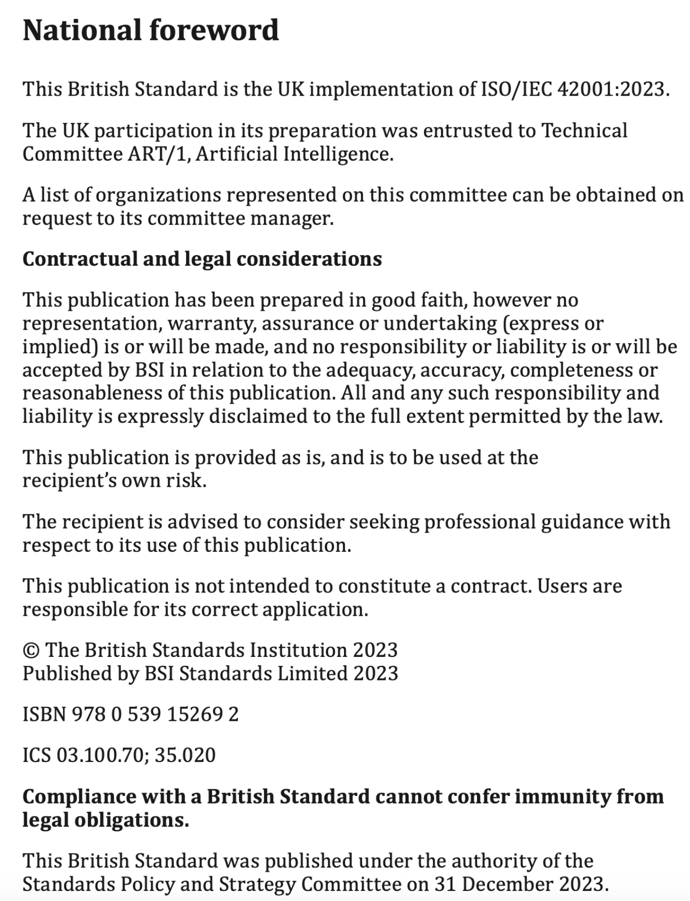
The Anatomy of ISO 42001

SCSD Lecture 1 Feb 2024

The Foreword



National foreword

This British Standard is the UK implementation of ISO/IEC 42001:2023.

The UK participation in its preparation was entrusted to Technical Committee ART/1, Artificial Intelligence.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 15269 2

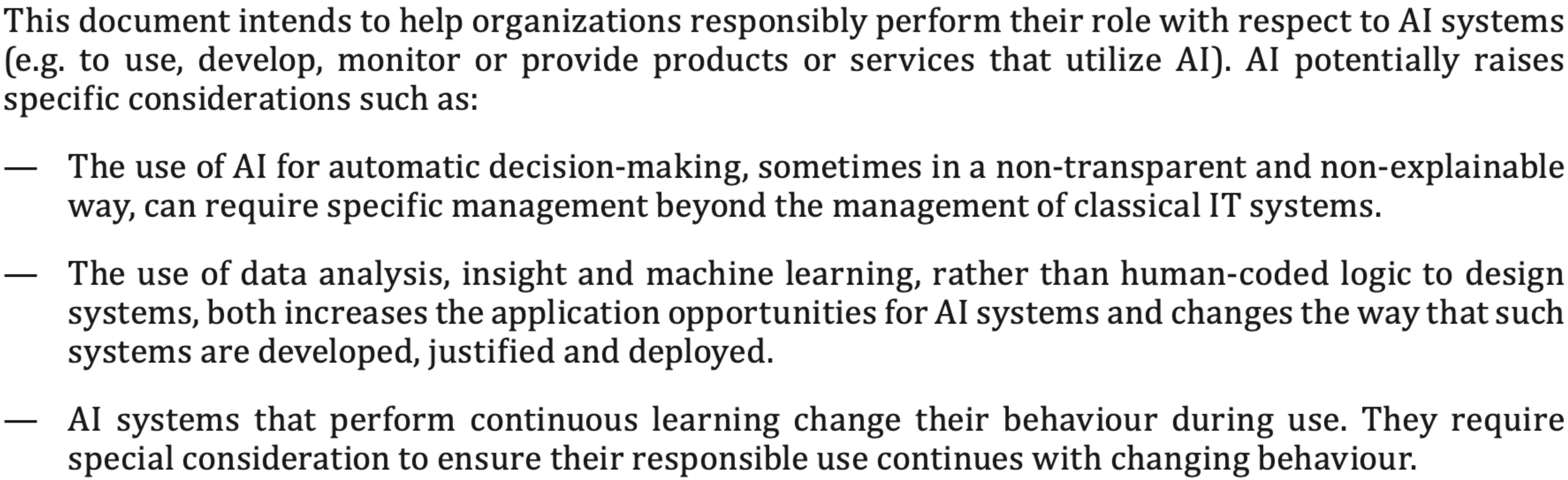
ICS 03.100.70; 35.020

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2023.

- No responsibility, liability, etc
- Users take the risk
- Who is a ”professional”?
- What is “correct application”?

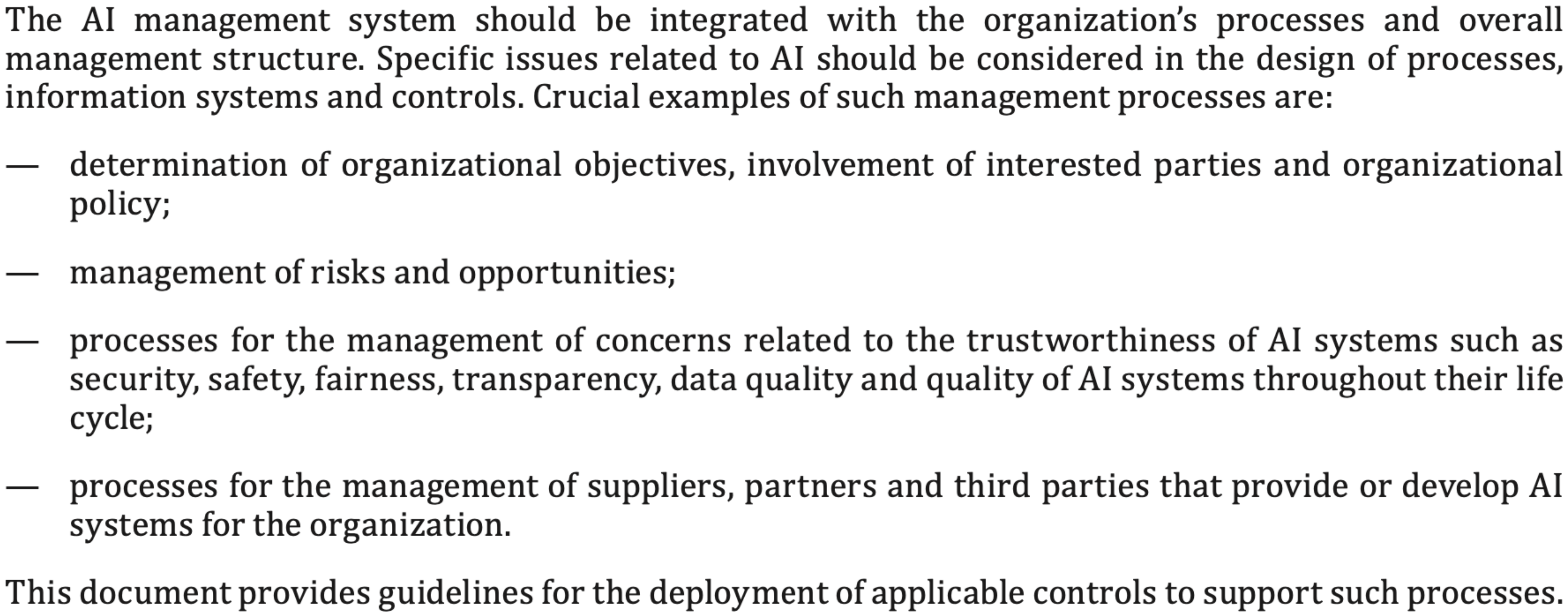
How should it help us?



This document intends to help organizations responsibly perform their role with respect to AI systems (e.g. to use, develop, monitor or provide products or services that utilize AI). AI potentially raises specific considerations such as:

- The use of AI for automatic decision-making, sometimes in a non-transparent and non-explainable way, can require specific management beyond the management of classical IT systems.
- The use of data analysis, insight and machine learning, rather than human-coded logic to design systems, both increases the application opportunities for AI systems and changes the way that such systems are developed, justified and deployed.
- AI systems that perform continuous learning change their behaviour during use. They require special consideration to ensure their responsible use continues with changing behaviour.

It should help with processes



The AI management system should be integrated with the organization’s 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 organizational objectives, involvement of interested parties and organizational 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 organization.

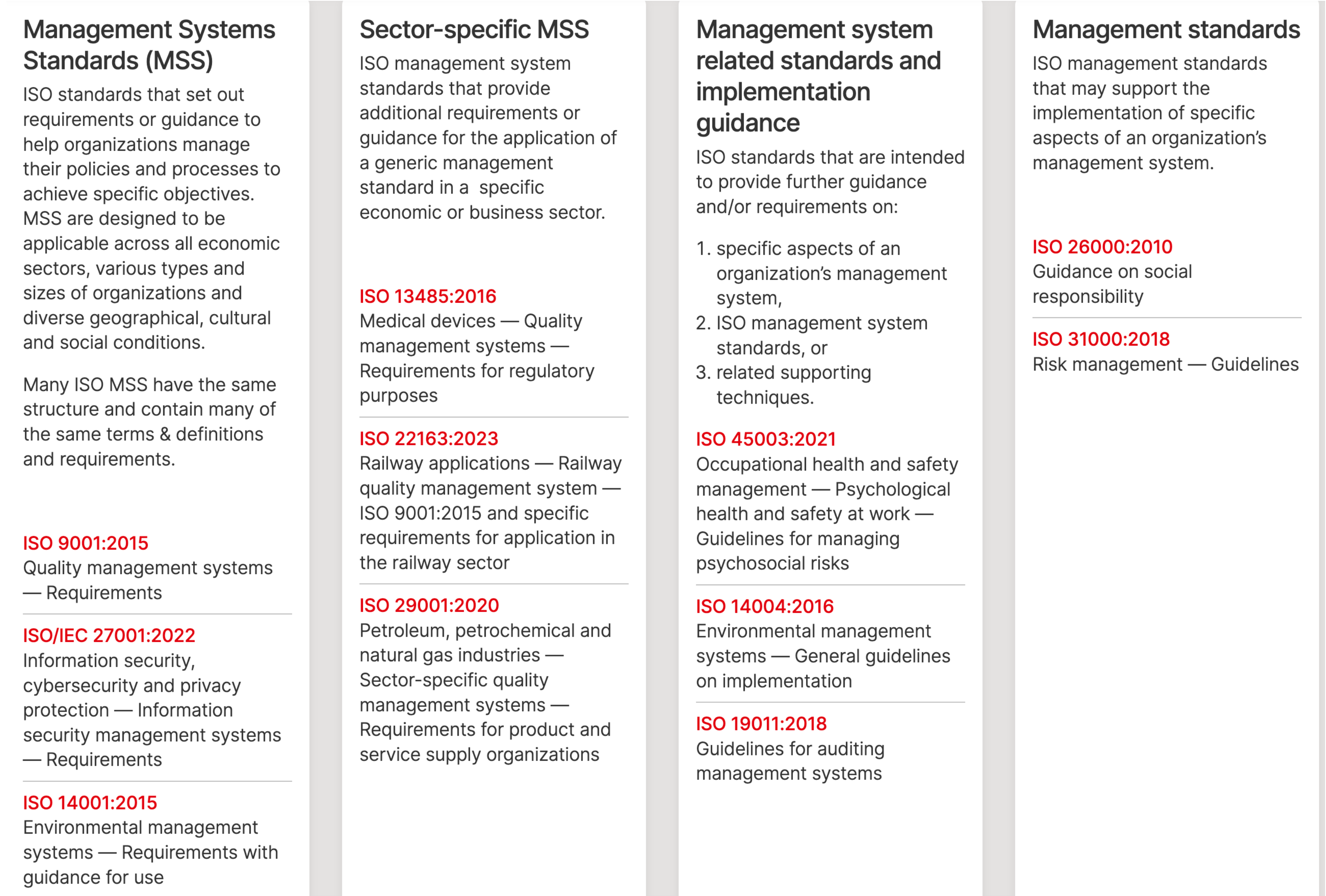
This document provides guidelines for the deployment of applicable controls to support such processes.

What does this mean?

- The first point relates to requirements on the process: why are you using AI at all? What is the aim of the organization? Who are the stakeholders?
- Risk management is an essential aspect of any process management system (and there is a generic approach to it that gets specialized).
- The next point is a list of “concerns” around others – can you think of others?
- The final point raises the issue of the ”AI supply chain” what does it look like and who is involved in creating and deploying models.

Compatibility with other management system standards

This document applies the harmonized structure (identical clause numbers, clause titles, text and common terms and core definitions) developed to enhance alignment among management system standards (MSS). The AI management system provides requirements specific to managing the issues and risks arising from using AI in an organization. This common approach facilitates implementation and consistency with other management system standards, e.g. related to quality, safety, security and privacy.



Management Systems Standards (MSS)

ISO standards that set out requirements or guidance to help organizations manage their policies and processes to achieve specific objectives. MSS are designed to be applicable across all economic sectors, various types and sizes of organizations and diverse geographical, cultural and social conditions.

Many ISO MSS have the same structure and contain many of the same terms & definitions and requirements.

ISO 9001:2015
Quality management systems — Requirements

ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO 14001:2015
Environmental management systems — Requirements with guidance for use

Sector-specific MSS

ISO management system standards that provide additional requirements or guidance for the application of a generic management standard in a specific economic or business sector.

ISO 13485:2016
Medical devices — Quality management systems — Requirements for regulatory purposes

ISO 22163:2023
Railway applications — Railway quality management system — ISO 9001:2015 and specific requirements for application in the railway sector

ISO 29001:2020
Petroleum, petrochemical and natural gas industries — Sector-specific quality management systems — Requirements for product and service supply organizations

Management system related standards and implementation guidance

ISO standards that are intended to provide further guidance and/or requirements on:

1. specific aspects of an organization's management system,
2. ISO management system standards, or
3. related supporting techniques.

ISO 45003:2021
Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks

ISO 14004:2016
Environmental management systems — General guidelines on implementation

ISO 19011:2018
Guidelines for auditing management systems

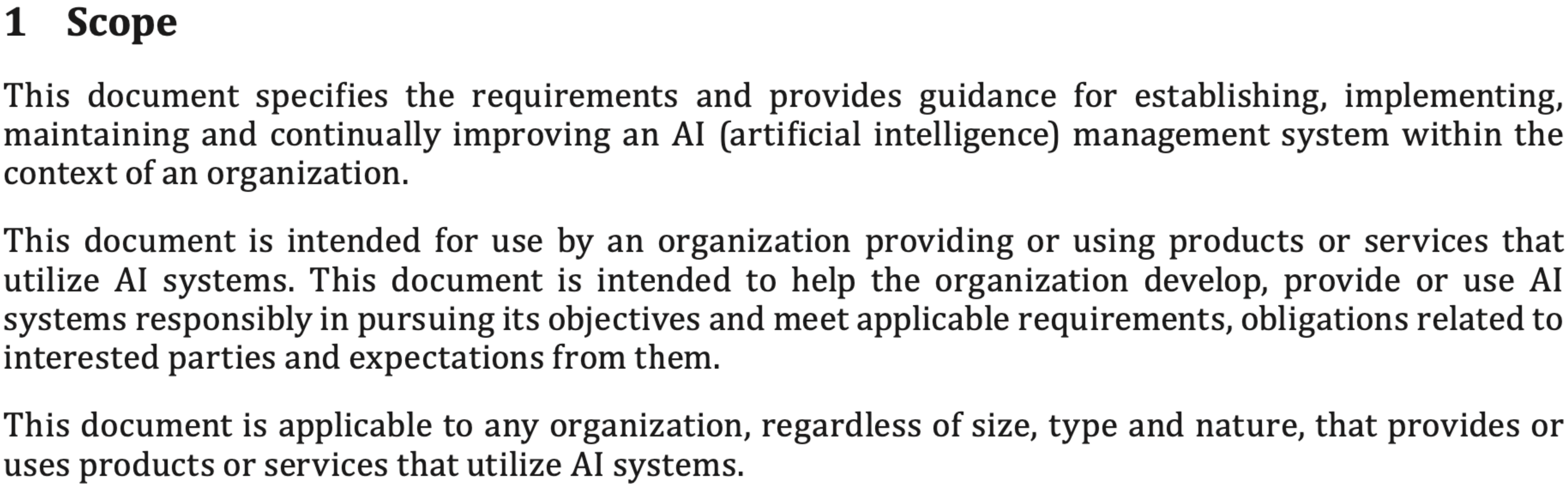
Management standards

ISO management standards that may support the implementation of specific aspects of an organization's management system.

ISO 26000:2010
Guidance on social responsibility

ISO 31000:2018
Risk management — Guidelines

The **scope** tells you what the standard is for



1 Scope

This document specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI (artificial intelligence) management system within the context of an organization.

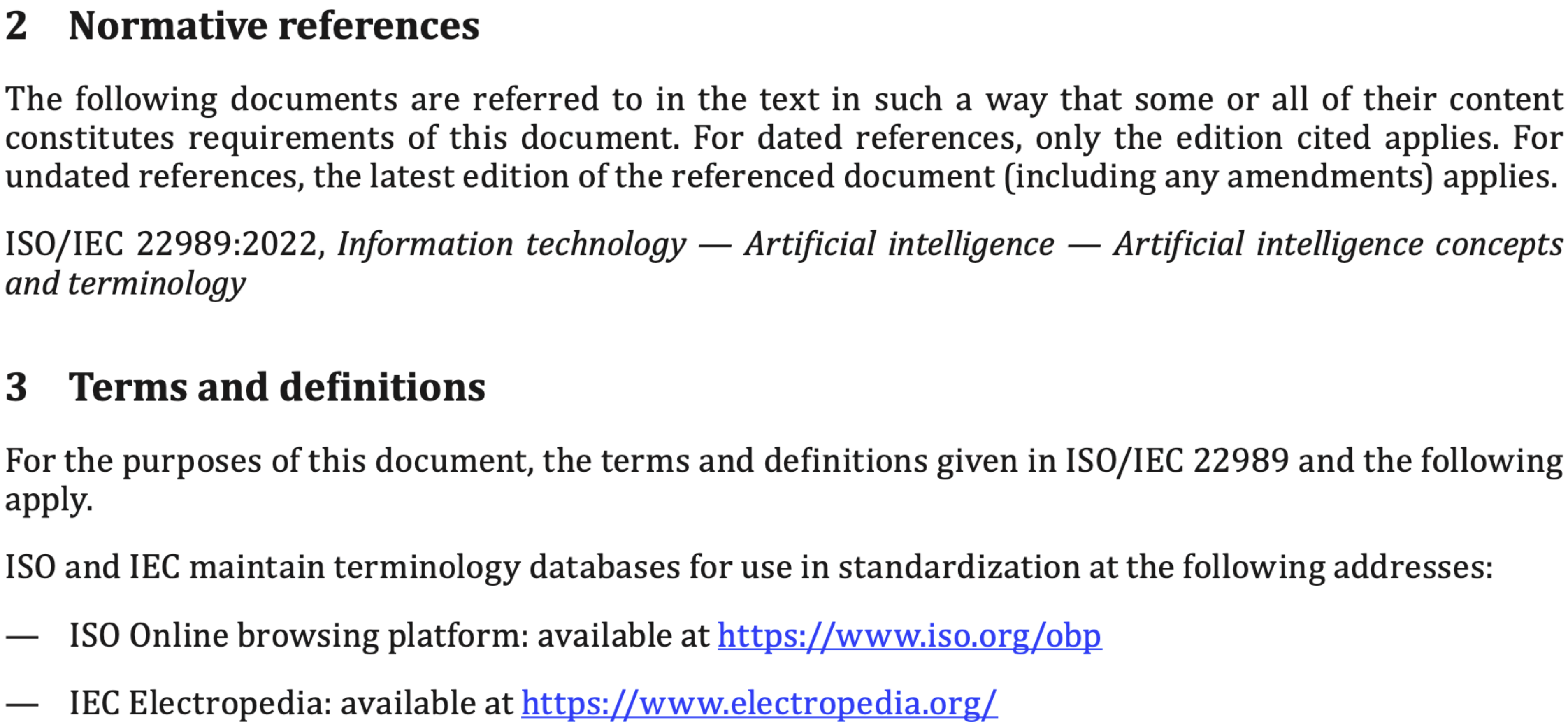
This document is intended for use by an organization providing or using products or services that utilize AI systems. This document is intended to help the organization develop, provide or use AI systems responsibly in pursuing its objectives and meet applicable requirements, obligations related to interested parties and expectations from them.

This document is applicable to any organization, regardless of size, type and nature, that provides or uses products or services that utilize AI systems.

What is the scope telling you

- **What:** the standard sets out to do: “*This documents specifies the requirements….*”
- **Who***:* the standard sets out who should be interested in using the standard: “*intended for use by an organization providing or using products or services that utilize AI systems.*”

Other standards, and terminology



2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22989:2022, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

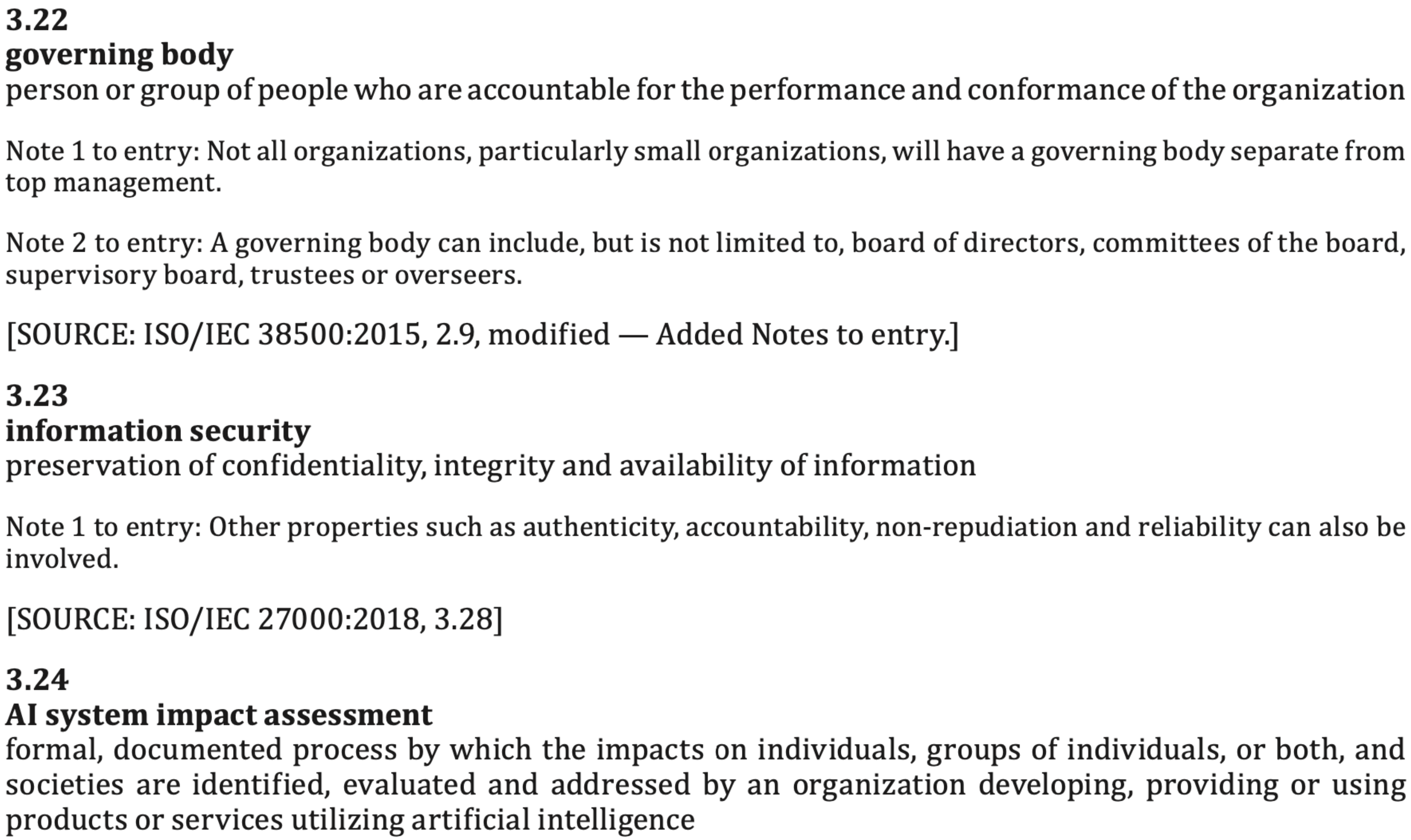
3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22989 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

Terminology



3.22
governing body
person or group of people who are accountable for the performance and conformance of the organization

Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management.

Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees or overseers.

[SOURCE: ISO/IEC 38500:2015, 2.9, modified — Added Notes to entry.]

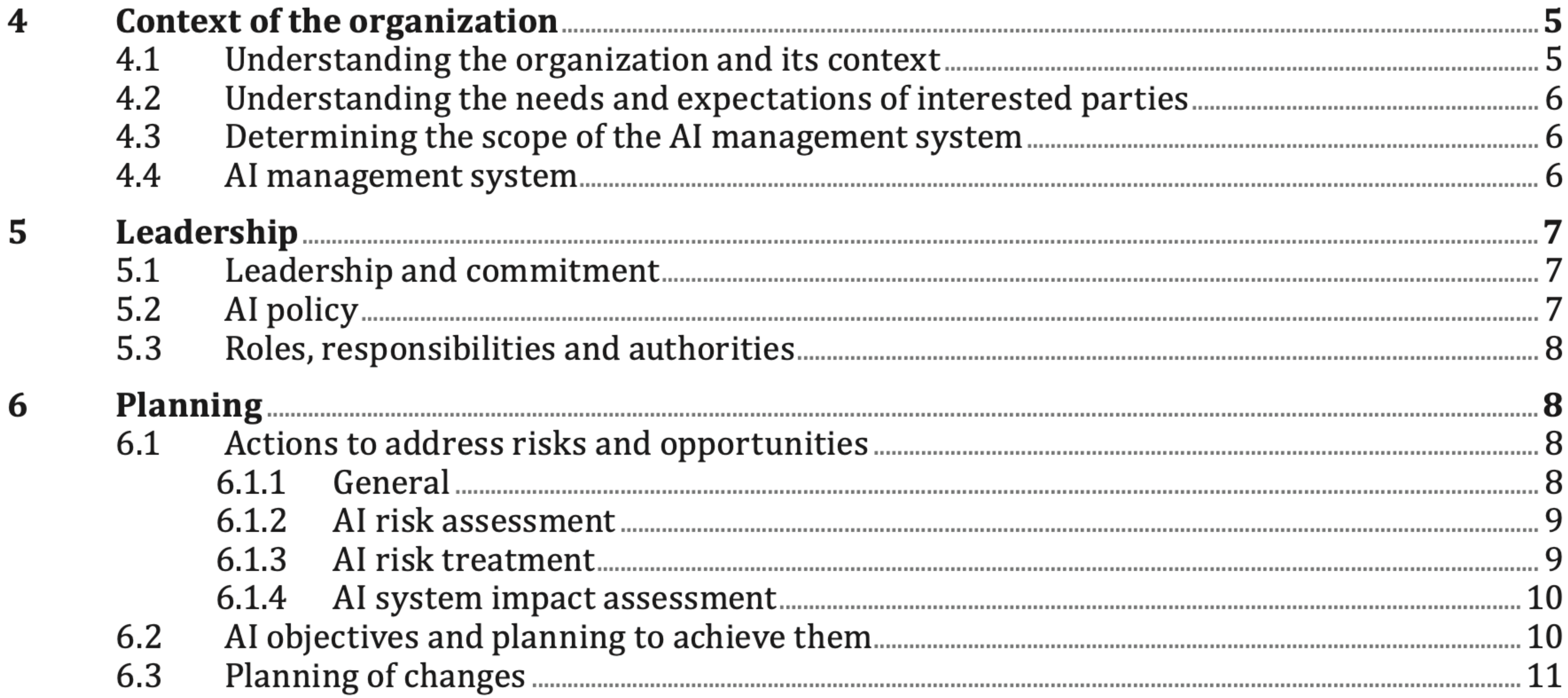
3.23
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: Other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

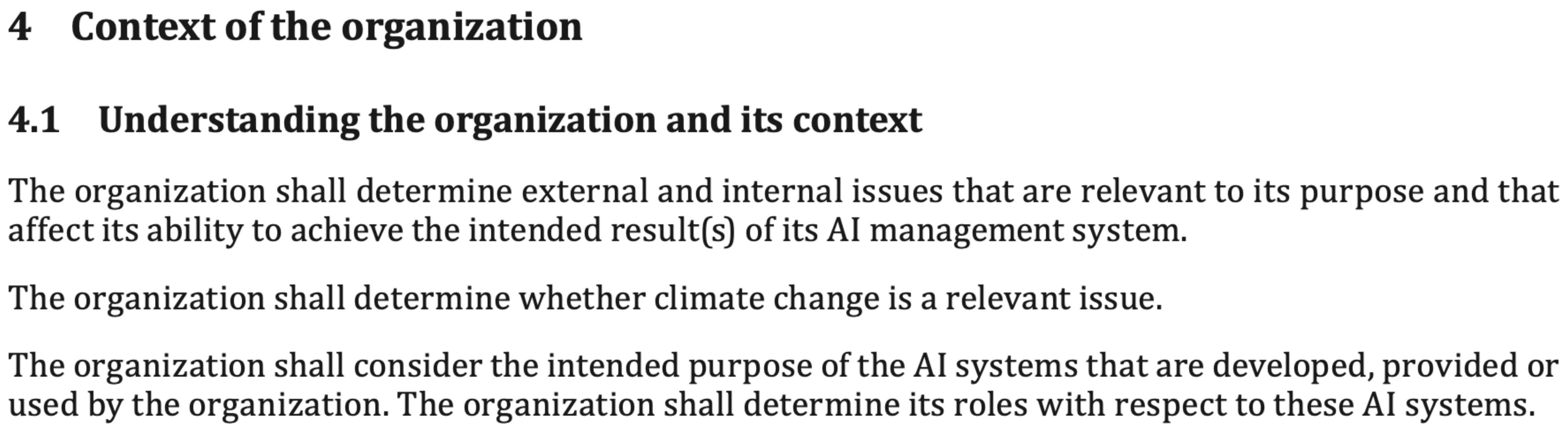
[SOURCE: ISO/IEC 27000:2018, 3.28]

3.24
AI system impact assessment
formal, documented process by which the impacts on individuals, groups of individuals, or both, and societies are identified, evaluated and addressed by an organization developing, providing or using products or services utilizing artificial intelligence

Main body of the standard



Requirements



4 Context of the organization

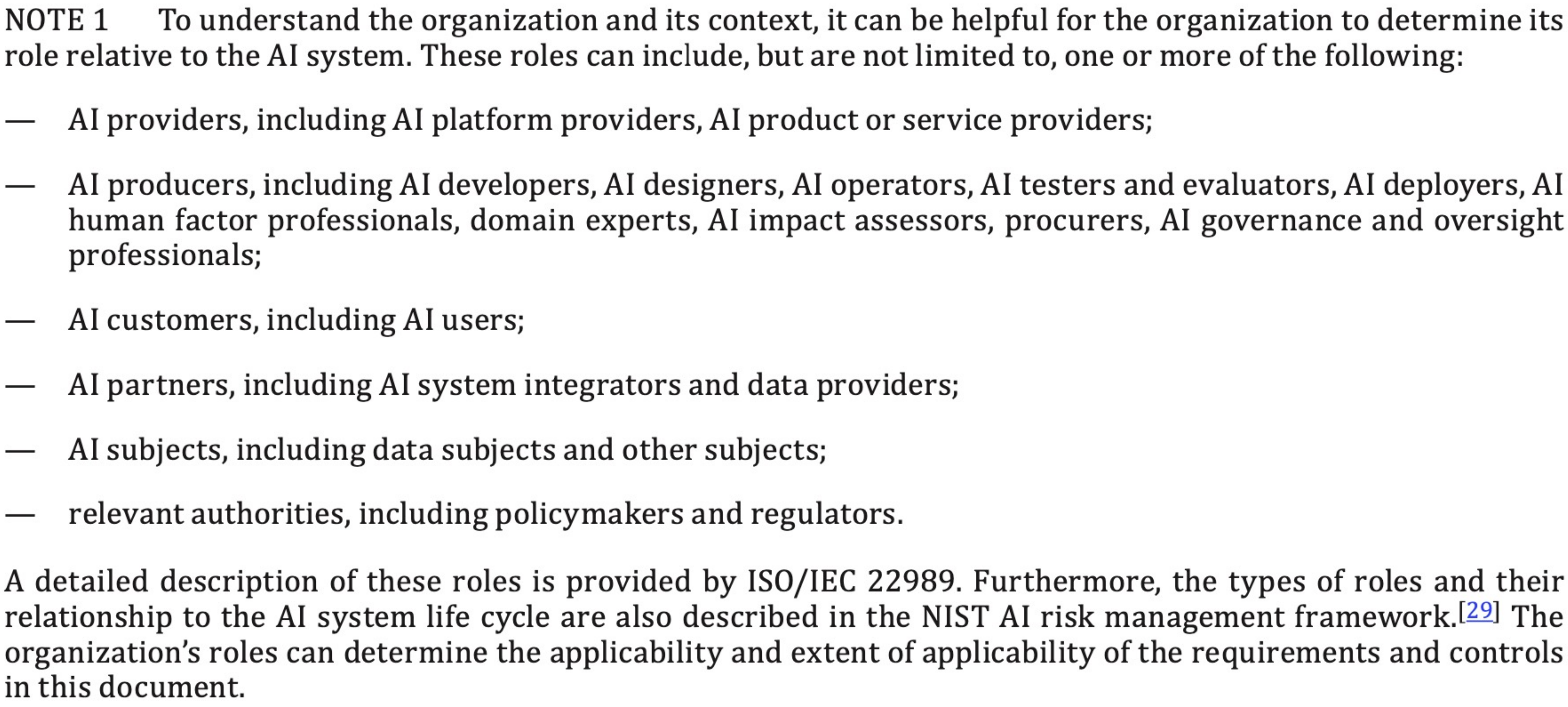
4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its AI management system.

The organization shall determine whether climate change is a relevant issue.

The organization shall consider the intended purpose of the AI systems that are developed, provided or used by the organization. The organization shall determine its roles with respect to these AI systems.

Explanatory notes



NOTE 1 To understand the organization and its context, it can be helpful for the organization to determine its role relative to the AI system. These roles can include, but are not limited to, one or more of the following:

— 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;

— relevant authorities, including policymakers and regulators.

A detailed description of these roles is provided by ISO/IEC 22989. Furthermore, the types of roles and their relationship to the AI system life cycle are also described in the NIST AI risk management framework.[29] The organization's roles can determine the applicability and extent of applicability of the requirements and controls in this document.

Referring to Standards

- BS EN ISO/IEC 22989:2023
- Information technology — Artificial intelligence — Artificial intelligence concepts and terminology

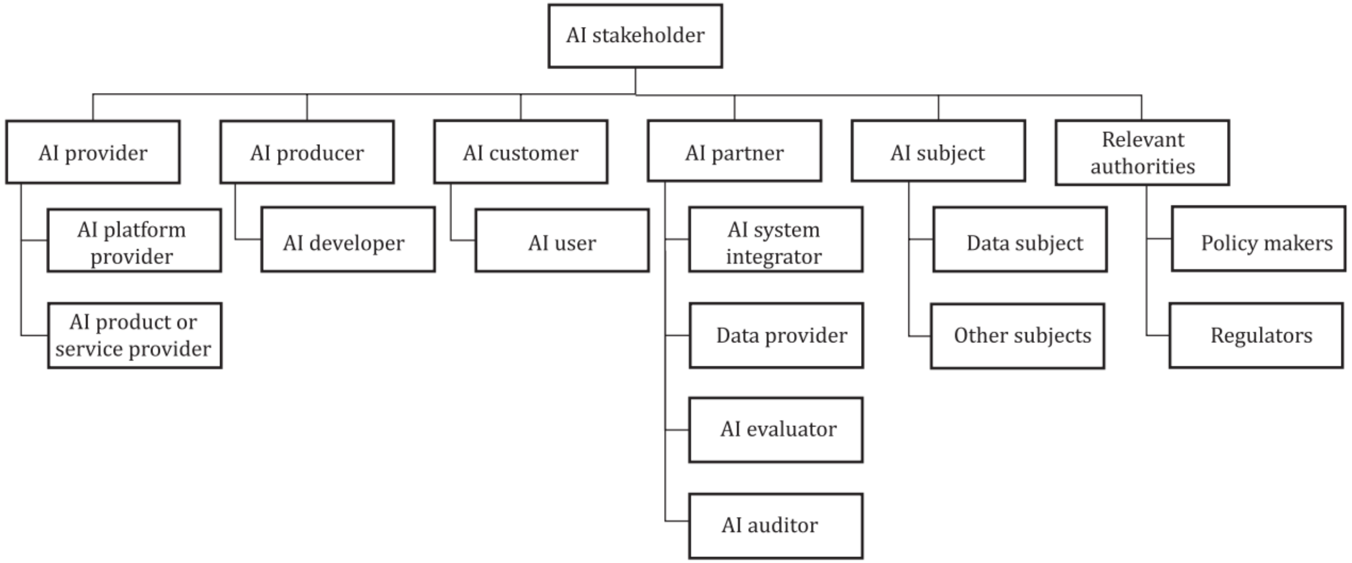
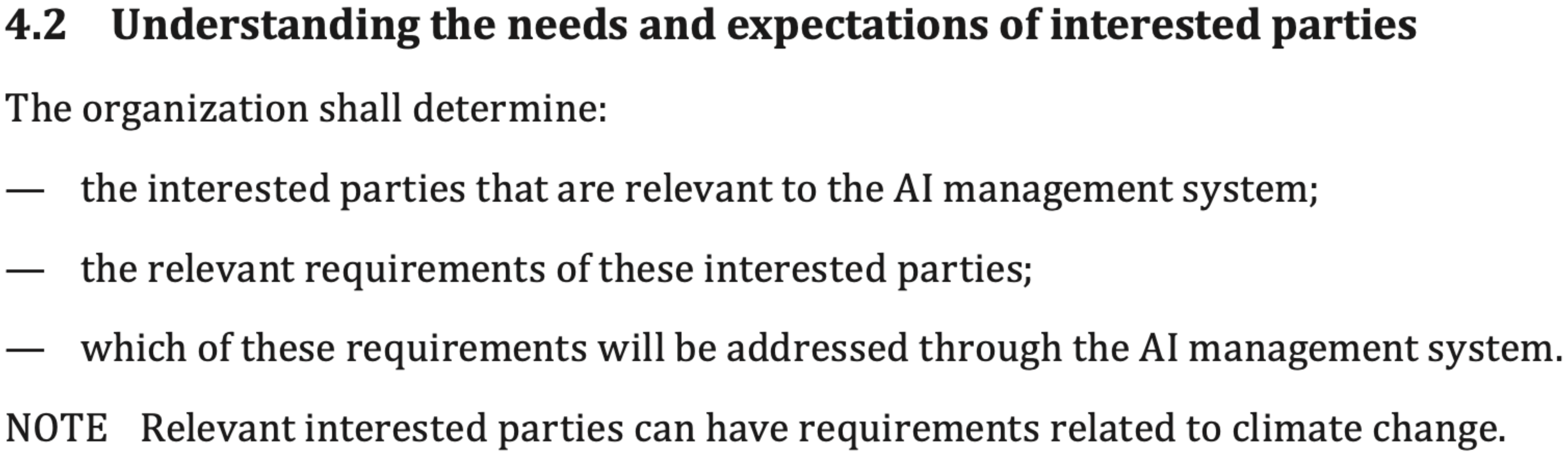


Figure 2 — AI stakeholder roles and their sub-roles

Testable?



4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

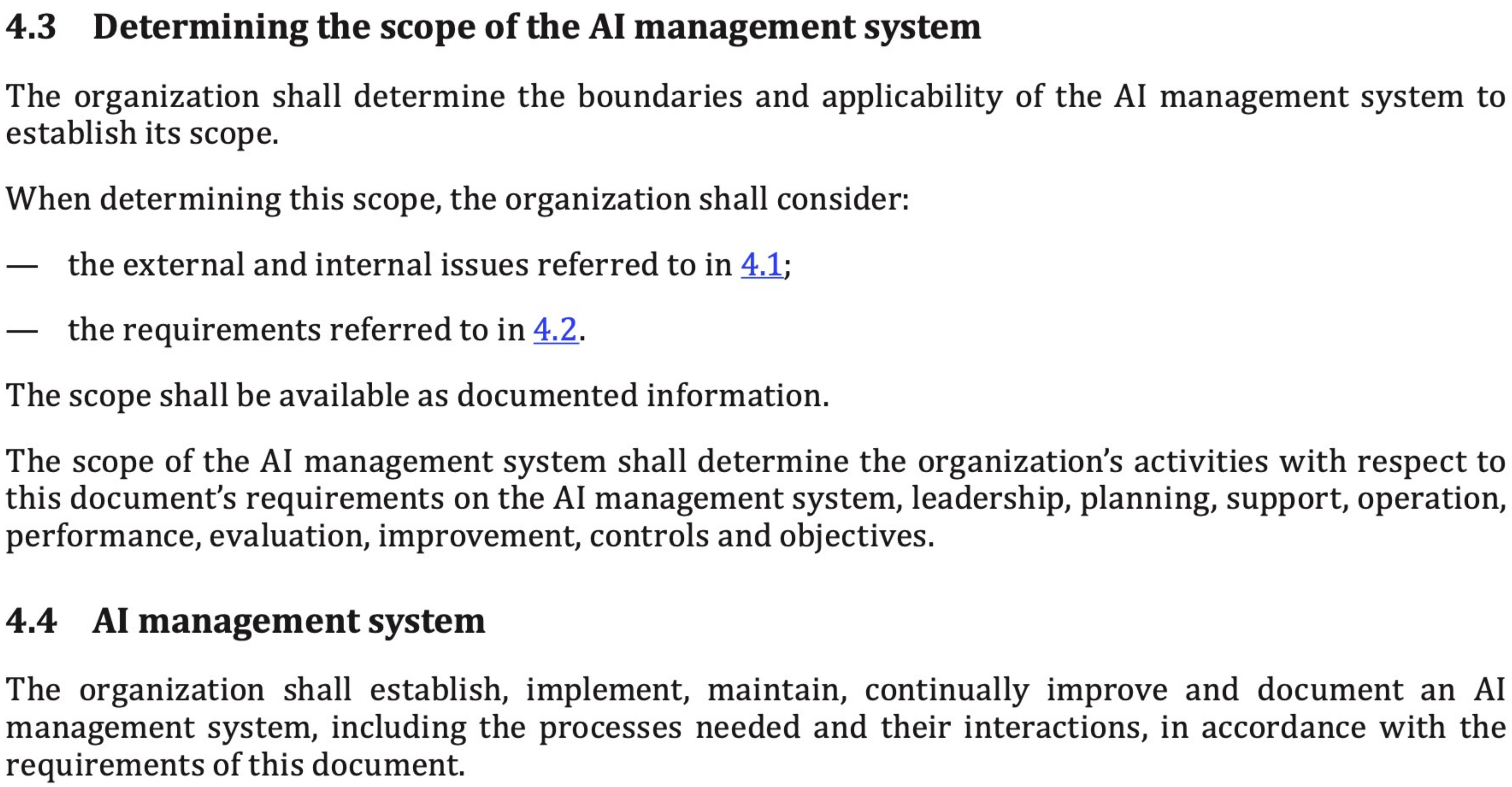
— the interested parties that are relevant to the AI management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the AI management system.

NOTE Relevant interested parties can have requirements related to climate change.

Documentation



4.3 Determining the scope of the AI management system

The organization shall determine the boundaries and applicability of the AI management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

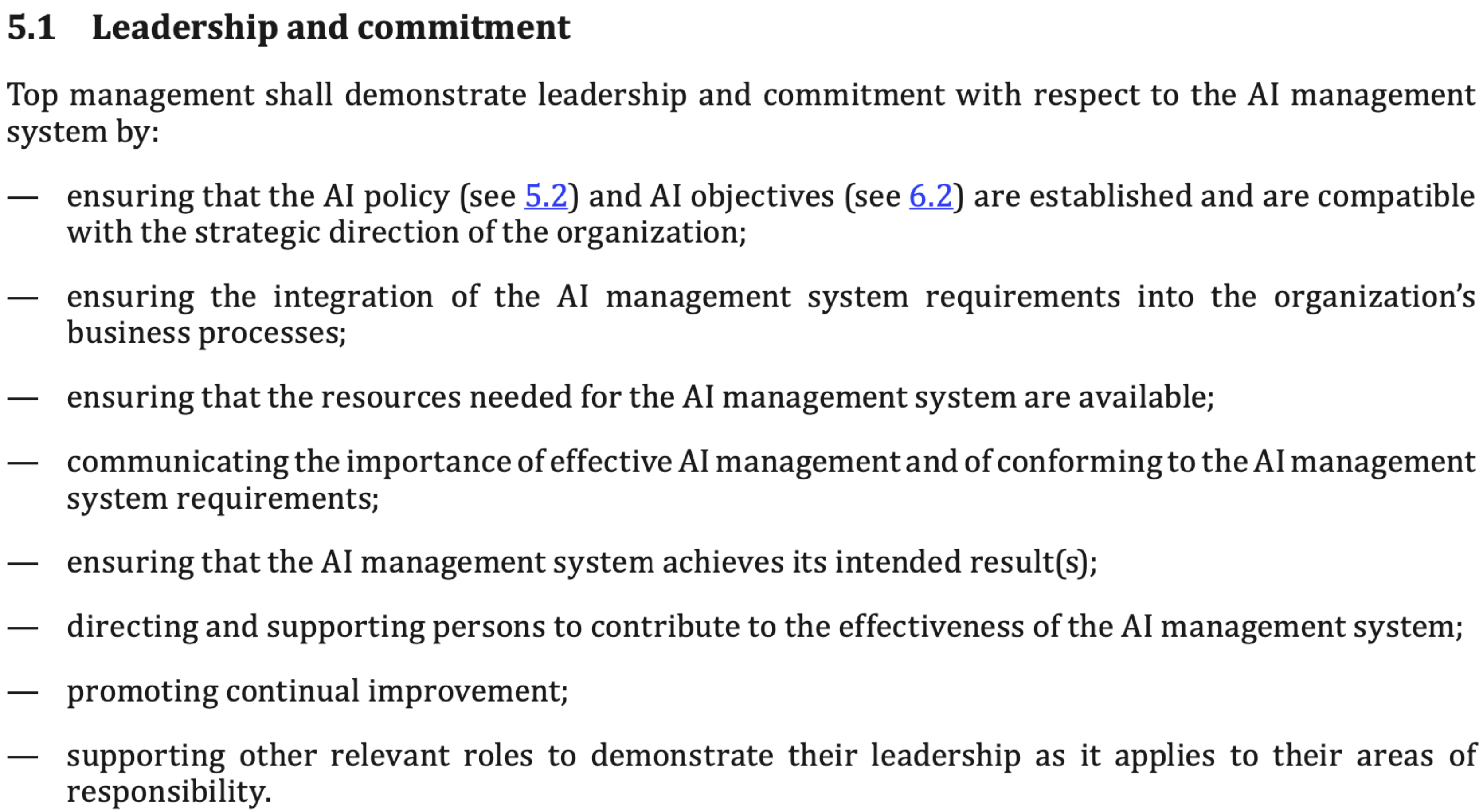
The scope shall be available as documented information.

The scope of the AI management system shall determine the organization's activities with respect to this document's requirements on the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives.

4.4 AI management system

The organization shall establish, implement, maintain, continually improve and document an AI management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Organizational perspective

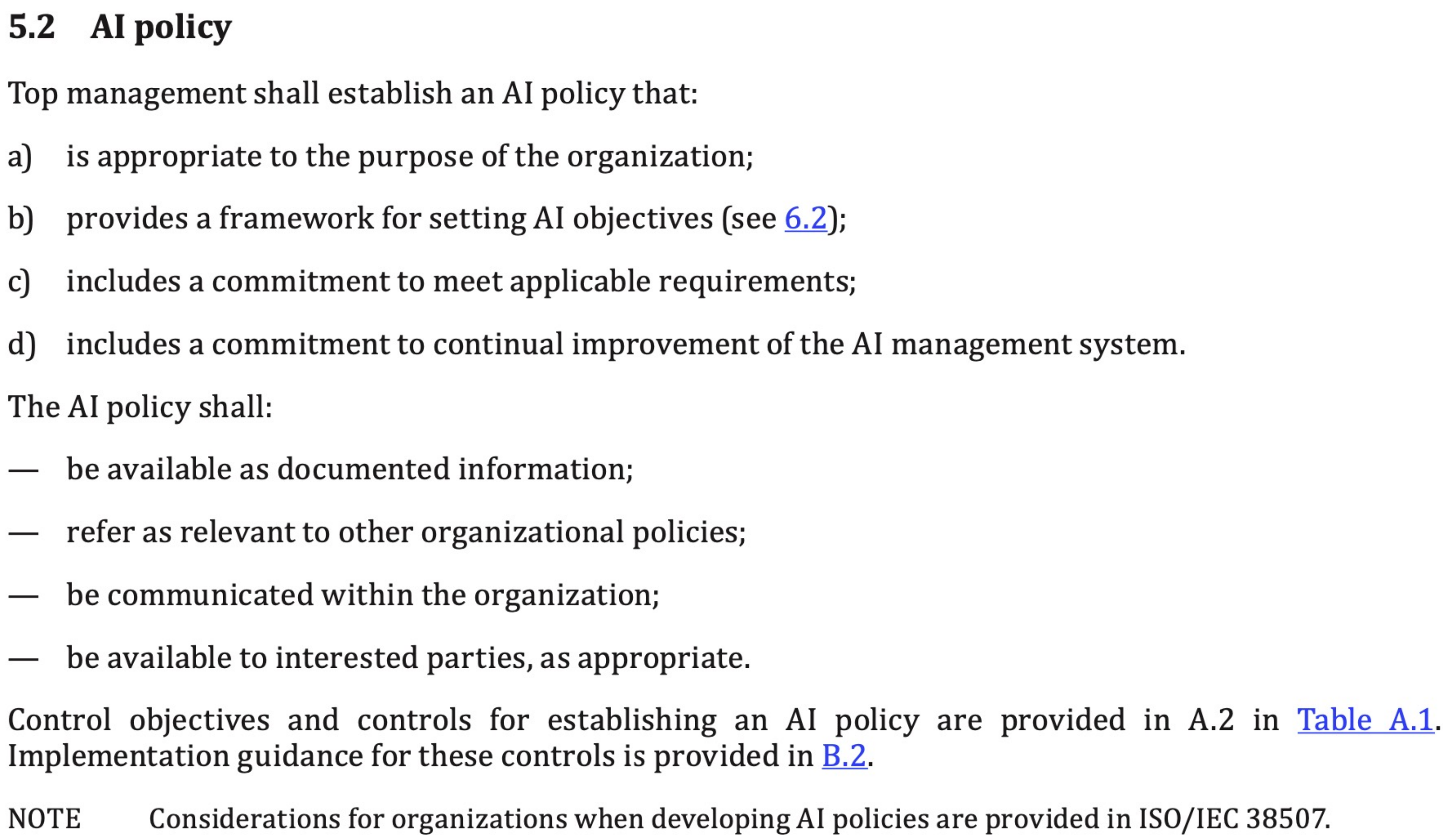


5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the AI management system by:

- ensuring that the AI policy (see 5.2) and AI objectives (see 6.2) are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the AI management system requirements into the organization's business processes;
- ensuring that the resources needed for the AI management system are available;
- communicating the importance of effective AI management and of conforming to the AI management system requirements;
- ensuring that the AI management system achieves its intended result(s);
- directing and supporting persons to contribute to the effectiveness of the AI management system;
- promoting continual improvement;
- supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

Organisational Policy



5.2 AI policy

Top management shall establish an AI policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting AI objectives (see 6.2);

c) includes a commitment to meet applicable requirements;

d) includes a commitment to continual improvement of the AI management system.

The AI policy shall:

— be available as documented information;

— refer as relevant to other organizational policies;

— be communicated within the organization;

— be available to interested parties, as appropriate.

Control objectives and controls for establishing an AI policy are provided in A.2 in Table A.1. Implementation guidance for these controls is provided in B.2.

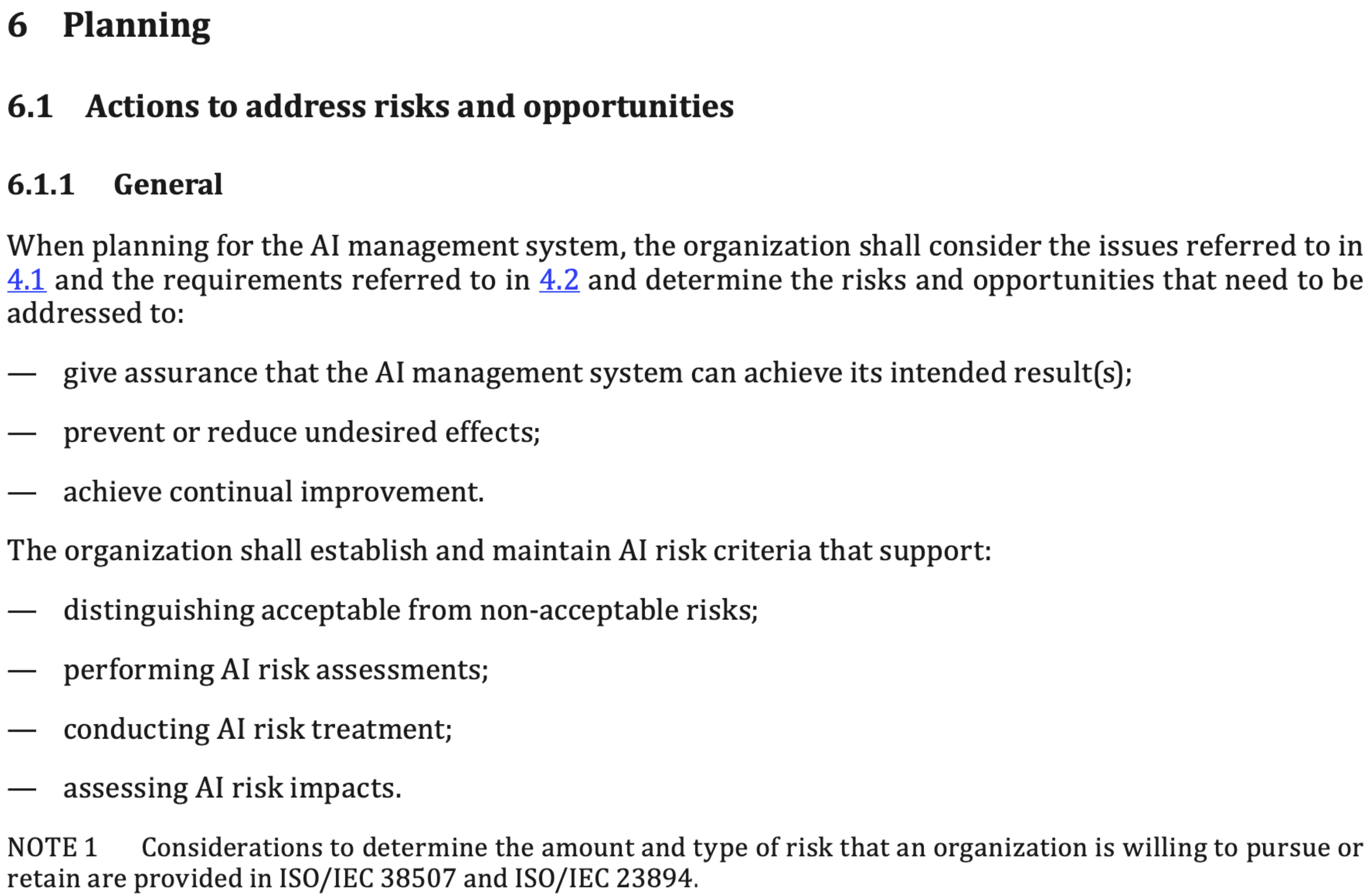
NOTE Considerations for organizations when developing AI policies are provided in ISO/IEC 38507.

BS ISO/IEC 38507:2022

BSI Standards Publication

Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

Planning



6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the AI management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

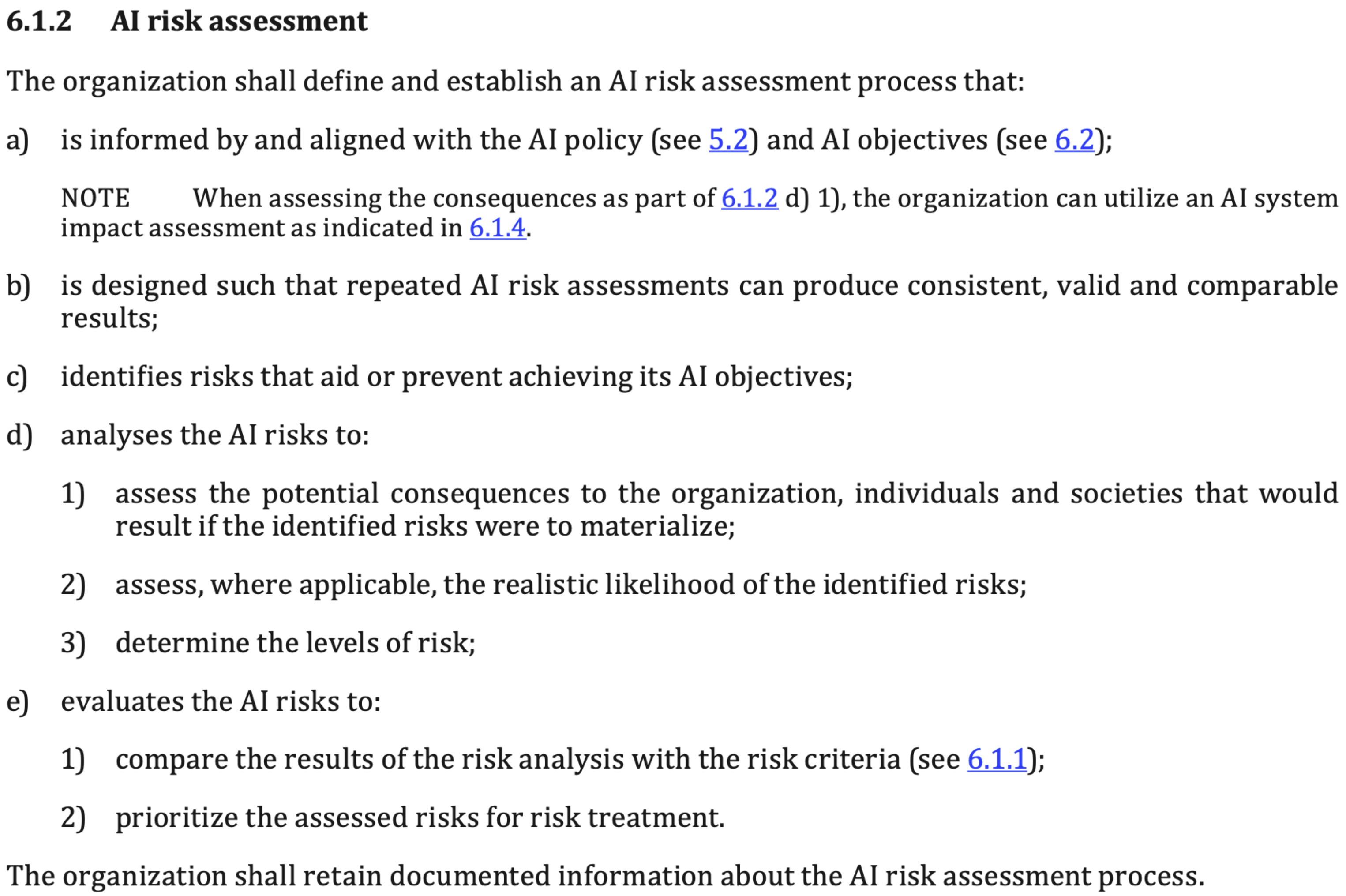
- give assurance that the AI management system can achieve its intended result(s);
- prevent or reduce undesired effects;
- achieve continual improvement.

The organization shall establish and maintain AI risk criteria that support:

- distinguishing acceptable from non-acceptable risks;
- performing AI risk assessments;
- conducting AI risk treatment;
- assessing AI risk impacts.

NOTE 1 Considerations to determine the amount and type of risk that an organization is willing to pursue or retain are provided in ISO/IEC 38507 and ISO/IEC 23894.

Risk



6.1.2 AI risk assessment

The organization shall define and establish an AI risk assessment process that:

a) is informed by and aligned with the AI policy (see 5.2) and AI objectives (see 6.2);

NOTE When assessing the consequences as part of 6.1.2 d) 1), the organization can utilize an AI system impact assessment as indicated in 6.1.4.

b) is designed such that repeated AI risk assessments can produce consistent, valid and comparable results;

c) identifies risks that aid or prevent achieving its AI objectives;

d) analyses the AI risks to:

1) assess the potential consequences to the organization, individuals and societies that would result if the identified risks were to materialize;

2) assess, where applicable, the realistic likelihood of the identified risks;

3) determine the levels of risk;

e) evaluates the AI risks to:

1) compare the results of the risk analysis with the risk criteria (see 6.1.1);

2) prioritize the assessed risks for risk treatment.

The organization shall retain documented information about the AI risk assessment process.

Summary

- Although we have looked at ISO 42001 this lecture has started to look at the general structure of management/quality standards.
- Standards generally avoid legally binding commitments
- Standards often sit inside closely related standards
- Standards attempt to have focused scope and refer to other standards.
- Standards requirements should be testable
- Standards often mandate documentation of policies, assessments, plans, …
- Risk is a key concept in planning