful suggestions on how those controls could be implemented.

This [free ISO 42001 Foundations Course](#) gives you a detailed breakdown of all the controls.

13) Implement training & awareness (clauses 7.2 and 7.3)

In parallel with your implementation of AI controls, you'll have to explain to your employees why you need all of these controls, as well as how to use them in their everyday work.

This is why awareness (where you give the answer to the question "Why?") and training (the answer to the question "How?") are crucial — without them, your AI governance will probably fail.

14) Operate the AIMS (clause 8)

Once you implement all the AI controls, you have to start to use (i.e., to operate) them in your daily work — this is when your AI Management System starts to blend with your regular activities.

Even though this is displayed as a step, it is performed continuously — your employees must follow all the AI policies and procedures in their regular work.

15) Monitor and measure the AIMS (clause 9.1)

To know if your AIMS is performing as you expected (for example, if it fulfills the objectives you have set), you have to define how you're going to perform measurement — e.g., specify data sources, frequency, and owners for this activity.

Then you need to start collecting all the data — e.g., track incidents, user satisfaction, system performance, and anything else that you consider important. Then you have to analyze trends and feed results into improvements.

16) Internal audit (clause 9.2)

You must perform the first internal audit before you go for the certification, and then afterwards at least once a year.

Make sure you use an internal auditor who is competent for performing this job, and to create an Internal Audit Report where all the nonconformities are specified.

To learn how to perform internal audits, sign up for this [free ISO 42001 Internal Auditor Course](#).

17) Management review (clause 9.3)

The senior management does not need to handle the details of each AI system, but they must control the overall AIMS — ISO 42001 requires them to do this through a management review.

This management review must use various reports about the AIMS as inputs, and, based on these, the CEO and other senior managers must make crucial decisions about the AI governance — e.g., setting new goals, changes to the budget, new roles and responsibilities, etc.

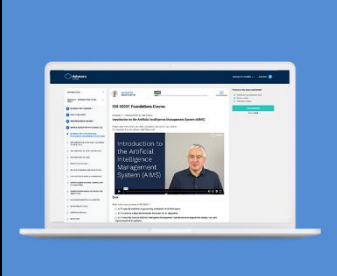
18) Corrective actions and continual improvement (clause 10)

When something goes wrong, ISO 42001 requires you to find the cause of this nonconformity, and fix this cause, so that the problem does not happen again.

Besides nonconformities, you have to find opportunities to make small improvements to your AIMS — this could be something as simple as correcting your policies and procedures, but also larger things like improving your AI controls, introducing new technologies, etc.

There are various groups of people who have an interest in your AI systems — besides customers, these could also be your employees, regulatory agencies, and even society as

a whole. What is important is that you collect their expectations related to AI, because this will drive how you manage your AI systems.



ISO 42001 Online Courses

Free online courses to learn how to comply with ISO 42001

[Enroll for free](#)

6. Organizing ISO 42001 training and awareness

If you're implementing ISO 42001 requirements for training and awareness, you're probably wondering what needs to be done and which options exist. Below you'll find an explanation of ISO 42001 requirements and suggestions on how to move forward with these very important activities.

6.1. ISO 42001 training & awareness requirements — clauses 7.2 and 7.3

In its clause 7.2 called “Competence,” ISO 42001 doesn't say much, but it requires that companies (1) define competencies that are needed for particular roles; (2) evaluate if the employees actually have the required competencies based on their education, training, or experience; and (3) acquire the necessary competencies if they are needed.

Let's say that you want to employ an ISO 42001 internal auditor — you would like this person to have thorough knowledge of the standard and to have auditing skills; you would check if this person has those competencies by asking about his or her experience and for certificates; and if this person does not have the required competencies, you would send them to a course where they would learn about the standard and about auditing techniques.

Clause 7.3 “Awareness” is also quite short — it requires that people working for the company must be aware of the AI policy, their contribution to AI governance, and the implications of not complying with AI policies and procedures.

So, how do you implement all of those requirements?

6.2. How to organize ISO 42001 training

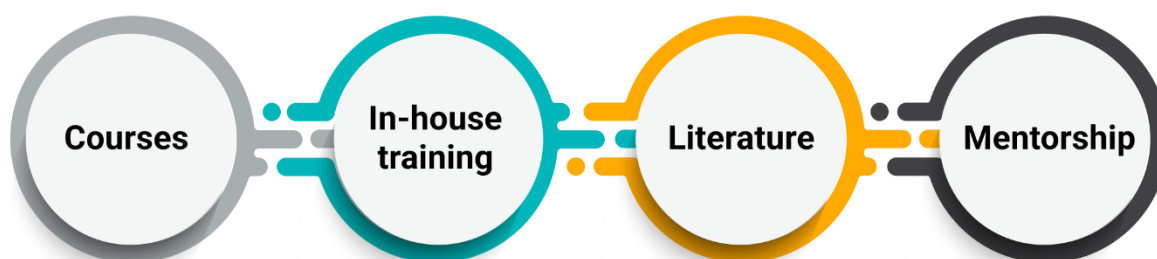
6.2.1. *Training methods*

There are many methods for acquiring competencies, i.e., how to train your employees — for example:

- **Attending courses:** This option is the most suitable for individuals who have a specific role in the company — such as, as already mentioned, the internal auditor, but this could also be, e.g., a software developer who is working with a particular AI technology.
- **Organizing in-house training:** This is suitable if you have a group of people who need to acquire certain knowledge — for example, what are the main requirements of ISO 42001, how to organize AI governance, etc.

- Reading literature: This method does provide in-depth knowledge, but it is often time-consuming and does not involve interaction — therefore, it is probably best used as an “add-on” to some other kind of training.
- Mentorship: This method is best suited for an individual with a specific role where there is already an employee with deeper experience.
- etc.

ISO 42001 training methods



6.2.2. ISO 42001 courses

Regarding courses, the following courses are typically available from various training providers:

- [ISO 42001 Foundations Course](#) — intended for members of the AI governance project team, mid- or senior-level management, and scholars.
- [ISO 42001 Internal Auditor Course](#) — intended for people who are in charge of the ISO 42001 internal audit in their companies.
- [ISO 42001 Lead Auditor Course](#) — intended for auditors who want to perform certification audits, but also for consultants who want to boost their credentials.
- [ISO 42001 Lead Implementer Course](#) — intended for AI officers and other people in charge of implementing AI governance in their companies, but also for consultants who want to offer ISO 42001 compliance as a service.

6.2.3. Organizing in-house training

When you organize an in-house training for a group of your employees, the most important thing is to match your audience with the appropriate topics.

To define the audience, you should segment the employees in your company so that they have similar training needs — for example, you might have:

- Employees in a particular department — e.g., the software development department
- Employees in a particular hierarchy — e.g., members of the middle management
- Employees who are part of a particular process — e.g., handling suppliers of AI products
- etc.

Once you have segmented the employees, for each group you should define the most appropriate training topics — of course, you will start with the required competencies for their roles, but you should also consider the following:

- Specific requirements of the standard and of internal policies and procedures
- The department or the process they work in
- Whether the training should be made for beginners or advanced users
- Training duration

For example, you could organize a training about the basics of AI governance for your senior management, which would last one hour, and where you would present the most important requirements from ISO 42001 and from the company's top-level AI policy.



6.3. How to organize AI awareness / AI literacy

There are several methods of raising awareness:

- Videos: This is a very powerful method for presenting any topic, because videos are easily distributed and easily remembered by the participants.
- Articles on your intranet or newsletter: Offer simple stories (with as many examples as possible) that can help employees understand why AI governance is important.
- Presentations: Organize shorter meetings where you can explain what new policies and procedures are being published, ask your employees for opinions about them, and clarify any misunderstandings.
- Discussions through internal forums: You can initiate and participate in concrete conversations arising from the use of AI systems.
- Etc.

Even though ISO 42001 uses the term “awareness,” the EU AI Act in its Article 4 introduces mandatory “AI literacy” — this literacy could be interpreted as raising awareness about AI systems. This is why you’ll often see the term “AI literacy” instead of “AI awareness.”

6.4. Options for delivering in-house training and awareness videos

There are basically three options to deliver in-house training or awareness videos:

Instructor-led in-classroom training. This is the traditional way of delivering training — you place everyone in a room, and the instructor presents all the relevant topics face to face. This enables attendees to ask questions and allows for some interactivity through shorter workshops, but organizing such training is difficult.

Instructor-led online training. This is similar to instructor-led in-classroom training; however, the main difference is that there is no physical classroom — the training is delivered through online tools like MS Teams, Zoom, or similar. This still enables attendees to ask questions and organize short workshops; while organizing such training is easier, there are still challenges because all attendees must be present at the same time.

Pre-recorded online training delivered via a training platform. This approach is different from the first two options — here, all the videos are pre-recorded and uploaded to learning management system (LMS) software that distributes the videos to attendees and tracks their attendance (and test results, if needed). This doesn't allow direct engagement with the instructor (although some AI solutions are now addressing this problem), but organizing such training is far easier.

To learn how to choose between those options, read this article: [Options for delivering NIS 2, DORA, and ISO 27001 training.](#)

7. ISO 42001 certification

7.1. Who can get ISO 42001 certified?

Both individuals and companies can get certified. However, the processes of certification will be very different — the text below explains the details for both of them.



7.2. ISO 42001 certification for individuals

7.2.1. Certification process for individuals

The process is very simple — anyone who wants to get a certificate must go through an ISO 42001 course and pass the exam.

Once he or she passes the exam, the course provider will issue a certificate to this person.

7.2.2. Types of ISO 42001 courses

There are different ISO 42001 courses, and each one is intended for a specific target group.

Here are the four most popular ISO 42001 courses:

- [ISO 42001 Foundations Course](#)
- [ISO 42001 Internal Auditor Course](#)
- [ISO 42001 Lead Auditor Course](#)

- [ISO 42001 Lead Implementer Course](#)

Here you can sign up for [free ISO 42001 courses](#).

7.3. ISO 42001 certification for companies

7.3.1. *Is ISO 42001 certification mandatory?*

Currently, it is not mandatory to obtain ISO 42001 for companies.

However, in the future, some countries might introduce an obligation for ISO 42001 compliance, as is the case with some other standards like ISO 27001 or ISO 13485.

7.3.2. *Which types of companies should go for ISO 42001?*

ISO 42001 is written in such a way that any type or size of company that develops or uses AI systems can implement it.

However, the following companies will probably be the most interested in ISO 42001 certification:

- Developers of AI models
- Developers of AI applications
- Companies that provide or sell AI applications to customers
- Companies that use AI systems for important processes or sensitive data

7.3.3. *What is the process to get ISO 42001 certified?*

Overall, a company first needs to implement ISO 42001, i.e., fully comply with all of its requirements as described in the section “ISO 42001 checklist of implementation steps.”

Typically, the last steps in the implementation will be the following:

- Internal audit
- Management review
- Corrective actions

After the implementation has been completed, the company needs to invite a certification body to perform the certification audit.

7.3.4. *What are the ISO 42001 certification steps?*

As mentioned above, the certification is performed by a certification body — it is performed in three stages:

- The Stage 1 audit is called “Document review” — this is where a certification auditor checks if all AI governance documents comply with ISO 42001.
- The Stage 2 audit is called “Main audit” — this is where a certification auditor checks if everyday activities in the company are compliant with their AI governance documentation.

If the certification auditor does not find any major nonconformity, then the company will get the ISO 42001 certificate; if the auditor does find a major nonconformity, then the company will typically have 90 days to resolve this nonconformity and ultimately get the certificate.

After the certificate is issued, it will be valid for three years — during that time, the certification body performs the last stage:

- The Stage 3 audit is called “Surveillance audit” — this is where the auditor visits the company at least once a year and checks if the company maintains its Artificial Intelligence Management System (AIMS).

7.3.5. How long does the certification process take?

The implementation process for ISO 42001 typically takes between three and 12 months, depending on the size of the company.

However, the certification audit itself is much quicker:

- The Stage 1 audit takes a minimum of two days for very small companies, and is longer for larger companies.
- The Stage 2 audit takes a minimum of four days for very small companies, and could go up to 30 days for larger companies.

Usually, there is at least a two-week period between Stage 1 and Stage 2 audits — sometimes this in-between period can be up to a couple of months.

7.3.6. How long is the ISO 42001 certificate valid?

The ISO 42001 certificate is valid for 3 years.

However, a certification body can withdraw this certificate (while it is still valid) if a certification auditor finds a major nonconformity during the surveillance audit.

Once the certificate expires, a company can go for ISO 42001 re-certification — this process is very similar to the initial Stage 1 and Stage 2 audits.

7.3.7. How much does ISO 42001 certification cost?

The cost of certification bodies varies significantly from one country to another. In general, ISO 42001 certification costs in Western Europe and North America start from US\$6,000 for very small companies, while larger companies pay several times that amount.

7.3.8. Is an ISO 42001 gap assessment required?

Gap assessment is not required by the standard, nor by the certification body.

In general, gap assessment is not recommended for smaller companies (because it will unnecessarily delay the implementation process), whereas for larger companies, it might be useful to get a rough estimate of the required time and resources for the implementation.

7.3.9. Is it possible to certify against ISO 42001, ISO 27001, and ISO 9001 at the same time?

Yes, it is possible to go for a so-called “integrated certification audit” where the certification body checks compliance with several standards at the same time.

Once a company passes such an integrated audit, the certification body will issue separate certificates for each standard.

7.3.10. What are the main benefits of ISO 42001 certification?

There are several benefits of ISO 42001 implementation and certification:

1. **A better reputation brings more sales.** As mentioned before, when a company shows an ISO 42001 certificate to its customers and other stakeholders, the company will be perceived as one that manages its AI systems in a systematic way. This may bring additional revenues to this company and enable easier handling of AI stakeholders.
2. **A structured framework brings quicker compliance.** The EU AI Act has very strict requirements for high-risk AI systems that can be more easily complied with when companies use ISO 42001 as guidance.
3. **Lower risks bring lower costs.** Uncontrolled usage of AI systems will produce various incidents — when such incidents are prevented by systematic AI governance according to ISO 42001, then related costs will be avoided.
4. **Better organization brings less wasted time.** When clear rules are set on how to develop and use AI systems, employees will spend less time trying to figure out what to do and more time on productive activities.

8. ISO 42001 vs. ISO 27001: Similarities and differences

Many professionals who have started their governance journey with ISO 27001 are now looking towards ISO 42001 — the standard that defines the AI governance framework. So, how is ISO 27001 similar to ISO 42001, and can you use any elements from an ISMS in an AIMS?

8.1. Similarities between ISO 27001 and ISO 42001

Let's start with what is similar between these two standards.

Both standards have very similar structures according to the high-level structure (HLS) that is set by the International Organization for Standardization (ISO) for management system standards. This means that the main clauses (and almost all subclauses) are the same in both of these standards.

The purpose of Annex A in both standards is the same — they provide a list of controls from which companies can choose which ones are applicable to them; these controls are rather generic, so it is up to each company to decide how to implement them.

Learn more here: [Understanding the ISO 27001 controls from Annex A](#).

The method for choosing those controls is also the same — both standards require companies to perform risk assessment, and then, during the risk treatment, to choose appropriate controls from Annex A. Interestingly enough, both standards require documenting the decision on which controls they will use in the Statement of Applicability, and both standards specify very similar structures for this document.

See also: [Statement of Applicability in ISO 27001 – What is it and why does it matter?](#)


Finally, both standards require the writing of the Risk Treatment Plan, which specifies how to implement those controls.

Of course, ISO 42001 has all other elements that are common not only with ISO 27001, but also with other management standards:

- Definition of objectives
- Top-level policy
- Training and awareness

- Managing documents and records
- Internal audit
- Management review
- Corrective actions
- etc.

To learn about these details, see this article: [How to implement integrated management systems.](#)



ISO 27001 vs. ISO 42001 Matrix

Free matrix that shows the relationship between ISO 27001 and ISO 42001 clauses

[Download now](#)

8.2. Main differences

Now let's see what the main differences are.

Focus. whereas ISO 27001 focuses on cybersecurity governance, i.e., the protection of confidentiality, integrity, and availability, ISO 42001 focuses on AI governance with very different goals — for example, accountability, environmental impact, fairness, privacy, robustness, safety, transparency, etc.

Therefore, the following clauses in ISO 27001 and ISO 42001 are different:

- Clause 6.1 of ISO 42001 specifies the risk management in a moderately different way from ISO 27001.
- Clause 8 of ISO 42001 is slightly different from that of ISO 27001.

Of course, Annex A controls are very different from those in ISO 27001.

There are also some completely new things.

Roles. Clause 4.1 requires that companies need to define their role — i.e., AI provider, AI producer, AI customer, AI partner, AI subject, or government authority. There is no such thing in ISO 27001.

AI system impact assessment. In ISO 42001, there is a new sub-clause, 6.1.4 AI system impact assessment, which requires an additional assessment on top of the risk

assessment defined in 6.1.2. There is no such concept in ISO 27001, although this concept is kind of similar to the business impact analysis in ISO 22301.

See also: [How to implement business impact analysis \(BIA\) according to ISO 22301.](#)

However, this AI system impact assessment is very different from the BIA in ISO 22301, and focuses on assessing potential consequences of AI systems to individuals or societies. It is also different from the risk assessment prescribed by ISO 42001 itself, because this impact assessment focuses on very likely outcomes of AI systems, whereas risk assessment is more theoretical because it also covers risks that are not likely; the second difference is that impact assessment is only external, since it covers individual users and whole societies, whereas risk assessment also covers the risks for the company itself.

Annexes. ISO 27001 has only Annex A, whereas ISO 42001 also has annexes B, C, and D. Annex B is the most interesting one, because it serves the same purpose that ISO 27002 does for ISO 27001 — ISO 42001 Annex B provides guidance for the implementation of controls from Annex A.

Learn more here: [What is ISO 27002?](#)

Annex C could also be useful, since it provides a list of potential objectives, but also risk sources (i.e., “threats” in the cyber terminology), while Annex D provides some ideas on what kinds of sectors could use ISO 42001, as well as some ideas for integrating this standard with other standards (very general annex, not very useful.)



8.3. Comparison of clauses

So, let's see the breakdown of these clauses and how similar they are.

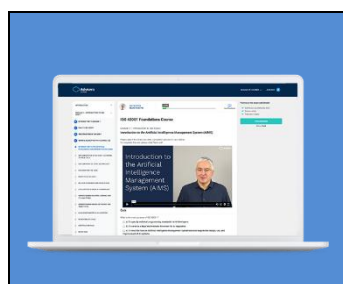
Clauses in ISO 27001 and ISO 42001	Difference	Comment
4.1 Understanding the organization and its context	Moderate	
The rest of clause 4 Context of the organization	Low	
5 Leadership	Low	
6.1.4 AI system impact assessment	High	New clause
The rest of clause 6.1 Actions to address risks and opportunities	Moderate	
6.2 AI objectives and planning to achieve them	Low	
6.3 Planning of changes	Low	
7 Support	Low	
8 Operation	Moderate	
9 Performance evaluation	Low	
10 Improvement	Low	
Annex A	High	Different set of controls
Annexes B, C, and D	High	No such annexes in ISO 27001

8.4. Integration of ISO 27001 and ISO 42001?

So, are these similarities going to help companies integrate ISO 27001 and ISO 42001?

Up to a point, this will be possible — you can already integrate certain elements of the ISO standards described in the first section of this article, since they are all aligned. ISMS processes that specify the protection of confidentiality, integrity, and availability will certainly need to cover AI systems as well.

However, for the core elements of ISO 42001 — risk assessment, risk treatment, and implementation of AI controls — it seems to me these things will have to be mainly separated from ISO 27001, especially AI system impact assessment.



ISO 42001 Online Courses

Free online courses to learn how to comply with ISO 42001

[Enroll for free](#)

9. Thirteen key AI concepts important for AI governance

If you need to manage your AI systems, you first have to understand some basic concepts if you want your AI governance to work properly. This article presents 13 basic things about AI that are relevant for AI governance.

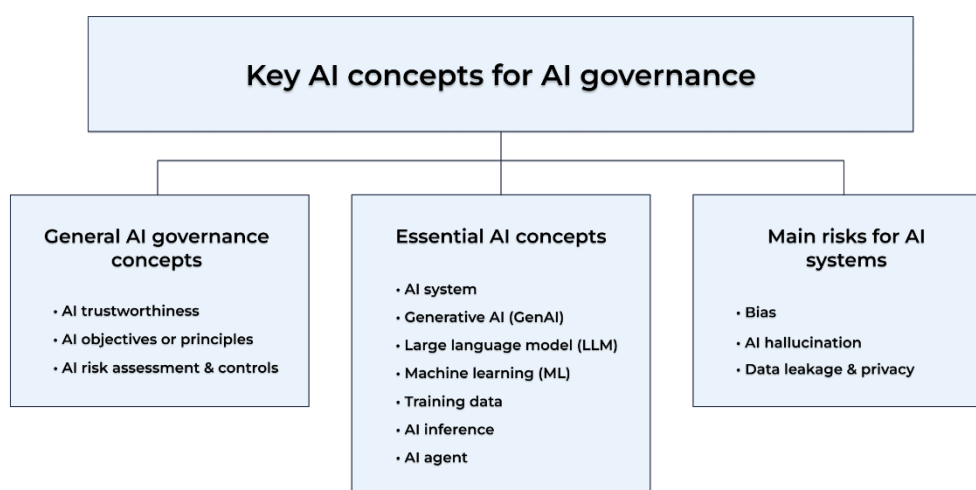
9.1. General AI governance concepts

First, let's start with some general concepts that are important for AI governance.

AI trustworthiness is the ultimate goal of what you want to achieve with AI systems using AI governance. Sometimes, the goals of safe, responsible, and ethical AI systems are also mentioned, but those could all be included in the trustworthiness goal. AI trustworthiness is basically the ability for stakeholders to check if the results from AI systems are meeting their expectations.

AI objectives or principles are high-level directives that you want your AI governance to comply with — those could include accountability, environmental impact, fairness, maintainability, privacy and security, robustness, safety, transparency and explainability, human oversight, etc.

AI risk assessment & controls are at the core of how AI governance works: You need to find out which potential bad things (risks) could happen because of AI systems, and then you have to find appropriate ways to decrease those risks (controls).



9.2. Key elements of AI

Here are a couple of concepts that explain key elements of AI.

An **AI system** is an IT system that generates various types of outputs like answers, forecasts, decisions, and others in textual, video, audio, and other formats, based on requests made by humans.

Generative AI (GenAI) is any AI system that creates new content: text, images, audio, video, code, designs, etc. Different types of generative AI exist: large language models, diffusion models, video models, audio models, multimodal models, code generation models, etc.

A **large language model** (LLM) is a model trained on a vast amount of text and is designed for natural language processing tasks, especially language generation. Each major chatbot, like ChatGPT, Claude, Gemini, and others, has an LLM behind it as an engine that enables it to speak to you.

Machine learning (ML) is the process of optimizing parameters for large language models (or other AI models) using the processing power of computer chips. A huge amount of processing power is needed to optimize the model behavior so that it provides outputs that are acceptable — for example, that it provides an answer in a language that you speak, not in some other language.

Training data is the information used to teach an AI model how to recognize patterns and generate outputs. For LLMs, the built-in training data comes from massive datasets collected and processed by the model creator before release, and it shapes the model's general knowledge and behavior. User-provided training data (prompts, documents, fine-tuning datasets) is added later and influences how the model performs for a specific organization or task, without changing the underlying original model unless explicitly fine-tuned.

AI inference is the conclusion that AI systems make based on data and reasoning — this is basically about the processing of any request sent to AI. Since a huge amount of processing power is needed, specialized data centers are built around the world to process and answer all those prompts that people are entering. Of course, inference is not only about answering prompts; it is also about processing any other AI activity, including those from AI agents.

An **AI agent** is a part of an AI system that understands its environment and takes actions autonomously to achieve its goals — in other words, they do not need a human to trigger an activity; they can do this alone. It is predicted that AI agents will take over lots of repetitive tasks, but perhaps also some non-repetitive tasks as well.

9.3. Main risks for AI systems

Lastly, let's look at some very common risks related to AI systems.

Bias is when an AI system systematically treats certain individuals or groups of people differently from others. An example could be an AI system for hiring new employees that prefers men over women.

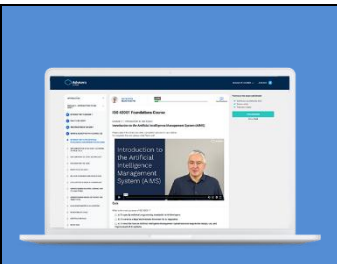
AI hallucination is a response generated by AI that contains false or misleading information, which is presented as fact. The problem with chatbots is that they present such false or misleading information very convincingly, so it is very hard to know whether it is true or not.

Data leakage and privacy. AI systems can leak data when sensitive information used in training or prompts becomes exposed through model outputs or unauthorized access. This creates privacy risks, because personal or confidential data could become available to attackers or unintended users.

9.4. How to approach AI governance?

It might seem overwhelming to take all of these things into account and manage AI systems in a systematic way. However, this is where ISO 42001, an international standard for AI Management Systems (i.e., AI governance) is of great help.

ISO 42001 defines how to set a clear direction for AI governance, how to perform risk assessment, which documents to write, what the roles and responsibilities are, and how to manage AI systems throughout their lifecycles. In other words, it clarifies how the whole AI governance needs to be implemented.



ISO 42001 Online Courses

Free online courses to learn how to comply with ISO 42001

[Enroll for free](#)

Sources:

- [Series of ISO 42001 articles on Advisera.com](#)

Author:

Dejan Kosutic  

CEO & Lead Expert for ISO 27001 and ISO 42001

Leading expert on cybersecurity and AI governance and the author of several books, articles, webinars, and courses. As a premier expert, Dejan founded Advisera to help small and medium businesses obtain the resources they need to become compliant with EU regulations and ISO standards. He believes that making complex frameworks easy to understand and simple to use creates a competitive advantage for Advisera's clients, and that AI technology is crucial for achieving this.

As an ISO 27001 and ISO 42001 expert, Dejan helps companies find the best path to compliance by eliminating overhead and adapting the implementation to their size and industry specifics.

Advisera Expert Solutions Ltd

for electronic business and business consulting
www.advisera.com

Our offices

US Office

1178 Broadway, 3rd Floor #3829
New York NY 10001
United States

EU Office

Zavizanska 12
10000 Zagreb
Croatia, European Union

EMAIL:

support@advisera.com

