ISO/IEC xxxxx:202x
Information technology – Artificial intelligence – High-level framework and guidance for the development of conformity assessment schemes for AI systems

Draft 5, 2024-06-02

Foreword

DRAFTING NOTE: Use ISO standards template.

Contents

Introduction

DRAFTING NOTE: The paragraphs of the Introduction are numbered in this draft for ease of referencing when making comments. The numbering will be removed prior to publication.

0.1 This document provides a high-level framework and guidance for the development and operation of conformity assessment schemes, including certification schemes, for artificial intelligence (AI) systems.

0.2 This document is based on:

a) generic horizontal guidance and requirements for internationally accepted and adopted conformity assessment practice developed by the ISO Policy Development Committee on Conformity Assessment (CASCO) on behalf of ISO and IEC; and

b) specific guidance and requirements for conformity assessment for the information technology sector developed by the ISO/IEC Joint Technical Committee 1 Information technology (JTC1) and its subcommittees.

0.3 The intended audience for this document is primarily conformity assessment scheme developers, owners and operators that evaluate, test, assess and certify AI systems. Conformity assessment scheme owners and operators include, but are not limited to:

a) governments and regulators;

b) industry and professional bodies and associations;

c) procurement and purchasing agencies;

d) non-government organizations;

e) consumer organizations; and

f) bodies undertaking conformity assessment activities.

0.4 This document is also useful for organizations and people that are not scheme owners or operators, such as conformity assessment practitioners and AI system stakeholders including AI system developers, providers, customers, partners and regulatory authorities.

0.5 To be relevant and useful, conformity assessment schemes for AI systems take into account legislative and regulatory compliance requirements that apply wherever the AI system(s) are developed or used.

0.6 Conformity assessment schemes for AI systems may incorporate conformity assessment results related to:

a) fulfilment by the AI system of product, process and service requirements (e.g. product certification); and

b) the fulfilment by the user of the AI system of management system requirements (e.g. management system certification).

0.7 The provisions of conformity assessment schemes can require relevant AI stakeholder(s) (including interested parties) that use AI systems to fulfil management system requirements, for example, but not limited to:
- ISO/IEC 42001: Artificial Intelligence Management Systems (AIMS)
- ISO/IEC 9001: Quality Management Systems (QMS)
- ISO/IEC 20000: Information Technology Service Management Systems (ITSMS)
- ISO/IEC 27001: Information Security Management Systems (ISMS)
- ISO/IEC 27701: Privacy Information Management Systems (PIMS)
- ISO 37301: Compliance Management Systems (CMS)
- ISO 13485: Medical devices quality management systems (MDQMS)

0.8 A conformity assessment scheme that includes product certification and management system certification for AI systems that specifically leverages ISO/IEC 42001 can be referred to as a 'joint certification' model.

DRAFTING NOTE: The label 'joint certification' has drawn commentary from some conformity assessment colleagues. The views expressed include, but are not limited to:

a) support for the concept, especially on the understanding that when it comes to trust in the safe development, provision and use of an AI system, the strongest combination is the certification of the AI system itself as the 'product', (product certification by a product certification body conforming with ISO/IEC 17065) and certification of the 'AI management system of the organization' that is developing/providing/using the AI system (management system certification by a management system certification body conformity with ISO/IEC 17021-1 – ISO/IEC 42006);

b) a view pointing to the fact that in many long standing product certification schemes, assessment of management system requirements is already incorporated within the product certification scheme requirements and are an integral component of normal assessment processes that results in a product certification – i.e. there is no need to confuse the market with the new label of 'joint certification' because the same outcome is already achieved under the existing 'label' of 'product certification', assuming the product certification scheme includes assessment to management system requirements. FURTHER DRAFTING NOTE: It is noted 'joint certification' is just a label and we don't have to call it that. The concept that is trying to be expressed is in 'joint certification' the controls that are specified in the MSS (e.g. 42001, and/or 27001 and/or 27701, etc.) are especially leveraged and considered during product certification evaluation activities – it is intended these MSS controls are much more amplified and focused on than is normally the case in Type 5 and 6 product certification schemes which may simply rely upon the fact that the associated MSS covering the production/supply of the product has a MSS certificate; and

c) a view that does not support reliance on management system requirements in any case, as it is understood that it is up to the organization implementing the management system to define its own objectives, and to undertake its own risk assessment, etc., which may fall short of the level that some stakeholders would expect or accept – hence management system certification is not a primary consideration, rather it is better to simply focus on the AI system as the 'object of conformity' for product certification; and

d) the view that the role of 42001 is too prominent in this framework document, particularly given the regulatory requirements defined by the EC aka EU AI Act and Standardization request. Leaving reference to ISO 42001 in this document and including 'joint certification' infringes on the flexibility of this framework document.

Obviously these divergent views need to be further discussed in the WG when drafting this high-level framework guidance for conformity assessment schemes for AI systems. As a discussion at the international level within the ISO/IEC, consideration needs to be given to situations where there are no existing regulations for AI systems; there are differing levels of economic and technical development; and, where conformity assessment schemes developed in accordance with this guidance document are likely to be voluntary non-regulatory certification schemes in the first instance.

0.9 Conformity assessment schemes for AI systems should take into account:

a) the objectives of the AI system;

b) the intended purpose and intended results of the AI system, and the intended use cases for the AI system;

NOTE Reference to 'intended use cases' is common language, but to reflect the wording in ISO/IEC 42005, the term 'intended use' and 'intended uses' in this document has the same meaning as 'intended use cases'.

c) existing conformity assessment systems and schemes (voluntary or regulatory) in other related fields of international technology standardisation, such as in information security and cybersecurity, and in specific sectors, such as automated systems, medical devices, transport, etc.;

d) the life-cycle stages of an AI system;

NOTE ISO 22989 outlines the AI system life-cycle and ISO/IEC 5338 provides specific details. The life-cycle stages of AI systems in ISO/IEC 22989 include: inception; design and development; verification and validation; deployment; operation and monitoring (including continuous validation; re-evaluation; and retirement.

DRAFTING NOTE: The following list of properties comes mostly from ISO/IEC 22989. Please see subclause 9.2 that provides more elaboration on the list properties and make your comments under that subsection. This duplicate list in the Introduction will be subsequently updated after taking into account drafting decisions made on subclause 9.2.
Furthermore, informal comments received on the list:

a) suggest the properties included should only be drawn from ISO/IEC 22989 and ISO/IEC TS 5723 related to trustworthiness frameworks, however, there are also opposing comments questioning this approach, and recommending removing any reference or reliance to ISO TS 5723; and
b) reaction to the length of the list based on the understanding that it would be near impossible and take forever to evaluate an AI system if every property listed was included in a conformity assessment scheme.

Given this feedback the following clarification and commentary is provided:

a) the list of properties eventually to be included under 9.2 are not intended to be exhaustive, nor are they expected to all be included in a scheme which is based on this guidance document. It is only a listing of possible properties and the scheme owners can pick and choose what combination of properties that they want to include in their scheme. It is highly likely that only a small number of properties will be selected in the first instance – what is important for this high-level guidance document is for the all possible properties to be included and described so

there is some standardisation about what each property is called/labelled and what does each property mean or encompass;

b) the properties listed started with the properties listed in ISO/IEC 22989. Additional properties have then be suggested through informal comments. For the purposes of this New Work Item Proposal (NP) and this associated document, the long-list of possible properties of AI systems that could be subject to conformity assessment have been listed. If the NP is approved, then it will be up to the WG to review, define, compare, contrast, debate, challenge and come to a consensus decision on the final list of properties that we want to include in this high-level guidance document. The list will probably become shorter through this process but it is important at this time not to pre-emptively curtail the list before the WG have had the opportunity to discuss the matter; and

c) the implication of retaining a property on the list is it will eventually need to be described in some measurable and assessable way (i.e. the property needs to be able to state (either directly or by references to other documents) as 'specified requirements') so that conformity assessment can be carried out. If it is impossible to describe the property in a way which allows for 'specified requirements' to be stated, then that property is unlikely to be includes in the high-level guidance document because conformity assessment will not be possible.

It is appreciated that this will be one of the core discussion topics for the WG development process, and while it is currently presented as the description and listing of AI system properties, the WG may decide an alternative way to describe and define the assessable elements of an AI system which would be used as the basis of conformity assessment and certification.

e) the properties of AI systems, including, but not limited to:

- Accuracy
- Availability
- Bias and fairness
- Compatibility
- Controllability
- Explainability
- Interoperability
- Maintainability
- Portability
- Predictability
- Privacy
- Quality
- Reliability
- Resilience
- Resource use efficiency (e.g. energy consumption, memory)
- Robustness
- Safety
- Security
- Suitability
- Traceability
- Transparency
- Truthfulness
- Trustworthiness
- Useability
- Verifiability

f) the properties of AI systems in use, including, but not limited to:

- Context of coverage
- Extent of risk
- Effectiveness
- Efficiency
- Satisfaction

g) AI system impact assessment;

h) AI system risk management, including the application of controls; and

i) AI system performance evaluation and continual improvement.

0.10 The structure of this document follows the structure of the new revised edition of ISO/IEC WD 17067.2:2024 which is currently under development and which provides guidance for all conformity assessment schemes, irrespective of the object of conformity. ISO/IEC xxxxx (this document) applies the generic content of ISO/IEC 17067 to the more specific for situations where the object of conformity assessment is an AI system. This document also takes into account the content of IAF MD25 Criteria for Evaluation of Conformity Assessment Schemes.

0.11 This document has been developed with certification in mind. Certification is a form of conformity assessment where the assessment activities and attestation are undertaken by an independent third-party certification body. This does not preclude the use of this document as guidance for conformity assessment schemes that are developed and implemented by a first party (i.e. the developer or provider of the AI system) to make a declaration of conformity, or a second party (i.e. a party that has a direct interest in the AI system, such as a AI system product or service provider using a provider's AI system or subscription service; or a user interest in the AI product or system (e.g. any person or organization that will use the AI product or system or anyone who is impacted by the use of the AI product or system)).

1 Scope

This document provides a high-level framework and guidance for the development and operation of conformity assessment schemes, including certification schemes, for artificial intelligence (AI) systems.

2 Normative references[1]

- ISO/IEC 17000:2020 Conformity assessment — Vocabulary and general principles
- ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system
- ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary

DRAFTING NOTE: If the New Work Item Proposal (NP) for this document is approved, the WG will have to follow the ISO/IEC Directives rules for what is and is not to be included in Normative references clause. Normative references are generally reserved for other documents whose content is made normative (mandatory) in this document. Because this high-level document contains only guidance and no normative 'shall' requirements or provisions there may not be any normative references other than the vocabulary standards. This will be sorted out during the drafting process. Documents that have been suggested in the informal comments received have all been listed in the Bibliography.

3 Terms and definitions

DRAFTING NOTE: This terms and definitions clause will contain selected terms and definitions from ISO/IEC 22989, ISO/IEC 17000, ISO 42001 and ISO/IEC TS 5723:2022 and other relevant documents, such as where applicable, the EU Artificial Intelligence Act (a legal framework for AI adopted in March 2024) and the U.S. Executive Order on Safe, Security, and Trustworthy Intelligence (issued October 2023).

In addition, this clause will establish any new concepts, terms and definitions if required (e.g. if it is considered useful and not already covered somewhere else, the concept of 'static' and 'dynamic/continuous' assessment/evaluation and surveillance (i.e. trying to capture the concept of using AI to assess/evaluate AI at a single point in time, or continuously). It is noted existing conformity assessment schemes do have the concept of dynamic/continuous assessment/evaluation so it is not new, especially when certifying products that are tested/inspected during production activities, or while in use. How much these current practices can apply to the development, implementation and ongoing operation of AI systems needs to be discussed within the WG.

Drafting questions:

(1) Do we use 'assessment' or 'evaluation'? Within ISO/IEC 17065 product certification 'evaluation' has a specific meaning (it's the combination of the ''determination' and 'review' of the fundamental functional approach to conformity assessment described in the ISO/IEC 17000 Annex A). In contrast 'assessment' is a much more general term, effectively using the normal dictionary meaning of the word. We note under the

[1] See Bibliography for further information.

Common Criteria approach 'evaluation' appears to be the preferred term, but for this higher level framework document it may be appropriate for 'assessment' to be the preferred terms allowing for more flexibility. A specific conformity assessment scheme that follows this high-level framework can then bring more precision if they are focusing on product certification, and use the term 'evaluation' instead of 'assessment'.

(2) What is the best term for the provider of the AI system that will be the 'object of conformity' in the assessment/evaluation? The AI system provider could be just about any of the 'AI stakeholders' identified in ISO/IEC 22989, but should it be referred to in this new document as the 'applicant'/'client'/'responsible party'/'vendor' that is seeking to have their AI system assessed (and certified)? In 17000, 17021-1 management system certification and 17065 product certification the term used is 'client', but it is not clear whether 'client' translates very well into 'AI land'. What does ISO/IEC 27006, ISO/IEC 27021 and ISO/IEC 42006 use?

(3) We need to discuss as part of this clause the use of terms and definitions that have been standardised at the international level and published in ISO/IEC standards, and similar terms and definitions for the same concept that may be specified in national or regional regulation (e.g. the EU AI Act) and in any relevant international agreements or conventions.

3.1
artificial intelligence system
AI system
engineered system that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives

Note 1 to entry: The engineered system can use various techniques and approaches related to artificial intelligence to develop a model to represent data, knowledge, processes, etc. which can be used to conduct tasks.

Note 2 to entry: AI systems are designed to operate with varying levels of automation.

[SOURCE: ISO/IEC 22989:2022, 3.1.4]

3.2
conformity assessment
demonstration that specified requirements (3.5) are fulfilled conformity assessment

[SOURCE: ISO/IEC 17000:2020, 4.1, modified – Notes to entry removed]

3.3
object of conformity assessment
object
entity to which specified requirements (3.5) apply

EXAMPLE Product, process, service, system, installation, project, data, design, material, claim, person, body or organization, or any combination thereof.

[SOURCE: ISO/IEC 17000:2020, 4.2, modified – Note 1 to entry removed]

3.4
conformity assessment scheme
conformity assessment programme
set of rules and procedures (3.6) that describes the objects of conformity assessment (3.3), identifies the specified requirements (3.5) and provides the methodology for performing conformity assessment (3.2)

Note 1 to entry: A conformity assessment scheme can be managed within a conformity assessment system.

Note 2 to entry: A conformity assessment scheme can be operated at an international, regional, national sub-national, or industry sector level.

[SOURCE: ISO/IEC 17000:2020, 4.9, modified – Note 1 and Note 2 to entry removed]

3.5
specified requirement
need or expectation that is stated

Note 1 to entry: Specified requirements can be stated in normative documents such as regulations, standards and technical specifications.

Note 2 to entry: Specified requirements can be detailed or general.

[SOURCE: ISO/IEC 17000:2020, 5.1]

3.6
procedure
specified way to carry out an activity or a process

Note 1 to entry: In this context, a process is defined as a set of interrelated or interacting activities that use inputs to deliver an intended result.

[SOURCE: ISO 9000:2015, 3.4.5, modified — The original Note to entry has been replaced with a new Note to entry.]

3.7
attestation
issue of a statement, based on a *decision* (x.x), that fulfilment of *specified requirements* (3.5) has been demonstrated

Note 1 to entry: The resulting statement, referred to in this document as a "statement of conformity", is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, provide contractual or other legal guarantees.

Note 2 to entry: First-party attestation and third-party attestation are distinguished by the terms *declaration* (3.8), *certification* (3.9) and *accreditation* (3.10), but there is no corresponding term applicable to second-party attestation.

[SOURCE: ISO/IEC 17000:2020, 7.3]

3.8
declaration

first-party *attestation* (3.7)

[SOURCE: ISO/IEC 17000:2020, 7.5]

3.9
certification
third-party *attestation* (3.7) related to an *object of conformity assessment* (3.3), with the exception of *accreditation* (3.10)

[SOURCE: ISO/IEC 17000:2020, 7.6]

3.10
accreditation
third-party *attestation* (3.7) related to a *conformity assessment body* (3.11), conveying formal demonstration of its competence, *impartiality* (x.x) and consistent operation in performing specific conformity assessment activities

[SOURCE: ISO/IEC 17000:2020, 7.7]

3.11
conformity assessment body
body that performs conformity assessment activities, excluding *accreditation* (7.7)**8.1**

EXAMPLE Testing facility or laboratory, inspection body, certification body.

[SOURCE: ISO/IEC 17000:2020, 4.6, modified – EXAMPLE added]

3.12
surveillance
systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity

[SOURCE: ISO/IEC 17000:2020, 8.1]

4 Principles

The principles on ISO/IEC 17067 apply.

NOTE The new edition of ISO/IEC 17067 under development contains the following principles:

- conformity assessment schemes and conformity assessment systems
- comparability of conformity assessment results
- reproducibility of conformity assessment results
- reference to conformity assessment schemes

5 Inception and need for a conformity assessment scheme for AI systems

DRAFTING NOTE: Copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems.

Include also guidance to scheme owners that they need to consider existing regulatory and voluntary standards and schemes that may already cover their needs, or could be

referenced or incorporated into their own conformity assessment system/scheme design. This can include reference to existing sector-specific schemes and standards, and to schemes and standards relevant to different geographical regions.
The idea here is to discourage the unnecessary proliferation of schemes which can end up confusing the users of AI systems and act as a barrier to entry due the expense of obtaining and maintaining a multiplicity of overlapping certifications, etc. which add little or no value.

6 AI stakeholders, interested parties and consultation about the conformity assessment scheme

DRAFTING NOTE: Copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems. Include also the understanding of AI stakeholders of AI stakeholders from ISO/IEC 22989.

7 Confirmation of the conformity assessment scheme purpose, scope, scheme objectives, outline and intended users

DRAFTING NOTE: Copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems. Include also mention of:
- *how the scheme may be referenced (e.g. in legislation or regulation, or commercial agreements);*
- *intended uses of the resulting statements of conformity (e.g. the certificate).*

8 Conformity assessment scheme roles and responsibilities

DRAFTING NOTE: Copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems. Include also mention of:
- *conformity assessment scheme ownership;*
- *conformity assessment scheme operation;*
- *the decisions that the WG has made in addressing the above drafting note on the terms to use covering 'applicant'/'client'/'responsible party'/'vendor', etc.*
- *AI stakeholders and interested parties; and*
- *liability.*

9 Selecting the object of conformity for conformity assessment

9.1 The scheme owner should establish a process that results in the clear and unambiguous identification of the specific AI system(s), or type of AI system, that will be assessed/evaluated within the scheme.

NOTE 1 The selected AI system or type of AI system will be the object of conformity that will be subject to subsequent assessment/evaluation activities. For example, in information technology security a target of evaluation (TOE) is a specific term for an object of conformity (see ISO 15408).

NOTE 2 The process to identify the AI system as the object of conformity can result in the scheme owner itself identifying the specific AI systems that can be covered by their scheme (e.g. by referring to a specific AI system standard(s)), or, it can allow for applicants/clients/responsible parties/vendors to identify their own AI system in accordance with AI system parameters prescribed by the scheme.

9.2 In fulfilling 9.1, the scheme owner should ensure its process requires it, or the applicant/client/responsible party/vendor, to identify:

a) the objectives of the AI system;

NOTE Identification of the objectives of the AI system as a fundamental part of the definition of AI system. The use of the word 'objectives' in this list item is the same as the general English language dictionary meaning of the word, and should not be confused with the more specific use of the word 'objective' in the term 'control objective' that is used in ISO 42001;

b) the intended purpose and intended results of the AI system, and the intended use for the AI system;

NOTE Intended use is defined in ISO/IEC 42005 as 'purposes for which an AI system is designed, trained, and tested'. Intended use can take into account the competence of the user of the AI system, including those users that might be vulnerable to inappropriate use of the AI system (e.g. children, aged population or those without or limited understanding or exposure to information technology). Intended use can also explicitly identify limitations, constraints or boundaries outside of which the use the AI system is not intended or applicable. It is noted that AI systems and their results are context/domain dependent. Each conformity assessment scheme can take this into account,
The EU AI Act used "intended purpose" in focus (mentioned 50 times in the text).
"The objectives of the AI system may be different from the intended purpose of the AI system in a specific context".

c) the AI system life-cycle, and the life-cycle stage(s):

i. which are covered by the scheme;

ii. that are included in specific assessment/evaluation of the applicant/client/responsible party/vendor's AI system;

NOTE ISO/IEC 22989 outlines the AI system life-cycle and ISO/IEC 5338 provides specific details. For each assessment/evaluation carried out under the scheme it is expected that the AI system life cycle stages being included are explicitly acknowledged and subsequently referenced in the resulting statement of conformity (e.g. certificate).

d) the specific components of AI system(s), when the scheme allows for the assessment/evaluation at a component level;

e) any specific relationship with any underlying management system, for example an artificial intelligence management systems (ISO/IEC 42001);

f) inputs into the AI system, and the extent to which sources, format and quality of data and information used by the AI system is to be included in the assessment/evaluation activities;

NOTE This can include considerations of legitimate access and use of data and information, including confidentiality, big data sources (e.g. ISO/IEC 20546), security and privacy (ISO/IEC 27000 series standards), data quality (e.g. ISO/IEC 25012 and associated standards), etc.

g) outputs from the AI system and how outputs are to be made available to users and other AI systems and how these outputs are used;

NOTE As described in ISO 22989, output from AI systems may include, but is not limited to, content, forecasts, recommendations and decisions. The type of output and the degree of human agency in using this output can influence the subsequent risk assessment and selection of the assessment/evaluation activities.

h) the AI system properties that:

i. are covered by the scheme;

ii. that are included in specific assessment/evaluation of the applicant/client/responsible party/vendor's AI system.

NOTE AI systems properties that can be covered by the scheme can be, but are not limited to:

- Accuracy
- Availability
- Bias and fairness
- Compatibility
- Controllability
- Explainability
- Interoperability
- Maintainability
- Portability
- Predictability
- Privacy
- Quality
- Reliability
- Resilience
- Resource use efficiency (e.g. energy consumption, memory)
- Robustness
- Safety
- Security
- Suitability
- Traceability
- Transparency
- Truthfulness
- Trustworthiness
- Useability
- Verifiability

Most of these properties are described in ISO 22989, and further explanation is provided in Annex A.

NOTE Identification of the specific AI system in accordance with this subclause is a critical activity as it helps determine the subsequent applicable specified requirements, risk assessment activities, assessment/evaluation activities and content of the resulting statement of conformity (e.g. certificate).

10 Risk management in conformity assessment scheme design

DRAFTING NOTE: This clause is principally designed to give guidance the scheme owner that it should take a 'risk-based approach' when designing and implementing their scheme.

This is to ensure their scheme is effective, efficient and fit-for-purpose, and is not unnecessarily complex or over-engineered resulting in a scheme which is costly, consuming and administrative burdensome for little extra value. This clause also invites the scheme owner to consider what risk management provisions, if any, it wishes to specify that should apply to the assessment/evaluation of the AI system, and/or to the use of the AI system. In other words, this clause endeavours to address risk management at both levels. It is recognised this may cause some confusion so WG discussion on the inclusion and content of this clause is certainly necessary.

10.1 The scheme owner should implement a risk-based approach when designing and implementing the scheme to meet scheme objectives. This includes taking a risk-based approach when selecting the:

a) AI systems to be covered in the scheme;

b) AI system properties;

c) specified requirements that the AI system has to fulfil, including any risk treatments and controls; and

NOTE ISO 42001 includes detailed annexes on organization-level risk management as part of effective AI management systems implementation. These annexes can also be a useful reference to scheme owners when specifying risk treatments and controls for AI systems.

d) assessment/evaluation processes.

10.2 The scheme owner should ensure the assessment/evaluation process specified in the scheme takes a risk-based approach, including defining the extent to which any risk assessment (risk identification, risk analysis, risk evaluation), risk treatment or controls are identified and are required to be fulfilled. This may include:

a) specifying any relationship and the consideration of the results from any underlying management system, for example an artificial intelligence management system (e.g. ISO 42001);

b) specifying different levels of assessment/evaluation to reflect the nature of the risks and the potential impact of nonconformity in specific AI systems, including AI system impact assessment (ISO/IEC 42001 Annexes A and B and ISO/IEC DIS 42005, ISO/IEC 15408).

10.3 The scheme owner should have a process to ensure that risks, limitations or prohibitions associated with using an AI system that has been assessed/evaluated under its scheme are clearly communicated to the user and relevant AI stakeholders.

NOTE AI system users and AI stakeholders can take into account ISO/IEC 23894:2023 *Information technology — Artificial intelligence — Guidance on risk management* and can implement a management system that fulfils the requirements of ISO/IEC 42001. Risk management for AI systems may also be addressed in relevant sectorial standards, such as ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes, ISO 12100:2010 Safety of machinery — General principles for design — Risk assessment and risk reduction, ISO 14971:2019 Medical devices — Application of risk management to medical devices, IEC 61508 Functional safety of

electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, IEC 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements , IEC 61511 Safety instrumented systems (for process industry).

11 Selecting the specified requirements for use during conformity assessment of AI systems

11.1 The scheme owner should select specified requirements that can be used as the basis for assessment/evaluation activities of AI systems and for their use.

11.2 Specified requirements for AI systems and for their use should:

a) include reference to all legislative and regulatory requirements relevant to the AI system where that AI system is intended to be used;

NOTE It is expected that the statement of conformity will enable reference to the specific legal jurisdictions and regulations to which the AI system has been assessed/evaluated.

b) be consistent with the general guidance in ISO/IEC 17007:2009 *Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment*;

c) reference existing internationally accepted standards wherever possible;

NOTE For example, in relation to information security, international standards such the Common Criteria for Information Security Evaluation (ISO/IEC 15408-1, ISO/IEC 15408-2 and ISO/IEC 15408-3), could be referenced. Similar future international standards may cover matters such as trustworthy AI systems evaluation criteria (TAISEC) and trustworthy AI systems evaluation methodology (TAISEM) using specified protection profiles (PP).

NOTE Related to "joint certification," scheme owners could reference the controls in Annex A of ISO/IEC 42001 as a basis for specified requirements for assessment activities of an AI system in conjunction with assessment of the organization's management system.

d) include provisions that are consistent with matters covered in clauses 9 and 10 above;

e) include provisions that are specific for the AI system product, process or service (including any specific requirements around data acquisition, quality and management, models, output and learning guardrails);

f) provisions associated with risk treatments and controls;

g) be relevant to the life-cycles stages of the AI systems covered by the conformity assessment scheme; and

h) give consideration to, in addition to product, process or service requirements, requirements for AI stakeholders that develop, provide or use the AI system to fulfil

the requirements of ISO/IEC 42001 and any other relevant management system standard.

NOTE Relevant management system standards for the user of the AI system may include:
- ISO/IEC 42001: Artificial Intelligence Management Systems (AIMS)
- ISO/IEC 9001: Quality Management Systems (QMS)
- ISO/IEC 20000: Information Technology Service Management Systems (ITSMS)
- ISO/IEC 27001: Information Security Management Systems (ISMS)
- ISO/IEC 27701: Privacy Information Management Systems (PIMS)
- ISO 37301: Compliance Management Systems (CMS)
- ISO 13485: Medical Device Quality Management Systems (MDQMS)

12 Conformity assessment activities to be used in the scheme

12.1 The scheme owner should specify the conformity assessment activities that are to be undertaken to assess/evaluate the AI system's conformity with specified requirements, including any relevant sampling protocols and test methods.

NOTE 1 For example, in relation to information security, international standards such the Common Criteria for Information Security Evaluation (ISO/IEC 15408-1, ISO/IEC 15408-2 and ISO/IEC 15408-3), could be referenced. Similar future international standards may cover matters such as trustworthy AI systems evaluation criteria (TAISEC) and trustworthy AI systems evaluation methodology (TAISEM) using specified protection profiles (PP).

NOTE 2 Conformity assessment activities can include one or more of the following:
- Sampling
- Testing
- Auditing
- Inspection
- Validation
- Verification

DRAFTING NOTE: Consideration needs to be given to whether the guidance will address validation/verification of claims as activities in schemes for AI products and systems. Such guidance would need provide an explanation of AI products and systems, and claims regarding AI products and systems, as two separate and distinct objects of conformity assessment. References to validation and verification would be pertinent only if a scheme described claims as an object of conformity assessment and identified specified requirements for claims about AI products and systems. A key consideration would be the extent to which schemes would likely include both AI products and systems as well as claims as objects of conformity. If schemes are unlikely to include both then there is little reason to have guidance refer to validation/verification and little reason for guidance about claims within a scheme.

This necessary discussion about validation and verification from a conformity assessment perspective will take place with a backdrop that validation and verification are also terms that feature prominently in the life-cycle of an AI system. ISO/IEC 22989 outlines the AI system life-cycle and ISO/IEC 5338 provides specific details. The life-cycle stages of AI systems in ISO/IEC 22989 include: inception; design and development; verification and validation; deployment; operation and monitoring (including continuous validation); re-evaluation; and retirement. Given the use of these terms within a normal AI system life-cycle and to avoid confusion, care needs to be taken in drafting this high-level guidance document to make sure the readers understand whether we are talking about validation,

verification and evaluation from a conformity assessment perspective or a AI system life-cycle perspective.

NOTE 3 The selected conformity assessment activities should be relevant to the assessment/evaluation of the specified requirements identified in clause 10.

NOTE 4 It is noted that depending on the risk and potential impact of nonconformities, the scheme owner can specify varying evaluation levels of technical depth and assessment. When specifying any evaluation levels, the scheme owner can take into account whether an applicant/client/responsible party/vendor operates a conforming management system that covers the relevant life-cycle stages of the AI system.

12.2 The scheme owner should specify the persons or bodies that are authorised to undertake the assessment/evaluation methods, including provisions for their competency, impartiality and consistent operation (including any requirements associated with administration and reporting, operational procedures, internal management systems and documented information management).

NOTE 1 Annex B provides a reference to commonly used standards for conformity assessment activities and bodies, and possible conformity recognition pathways for those conformity assessment bodies.

NOTE 2 The scheme owner can add further requirements to the requirements contained in the documents identified in Annex B in terms of conformity assessment body and accreditation body activities, for example, additional specific provisions related to:
— certification or accreditation agreements;
— reporting requirements to the scheme owner;
— additional complaints handling or appeal provisions for the purposes of scheme integrity; and
— actions to be undertaken in the case of concerns form market feedback or fraudulent behaviour.

12.3 The scheme owner should specify the extent to which, and conditions for, any consideration of conformity assessment results that were generated prior to the submission of the AI system for assessment/evaluation under the scheme.

NOTE This can include specifying conditions under which pre-existing, previous or current conformity assessment results, are used in the ongoing assessment/evaluation include whether those results are acceptable if generated competently by the applicant/client/responsible party/vendor or an independent third-party.

12.4 If the scheme permits, the scheme owner should specify any requirements associated with subcontracting or outsourcing conformity assessment activities, especially in relation to:

a) obtaining prior approval of the applicant/client/responsible party/vendor of the AI system;

b) non-disclosure and confidentiality provisions;

c) competency, impartiality and consistent operation of the subcontracted or outsourcing person or body; and

d) ownership and use of assessment/evaluation data, information and records, and conformity assessment results.

13 Basic process for undertaking conformity assessment activities

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems. Make reference to:

- *Pre-conditions*
- *Applications*
- *Application review/Pre-engagement*
- *Agreement*
- *Planning*
- *Execution*
- *Static or dynamic/continuous assessment*
- *Nonconformity management, especially in relation to:*
    a. *definitions and any categorisations of nonconformities (e.g. minor, major, critical etc.)*
    b. *the expectations for root cause analysis, corrective actions and nonconformity close-out timeframes*
    c. *any prescribed follow-up actions or sanctions (suspension, withdraw of conformity assessment (certification) status, etc.*
- *Review*
- *Decision and attestation*

14 Appeals of conformity assessment decisions

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make specific for conformity assessment schemes covering AI systems.

15 Statement of conformity, certificates, licensing and use of marks

15.1 The scheme owner should specify the statement of conformity, including:

a) the format of the statement;

b) the content of the statement, including:

c) the period of validity of the statement.

NOTE 1 Statements of conformity can include declarations or certificates.

NOTE 2 See Annex C for further information.

15.2 The scheme owner should identify any licensing or other requirements that enable the use of the statement of conformity and any associated conformity marks or symbols.

15.3 First-party attestations should be in the form of suppliers declarations of conformity that fulfil the requirements of ISO/IEC 17050, and should contain the same information as specified in 19.1 b).

16 Conditions associated with conformity assessment results

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems. Make reference to:

- *Granting, maintaining, and continuing certification*

— *Changing the scope of certification*
— *Suspending or withdrawing certification*
— *Actions required by the certificate holder should the certification status change – e.g. public notification, product fixes, patches, updates, or product recall, etc.*

17 AI system vulnerabilities, patches, updates and conformity assessment

DRAFTING NOTE: Not sure how to tackle this. I suppose it is a matter of degree. If an vulnerability (is that only a IT security term?), bug, problem with the AI system is found after certification, then to what extent can a patch, update or improvement be made and the AI system remain the same and not trigger the need for an reassessment/re-evaluation? Do we just write that the scheme owner must consider and state something in their scheme to cover this eventuality?
Does certification remain valid on an ongoing basis forever unless there is a degradation of the properties/control objectives of AI system (e.g. its becomes less robust, less secure, etc) – Is this then Type 1 product certification i.e. certification to type, where the specific AI system may be both the 'type' and the unique individual instance of that 'type'?

18 Conformity assessment surveillance activities

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems. Make reference to:
— *Static/periodic surveillance*
— *Dynamic/continuous surveillance*

19 Conformity assessment scheme performance and integrity

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems. Make reference to:
— *Scheme administration and management*
— *Documented information and access to information*
— *Retention of documents and records (e.g. by scheme owners and certification bodies)*
— *Performance measurement, monitoring, analysis and evaluation*
— *Impact measurement, monitoring, analysis and evaluation*
— *Complaints handling*
— *Fraudulent use of conformity assessment results*
— *Investigating and responding to certified AI system issues*
— *Scheme resilience*

20 Conformity assessment scheme acceptance and recognition

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems. Make reference to:
— *Regulatory approval and acceptance*
— *Contractual/value chain/supply chain acceptance*
— *Accreditation*
— *Peer assessment*
— *Mutual recognition of conformity assessment results*
— *Access of conformity assessment bodies to the scheme*

— *Access of clients to the scheme*

21 Communication about the conformity assessment scheme

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems. Make reference to:

— *Internal and external reporting*
— *Public information*
— *Promotion and marketing*
— *Crisis communications and reputational management*

22 Changes to the conformity assessment scheme and specified requirements

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems.

23 Review of the conformity assessment scheme and specified requirements

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems.

24 Ending a conformity assessment scheme or transfer of ownership

DRAFTING NOTE: Cross reference or copy the same clause from the revised ISO/IEC 17067 and modify to make it specific for conformity assessment schemes covering AI systems.

Annex A
AI system properties for use in conformity assessment schemes
(informative)

DRAFTING NOTE: Ideally this is where a table or matrix would be that describes all the AI system properties, and identifies common controls, conformity assessment methods and reference standards. However not sure if this duplicates what is already covered in ISO 42001 annexes (but I understand those are orientated on the organisation developing or using the AI system?), or how this might intersect with ISO/IEC DIS 42005 Information technology - Artificial intelligence - AI system impact assessment?

A.1 Figure A.1 provides and description of AI system properties, and identifies common controls, conformity assessment methods and reference standards.

Figure A.1
AI system properties, common controls, conformity assessment methods and reference standards

	Description (see also ISO/IEC 22959)	**Common controls**	**Conformity assessment methods**	**Reference standards**
Accuracy				
Availability				
Bias and fairness				
Compatibility				
Controllability				
Explainability				
Interoperability				
Maintainability				
Portability				
Predictability				
Privacy				
Quality				
Reliability				
Resilience				
Resource use efficiency (e.g. energy, memory)				
Robustness				
Safety				
Security				
Suitability				
Traceability				

	Description (see also ISO/IEC 22959)	**Common controls**	**Conformity assessment methods**	**Reference standards**
Transparency				
Truthfulness				
Trustworthiness				
Usability				
Verifiability				

Annex B
Conformity assessment activities, competence requirements and their fulfilment
(informative)

B.1 Figure B.1 lists commonly used conformity assessment activities. It highlights the relevant international standards for competency, impartiality and consistent operation (including requirements associated with administration and reporting, operational procedures, internal management systems and management of documented information). Figure B.1 also identifies options for demonstrating fulfilment of those requirements.

Figure B.1
Conformity assessment activities, competence requirements and recognition

	Conformity assessment activity	Competency requirements	Fulfilment can be demonstrated by
1	Testing	ISO/IEC 17025 covering relevant scopes of testing	a) accreditation by an accreditation body that is a signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) for ISO/IEC 17025 ; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO/IEC 17025 for testing activities; or c) self-declaration of conformity in accordance with ISO/IEC 17050.
2	Inspection	ISO/IEC 17020 covering relevant scopes of inspection	a) accreditation by an accreditation body that is a signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA) for ISO/IEC 17020; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO/IEC 17020 for inspection activities; or c) self-declaration of conformity in accordance with ISO/IEC 17050.
3	Management system auditing	ISO 19011 covering relevant scopes of management system	a self-declaration of conformity in accordance with ISO/IEC 17050.
4	Management system certification	ISO/IEC 17021-1 covering relevant scopes of management system certification	a) accreditation by an accreditation body that is a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Arrangement (MLA) for ISO/IEC 17021-1; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO/IEC 17021-1 for management system certification activities; or c) self-declaration of conformity in accordance with ISO/IEC 17050.

	Conformity assessment activity	Competency requirements	Fulfilment can be demonstrated by
5	Product certification	ISO/IEC 17065 covering relevant scopes of product certification	a) accreditation by an accreditation body that is a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Arrangement (MLA) for ISO/IEC 17065; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO/IEC 17065 for product system certification activities, or c) self-declaration of conformity in accordance with ISO/IEC 17050.
6	Validation	ISO/IEC 17029 covering relevant scopes of validation	a) accreditation by an accreditation body that is a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Arrangement (MLA) for ISO 14065; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO 14065 for validation activities; or c) self-declaration of conformity in accordance with ISO/IEC 17050.
7	Verification	ISO/IEC 17029 covering relevant scopes of verification	a) accreditation by an accreditation body that is a signatory to the International Accreditation Forum (IAF) Multilateral Recognition Arrangement (MLA) for ISO 14065; or b) current full membership of a peer assessment arrangement group that fulfils the requirements of ISO/IEC 17040 and normatively references ISO 14065 for verification activities, or c) self-declaration of conformity in accordance with ISO/IEC 17050.

Annex C
Content of statements of conformity (e.g. certificates) for AI systems
(informative)

C.1 The following list provides the elements that can be included in a statement of conformity (e.g. certificate) for an AI system that fulfils specified requirements:

a) unique statement of conformity (e.g. certificate) number or other identifier;

b) the name of the conformity assessment scheme;

c) the name of the organization that is the conformity assessment scheme owner;

d) the name of specified requirements (including dates of publication) for which conformity has been demonstrated;

e) the name and unique identification of the object of conformity (i.e. the AI system) that has been assessed and demonstrates conformity with the specified requirements;

f) the purpose, intended users, and intended uses, for which the object of conformity (i.e. the AI system) is intended (and, where relevant, any purposes, intended users or uses for which the object of conformity (i.e. the AI system) is not to intended to be used;

NOTE This may include reference to inclusions or limitations associated with the object of conformity (AI system) and its intended users and uses (e.g. including geographical or demographic parameters)

g) the name and contact details of the owner of the owner/provider/user of the object of conformity (i.e. AI system);

h) the name of the organization and person issuing the statement of conformity and the contact details of that organization;

i) a legally binding signature(s) of person(s) authorized to sign on behalf of the conformity assessment body issue the statement of conformity;

NOTE In some economies, legally binding authorization of a statement of conformity is accomplished by other means, e.g. by legally binding seals.

j) the date of issue of the statement of conformity;

k) the date of expiry of the statement of conformity;

l) the period of validity for the statement of conformity, if any;

m) the date that any future conformity assessment activity must be completed to ensure ongoing fulfilment of specified requirements for the statement of conformity to remain valid, if any;

n) if applicable, the names and contact details of the conformity assessment bodies that undertook the assessment/evaluation activities; and

o) if applicable, the accreditation or recognition status of the conformity assessment bodies that undertook the assessment/evaluation of the object of conformity.

p)

Bibliography

DRAFTING NOTE: A check needs to be made of the documents listed in the Bibliography in accordance with ISO/IEC Directives Part 2.

https://en.wikipedia.org/wiki/Software

https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

CEN/CLC/TR 17894 – Artificial Intelligence Conformity Assessment

EU Artificial Intelligence Act
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

European Cyber Security Organisation (ECSO), 2017, European Cyber Security Certification: A Meta-Scheme Approach v1.0.

European Union Agency for Cybersecurity (ENISA), 2020, Cybersecurity Certification

IAF MD25 Criteria for Evaluation of Conformity Assessment Schemes

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements

IEC 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements

IEC 61511 Safety instrumented systems (for process industry)

ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model Part 2: Security Architecture

ISO 9000:2015 Quality management systems — Fundamentals and vocabulary

ISO 9001 Quality management systems — Requirements

ISO 9241-11 Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts

ISO 9241-210 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems

ISO 9241-220 Ergonomics of human-system interaction — Part 220: Processes for enabling, executing and assessing human-centred design within organizations

ISO 10007 Quality management — Guidelines for configuration management

ISO 10015:2019 Quality management — Guidelines for competence management and people development

ISO 12100:2010 Safety of machinery — General principles for design — Risk assessment and risk reduction

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

ISO 14971:2019 Medical devices — Application of risk management to medical devices

ISO 30422:2022 Human resource management — Learning and development

ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model

ISO/IEC 20546:2019 Information technology — Big data — Overview and vocabulary

ISO/IEC 20547-3:2020 Information technology — Big data reference architecture — Part 3: Reference architecture

ISO/IEC 22123-1:2023 Information technology - Cloud computing- Part 1: Vocabulary

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

ISO/IEC 2382:2015 Information technology — Vocabulary

ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management

ISO/IEC 24029-2:2023 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods

ISO/IEC 24668:2022 Information technology — Artificial intelligence — Process management framework for big data analytics

ISO/IEC 24773-1:2019 Software and systems engineering — Certification of software and systems engineering professionals — Part 1: General requirements

ISO/IEC 24773-3:2021 Software and systems engineering — Certification of software and systems engineering professionals — Part 3: Systems engineering

ISO/IEC 24773-4:2023 Software and systems engineering — Certification of software and systems engineering professionals — Part 4: Software engineering

ISO/IEC 24775-2:2021 Information technology Storage management Part 2: Common Architecture

ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE

ISO/IEC 25001:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Planning and management

ISO/IEC 25002:2024 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model overview and usage

ISO/IEC 25010:2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Product quality model

ISO/IEC 25012:2008 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model

ISO/IEC 25019:2023 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality-in-use model

ISO/IEC 25020:2019 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality measurement framework

ISO/IEC 25021:2012 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality measure elements

ISO/IEC 25022:2016 Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Measurement of quality in use

ISO/IEC 25023:2016 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality

ISO/IEC 25024:2015 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of data quality

ISO/IEC 25030:2019 Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Quality requirements framework

ISO/IEC 25040:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process

ISO/IEC 25041:2012 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation guide for developers, acquirers and independent evaluators

ISO/IEC 25045:2010 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation module for recoverability

ISO/IEC 25051:2014 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing

ISO/IEC 25059:2023 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems

ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

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

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls

ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance

ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

ISO/IEC 27006-1:2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General

ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

ISO/IEC 27010:2015 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

ISO/IEC 27011:2016/Cor 1:2018 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations — Technical Corrigendum 1

ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection — Governance of information security

ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry

ISO/IEC 27021:2017 Information technology — Security techniques — Competence requirements for information security management systems professionals

ISO/IEC 27021:2017/Amd 1:2021 Information technology — Security techniques — Competence requirements for information security management systems professionals — Amendment 1: Addition of ISO/IEC 27001:2013 clauses or subclauses to competence requirements

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security

ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts

ISO/IEC 27033-2:2012 Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

ISO/IEC 27033-4:2014 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-5:2013 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27033-6:2016 Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access

ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security — Part 1: Overview and concepts

ISO/IEC 27034-1:2011/Cor 1:2014 Information technology — Security techniques — Application security — Part 1: Overview and concepts — Technical Corrigendum 1

ISO/IEC 27034-2:2015 Information technology — Security techniques — Application security — Part 2: Organization normative framework

ISO/IEC 27034-3:2018 Information technology — Application security — Part 3: Application security management process

ISO/IEC 27034-5:2017 Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure

ISO/IEC 27034-6:2016 Information technology — Security techniques — Application security — Part 6: Case studies

ISO/IEC 27034-7:2018 Information technology — Application security — Part 7: Assurance prediction framework

ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27035-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations

ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships — Part 1: Overview and concepts

ISO/IEC 27036-2:2022 Cybersecurity — Supplier relationships — Part 2: Requirements

ISO/IEC 27036-3:2023 Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security

ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27038:2014 Information technology — Security techniques — Specification for digital redaction

ISO/IEC 27039:2015 Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

ISO/IEC 27040:2024 Information technology — Security techniques — Storage security

ISO/IEC 27041:2015 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method

ISO/IEC 27042:2015 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

ISO/IEC 27070:2021 Information technology — Security techniques — Requirements for establishing virtualized roots of trust

ISO/IEC 27071:2023 Cybersecurity — Security recommendations for establishing trusted connections between devices and services

ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines

ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework

ISO/IEC 27557:2022 Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management

ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework

ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

ISO/IEC 38500:2024 Information technology- Governance of IT for the organization

ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system

ISO/IEC DIS 42005 Information technology — Artificial intelligence — AI system impact assessment

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

ISO/IEC 5338:2023 Information technology — Artificial intelligence — AI system life cycle processes

ISO/IEC 5339:2024 Information technology — Artificial intelligence — Guidance for AI applications

ISO/IEC 8183:2023 Information technology — Artificial intelligence — Data life cycle framework

ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making

ISO/IEC TR 24028:2020 Information technology — Artificial Intelligence — Overview of trustworthiness in artificial intelligence

ISO/IEC TR 24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview

ISO/IEC TR 24368:2022 Information technology — Artificial intelligence — Overview of ethical and societal concerns

ISO/IEC TR 27103:2018 Information technology — Security techniques — Cybersecurity and ISO and IEC Standards

ISO/IEC TR 27550:2019 Information technology - Security techniques - Privacy engineering for system life cycle processes

ISO/IEC TR 27550:2019 Information technology — Security techniques — Privacy engineering for system life cycle processes

ISO/IEC TR 27563:2023 Security and privacy in artificial intelligence use cases — Best practices

ISO/IEC TR 29119-11:2020 Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems

ISO/IEC TR 29119-6:2021 Software and systems engineering — Software testing — Part 6: Guidelines for the use of ISO/IEC/IEEE 29119 (all parts) in agile projects

ISO/IEC TR 5469:2024 Artificial intelligence — Functional safety and AI systems

ISO/IEC TS 25052-1:2022 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE): cloud services — Part 1: Quality model

ISO/IEC TS 25058:2024 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems

ISO/IEC TS 27006-2:2021 Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems

ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls

ISO/IEC TS 27022:2021 Information technology — Guidance on information security management system processes

ISO/IEC TS 27034-5-1:2018 Information technology — Application security — Part 5-1: Protocols and application security controls data structure, XML schemas

ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts

ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

ISO/IEC TS 4213:2022 Information technology — Artificial Intelligence — Assessment of machine learning classification performance

ISO/IEC TS 5723:2022 Trustworthiness — Vocabulary

ISO/IEC/IEEE 12207:2017 Systems and software engineering - Software life cycle processes

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

ISO/IEC/IEEE 15289:2017, Systems and software engineering — Content of systems and software life cycle process information products (documentation)

ISO/IEC/IEEE 24748-1:2018 Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management

ISO/IEC/IEEE 24748-2:2018 Systems and software engineering — Life cycle management — Part 2: Guidelines for the application of ISO/IEC/IEEE 15288 (System life cycle processes)

ISO/IEC/IEEE 24748-3:2020 Systems and software engineering — Life cycle management — Part 3: Guidelines for the application of ISO/IEC/IEEE 12207 (software life cycle processes)

ISO/IEC/IEEE 24748-4:2016 Systems and software engineering — Life cycle management — Part 4: Systems engineering planning

ISO/IEC/IEEE 24748-5:2017 Systems and software engineering — Life cycle management — Part 5: Software development planning

ISO/IEC/IEEE 24748-6:2023 Systems and software engineering — Life cycle management — Part 6: System and software integration

ISO/IEC/IEEE 24748-7:2019 Systems and software engineering — Life cycle management — Part 7: Application of systems engineering on defense programs

ISO/IEC/IEEE 24748-7000:2022 Systems and software engineering — Life cycle management — Part 7000: Standard model process for addressing ethical concerns during system design

ISO/IEC/IEEE 24748-8:2019 Systems and software engineering — Life cycle management — Part 8: Technical reviews and audits on defense programs

ISO/IEC/IEEE 24748-9:2023 Systems and software engineering — Life cycle management — Part 9: Application of system and software life cycle processes in epidemic prevention and control systems

ISO/IEC/IEEE 24765:2017 Systems and software engineering — Vocabulary

ISO/IEC/IEEE 24774:2021 Systems and software engineering — Life cycle management — Specification for process description

ISO/IEC/IEEE 26515:2018 Systems and software engineering - Developing information for users in an agile environment

ISO/IEC CD 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems

ISO/IEC WD 27091.2 Cybersecurity and Privacy — Artificial Intelligence — Privacy protection

ISO/IEC/IEEE 29119-1:2022 Software and systems engineering — Software testing — Part 1: General concepts

ISO/IEC/IEEE 29119-2:2021 Software and systems engineering — Software testing — Part 2: Test processes

ISO/IEC/IEEE 29119-3:2021 Software and systems engineering — Software testing — Part 3: Test documentation

ISO/IEC/IEEE 29119-4:2021 Software and systems engineering — Software testing — Part 4: Test techniques

ISO/IEC/IEEE 29119-5:2016 Software and systems engineering — Software testing — Part 5: Keyword-Driven Testing

ISO/IEC/IEEE 29148, Systems and software engineering — Life cycle processes — Requirements engineering

ISO/IEC/IEEE 90003:2018 Software engineering Guidelines for the application of ISO 9001:2015 to computer software

OECD, “Recommendation of the Council on Artificial Intelligence” (2019) Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Conformity assessment

ISO/IEC Guide 68:2002 Arrangements for the recognition and acceptance of conformity assessment results

ISO/IEC 17000:2020 Conformity assessment — Vocabulary and general principles

ISO/IEC 17007:2009 Conformity assessment — Guidance for drafting normative documents suitable for use for conformity assessment

ISO/IEC 17011:2017 Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies

ISO/IEC 17020:2012 Conformity assessment — Requirements for the operation of various types of bodies performing inspection

ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements

ISO/IEC TS 17023:2013 Conformity assessment — Guidelines for determining the duration of management system certification audits

ISO/IEC 17024:2012 Conformity assessment — General requirements for bodies operating certification of persons

ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories

ISO/IEC TR 17026:2015 Conformity assessment — Example of a certification scheme for tangible products

ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons

ISO/IEC TR 17028:2017 Conformity assessment — Guidelines and examples of a certification scheme for services

ISO/IEC 17029:2019 Conformity assessment — General principles and requirements for validation and verification bodies

ISO/IEC 17030:2021 Conformity assessment — General requirements for third-party marks of conformity

ISO/IEC TR 17032:2019 Conformity assessment — Guidelines and examples of a scheme for the certification of processes

ISO/TS 17033:2019 Ethical claims and supporting information — Principles and requirements

ISO/IEC 17040:2005 Conformity assessment — General requirements for peer assessment of conformity assessment bodies and accreditation bodies

ISO/IEC 17043:2023 Conformity assessment — General requirements for the competence of proficiency testing providers

ISO/IEC 17050-1:2004 Conformity assessment — Supplier's declaration of conformity — Part 1: General requirements

ISO/IEC 17050-2:2004 Conformity assessment — Supplier's declaration of conformity — Part 2: Supporting documentation

ISO/IEC 17060:2022 Conformity assessment — Code of good practice

ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services

ISO/IEC 17067:2013 Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes

Others… including referencing other various other relevant ISO/IEC JTC1 standards