Management Systems for Artificial Intelligence ISO/IEC 42001

Danilo Diomede, Cyber & IT Product Manager

RINA today

5300 colleagues

200 offices

70 countries

Our resources

More than **90 nationalities**

80%+ educated to **degree level**

42 average **age**

What we do

Energy

Energy solutions from O&G to renewables, taking care of sustainability and environmental impacts

Marine

Rules, technologies and innovative services to manage transport and pleasure vessels

Certification

Solutions to support products, people and processes on their way to excellence

Infrastructure & Mobility

The path to the next generation of infrastructure and buildings by ensuring their safety and efficiency

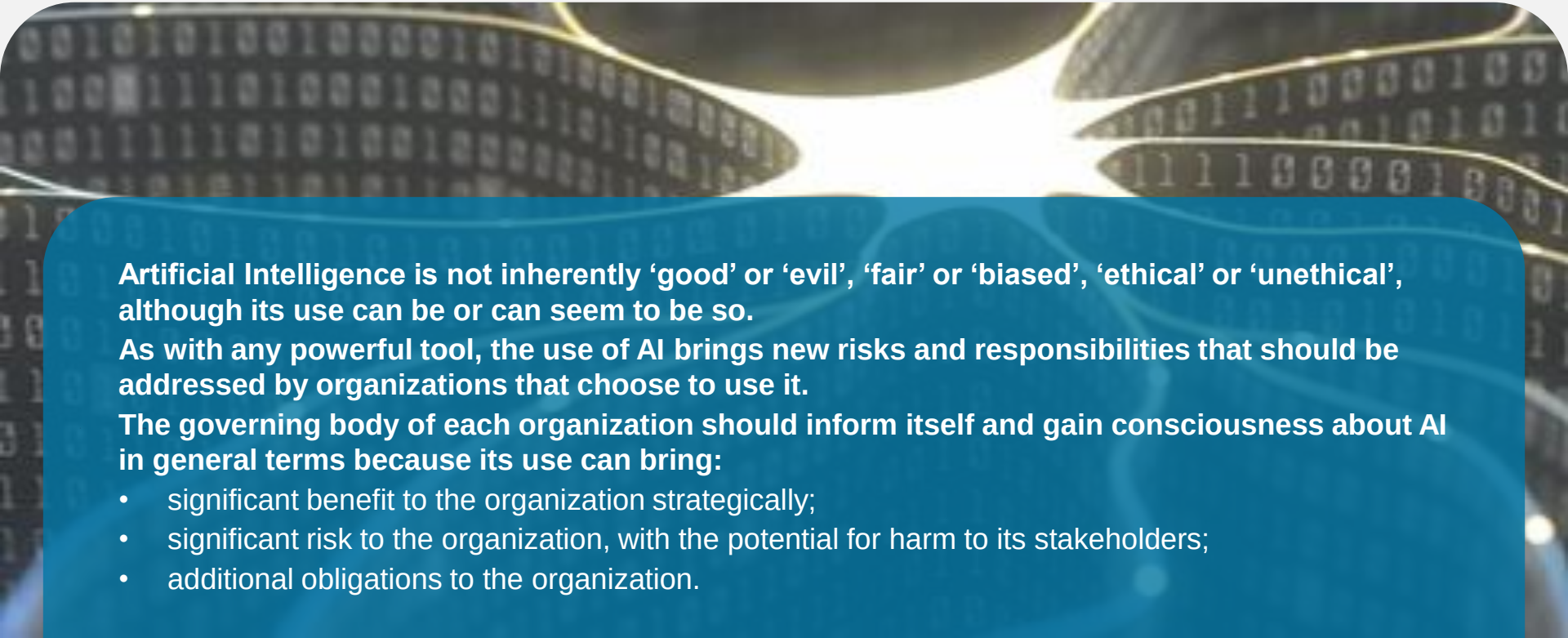
Industry

Accelerating clients' success with technology-driven strategies and solutions

Real Estate

Innovative value proposition of integrated services: Rina Prime Value Services is able to cover all the real estate lifecycle

Artificial Intelligence



Artificial Intelligence is not inherently ‘good’ or ‘evil’, ‘fair’ or ‘biased’, ‘ethical’ or ‘unethical’, although its use can be or can seem to be so.

As with any powerful tool, the use of AI brings new risks and responsibilities that should be addressed by organizations that choose to use it.

The governing body of each organization should inform itself and gain consciousness about AI in general terms because its use can bring:

- significant benefit to the organization strategically;
- significant risk to the organization, with the potential for harm to its stakeholders;
- additional obligations to the organization.

New implications arising from the use of AI

Increased reliance on technology and systems for the acquisition of data and assurance of its quality

Accepting the use of AI systems without awareness or consideration of potential bias, error or harm

The possibility that existing direction and controls are not appropriate to ensure required outcomes

Competitive pressure due to the sales and operations of an organization not using AI

Transparency and explainability of AI systems

The impact on commercial operations and to brand reputation

The impact of AI on the workforce

Disparity between the speed of change in automated learning systems and the human controls of compliance

Properties / Objectives of AI systems

Accountability

State of being answerable for actions, decisions and performance

Availability

Property of being accessible and usable on demand by an authorized entity

Controllability

Property of an AI system that allows a human or another external agent to intervene in the system's functioning

Explainability

Property of an AI system to express important factors influencing the AI system results in a way that humans can understand

Predictability

Property of an AI system that enables reliable assumptions by stakeholders about the output

Reliability

Property of consistent intended behaviour and results

Robustness

Ability of a system to maintain its level of performance under any circumstances

Transparency

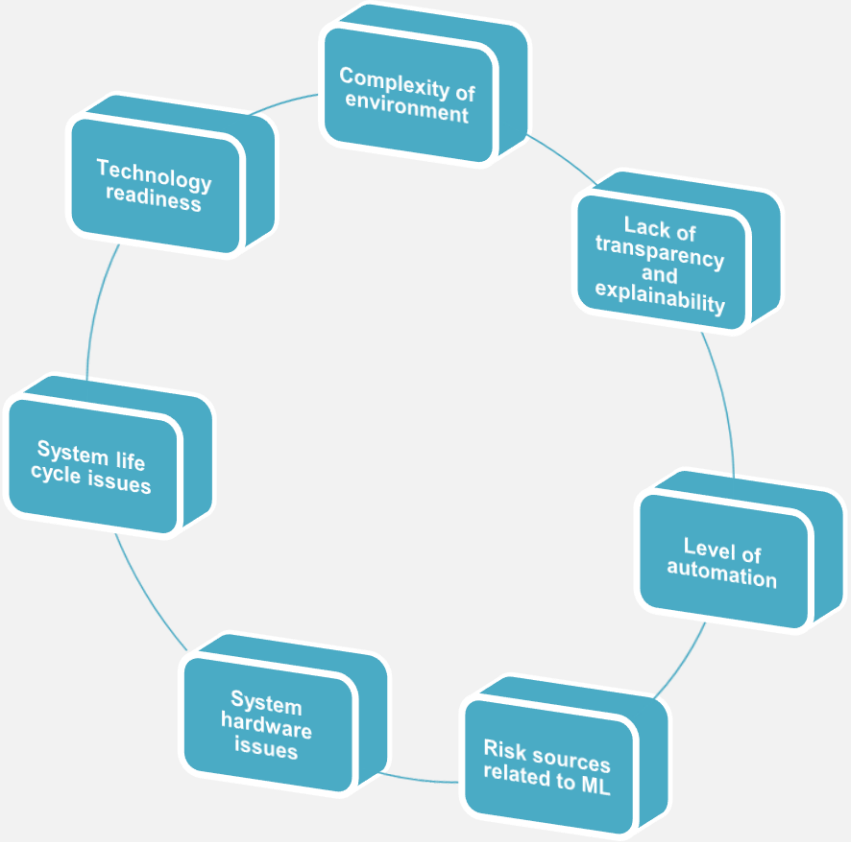
Property of a system that appropriate information about the system is made available to relevant stakeholders

Trustworthiness

Ability to meet stakeholder expectations in a verifiable way (ie.: environmental impact, fairness, maintainability, expertise, resilience, security, privacy, safety, integrity, authenticity, quality and usability)

AI-related risk sources

ISO/IEC 42001 lists some risk sources that can have an impact on the objectives of the AI management system and that feed the AI risk assessment process



Impacted business sectors

- Marketing and Retail
- Trade
- Healthcare
- Finance, Bank & Insurance
- Automotive
- Manufacturing
- Utilities
- Space Technology
- Telecommunication
- Media & Entertainment
- Public Administration
- Defence
- Security
- Biometric identification and categorisation
- Critical Infrastructure
- Education and vocational training
- Employment, workers management
- Essential private/public services and benefits
- Law enforcement
- Migration, asylum and border control
- Administration of Justice

Roles of Organizations

AI providers, including AI platform providers, AI product or service providers

AI producers, including AI developers, AI designers, AI operators, AI testers and evaluators, AI deployers, AI human factor professionals, domain experts, AI impact assessors, procurers, AI governance and oversight professionals

AI customers, including AI users

AI partners, including AI system integrators and data providers

AI subjects, including data subjects and other subjects

Rationale for an AI Management System

AI systems consist not only of components using AI technology, but can use a variety of technologies and components.

Responsible development, provision and use of an AI system therefore requires taking into account **not only AI-specific considerations**, but also the **system as a whole** with all the organization, resources, processes, technologies and components that are used.

In other words, a Management System is needed !

Even for the AI technology specific part, other aspects besides AI-specific considerations should be taken into account. For example, as AI is an information processing technology, information security applies generally to it.

Objectives such as safety, security, privacy and environmental impact should be managed holistically and not separately for AI and the other components of the management system.

ISO/IEC 42001:2023

Information technology — Artificial intelligence — Management system

- Published 18th December, 2023
- Based on ISO **HS structure**, for the purpose of integrating with other MS standards' requirements within an Integrated Management System
- **Applicable to any organization**, regardless of size, type and nature, that **develops, provides** or **uses** products or services that utilize AI systems

Standards related to ISO/IEC 42001

ISO/IEC 22989:2022
Artificial intelligence concepts and terminology

ISO/IEC 23894:2023
Guidance on risk management

ISO/IEC TR 24368:2022
Overview of ethical and societal concerns

ISO/IEC 38507:2022
Governance implications of the use of artificial intelligence by organizations

ISO/IEC DIS 42006
Requirements for bodies providing audit and certification of artificial intelligence management systems

Definitions

AI system
Engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

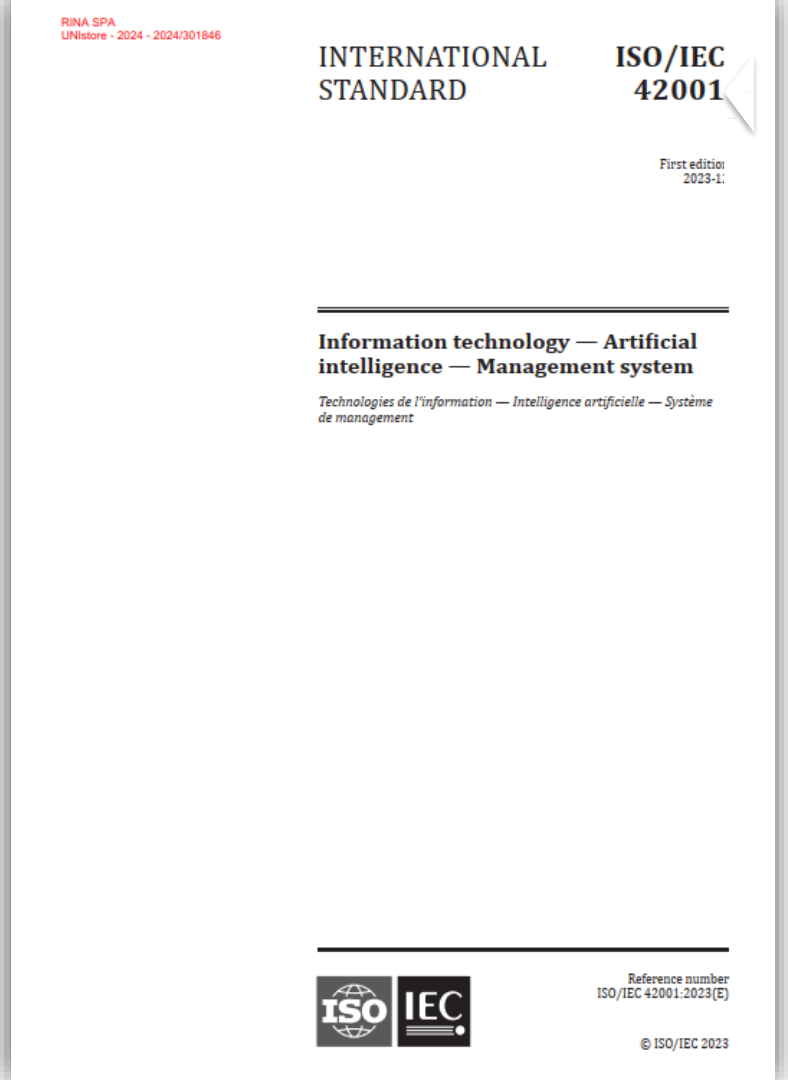
Management System
Set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives

Artificial Intelligence Management System (AIMS)
Set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives, in the provision, development or use of an AI system

Risk
Effect of uncertainty

Structure of the standard

1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
5 Leadership
6 Planning
7 Support
8 Operation
9 Performance evaluation
10 Improvement
Annex A Reference control objectives and controls
Annex B Implementation guidance for AI controls
Annex C Potential AI-related organizational objectives and risk sources
Annex D Use of the AI management system across domains or sectors



INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Reference number
ISO/IEC 42001:2023(E)

Life cycle of the AIMS

INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

Reference number
ISO/IEC 42001:2023(E)

Core elements of the AIMS

AI risk assessment

Identification and evaluation of the risks that may prevent achieving the AI objectives

AI risk treatment plan

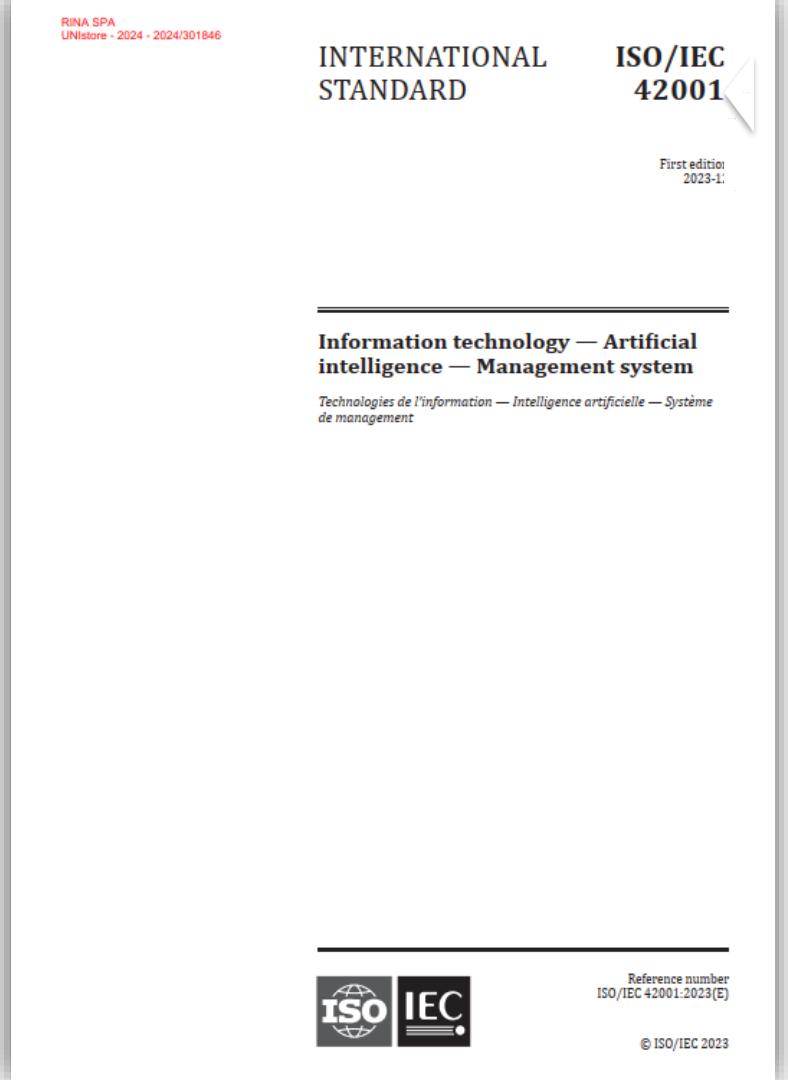
Determination of all needed controls that are necessary to prevent or mitigate the assessed risks

AI system impact assessment

Assessment of the potential consequences for individuals, group of individuals, and societies that can result from the development, provision or use of AI systems (ie.: on environment, economy, government, health & safety, traditions, culture and values)

Statement of Applicability (SoA)

Documentation of all necessary controls used for preventing or mitigating the risks for achieving the AI objectives (ref. Annex A)



INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

ISO IEC

Reference number
ISO/IEC 42001:2023(E)

Annex A

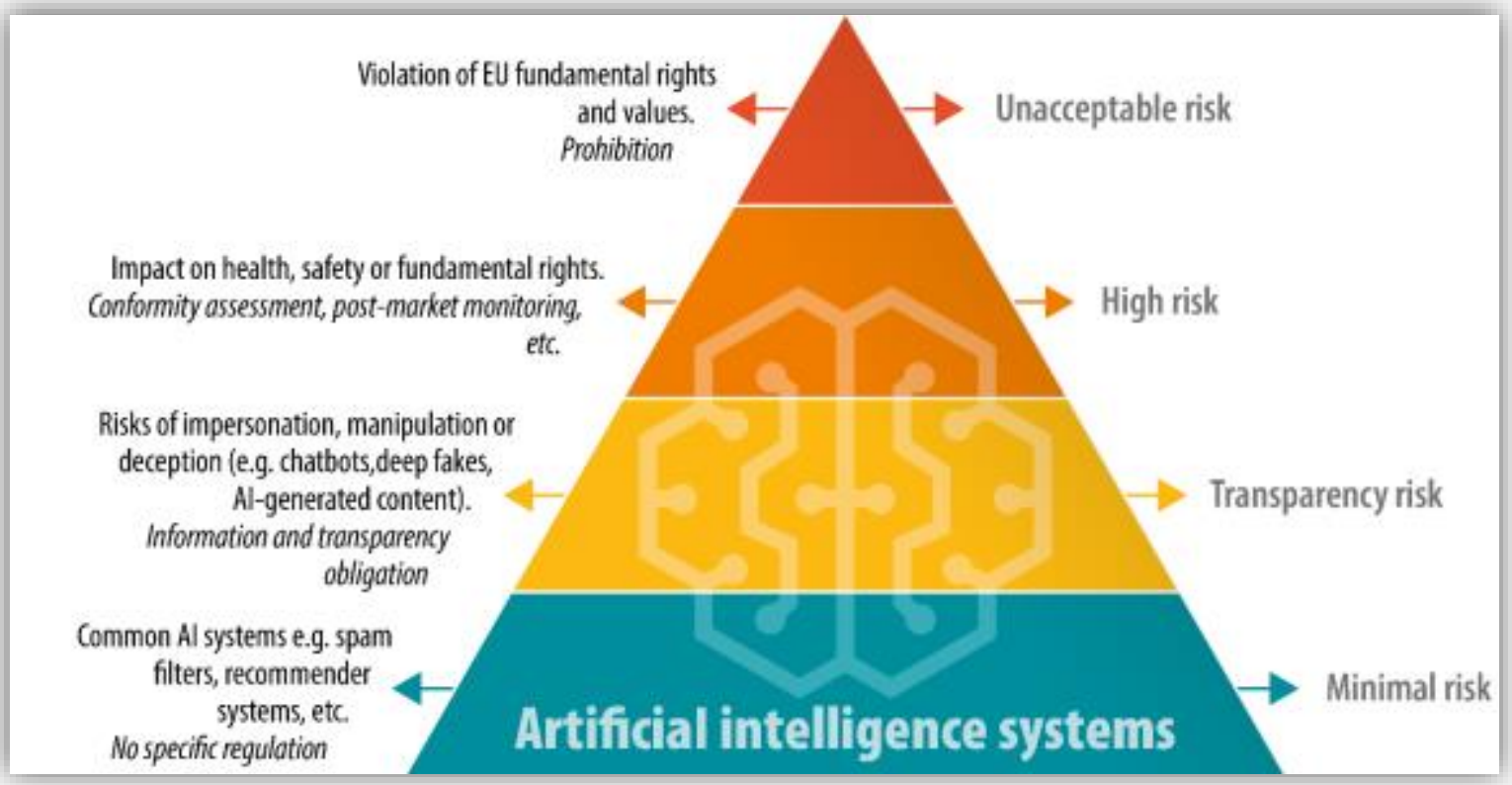
ID	CONTROL OBJECTIVE
A.2	Policies related to AI (3 controls)
A.3	Internal organization (2 controls)
A.4	Resources for the AI systems (5 controls)
A.5	Assessing impacts of AI systems (4 controls)
A.6	AI system life cycle (9 controls)
A.7	Data for AI systems (5 controls)
A.8	Information for interested parties of AI systems (4 controls)
A.9	Use of AI systems (3 controls)
A.10	Third-party and customer relationships (3 controls)

ISO/IEC 42001 vs. EU AI Act

The AI Act is the first binding worldwide horizontal regulation on AI, that sets a common framework for the use and supply of AI systems in the EU.
It offers a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'.

- AI systems presenting **unacceptable** risks are prohibited across the EU.
- H**igh-risk** AI systems are authorised, but subject to a set of requirements and obligations to gain access to the EU market.
- AI systems posing **limited** risk because of their lack of transparency will be subject to information and transparency requirements.
- AI systems presenting only **minimal** risk for people will not be subject to further obligations.

EU AI Act risk-based approach



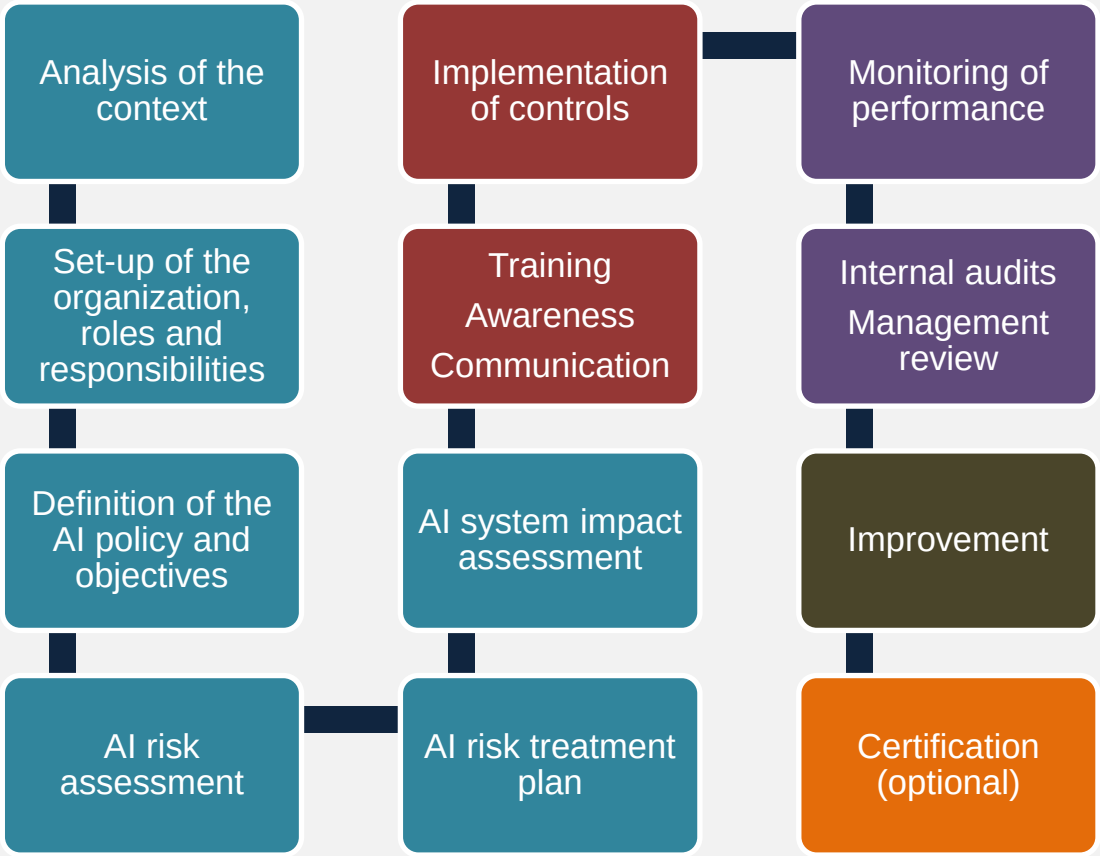
Source: European Parliament

High-risk AI systems

High-risk AI systems, that can have a detrimental impact on people's health, safety or on their fundamental rights, are subject to a set of requirements and obligations to gain access to the EU market:

- AI systems that are used in products falling under the EU's product safety legislation. This includes toys, aviation, cars, medical devices and lifts.
- AI systems falling into specific areas that will have to be registered in an EU database:
    - Management and operation of critical infrastructure
    - Education and vocational training
    - Employment, worker management and access to self-employment
    - Access to and enjoyment of essential private services and public services and benefits
    - Law enforcement
    - Migration, asylum and border control management
    - Assistance in legal interpretation and application of the law.

The road to conformity



Why adopt / certificate an AIMS ?

Regulation

An AIMS helps Organisations to comply with local and international laws and rules, preventing sanctions and fines

Reputation

Customers like transparent and reliable Organisations

Saving

The responsible, secure and efficient adoption of AI helps saving money and resources

Performance

An AIMS supports the continuous improvement of processes

Attractivity

Modern, reliable, efficient and sustainable Organisations attract partnerships and investments

Public procurement

A (certified) AIMS leads to a better positioning in public tendering

For more info:

Thank you for your attention

danilo.diomede@rina.org

Our experience. Your growth.