Alcumus ISOQAR

Customer Guidance and Gap Analysis for the certification and delivery of audit of the Artificial Intelligence Management System

ISO/IEC 42001:2023

isoqar.com

ISO/IEC 42001:2023 Gap Analysis

The purpose of this document is to give guidance on the criteria, processes, and information requirements relating to the delivery of an audit to ISO/IEC 42001:2023.

Artificial intelligence (AI) is increasingly applied across all sectors utilizing information technology and is expected to be one of the main economic drivers. A consequence of this trend is that certain applications can give rise to societal challenges over the coming years.

Your business needs and objectives, processes, size and structure as well as the expectations of various interested parties influence the establishment and implementation of the AI management system.

Another set of factors that influence the establishment and implementation of the AI management system are the many use cases for AI and the need to strike the appropriate balance between governance mechanisms and innovation.

You can elect to apply these requirements using a risk-based approach to ensure that the appropriate level of control is applied for the particular AI use cases, services or products within your scope and boundaries.

The AI management system should be integrated with your processes and overall management structure.

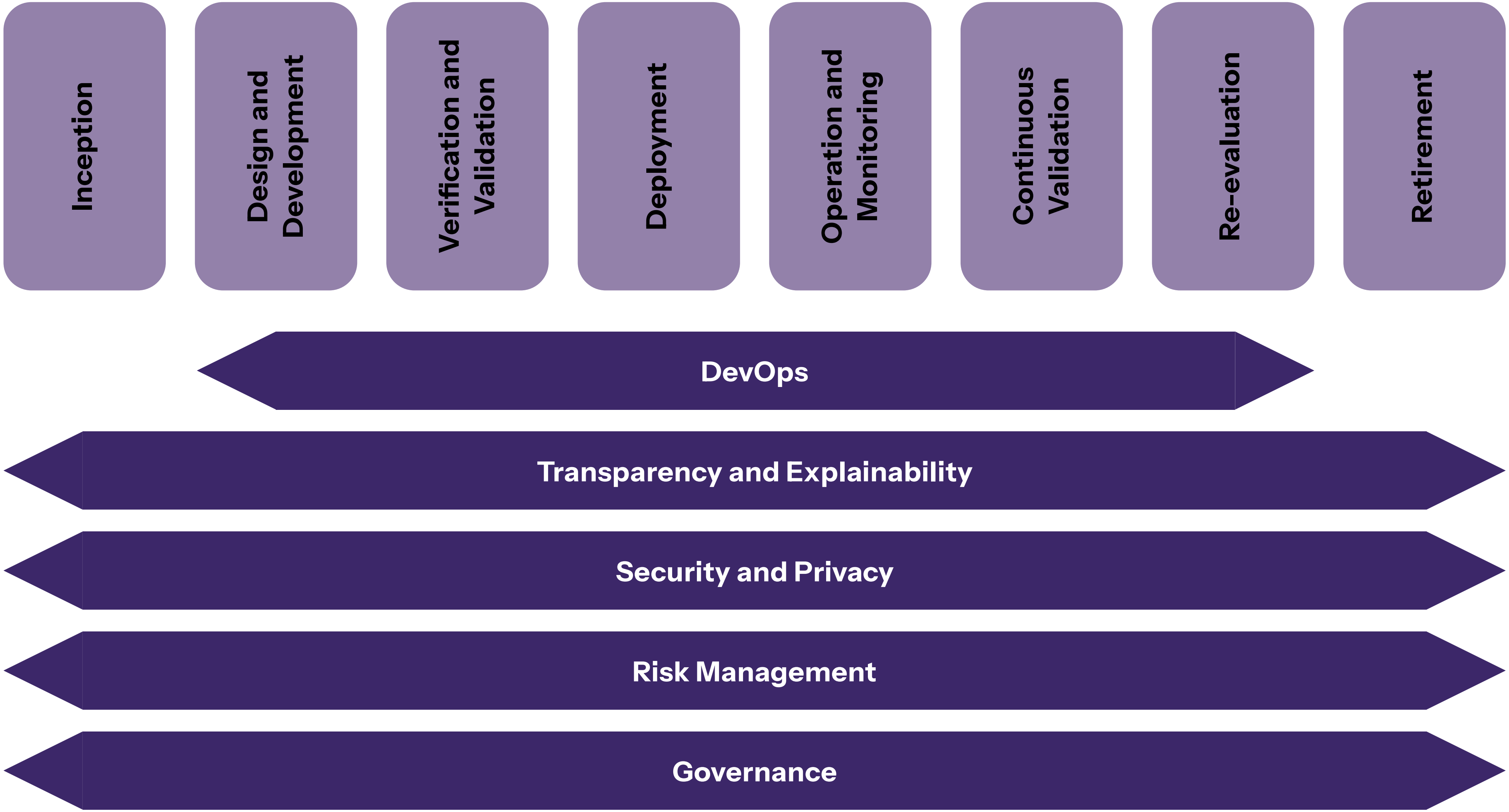
Specific issues related to AI should be considered in the design of processes, information systems and controls. Crucial examples of such management processes are:

- Determination of organisational objectives, involvement of interested parties and organisational policy.
- Management of risks and opportunities.
- Processes for the management of concerns related to the trustworthiness of AI systems such as security, safety, fairness, transparency, data quality and quality of *AI systems throughout their life cycle.*
- Processes for the management of suppliers, partners and third parties that provide or develop AI systems for the organisation.

Artificial intelligence (AI) systems in the fields of computer vision and image recognition, natural language processing, fraud detection, automated vehicles, predictive maintenance and planning have achieved remarkable successes. To build and maintain an AI system, it is an efficient approach to extend the life cycle processes for a traditional software system to include AI-specific life cycle characteristics.

ISO/IEC 5338:2023 - Information Technology

Artificial intelligence — AI system life cycle processes
AI system life cycle model stages and high-level processes



AI system life cycle processes relative to ISO/IEC/IEEE 15288:2023

Agreement Processes

- Acquisition process (6.1.1) — Modified
- Supply process (6.1.2) — Modified

Organisational project-enabling Processes

- Life cycle model management process (6.2.1) — Generic
- Infrastructure management process (6.2.2) — Generic
- Portfolio management process (6.2.3) — Modified
- Human resource management process (6.2.4) — Modified
- Quality management process (6.2.5) — Modified
- Knowledge management process (6.2.6) — Modified

Technical Management Processes

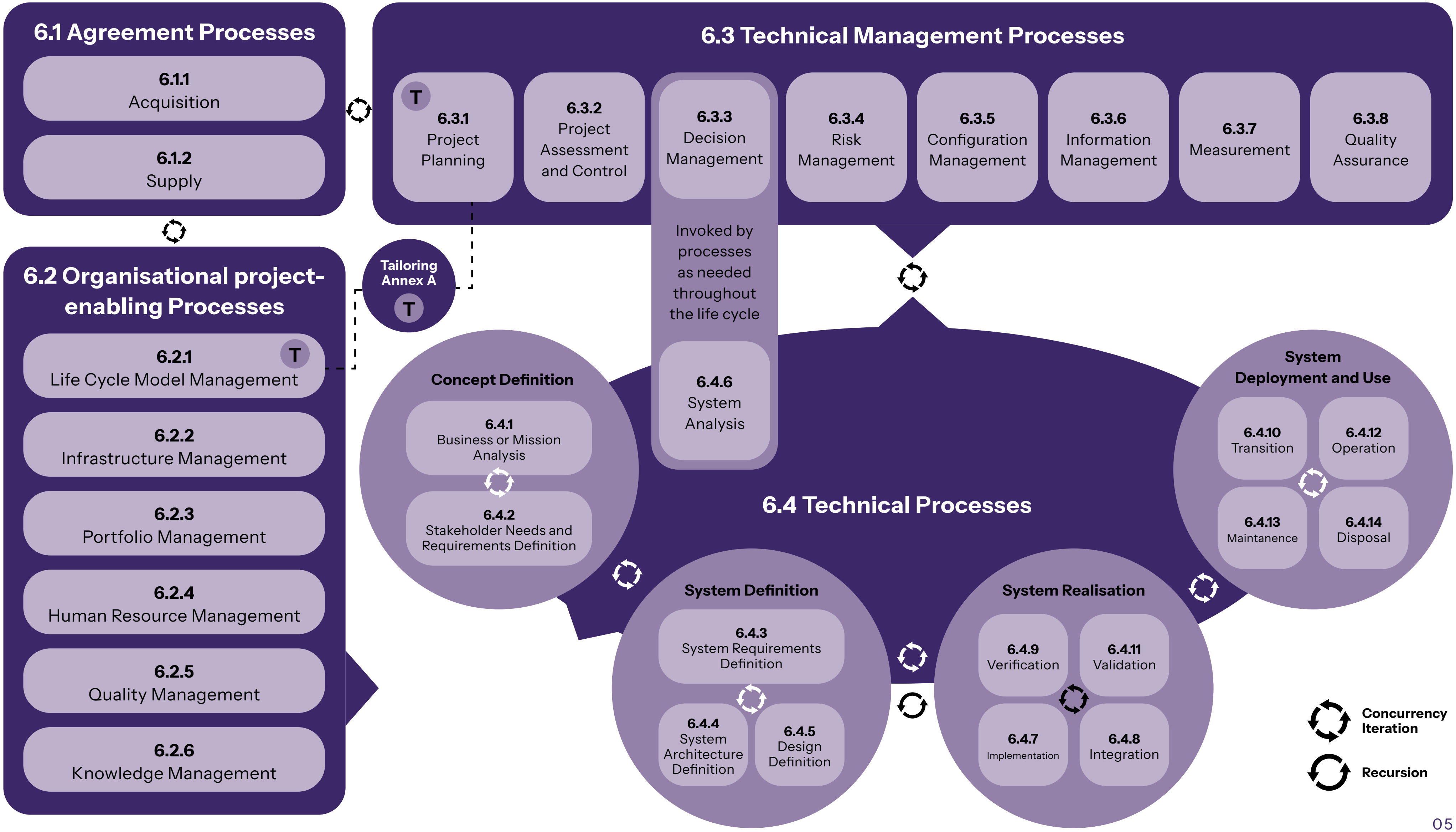
- Project planning process (6.3.1) — Modified
- Project assessment and control processes (6.3.2) — Modified
- Decision management process (6.3.3) — Modified
- Risk management process (6.3.4) — Modified
- Configuration management process (6.3.5) — Modified
- Information management process (6.3.6) — Modified
- Measurement process (6.3.7) — Generic
- Quality assurance process (6.3.8) — Modified

Technical Processes

- Business or mission analysis process (6.4.1) — Modified
- Stakeholder needs and requirements definition process (6.4.2) — Modified
- System requirements definition process (6.4.3) — Modified
- System architecture definition process (6.4.4) — Generic
- Design definition process (6.4.5) — Generic
- System analysis process (6.4.6) — Generic
- Knowledge acquisition process (6.4.7) — AI-specific
- AI data engineering process (6.4.8) — AI-specific
- Implementation process (6.4.9) — Modified
- Integration process (6.4.10) — Generic
- Verification process (6.4.11) — Modified
- Transition process (6.4.12) — Modified
- Validation process (6.4.13) — Modified
- Continuous validation process (6.4.14) — AI-specific
- Operation process (6.4.15) — Modified
- Maintenance process (6.4.16) — Modified
- Disposal process (6.4.17) — Modified

AI Interaction of processes

taken from ISO/IEC/IEEE 15288:2023 - Systems and software engineering — System life cycle processes:



6.1 Agreement Processes

- 6.1.1 Acquisition
- 6.1.2 Supply

6.2 Organisational project-enabling Processes

- 6.2.1 Life Cycle Model Management T
- 6.2.2 Infrastructure Management
- 6.2.3 Portfolio Management
- 6.2.4 Human Resource Management
- 6.2.5 Quality Management
- 6.2.6 Knowledge Management

Tailoring Annex A T

6.3 Technical Management Processes

- T 6.3.1 Project Planning
- 6.3.2 Project Assessment and Control
- 6.3.3 Decision Management
- 6.3.4 Risk Management
- 6.3.5 Configuration Management
- 6.3.6 Information Management
- 6.3.7 Measurement
- 6.3.8 Quality Assurance

Invoked by processes as needed throughout the life cycle

6.4.6 System Analysis

6.4 Technical Processes

Concept Definition

- 6.4.1 Business or Mission Analysis
- 6.4.2 Stakeholder Needs and Requirements Definition

System Definition

- 6.4.3 System Requirements Definition
- 6.4.4 System Architecture Definition
- 6.4.5 Design Definition

System Realisation

- 6.4.9 Verification
- 6.4.11 Validation
- 6.4.7 Implementation
- 6.4.8 Integration

System Deployment and Use

- 6.4.10 Transition
- 6.4.12 Operation
- 6.4.13 Maintanence
- 6.4.14 Disposal

Concurrency Iteration

Recursion

Scope of certification

The scope statement is a key part of setting the areas that are within the boundaries of the development and use of AI. The consensus is that it should be specific to the user, their role, and who is responsible.

It should reference the role of the organisation in the use of AI (AI Producer, AI Developer, AI Provider, AI User), the activities and boundaries of the AI use, including a reference to the SoA.

ISO/IEC 42001:2023

9.1.3.1 General
The audit programme for AIMS-audits need to provide for all determined measures.

The audit programme for an ISO/IEC 42001: — audit shall identify the role of the client as an AI provider, AI developer or AI user.

9.1.4.2 Scope of certification
Certification bodies shall ensure that the risk assessment and risk treatment of the client's AI management system adequately reflects its activities and extends to the boundaries of the activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their AIMS and statement of applicability (SoA).

The following are examples:

a. The Artificial Intelligence Management System (AIMS), acting as an AI User, of a cloud/hosted services platform, used for the validation and reporting of sales and marketing data of the ISOQAR products, used exclusively by the tactical level operation managers of the sales and marketing teams, in accordance with Statement of Applicability Revision 3.

b. The Artificial Intelligence Management System (AIMS), acting as an AI Developer and AI User, for the development of the ISOQAR AI Platform (ISOMarket©) by the specific development project team. The AI platform is used for the validation of sales, marketing, and service data, used both by clients and internally by the relevant sales and marketing managers. Delivered in accordance with Statement of Applicability Revision 3.

AI Role Descriptions

Ser	General	Subcategory	Description
1	**AI Provider**		An AI provider is an organisation or entity that provides products or services that uses one or more AI systems. AI providers encompass AI platform providers and AI product or service providers.
1.a		**AI Platform Provider**	An AI platform provider is an organisation or entity that provides services that enable other stakeholders to produce AI services or products.
1.b		**AI Service or Product Provider**	An AI service or product provider is an organisation or entity that provides AI services or products either directly usable by an AI customer or user, or to be integrated into a system using AI along with non-AI components.
2	**AI Producer**		An AI producer is an organisation or entity that designs, develops, tests and deploys products or services that use one or more AI system.
2.a		**AI Developer**	An AI developer is an organisation or entity that is concerned with the development of AI services and products. Examples of AI developers include, but are not limited to: — Model designer: the entity that receives data and a problem specification and creates an AI model. — Model Implementer: the entity that receives an AI model and specifies what computation to execute (the implementation to use and on what computer resources, for example CPU, GPU, ASIC, FPGA). — Computation Verifier: the entity that verifies that a computation is being executed as designed. — Model Verifier: the entity that verifies that the AI model is performing as designed.
3	**AI Customer**		An AI customer is an organisation or entity that uses an AI product or service either directly or by its provision to AI users.
3.a		**AI Users**	An AI user is an organisation or entity that uses AI products or services.
4	**AI Partner**		An AI partner is an organisation or entity that provides services in the context of AI. AI partners can perform technical development of AI products or services, conduct testing and validation of AI products and services, audit AI usage, evaluate AI products or services and perform other tasks.

AI Role Descriptions

Ser	General	Subcategory	Description
4.a		**AI System Integrator**	An AI system integrator is an organisation or entity that is concerned with the integration of AI components into larger systems, potentially also including non-AI components.
4.b		**Data Provider**	A data provider is an organisation or entity that is concerned providing data used by AI products or services.
4.c		**AI Auditor**	An AI auditor is an organisation or entity that is concerned with the audit of organisations producing, providing or using AI systems, to assess conformance to standards, policies or legal requirements.
4.d		**AI Evaluator**	An AI evaluator is an organisation or entity that evaluates the performance of one or more AI systems.
5	**AI Subject**		An AI subject is an organisation or entity that is impacted by an AI system, service or product.
5.a		**Data Subject**	A data subject is an organisation or entity that is affected by AI systems with following aspects: — Subject of training data: where data pertaining to an organisation or human is used in training an AI system, there can be implications for security and privacy, for the latter particularly where that subject is an individual human.
5.b		**Other Subjects**	Other organisations or entities impacted by an AI system, service or product can be for example in the form of an individual or a community. For example, consumers who interacts with a social network that provides recommendations based on AI, drivers of vehicles with AI-based automation.
6	**Relevant Authorities**		Relevant authorities are organisations or entities that can have an impact on an AI system, service or product.
6.a		**Policy Makers**	These are organisations and entities that have the authority to set policies within an international, regional, national or industrial domain that can have an impact on an AI system, service or product.
6.b		**Regulators**	These are organisations and entities that have the authority to set, implement and enforce the legal requirements as intended in policies set forth by policy makers (6.a).

Performing an AI system impact assessment

For each intended use and reasonably foreseeable misuse of an AI system, your organisation should consider, as appropriate:

- Identification of reasonably foreseeable AI system impacts to all identified individuals, groups of individuals and to societies, and in other resources as appropriate. Both beneficial impacts and harmful impacts should be considered.
- Multiple types or dimensions of AI system impacts to groups of individuals, organisations and to societies including but not limited to:
  - Identify reasonably foreseeable potential impacts to individuals, groups, organisations and societies. It is important to consider how such impacts also translate into organisational risks.
  - Frequency of assessing and reassessing risks and impacts.
- Impacts to fundamental rights, as part of identifying impacts to individuals or groups of, including but not limited to:
  - Identify impacts to human rights periodically or as appropriate, e.g. as early as possible and at identified stages of the AI system life cycle. Non-exhaustive examples of rights to be considered are non-discrimination, right to life and personal security, privacy and freedom of expression.
  - Determine how impacts to fundamental and human rights will be addressed, by assessment of the magnitude and likelihood of identified impacts.

The results of the AI system impact assessment can play a crucial role in the responsible use and development of AI systems. The assessment should be analysed and incorporated into both technical and management decisions.

On a technical level, analysis can be used, for instance, to improve product or service quality, building-in safeguards against unintended use or misuse, improve safety and robustness of AI systems etc. This can also include determining the types of measures to address benefits and harm, the results of the assessment should be compared to the established thresholds and if these are not met, identify an action plan to remediate.

On a management level, analysis can be used to inform the organisational risk management processes on foreseeable impacts of AI systems. This can include consideration of individual system impact assessments, but also analysing several assessments holistically to determine how trends can affect organisational risks and objectives at a broad level.

Considerations for AI Business Impact Assessment Areas

Taken from ISO/IEC DIS 42005 - Information Technology — Artificial Intelligence — AI System Impact Assessment:

- Scope of the AI system impact assessment
- AI system information
  - AI system description
  - AI system features
  - AI system purpose
  - Intended uses
  - Unintended uses
- Data information and quality
  - Data information
  - Data quality documentation
- Algorithm and model information
  - Information on algorithms used by the organisation
  - Information on algorithm development
  - Information on models used in an AI system
  - Information on model development
- Deployment environment
  - Geographical area and languages
- Deployment environment complexity and constraints
- Relevant interested parties
- Actual and potential impacts
- Benefits and harms
- AI system failures and misuse or abuse
- Measures to address harms and benefits

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