



# AI Watch: AI Standardisation Landscape

## State of play and link to the EC proposal for an AI regulatory framework

NATIVI S. (DG JRC) and DE NIGRIS S.  
(DG JRC)



This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Name: Stefano NATIVI

Address: Via E. Fermi 749, 21027 Ispra VA (Italy)

Email: stefano.NATIVI@ec.europa.eu

Tel.: +39 0332 78075

EU Science Hub

<https://ec.europa.eu/jrc>

JRC125952

EUR 30772 EN

PDF

ISBN 978-92-76-40325-8

ISSN 1831-9424

doi:10.2760/376602

Luxembourg: Publications Office of the European Union, 2021

© European Union, 2021



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2021, except: page 24, Figure 5: pen icon, source: pixabay; known gaps icon, source: Matt Brooks in the Buzzword Collection; experts icon, source: Max Pixel.

How to cite this report: Stefano NATIVI, Sarah De Nigris, *AI Standardisation Landscape: state of play and link to the EC proposal for an AI regulatory framework*, EUR 30772 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-40325-8, doi:10.2760/376602, JRC125952

## Contents

Contents .....	2
Foreword .....	4
Acknowledgements .....	5
Authors .....	5
Disclaimer .....	5
Abstract .....	6
1 Introduction .....	7
1.1 Aim of the study .....	7
1.2 The role of standards .....	8
1.3 European Standards .....	8
1.4 Standardisation domain and processes.....	9
1.4.1 De-jure versus de-facto standards.....	9
1.4.2 Foundational versus implementation standards .....	10
1.4.3 Horizontal versus vertical specifications .....	10
1.4.4 Standards dependencies .....	11
1.5 Standards specific to AI .....	12
2 Overall Methodology adopted .....	13
3 AI Standards populations .....	15
3.1 Sources for the collection of existing standards .....	15
3.2 Outcome of AI standards collection: the general population of AI standards....	15
3.3 Significant subset of AI standards: the sub-population .....	16
3.4 Significant standards description .....	16
4 Artificial Intelligence Act (AIA) Requirements and applicable Standards .....	17
4.1 AIA scope.....	17
4.2 Useful definitions.....	17
4.3 The requirements for high-risk AI systems .....	17
5 High-level mapping of the significant AI standards onto the AIA requirements .....	20
5.1 Mapping Overview .....	20
5.2 Timeline of standards publication .....	21
5.3 Mapping limitations and detailed analysis .....	21
6 In-depth analysis and mapping .....	23
6.1 Methodology .....	23
6.1.1 Standards operationalisation and suitability calculation .....	23
6.1.2 Suitability index .....	24
7 Semi-structured AIA requirements .....	29
7.1 Executive version of the AIA requirements and the related keyword lists .....	29

7.1.1	R1. Data and data governance .....	29
7.1.2	R2. Technical documentation .....	30
7.1.3	R3. Record-keeping .....	30
7.1.4	R4. Transparency and provision of information to users .....	31
7.1.5	R5. Human oversight .....	32
7.1.6	R6. Accuracy, robustness and cybersecurity .....	32
7.1.7	R7. Risk management system .....	33
7.1.8	R8. Quality management system .....	34
8	Results of the in-depth mapping and gap identification .....	35
8.1	Artificial Intelligence concepts and terminology .....	35
8.2	Operationalisation and suitability analysis results .....	35
8.3	Operationalisation gaps .....	36
8.3.1	Discussion .....	43
8.3.2	Total Operationalisation index (southern hemisphere) .....	47
8.4	Suitability gaps .....	48
8.4.1	Southern hemisphere contribution to the suitability index (the total operationalisation index) .....	48
8.4.2	Northern hemisphere contribution to the suitability index .....	49
8.4.3	Viewpoint #1: EU regulatory framework implementers .....	49
8.4.4	Viewpoint #2: AI system developers .....	50
8.4.5	Discussion .....	51
9	Conclusions and Recommendations .....	52
Annex A.	ETSI standards and initiatives description .....	56
Annex B.	ISO and ISO/IEC standards and initiatives description .....	68
Annex C.	ITU-T standards and initiatives description .....	79
Annex D.	IEEE standards and initiatives description .....	84
Annex E	Standards mapping per Requirement .....	95
Annex F.	Standards mapping per SDO .....	99
Annex G1.	Fiches generated by the detailed analysis for ISO/IEC standards .....	103
Annex G2.	Fiches generated by the detailed analysis for ETSI standards .....	122
Annex H.	Terms definition .....	128
10	References .....	130
11	List of Tables .....	132
12	List of Figures .....	133
13	Glossary .....	134

## Foreword

This report is produced in the context of AI Watch, the European Commission knowledge service to monitor the development, uptake and impact of Artificial Intelligence (AI) for Europe, launched in December 2018. AI has become an area of strategic importance with potential to be a key driver of economic development. AI also has a wide range of potential social implications. As part of its Digital Single Market Strategy, the European Commission put forward in April 2018 a European strategy on AI in its Communication "Artificial Intelligence for Europe" COM(2018)237.

The aims of the European AI strategy announced in the communication are:

- To boost the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors.
- To prepare for socio-economic changes brought about by AI
- To ensure an appropriate ethical and legal framework.

Subsequently, in December 2018, the European Commission and the Member States published a "Coordinated Plan on Artificial Intelligence", COM(2018)795, on the development of AI in the EU.

In April 2021, the European Commission adopted an AI Package. This package includes proposal for the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally (European Commission, 2021) and 2021 review of the the Coordinated Plan (European Commission, 2021).

The 2021 Review of the Coordinated Plan on AI puts forward a concrete set of joint actions for the European Commission and Member States on how to create EU global leadership on trustworthy AI. The proposed key actions reflect the vision that to succeed, the European Commission together with Member States and private actors need to:

- accelerate investments in AI technologies to drive resilient economic and social recovery facilitated by the uptake of new digital solutions;
- act on AI strategies and programmes by implementing them fully and in a timely manner to ensure that the EU reaps the full benefits of first-mover adopter advantages; and
- align AI policy to remove fragmentation and address global challenges.

Standardisation activities are one of the action areas identified in the 2021 Coordinated Plan as an area for joint action between European Commission and Member States.

This report is one of the deliverables of AI watch specifically focusing on the mapping of the AI standards onto the requirements introduced by the European Commission AI Act.

**This is the 3nd version of the study** reflecting updated input from stakeholders and the requirements, as present in the Commission's official proposal for a horizontal regulatory framework for AI.

Questions and comments on AI Watch can be sent to [EC-AI-WATCH@ec.europa.eu](mailto:EC-AI-WATCH@ec.europa.eu)

## Acknowledgements

With special thanks to StandICT.eu European Observatory on ICT Standards (EUOS) Working Group 4. WG-AI-LAND Expert Advisors: Jens Gayko, Karl Grün, Fergal Finn, Ray Walshe, EUOS WG4 is Chaired by Lindsay Frost (NEC, ETSI).

The Authors also recognize the important contribution provided by Filipe Jones Mourao, Tatjana Evas, and Salvatore Scalzo (DG CNECT) on the AIA requirements and for the revision of this document. A similar gratitude goes to the colleagues Josep Soler Garrido and Paul Desruelle (DG JRC) for the valuable comments on the document. Finally, the Authors thank Eric Badiqué (former DG CNECT) and the EC-CEN/CENELEC coordination Working Group for the continuous collaboration and discussion on AI standardisation and the needs of high-risk systems.

A final thank goes to CEN/CENELEC, ETSI, and IEEE reviewers for their comments that helped to improve the document.

## Authors

Stefano NATIVI (DG JRC) and Sarah DE NIGRIS (DG JRC)

## Disclaimer

The mapping (carried out in this document) with regard to regulatory requirements does not aim to provide any form of endorsement from the EC on the content of any standards or specifications.

## Abstract

The present study surveys the ongoing standardisation activities on AI carried out by ESOs (European Standards Organizations) and international Standards Development Organizations (SDOs). In the present study we investigate the alignment between AI related standards published or in development and the requirements proposed in the proposal for Artificial Intelligence Act.. The aim is to identify possible gaps and underdeveloped areas in the current standardisation activities. The main goal is to provide a contribution to the definition of a European standardisation roadmap for implementing the Artificial Intelligence Act (AIA) (European Commission, 2021).

The document is organized as follows: Section 1 provides an overview of the different dimensions of standards and introduces the adopted landscaping methodology. Then, Sections 2 and 3 discuss the applied methodology to identify the standards relevant to the AIA and the considered standard population, respectively. Then, Section 4 delves into the proposed regulatory framework for AI (i.e. the AIA), introducing its scope and requirements. Section 5 provides a high-level analysis to map the identified standard populations onto the AIA requirements. Section 6 provides an in-depth analysis of the mapping, introducing an innovative methodology. Applying the proposed methodology, Section 7 discusses an executive version of the AIA requirements, according to a semi-structured model. Section 8 discusses the obtained results of the in-depth analysis and provides initial reflections on the possible gaps. Finally, Section 9 summarizes findings, outline possible recommendations, and introduce potential future work.

# 1 Introduction

## 1.1 Aim of the study

AI technologies may present new safety risks for users when they are embedded in products or used in services – addressing individuals, legal entities, and enforcement authorities (European Commission, 2021).

Therefore, the White Paper on AI, published in February 2020 by the European Commission (European Commission, 2020) recognized the need to provide an improved regulatory framework, including a possible new Regulation dealing with AI risks for safety and fundamental rights (European Commission, 2020).

A proposal for the new AI Regulation was adopted by the Commission on 21 April (European Commission, 2021). This Regulation follows the New-Legislative Framework approach.

According to this legislative technique, the legal provisions are typically high-level and framed as essential requirements. These set a technical objective that providers of AI systems are expected to fulfil; the so-called harmonised standards provide the detailed technical specifications through which economic operators can achieve compliance with the relevant legal requirements. If they so wish, however, economic operators can use any other technical solutions other than harmonised standards to demonstrate compliance.

**Harmonised standards** are produced by European standardisation organisations (notably CEN/CENELEC and ETSI) based on a **formal standardisation request** issued by the European Commission. Those standards are to be evaluated by the Commission services and, where they are deemed to satisfy the standardisation request, published in the Official Journal. Only standards published in the Official Journal can provide operators with a relevant legal presumption of conformity with the legal requirements of the EU harmonisation legislation in question. Regulation (EU) 1025/2012 sets the general rules regarding the functioning of the standardisation system, including the procedure for issuing standardisation mandates (Article 10).

Appropriate agreements in place between European Standardisation Organisations (ESOs) and International Standardisation Organisations (such as ISO or IEC) ensure that international standards can be taken over by ESOs and proposed as European harmonised standards in response to a standardisation request.

Harmonised standards are thus a key tool for the implementation of the legislation and contribute to the specific objective to ensure that AI systems are safe and trustworthy. Harmonised standards allow for technological evolution and the take-up of the latest state-of-the-art.

In April 2021, the European Commission published a proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (European Commission, 2021). This act aims at defining AI systems, and puts forward requirements for high-risk AI systems.

In this context, the objective of this document is multi-fold:

1. to provide a survey of the international standardisation initiatives and **specifications dealing with AI, which are relevant to high-risk applications and systems;** and
2. to analyse their relation to the **requirements of the proposed EU Artificial Intelligence Act;**
3. to assess their present **suitability and operationalisation level to implement these requirements** and recognize **possible gaps.**

This study considers ISO/IEC, ETSI, ITU-T, and IEEE standards dealing with AI; furthermore, ISO/IEC JTC1-SC42 and ETSI SAI standards were analysed in-depth. In the next future IEEE and ITU-T relevant standards will be also processed in-depth and such analysis will be included in a updated version of this report.

This study does not consider biometrics: an important topic for the future EU regulation. There already are many ISO standards dealing with such a topic and dedicated working items are likely to be launched to address specific needs stemming from the AIA.

This study does not consider the types of IPR that characterize the usage of the analysed standards and, thus, does not consider their possible impact.

## 1.2 The role of standards

According to the European Commission, a standard is defined as: "a technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory and which is one of the following (European Commission, 1998):

- international standard: a standard adopted by an international standardisation organisation and made available to the public;
- European standard: a standard adopted by a European standardisation body and made available to the public;
- national standard: a standard adopted by a national standardisation body and made available to the public".

Furthermore, as stated in its Regulation no. 1025/2012 on standardisation:

"the primary objective of standardisation is the definition of voluntary technical or quality specifications with which current or future products, production processes or services may comply. Standardisation can cover various issues, such as standardisation of different grades or sizes of a particular product or technical specifications in product or services markets where compatibility and interoperability with other products or systems are essential" (European Union, 2012).

EU lawmakers put standardisation at the centre of EU digital and industrial strategy (Regulation (EU) No 1025/2012, European Commission, 2015). While sustainability and safety standards help protect people and environment, in Europe standards play a special function by helping to make the single market a reality. Finally, standards empower digital transformation for the whole society, boosting market development, increasing the international competitiveness, and supporting regulations.

An International Standard can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards (ISO, 2021).

## 1.3 European Standards

The European regional standards organizations, known as ESOs (European Standards Organizations), are officially recognised by the European Commission (Regulation (EU) No 1025/2012) and act as a European platform through which European Standards are developed. ESOs include: the European Committee for Electrotechnical Standardisation (CENELEC), the European Committee for Standardisation (CEN) and the European Telecommunications Standards Institute (ETSI).

In the European Union, only standards developed by CEN, CENELEC and ETSI are recognised as 'European Standards' (Regulation (EU) No 1025/2012). These ESOs work

jointly in the interest of European harmonization, creating both standards requested by the market and harmonized standards in support of European legislation.

Moreover, these organizations are also the regional mirror bodies to their international counterparts, i.e. the International Organization for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union, telecommunication standardisation sector (ITU-T), respectively.

For the scope of this document, we consider ESOs and the relevant SDOs having a formal recognition by international treaties and regulation or SDOs participating to the bi-annual Global Standards Collaboration, which involves all major SDOs. Therefore, we investigate: ETSI, CEN-CENELEC, ISO/IEC, ITU-T, and the Institute of Electrical and Electronics Engineers (IEEE)

European standards play a very important role within the internal market, for instance through the use of harmonised standards.

## 1.4 Standardisation domain and processes

Standard specifications may cover a wide range of applications (from products to services), systems, and processes, with different purposes (from informative to normative), dealing with different phases of the subject lifecycle (from design to implementation and management). Therefore, standardisation processes and related stakeholders can be different considering (at least) three possible dimensionalities or concerns (explained below) that, thus, may be used to characterize the standards domain:

- **Business and legal concerns:** can give rise to either de-jure or de-facto/industrial standards.
- **Conceptual and process concerns:** lead generally to the development of either foundational/basic standards or technical/implementation standards.
- **Application and context-specific concerns:** are behind the distinction between standards covering a broad spectrum of sectors (commonly called horizontal standards) and standards intended for more application domain (or context specific use), generally indicated as vertical standards.

### 1.4.1 De-jure versus de-facto standards

A de-facto standard is one which has been widely accepted (e.g. by customers/users or by the market), becoming a well-regarded (or popular) standard for its purpose – even though it has no official status. Acceptance is often based on a proven track record for efficiency and reliability (de Vries, 1998).

De-facto standards which become accepted by an industry are also known as industry or professional standards.

On the other hand, de-jure describes a practice that is formally recognised, regardless of whether the practice exists in reality. Therefore, de-jure standards (or standards according to law) are those which have been approved by official organizations such as ISO and IEEE. These standards are critically assessed before being approved – examples of de-jure hardware standards include USB, FireWire and HDMI, while a significant example of software related standard is ASCII character set (deVries, 1998, Carpenter, 2012).

De-facto standards can become de-jure standards over time (i.e. by receiving an official status from a SDO) – e.g. HTML and PDF formats. HTML first became a de-jure standard in 1995 because of the standardisation effort led by the Internet Engineering Task Force (IETF) (Vaughan-Nichols, 2010) and PDF became in 2008 an ISO standard (ISO 32000-1) (Carpenter, 2012).

#### 1.4.2 Foundational versus implementation standards

Foundational or basic standards are commonly the basis for a series of standard specifications, defined by a SDO. This work focuses on those aspects that necessitate a common vocabulary, as well as agreed taxonomies and definitions (Bartram, 2018). Eventually, these standards will mean that a practitioner can talk the same language as a regulator and both can talk the same language as a technical expert. For example, ISO/IEC work on AI covers a number of key areas spanning technology, societal, and ethical considerations. Since many different stakeholders are addressed, there is the need to define a basic starting point by introducing a set of foundational standards.

**Example** ISO/IEC DIS 22989 - *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

The document establishes terminology for Artificial Intelligence (AI) and describes concepts in the field of AI. The document can be used in the development of other standards and in support of communications among diverse, interested parties/stakeholders.

According to the Open Geospatial Consortium, implementation standards are different from the abstract specification of foundational standards, since they are written for a more technical audience and detail technical aspects such as the interface structure between software components (OGC, 2020):

**Example** IEEE 802.3-2018 - IEEE Standard for Ethernet

Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 400 Gb/s using a common media access control (MAC) specification and management information base (MIB).

#### 1.4.3 Horizontal versus vertical specifications

As in many other standardisation domains, there may be two levels of standardisation activities: one dealing with general issues that apply in a cross-cutting way to several areas (horizontal) and another dealing with more specific issues relevant to a given sector of activity or application area (vertical).

A horizontal specification contains fundamental principles, concepts, definitions and similar general information that aims to be applicable over a broad set of subject areas.

**Example:** ISO/IEC AWI TR 24372 Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems

The specification aims to provide an overview of the state of the art of computational approaches for AI systems, by describing: a) main computational characteristics of AI systems; b) main algorithms and approaches used in AI systems, referencing use cases contained in ISO/IEC TR 24030.

On the other hand, vertical specifications aim to address application- or sector-specific areas and therefore only focus on the necessary information specific to that product application or sector. Such specifications, however, may be re-used in other sectors, possibly needing adaptation.

**Example:** ETSI DES/eHEALTH-008 - eHEALTH Data recording requirements for eHealth

The aim of this work is to identify the requirements for recording eHealth events, i.e. those from ICT based eHealth devices and from health practitioners. On the understanding, as illustrated in the use case document and in the White Paper, that health records are subject to security and privacy constraints, but at the same time need to be available to many different stakeholders across time and space without pre-cognition of who those stakeholders are.

#### 1.4.4 Standards dependencies

Standard specifications usually build on other already-existing standards to be cohesive, and avoid conflicts and duplications of work. Thus, to implement a standard commonly requires the implementation of some other, underpinning, standards; the latter, called second-level standards, in turn may be connected to other foundational ones, and so on.

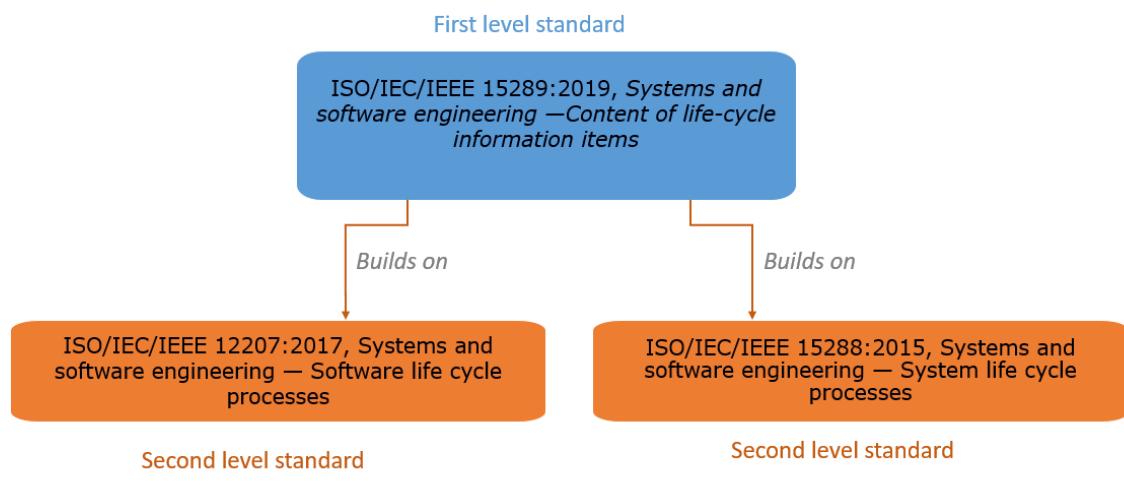
Commonly, a development of a new standards builds on one or more underpinning standards. The underpinning standards, in turn, may be connected to one or more foundational standards. This interconnectedness and layers in the development of standards aim to ensure consistency and avoid duplication of work. Therefore, generally when an AI system developer selects a first-level implementation standard, he/she discovers one or more propaedeutic standards to comply with —the second-level standards.

Therefore, we can define:

- **First-level standard:** The standard that an organization is asked to implement —and that commonly build on other existing (second level) standard specifications.
- **Second-level standard:** The standard that an organization may be asked to implement because it is foundational for the implementation of another standard —e.g. a first-level standard.

Starting from a set of first-level standards, it is possible to recognize a multi-level network of associated/connected standards —as showed in Figure 1, for example.

**Example:**



*Figure 1. Example of first-level standard and its connected/referenced second-level ones*

To address this challenge and support the developers in using the standards underlining the AI Act, it would be useful to investigate the network dimension of standards —see Recommendation 6 in Section 9.

### 1.5 Standards specific to AI

According to the AI Act (AIA) (European Commission, 2021), 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in the Annex I of the AIA and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

## 2 Overall Methodology adopted

The ICT and quality management domains related to AI systems and processes are quite vast. Therefore, the standardisation domain for AI is similarly large.

However, as stated in Section 1.1, this study is required to identify an executable, effective, and preliminary list of standards (existing or under development) relevant for high-risk AI applications that can be utilized to implement the European Regulatory framework on AI.

To this end, we adopted the following investigation methodology:

**Step 1. AI standards collection.** Collect existing survey studies on AI standardisation, directly access the ESO and international SDO portals and documents and gather input from standardisation experts.

**Step 2. High-level analysis and mapping to the AIA requirements (standard population refinement).** Analyse the collected set of AI standards and categorize the different types of standards into de-jure versus de-facto, foundational versus implementation and horizontal versus vertical specifications (see Sections 1.4.1-1.4.3).

Further refine the list of collected standards according to three criteria:

- consider standards dealing with AI-related risks.
- privilege horizontal implementation standards from international SDOs over foundational and vertical ones;
- consider first-level standards (see Section 1.4.4).

The resulting set of selected standards is mapped onto the requirements of the AIA (see Section 4 and Section 5).

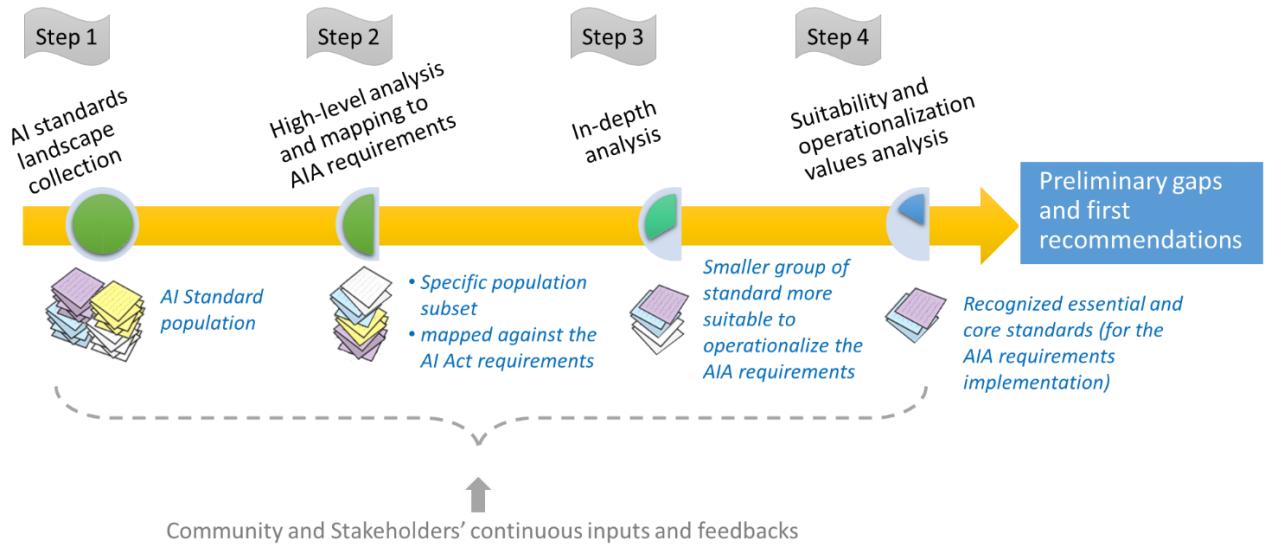
**Step 3. In depth analysis and mapping to the AIA requirements (estimation of operationalisation and suitability indexes of a smaller group of standards).** Systematically analyse the full text of a smaller group of relevant standards (i.e. those recognized through the high-level mapping) and estimate how suitable they are (presently) to operationalise the technological objectives underpinning the AIA requirements.

**Step 4. Suitability and operationalisation results analysis (gap recognition).**

Based on the operationalisation and suitability level previously estimated per each in depth analysed standard, possible gaps (and underrepresented AIA requirements) are recognized. This would originate the formulation of preliminary recommendations.

The outcome of Step 1 of the methodology is a **general set of potentially relevant AI standards** (i.e. the AI standard population) to be analysed by using their metadata information, including the abstract. Step 2 generates a **specific subset of the standards population** (i.e. a selected subset of the AI standard population), which are relevant for the AIA scope and, hence, can be mapped onto the regulatory framework requirements; this sub-population was assessed by the SDOs community. Step 3 evaluates in depth **a smaller group** of standards (part of the subset), calculating their suitability and operationalisation values. This group of standards was selected on the basis of the high-level mapping results (i.e. the most promising ones to operationalize the AIA requirements) and because their textual content was accessible. While the high-level analysis is based on the standards metadata, the in-depth analysis requires the access to the standards' text. Finally, building on the results of the in-depth analysis, Step 4 recognizes **essential and core standards**, some **preliminary gaps**, and **first recommendations**.

These different sub-sets will be characterized in Sections 3-8; while Figure 1 depicts the entire funnel process.



*Figure 2. Overall methodology adopted to identify most relevant standards, recognize gaps, and provide recommendations.*

### 3 AI Standards populations

#### 3.1 Sources for the collection of existing standards

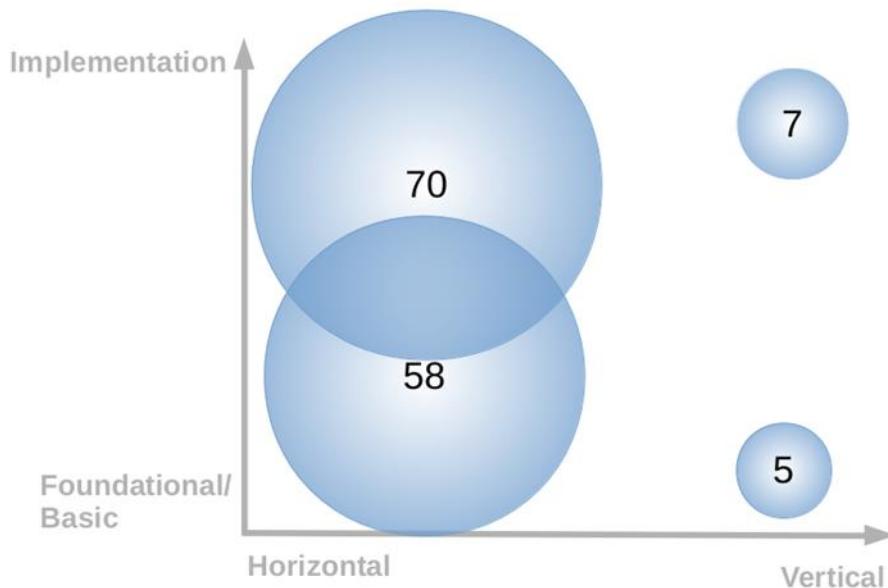
To recognize the general population of AI-related standards, we considered several sources and interacted with experts in the domain. In particular:

- We considered the outcomes of existing *surveys* on AI standardisation, e.g. the white paper of CEN/CELEC Focus Group on AI, the final report of the H2020 StandICT.eu project (ended in 2020), the technical report on “Standards for AI Governance” by the University of Oxford, the study of the AI Ethics Impact Group on “An interdisciplinary framework to operationalise AI ethics”, the new StandICT.eu European Observatory on ICT Standards (EUOS).
- We considered existing scientific publications e.g. manuscripts on the *Journal of ICT Standardisation*.
- We accessed the public, and sometimes restricted, websites and document sharing tools of ESOs and SDOs. We considered ETSI, IEEE, CEN/CENELEC, ISO/IEC JTC1, ITU-T.
- We analysed the existing *roadmaps* on AI standardisation: ETSI roadmap, CEN/CENELEC Roadmap, ISO/IEC JTC1 Roadmap, the German Standardisation Roadmap on Artificial Intelligence and the ITU-T AI roadmap.
- We engaged with a focus group, committees, and projects working on AI standardisation: ISO/IEC JTC1-SC2, EC - CEN CENELEC Focus Group on Artificial Intelligence; the Expert Advisory Group (EAG) of the new StandICT.eu project (started in 2020 and funded by H2020), the EU-Japan AI Joint Committee, etc.
- We participated and contributed to specific events dealing with ICT and AI standardisation - e.g. the webinar on AI Standardisation organized by DG CNECT (Sep 2020), the JRC Workshop on Standardisation (Dec 2020), the JRC PolicyLab on standards (Dec 2020), the DGs GROW-CNECT-JRC meeting on Standards (Jan 2021), etc.

#### 3.2 Outcome of AI standards collection: the general population of AI standards

The Step 1 of the methodology allowed us to recognize nearly 140 specifications dealing with AI. These initiatives encompass both standards that directly address AI-specific issues and standards that are more tangentially related to AI, such as standards on enabling technologies for AI, like for instance the standards on Big Data.

The general standardisation population thus collected was analysed, as described in the Step 2 of the methodology. We first categorized along the dimensions horizontal/vertical and foundational/implementation (as defined in Sections 1.4.1-1.4.3). We represent the obtained categories in a bi-dimensional space in Figure 3.



*Figure 3. AI-related general standards population, obtained as the outcome of Step 1 and categorized according the two dimensions horizontal/vertical and foundational/implementation.*

### 3.3 Significant subset of AI standards: the sub-population

As stated in the Section 1.1. of the Introduction, the aim of the present study is to focus on the operationalisation and suitability values of ongoing standardisation efforts in respect to the future EU legislation for AI (i.e. the proposed AIA).

Therefore, we focused our analysis on AI-centred standards that deal with AI risk characterization and management, with the final aim of mapping them to the requirements of the proposed EU AIA.

In Step 2 of our methodology, we identified a subset of AI standards (about 90), adopting the following criteria:

- AI-centred and dealing with AI-related risks;
- horizontal and implementation standards from international SDOs;
- first-level standards.

In addition, only standards managed by ESOs and international SDOs were considered, focusing on those horizontal domains that cover the topics of the requirements proposed for the future regulation (see Section 4).

This allowed us to recognize the most relevant standards for our aim, reducing the number of specifications to be mapped onto the future requirements of the proposed AIA.

### 3.4 Significant standards description

This sub-population of standards is presented in the Annexes A-D and mapped against the AIA requirements, in Section 5. This high-level mapping considered also the feedbacks provided by the international standardisation community.

## 4 Artificial Intelligence Act (AIA) Requirements and applicable Standards

### 4.1 AIA scope

In April 2021, the European Commission issued the proposal for a Regulation laying down harmonised horizontal rules on artificial intelligence (i.e. the Artificial Intelligence Act: AIA) (European Commission, 2021).

"By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of artificial intelligence can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy .... However, the same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society" (European Commission, 2021).

For these reasons, the proposed regulatory framework is based on a risk-based approach and aims to strike a balance between ensuring the rights and safety of consumers whilst avoiding being excessively prescriptive, in order to promote innovation and, especially, to support SMEs.

This proposal delivers on the political commitment by President von der Leyen, who announced in her political guidelines for the 2019-2024 Commission "A Union that strives for more" (von der Leyen, 2019), that the Commission would put forward legislation for a coordinated European approach on the human and ethical implications of AI. The proposal also responds to explicit requests from the European Parliament and the European Council, which have repeatedly expressed calls for legislative action to ensure a well-functioning internal market for artificial intelligence systems ('AI systems') where both benefits and risks of AI are adequately addressed at Union level.

The AIA is based on the new legislative framework. It defines a set of objective-based requirements that AI systems should comply with. In particular, the AIA introduces requirements for high-risk AI systems and obligations for operators of such systems, as well as harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content. The proposal also lays down obligations for providers and users of high-risk AI systems.

According to the AIA, "*Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation*" (European Commission, 2021).

### 4.2 Useful definitions

A set of applicable definitions, relevant for the purpose of this study, are provided in Annex H.

### 4.3 The requirements for high-risk AI systems

High-risk AI systems shall comply with a set of specific requirements, established by the AIA (European Commission, 2021).

Each key requirement for high-risk AI system included in the AIA is operationalised for this study (see below) by a streamlined explanation introducing the executive version of the main elements of the requirement:

#	Icon	Requirement theme	Executive description
---	------	-------------------	-----------------------

1		Data and data governance	High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation, and testing datasets that meet a set of quality criteria
2		Technical documentation	The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.  The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the AIA requirements.
3		Record-keeping	High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.
4		Transparency and provision of information to users	High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of (European Commission, 2021)
5		Human oversight	High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use
6		Accuracy, robustness, and cybersecurity	High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle
7		Risk management system	An assessment through internal checks for 'stand-alone' high-risk AI systems would require a full, effective and properly documented ex ante compliance with all requirements of the regulation and compliance with robust quality and risk management systems and post-market monitoring. A risk management system shall be established, implemented, documented, and maintained in relation to high-risk AI systems

8



### Quality management system

Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system.

In the next section, the existing standardisation work, considered relevant to the AIA scope, is mapped onto the diverse requirements. A full description of the mapped standards is provided in Annexes A-D, each annex focusing on an SDO.

## 5 High-level mapping of the significant AI standards onto the AIA requirements

### 5.1 Mapping Overview

In this section, the introduced AI standards (i.e. the sub-population introduced in Section 3.3 and described in the Annexes A-D) are mapped onto the AIA requirements. The high-level mapping is overviewed in Table 1.

In Annex E, the standards mapped for each requirement are reported (i.e. a requirement-based view). While, in Annex F, a SDO-based view reports the mapping characterizing each SDO.

*Table 1. Overall representation of mapped standards (already published standards are in bold)*

Requirements	Data and data governance	Risk management system	Technical data and Record keeping	Transparency and information to users	Human oversight	Accuracy, robustness, and cybersecurity	Quality management system
<b>SDO</b>							
<b>ISO and ISO/IEC JTC1</b>	<b>ISO/IEC 25024;</b> ISO/IEC 5259; ISO/IEC 24668;	ISO/IEC 4213; ISO/IEC 25059; ISO/IEC 24029-2	ISO/IEC 5338; ISO/IEC 5469; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668	ISO/IEC 24027; <b>ISO/IEC 24028;</b> ISO/IEC 5338; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668; ISO/IEC 4213		ISO/IEC 24027; <b>ISO/IEC 24028;</b> ISO/IEC 24029; ISO/IEC 5469	ISO/IEC 23894; ISO/IEC 38507; ISO/IEC 42001; ISO/IEC 25059
<b>IEEE</b>	<b>ECPAIS Bias;</b> IEEE P7002; IEEE P7003; IEEE P7004; IEEE P7005; IEEE P7006; IEEE P7009; IEEE P2801; IEEE P2801; IEEE P2807; IEEE P2863	IEEE P7009; IEEE P7003; IEEE P2807; IEEE P2846	<b>ECPAIS Transparency;</b> IEEE P7000; IEEE P7001; IEEE P7006; IEEE P2801; IEEE P2802; IEEE P2807; IEEE P2863; IEEE P3333.1.3	<b>ECPAIS Bias;</b> <b>ECPAIS Transparency;</b> <b>ECPAIS Accountability</b> ; IEEE P7000; IEEE P7006; IEEE P7001; IEEE P7003; IEEE P7004; IEEE P7005; IEEE P7007; IEEE P7008; IEEE P7009; IEEE P7011; IEEE P7012; IEEE P7014; IEEE P2863; IEEE P3652.1	<b>ECPAIS Accountability;</b> <b>ECPAIS Transparency;</b> IEEE P7000; IEEE P7006; IEEE P7001; IEEE 7010; IEEE P7003; IEEE P7014; IEEE P2863	<b>ECPAIS Transparency;</b> IEEE P7007; IEEE P7009; IEEE P7011; IEEE P7012; IEEE P2802; IEEE P2807; IEEE P2846; IEEE P2863; IEEE P3333.1.3	IEEE 2801; IEEE P2863; IEEE P7000
<b>ETSI</b>	DES/eHEALTH-008 ; GR CIM 007 ; GS CIM 009; ENI GS 001; GR NFV-IFA 041; DGR SAI 002; TR 103 674; TR 103 675; TS 103 327; TS 103 194; TS 103 195.2,	<b>GS ARF 003 ;</b> GR CIM 007 ; ENI GS 005 ; DGR SAI 002, SAREF Ontologies; GR CIM 007; GS CIM 009	DES/eHEALTH-008 ; <b>ENI GS 005</b> ; DGR SAI 002, SAREF Ontologies; GR CIM 007; GS CIM 009	DES/eHEALTH-008 ; GS CIM 009 ; DGR SAI 002; SAREF Ontology	DES/eHEALTH-008 ; DGR SAI 005	<b>GS ARF 003 ;</b> GR CIM 007 ; ENI GS 001; ENI GR 007 ; DGR SAI 001; DGR SAI 002; DGS SAI 003; GR SAI 004; <b>GS ZSM 002;</b> TR 103 674; TR 103 675; TS 103 327;	

	SAREF Ontologies	TS 103 194; TS 103 195.2; TR 103 821;				GS 102 181, GS 102 182	
ITU-T	ITU-T Y.3170; ITU-T Y.MecTa-ML ; ITU-T Y.3531 ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU-T Y.4470 ; Y.Supp.63 to ITU-T Y.4000 series	ITU-T Y.qos-ml-arc ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU-T Y.4470		ITU-T Y.4470 ;		ITU-T Y.3170 ; ITU-T Y.qos-ml-arc ; ITU-T Y.MecTa-ML ; ITU-T Y.3531 ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU-T Y.4470	

## 5.2 Timeline of standards publication

As depicted in Figure 4 below, the number of AI standards published per year has increased steadily, currently peaking at 21 standards expected for release in 2021. Moreover, the publication of new AI standards will remain significant at least until 2024.

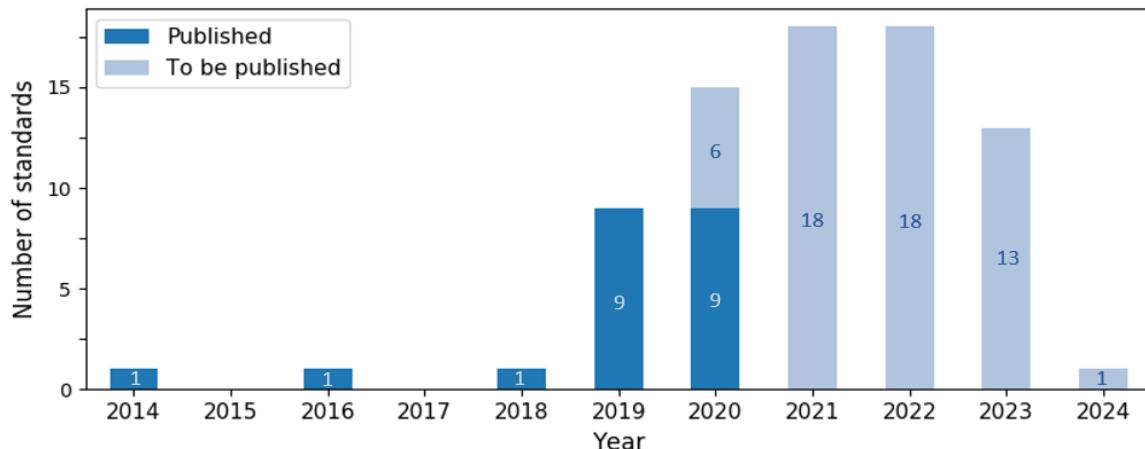


Figure 4: Yearly distribution of standard publication or expected publication. The numbers for years 2021-2024 are provisional, based on the specifications' metadata.

## 5.3 Mapping limitations and detailed analysis

The high-level mapping summarized in Table 1 represents a first analysis of the standards that are relevant for the application of the AIA requirements. However, this high-level mapping does not provide information about which part(s) of the requirement(s) each standard addresses nor to what extent.

The mapping mainly builds on the abstracts of the analysed standard and on the general description of the AIA requirements. Finally, the mapping by category (as represented in Table 1) includes all the experts' evaluations, not making any attempt at resolving possible divergences between expert's opinions.

The next section analyses in detail the specific relevance of the identified standards in respect to the AIA requirements. This analysis considers:

- (a) the full text of the standards;
- (b) a structured version of the legal description of the AIA requirements;
- (c) a less "subjective" procedure.

This development is described in the next section.

## 6 In-depth analysis and mapping

### 6.1 Methodology

#### 6.1.1 Standards operationalisation and suitability calculation

This section deals with a systematic analysis of relevant standards to estimate how suitable they are for operationalizing the AIA requirements. Interestingly, for a given standard, the generated suitability index can vary over time, reflecting content modification —as is the case of working items that still can evolve and include new topics.

The methodology applied to estimate the suitability indexes of identified AI standards and understand possible gaps (and then propose recommendations) consists of several steps, as also depicted in Figure 5:

- **Step 1. From unstructured to semi-structured requirements** From the unstructured (legal-oriented) text of the AIA, we generated semi-structured clauses in order to allow for the identification of core concepts and clauses, as well as the establishing of a hierarchy of clauses (and sub-clauses).
- **Step 2. Relevant keyword identification** From Step 1, we isolate relevant keywords characterizing each requirement. Furthermore, we also extend the list including technical words pertinent to the given requirement.
- **Step 3. Automatic text mining** The keyword lists, curated at Step 2, are the input for a code that searches for occurrences and, where relevant, co-occurrences of the keywords in the specification's text. The code also checks for a «positional» score, i.e. assessing the relevance of a keyword also depending on its position in the text. The code returns the keywords that were retrieved as well as their context for a better understanding of their significance.
- **Step 4. Expert control** The results of Step 3 provide a guidance to experts in the manual review of the recognized specifications: in the review, the specifications are read and the matching keywords are assessed in their context to evaluate their relevance with respect to the requirements.
- **Step 5. Operationalisation index calculation** The operationalisation index is calculated according to Equations (2), (3), and (4). These indexes provide a quantitative estimation of how relevant a standard is in turning the abstract AIA requirements into observables rules and features.
- **Step 6. Suitability index calculation** The suitability index is calculated according to Equation (1). These indexes provide a numeric estimation of the analysed suitability, based on a set of standard traits. In particular, the suitability index combines the previous calculated operationalisation index with few maturity and domain characteristics of the standard.
- **Step 7. Possible gap recognition and recommendations** An overall analysis of the standard suitability indexes, along with the analysis of the operationalisation indexes, for each of the eight AIA requirements, allows to recognize possible gaps and draw some recommendations.

The algorithms to calculate the operationalisation and suitability indexes are discussed in the next paragraphs.

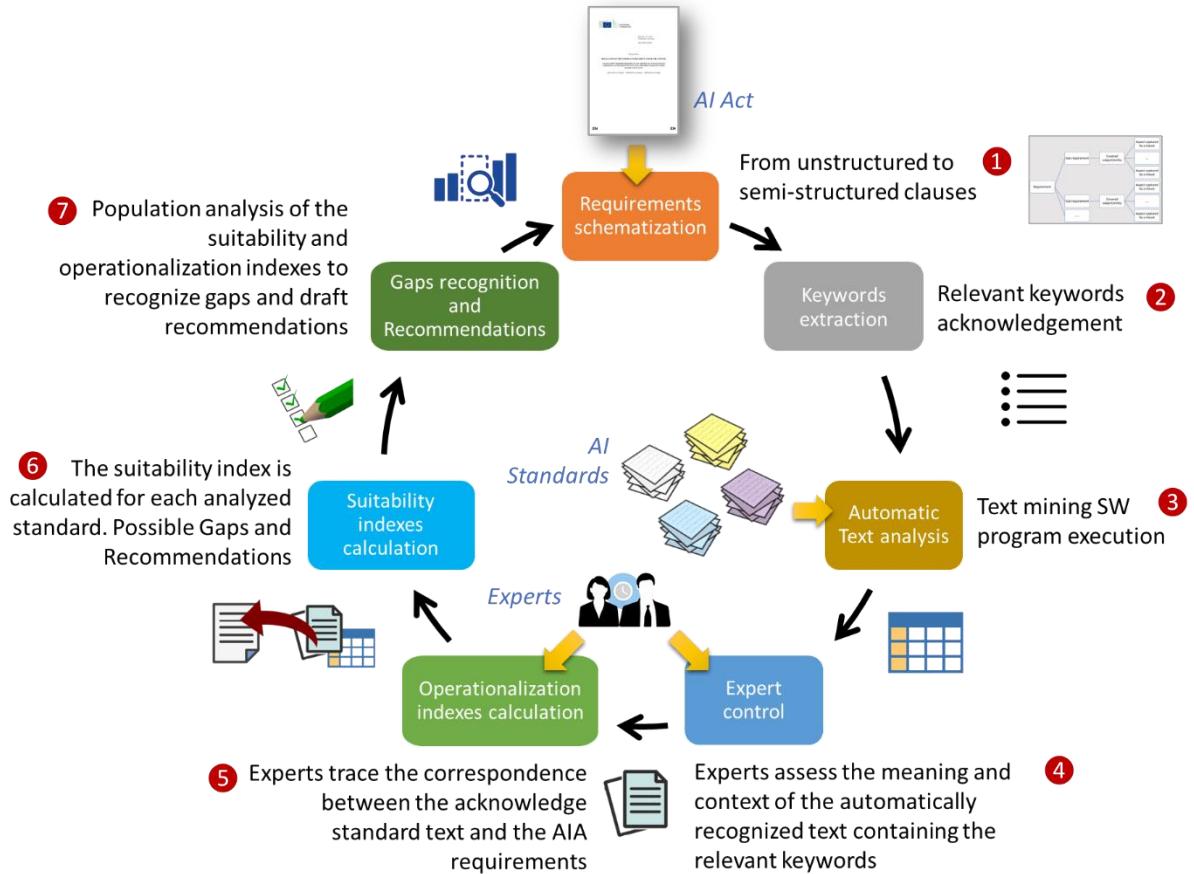


Figure 5. Methodology to analyse the operationalisation and then the suitability indexes characterizing the AI standards recognized in the high-level mapping

### 6.1.2 Suitability index

For each analysed standard, a suitability index (Si) is achieved by applying the following formula:

$$Si = \frac{w_1 * Oi + w_2 * \text{Domain generality} + w_3 * \text{Compliance management} + w_4 * \text{Typology} + w_5 * \text{Maturity}}{m}; \quad [0 \leq w_n \leq 1]; \quad m = \text{normalization factor}; \quad \left. \right\} (1)$$

Where  $w_n$  are weighting factors used to give more importance to some aspects in relation to others. This is the case of the *Operationalisation* aspect -which is evaluated by means of a total Operationalisation index (Oi).

The final goal is to develop a proximity diagram acknowledging which current specifications are presently closer to the AI act needs -as represented in Figures 16 and 17.

All the parameters composing the suitability index (see formula (1)) are described in the following paragraphs.

#### *6.1.2.1 Compliance management (characterizing a standard)*

For the scope of this study, compliance means conforming to a specification or standard. Compliance management is the process, utilized by relevant stakeholders and third parties, to ensure the compliance with a given specification or standard.

Given a technical specification or a standard, to measure how extensively a system or a product implements that, it is necessary to define a compliance management process - including activities such as: audits, reports and supporting documentation, compliance procedures, and compliance tests.

The importance of this parameter depends on the future development (and adequacy) of standalone conformity assessment standards, specifically targeting the AI Act -for example under possible future CEN-CENELEC JTC21 activity.

The existence of a formal compliance management process (or not) will characterize this dimension. Where a compliance management process exists but is not complete or fully formalized, intermediate values are possible.

According to ISO we can recognize three main instruments addressing providers and third parties (e.g. conformity assessment bodies), respectively.

##### For Providers:

- **Testing:** the determination of one or more of an object or product's characteristics and is usually performed by a laboratory. For example, many people have their blood tested which involves analysing the blood against a number of characteristics such as whether it shows the presence of a disease, or genetic disorder. ISO CASCO has developed a number of standards that laboratories can follow to help ensure that their results can be trusted.
- **Inspection:** describes the regular checking of a product to make sure it meets specified criteria. Fire extinguishers, for example, need regular inspections to ensure they are safe for use. ISO CASCO has developed a number of standards that inspection bodies can follow to help ensure that we can trust their work.

##### For Third parties (example, conformity assessment body):

- **Certification:** the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. Certification is also known as third party conformity assessment. Many companies and organizations decide to get certified to one of existing management system standards, such as ISO 9001. This is a way of showing outsiders that the organisation has an effective quality management system in place.

#### *6.1.2.2 Standard Typology*

There exist several different types of deliverables (e.g. documents) written, approved, and published by SDOs. In this context, a document is a standardisation draft or publication, produced by an SDO. For the scope of this study, in order of relevance, we acknowledge the following types of documents:

- **Harmonized standard:** are European standards produced (by an ESO) in response to an EC standardisation request (ETSI, 2021). They provide the technical detail necessary to achieve the 'essential requirements' of an EC legislation. They are thus key enablers of the European Single Market.
- **International standard:** a standard that is adopted by an international standardizing/standards organization and made available to the public (IEC, 2021). A standard is document (containing technical requirements) (ETSI, 2021), established by consensus and approved by a recognized body, that provides, for

common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context (IEC, 2021)

An International Standard can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards (ISO, 2021).

- **Technical specification:** a specification addressing work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard (ISO, 2021)

A Technical Specification is a document containing technical requirements (ETSI, 2021), for which there is the future possibility of agreement on an International Standard, but for which at present (IEC, 2021):

- the required support for approval as an International Standard cannot be obtained;
- there is doubt on whether consensus has been achieved;
- the subject matter is still under technical development, or
- there is another reason precluding immediate publication as an International Standard.

For some SDOs, a technical specification is produced when it is important that it is available for use quickly (ETSI, 2021). Commonly, a technical specification is approved by the Technical Committee that drafted it, only (ETSI, 2021).

- **Publicly Available Specification:** as with Technical Specifications, Publicly Available Specifications (PAS) are published for immediate use and also serve as a means to obtain feedback for an eventual transformation into an International Standard (ISO, 2021). PAS is a document to respond to an urgent market need, representing either (IEC, 2021):
  - a consensus in an organization external to the SDOs that publishes the specification, or
  - a consensus of the experts within a working group.

In the case of ISO, PAS has a maximum life of six years, after which they can be transformed into an International Standard or withdrawn (ISO, 2021).

- **Guide:** a document giving rules, orientation, advice or recommendations relating to international standardisation (IEC, 2021). A Guide helps readers understand more about the main areas where standards add value. Some Guides talk about how, and why, standards can make it work better, safer, and more efficiently (ISO, 2021). Commonly, it is submitted to the whole SDO membership for approval (ETSI, 2021).
- **Technical report:** a document containing collected data of a different kind from that normally published as an International Standard or Technical Specification (IEC, 2021). It may include data obtained from a survey, for example, or from an informative report, or information of the perceived "state of the art" (ISO, 2021). Commonly, it is used when the document contains explanatory material and is approved by the Technical Committee that drafted it (ETSI, 2021).

#### *6.1.2.3 Domain generality (of a Standard)*

As in many other standardisation domains, there may be two levels of AI standardisation activities: one dealing with general issues that apply in a cross-cutting way to several areas

(**horizontal**) and another dealing with more specific issues relevant to a given sector of activity, application, or technology area (**vertical**).

A horizontal specification contains fundamental principles, concepts, definitions and similar general information that aims to be applicable over a broad set of subject areas and/or technological frameworks.

On the other hand, vertical specifications aim to address application or sector-specific areas and, therefore, only concern the necessary information specific to that product application or sector -including technological sectors. Naturally, it is possible to have mixed situation: a standard that introduces some horizontal recommendations or rules, as well as some other vertical ones.

Generally, the distinction between horizontal and vertical scopes can be done (in a different mode) for both the application and technological domains. While for the application domain the distinction is immediate (e.g. two verticals healthcare or transport domains), in the case of technology domain, the discriminant deals with the generality level of the technological solution and/or reference framework considered in the analysed standard (e.g. Machine-Learning versus v Deep-Learning technologies, Narrow AI versus logic approaches for AIAI).

Therefore, it is possible to distinguish four topical situations, as described in Table 2.

*Table 2. Domain generality of an implementation standard: possible topical cases*

Application domain		Vertical	Horizontal
Technological domain	Vertical	V-V	V-H
Horizontal	Horizontal	H-V	H-H

#### *6.1.2.4 Maturity phase (of a standard)*

At the outset, each specification document (deliverable) is assigned to a standards development track. This track determines the timeframe of the specification project (e.g. 18, 24, or 36 months) as it passes through the various stages to publication (ISO, 2020). For example, the main stages of ISO life cycle are, in order:

1. PRELIMINARY
2. PROPOSAL
3. PREPARATORY
4. COMMITTEE
5. ENQUIRY
6. APPROVAL
7. PUBLICATION

#### *6.1.2.5 Operationalisation index (characterizing a standard)*

For the scope of this study, operationalisation means turning abstract concepts into measurable observations.

Given a textual requirement (e.g. one of the AIA design principle or policy requirements), the operationalisation process defines its extensions by describing what is and is not an instance of that requirement. Standards should specify how to operationalize and measure

design principles and policies expressed via textual requirements -as in the case of the AIA.

Figure 5 describes the methodology applied to evaluate the operationalisation level of a set of acknowledged specifications.

#### 6.1.2.6 Methodology for the operationalisation index analysis

The analysis of the standards and their alignment to the AIA requirements is performed both manually and automatically (as depicted in Figure 5) and is expressed by a total Operationalisation index ( $Oi$ ) calculated for each standard as the result of the combination of its operationalisation level for the eight different requirements (see Equations (2), (3), and (4)). The total operationalisation index considers only those requirements which the standard operationalizes —i.e. the operationalisation indicators that are different from zero ( $Oi_k \neq 0$ ):

$$\left. \begin{array}{l} \forall \text{ standard } s, Oi(s) = \frac{\sum_{k=1}^8 Oi(s)_k}{\text{counter}(s)}; \text{ where} \\ \text{counter}(s) = |\{Oi(s)_k \neq 0\}|; \end{array} \right\} (2)$$

$$\left. \begin{array}{l} \forall \text{ standard } s \text{ and } \forall \text{ AIA requirement } k, Oi(s, k)_l = \frac{\sum_{l=1}^{n_k} \theta(s, k)_l}{n_k}; \text{ where} \\ l(k) = \text{subrequirements of requirement } K; 1 \leq l(k) \leq n_k; \end{array} \right\} (3)$$

$$\left. \begin{array}{l} \theta(s, k)_l = \text{set of acknowledged textual statements (of } s\text{) that matches subrequirement } l(k); \\ \theta(s, k)_l = \begin{cases} 0 & \text{if } \text{text}_l = \emptyset \\ 1 & \text{if } \text{text}_l \neq \emptyset \end{cases}; \end{array} \right\} (4)$$

The objective of operationalisation index estimation is to provide, per each AIA requirement, a radar diagram showing the analysed standards that are “closer” to the different requirement aims -see for example Figure 7.

It is important to observe that, in Equation (2), the operationalisation index for a given standard is normalized by the number of requirements the standard is relevant for, instead of normalizing by the total number of requirements. This choice avoids the penalization of standards that are relevant just for a subset of requirements by avoiding to dilute their weight with a uniform normalization across all standards.

## 7 Semi-structured AIA requirements

### 7.1 Executive version of the AIA requirements and the related keyword lists

The AIA defines a set of requirements, which are presented as a (unstructured) text formulated for being discussed and approved by legal experts. Therefore, in the scope of the detailed analysis, to facilitate the mapping of standards content onto the different requirement prescriptive parts, it was necessary to further structure the requirements content, creating an executive version of that.

Executive version of requirement consists of a set of hierarchically structured sub-requirements -abbreviated as SR.#.# (for example: SR.1 or SR.1.1). They are 24 and are formally structured according to the model showed in Figure 6:

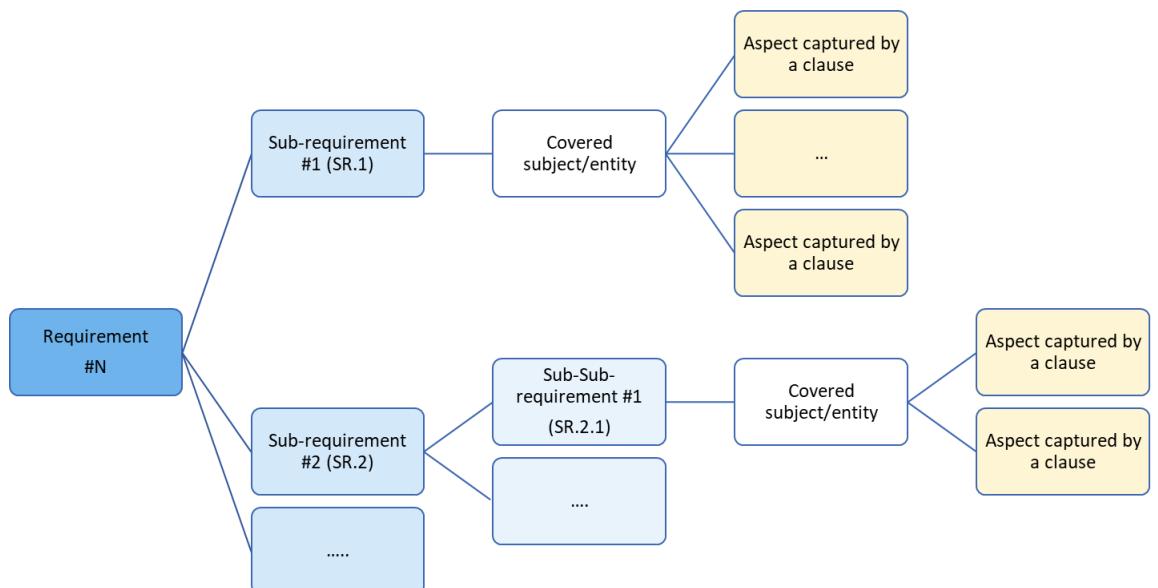


Figure 6. Semi-structured model applied to generate the executive version of the AIA requirements

The executive version of the requirements was instrumental to generate a list of representative keywords to ingest the data mining procedure and extract the relevant content of the analysed standards.

#### 7.1.1 R1. Data and data governance

Table 3. Executive version of the "Data and data governance" requirement

R1. Data and data governance		
Sub-req #	Covered subject/entity	Clauses aspect
SR.1	Training, validation, and testing datasets	Quality Criteria
		Management practices
SR.2		Management practices

	High-risk AI systems not using techniques involving models training	Data governance practices

Table 4. Keywords associated to the "Data and data governance" requirement

<b>Relevant keywords</b>
'data' , 'data governance', 'training', 'label', 'annotation', 'feature', 'bias', 'test', 'class imbalance', 'protected feature', 'ETL', 'coverage', 'representative', 'validation', 'feature importance', 'quality'

### 7.1.2 R2. Technical documentation

Table 5. Executive version of the "Technical documentation" requirement

<b>R.2 Technical documentation</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Technical documentation of the high-risk AI system	A general description of the AI system
		A detailed description of the elements of the AI system and of the process for its development
		Detailed information about the monitoring, functioning and control of the AI system
		A detailed description of the risk management system -see R1
		A description of any change made to the system through its lifecycle
		A list of the harmonised standards applied in full or in part
		A copy of the EU declaration of conformity
		A detailed description of the system in place to evaluate the AI system performance in the post-market phase
SR.2	High-risk AI system	The existence of only one technical documentation file

Table 6. Keywords associated to the "Technical documentation" requirement

<b>Relevant keywords</b>
'technical documentation' , 'document', 'description', 'monitor', 'lifecycle', 'control', 'risk management', 'compliant', 'compliance'

### 7.1.3 R3. Record-keeping

Table 7. Executive version of the "Record-keeping" requirement

<b>R3. Record-keeping</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	High-risk system automatic logging capability (the automatic recording of events while the high-risk AI systems is operating)	Level of Traceability of the logs
SR.2	High-risk system automatic logs content	period of each use of the system reference database against which input data has been checked by the system input data for which the search has led to a match identification of the natural persons involved in the verification of the results

Table 8. Keywords associated to the "Record-keeping" requirement

<b>Relevant keywords</b>
'record', 'log', 'monitor', 'control', 'data provenance', 'input', 'database'

#### 7.1.4 R4. Transparency and provision of information to users

Table 9. Executive version of the "Transparency and provision of information to users" requirement

<b>R4. Transparency and provision of information to users</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Documentation existence (High-risk AI System Operations Transparency)	instructions for use (in an appropriate digital format) or documentation that include (concise, complete, correct and clear) information that is relevant, accessible and comprehensible to users
SR.1.1	Instruction for use and operations documentation	identity and contact details of the provider and, where applicable, of its authorised representative performance (i.e. characteristics, capabilities and limitations)
SR1.1.1	Instruction and documentation content	(AI system) intended purpose; level of accuracy, robustness and cybersecurity tested and validated (possible) circumstance that may lead to risks (to the health and safety or fundamental rights) (AI system) performance for targeted users input data (and other relevant information) used for training, validation and testing
SR.1.2	Instruction for use and operations documentation	the changes (to the system and its performance) pre-determined by the provider for the initial conformity assessment human oversight measures (see R.5) expected lifetime (of the AI system) and necessary maintenance and care measures

*Table 10. Keywords associated to the "Transparency and provision of information to users" requirement*

<b>Relevant keywords</b>
'transparency', 'accuracy', 'security', 'test', 'performance', 'assess', 'human oversight', 'human control', 'human in the loop', 'robust', 'human computer interaction', 'human machine interaction'

### 7.1.5 R5. Human oversight

*Table 11. Executive version of the "Human oversight" requirement*

<b>R5. Human oversight</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Human oversight to preventing or minimize risks	Human health
		Human safety
SR.1.1	Human oversight measures	to be implemented by the system/service Provider
		to be implemented by the system/service User
SR1.2	Human oversight understanding and/or interpretation	Capacities and limitations of the AI system
		Automation biases
		AI system's output
		how not to use, override, or reverse the output of the AI system
		How to modify, interrupt, or stop the operation of the high-risk AI system

*Table 12. Keywords associated to the "Human oversight" requirement*

<b>Relevant keywords</b>		
'human oversight', 'human control', 'correct', 'prevent', 'decision', 'human in the loop', 'fundamental right', 'interpret', 'arrest', 'risk', 'health', 'safety'		

### 7.1.6 R6. Accuracy, robustness and cybersecurity

*Table 13. Executive version of the "Accuracy, robustness and cybersecurity" requirement*

<b>R6. Accuracy, robustness and cybersecurity</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Levels of accuracy and accuracy metrics	Declaration (in the instructions of use)

SR.2	Resilience/robustness as regards errors, faults or inconsistencies	Technical redundancy solutions (e.g backup or fail-safe plans)
		System vulnerabilities exploitation
		Training datasets manipulations (e.g. 'data poisoning', and 'adversarial examples')
		Cybersecurity appropriateness
SR.2.1	Self-learning systems (after being placed on the market or put into service)	'feedback loops' mitigation measures

Table 14. Keywords associated to the "Accuracy, robustness and cybersecurity" requirement

Relevant keywords
'accuracy', 'robust', 'resilient', 'redundancy', 'vulnerability', 'data poisoning', 'adversarial', 'inconsistencies', 'error', 'AUC', 'score', 'misclassification', 'false positive', 'feedback loop', 'interdependency', 'attack', 'risk', 'breach', 'performance', 'assess', 'failure', 'corner case'

### 7.1.7 R7. Risk management system

Table 15. Executive version of the "Risk management system" requirement

<b>R7. Risk management system</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Risk management system characterizing AI system	continuous iterative process run throughout the entire lifecycle
SR.2	Risk management process	identification of risks associated with AI system estimation and evaluation of the risks caused by (reasonably) foreseeable misuse evaluation of other possible risks
SR2.1	Risk management measures to eliminate or reduce risks	adequate design and development mitigation and control measures provision of information to user user training
SR.2	Required pre-conditions to operate the AI system	user's capacities (e.g. technical knowledge, experience, education, training) environment configuration (in which the system is intended to be used)
S.3	Testing of AI system	system performance system compliance (with previous requirements)
S.4	User's age	accessibility to children

*Table 16. Keywords associated to the "Risk management system" requirement*

<b>Relevant keywords</b>
'risk management system', 'risk', 'management', 'deployment', 'design', 'lifecycle', 'compliance', 'access', 'hazard', 'test', 'behaviour', 'service', 'child', 'threshold', 'confidence level', 'pre requisite', 'development', 'monitor'

### 7.1.8 R8. Quality management system

*Table 17. Executive version of the "Quality management system" requirement*

<b>R8. Quality management system</b>		
<i>Sub-req #</i>	<i>Covered subject/entity</i>	<i>Clauses aspect</i>
SR.1	Quality management system (written) description	policies
		procedures
		instructions
SR.1.1	Set of techniques, processes, and procedures (put in place to ensure quality)	compliance strategy
		design, design control and design verification
		development, quality control and quality assurance
		examination, test, and validation periodicity
		applied technical specifications (including standards)
		data management (including: data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention)
		risk management system (see previous R.7)
		post-market monitoring system
		reporting of serious incidents and of malfunctioning
		communication with (national) competent authorities
		record keeping of all relevant documentation and information
		resource management (including security of supply related measures)
		accountability framework

*Table 18. Keywords associated to the "Quality management system" requirement*

<b>Relevant keywords</b>
'quality management system', 'quality', 'policy', 'compliance', 'verification', 'public authorities', 'procedure', 'incident report', 'post-market', 'resource', 'responsibility', 'accountability', 'technical specification', 'design', 'control'

## 8 Results of the in-depth mapping and gap identification

### 8.1 Artificial Intelligence concepts and terminology

Defining artificial intelligence discipline and concepts is still an ongoing effort for the international scientific community<sup>1</sup>. The AIA provides (for the first time) a legal definition of AI system, which guided our work and analysis:

"'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

The in-depth analysis largely focuses on ISO/IEC standards managed by the JRC1/SC42 (Artificial Intelligence). This sub-committee has developed a specific standard (in the enquire phase) dealing with "Artificial intelligence concepts and terminology" (i.e. ISO/IEC DIS 22989). This standard defines AI from both an engineering and a disciplinary point of view. It is a foundational standard to be referenced by the other ISO standards dealing with AI. According to the present draft of ISO/IEC DIS 22989, AI is a "*set of methods or automated entities that together build, optimize and apply a model so that the system can, for a given set of predefined tasks, compute predictions, recommendations, or decisions. AI systems are designed to operate with varying levels of automation*".

Both ISO/IEC engineering definition of AI and the AIA definition of AI system build on the concept of software modeling and introduce the aim of computing predictions and generating recommendations or decisions to influence the external environment.

### 8.2 Operationalisation and suitability analysis results

For each analysed standard, a fiche was generated reporting the respective operationalisation and suitability values. All the generated fiches are reported in Annexes G1 and G2.

A fiche of a given standard consists of:

- (a) A text table summarizing the standard values for all the parameters composing the suitability index.
  - (b) A spider map depicting the operationalisation values against each of the eight AIA requirements and the other suitability parameter values.
  - (c) A text table containing the summary of the AIA sub-requirements affected by the standard context (as acknowledged by the supervised data mining procedure).
- 

<sup>1</sup> The European Commission, in its AI strategy communication (European Commission, 2020), considered the following definition: "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)." Subsequently, this definition was refined by the European High Level Expert Group on AI: "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions." (Highlevel Expert Group on Artificial Intelligence, 2019)

(d) A text table fully mapping the relevant content of the standard (as acknowledged by the supervised data mining procedure) and the AIA sub-requirements -in their semi-structured form.

Due to IPR reasons, in Annexes G1 and G2 only the first three results are included in this public report.

Analysing the operationalisation and suitability indexes, their distribution in respect to the AIA requirements, and (in general) the fiche mapping tables, it is possible to recognize some gaps.

### 8.3 Operationalisation gaps

While the total operationalisation index of a standard (i.e  $O_i$ ) contributes to form the suitability index, the operationalisation indexes calculated against each AIA requirement (i.e.  $O_{ik}$ ), are useful to understand the most promising standards and the existing gaps - at the level of specific requirements and sub-requirements. To visualize the result of such an analysis, a set of radar diagrams shows the "distance" distribution of the processed standards, in the respect of each AIA requirement objectives -see Figures Figure 7-Figure 14.

To appreciate the possible gaps at the sub-requirement level (see the executive version of the AIA requirements, in Section 7), the mapping among the processed standards and the sub-requirements is reported in Table 19.

Table 19. Role of the analysed standards in operationalisation the AIA sub-requirements. The outlined columns (with a pink background) shows the evident gaps, at the sub-requirements level.

Requirement	Data and data governance	Technical documentation	Record keeping	Transparency and information to users	Human oversight	Accuracy, robustness, and cybersecurity	Risk management system	Quality management system																
Standard	1	2	1	2	1	2	1	1.1	1.1.1	1.2	1	1.1	1.2	1	2	1	1.1	1.2	2	3	4	1	1.1	
AIA Sub-Requirement (SR.#.#.#)																								
ISO/IEC TS 4213	x								x						x	x					x			x
ISO/IEC AWI 5259-1	x																							x
ISO/IEC AWI 5259-2	x								x															x
ISO/IEC AWI 5259-3	x								x									x				x	x	
ISO/IEC AWI 5259-4	x														x									x
ISO/IEC AWI 5338	x													x		x		x	x	x	x	x		x
ISO/IEC TR 5469	x								x						x	x	x	x	x	x	x	x		
ISO/IEC 20547-3																								x
ISO/IEC 23894-2	x		x		x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	

ISO/IEC 24027	x			x			x	x	x	x					x						
ISO/IEC TR24028											x										
ISO IEC TR 24029-1	x						x							x	x	x		x		x	x
ISO/IEC DTR 24372																					
ISO/IEC CD 24668	x				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
ISO/IEC 38507	x						x	x	x	x	x	x	x			x	x	x	x	x	
ISO/IEC 42001	x		x				x	x	x	x	x	x	x	x	x	x	x	x	x	x	
ETSI GR SAI 001																					
ETSI GR SAI 002	x													x							
ETSI GR SAI 003														x							
ETSI GR SAI 004																					
ETSI GR SAI 005	x													x							
ETSI GR SAI 006														x							

The depicted radar diagrams distinguish four groups of standards characterized by their distance ranges to the AIA requirement aim:

- Very High operationalisation level of the requirement K ( $0i_k \geq 0.7$ )
- High operationalisation level of the requirement K ( $0.5 \leq 0i_k < 0.7$ )
- Medium operationalisation level of the requirement K ( $0.3 \leq 0i_k < 0.5$ )
- Low operationalisation level of the requirement K ( $0.1 \leq 0i_k < 0.3$ )

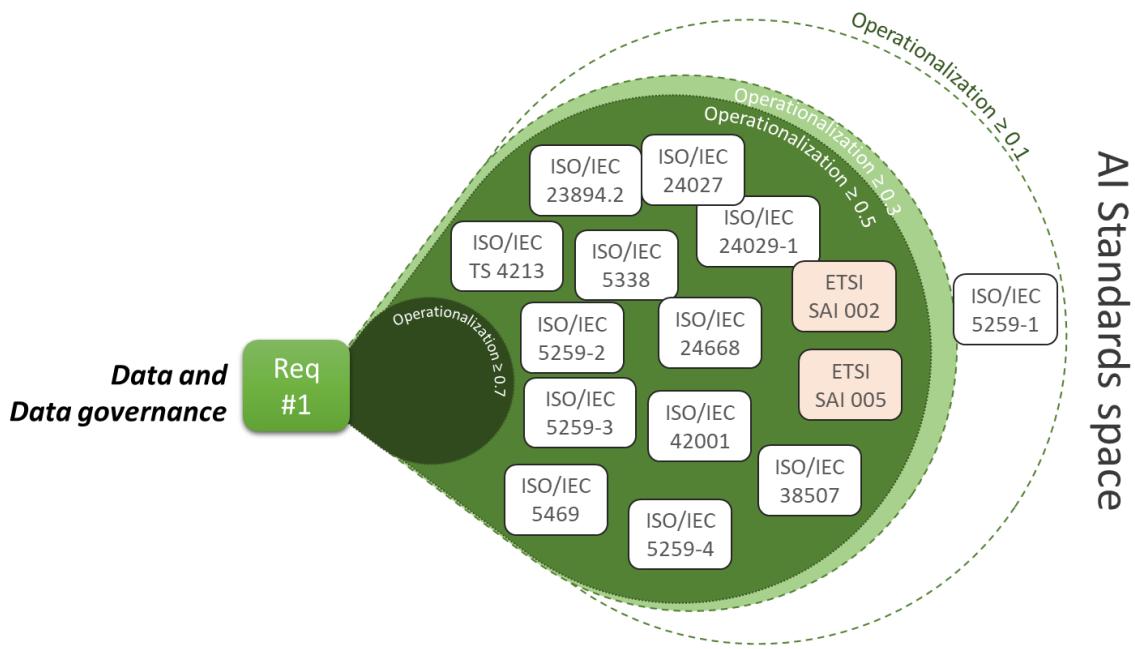


Figure 7. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Data and Data Governance" (ETSI standards are represented as pink boxes, while ISO/IEC standards have a white background)

## AI Standards space

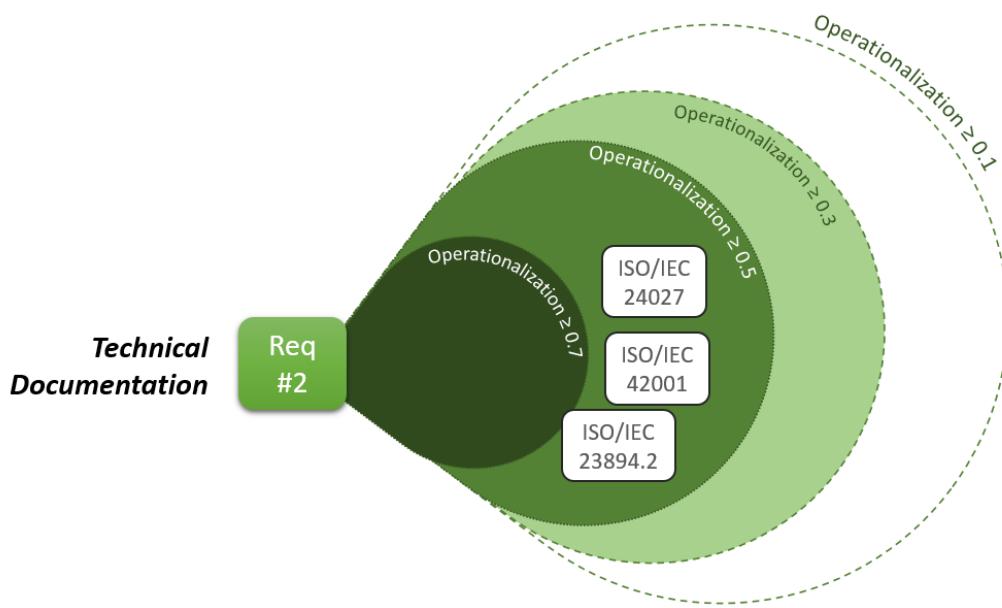


Figure 8. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Technical Documentation"

## AI Standards space

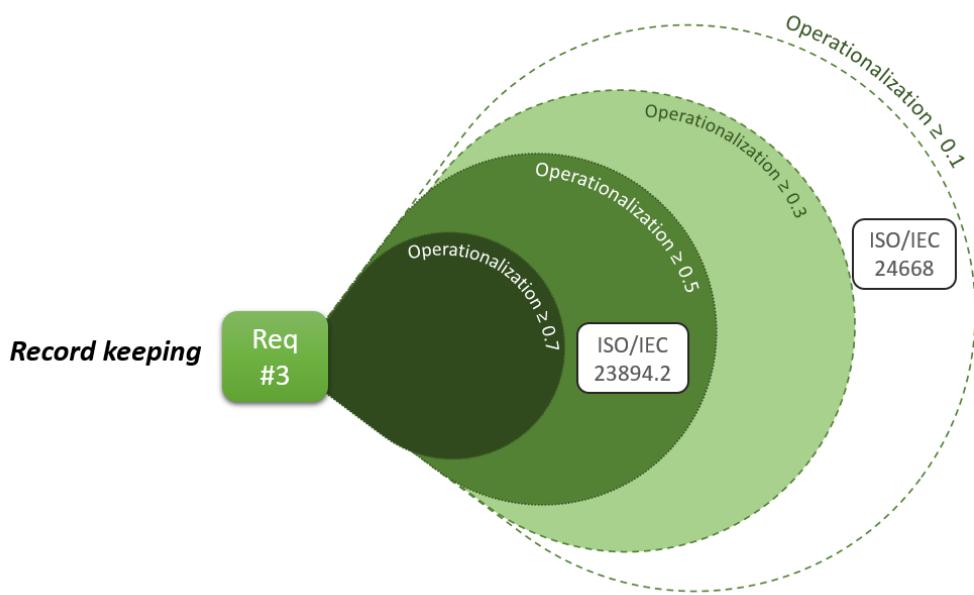


Figure 9. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Record Keeping"

## AI Standards space

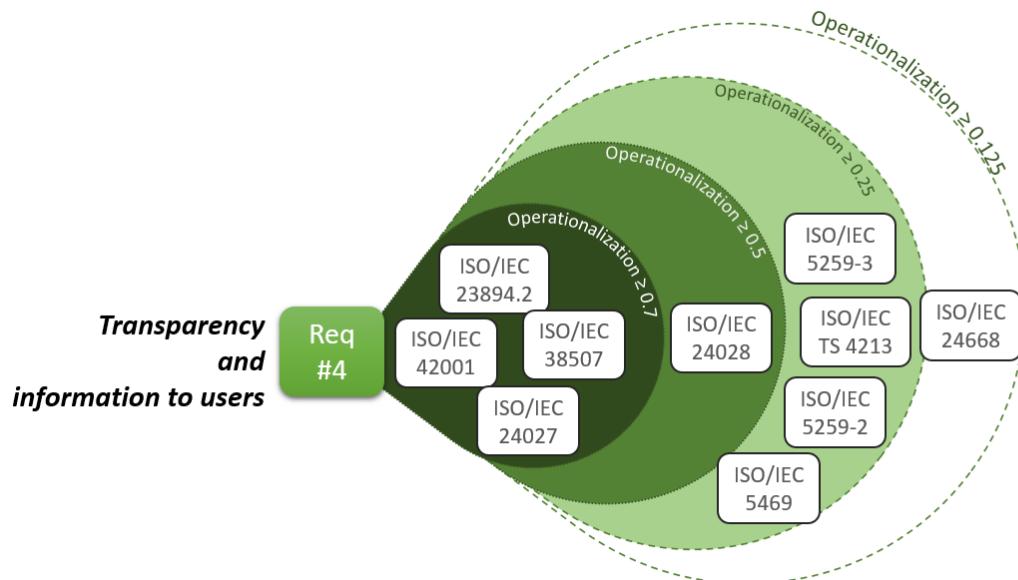


Figure 10. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Transparency and information to users"

## AI Standards space

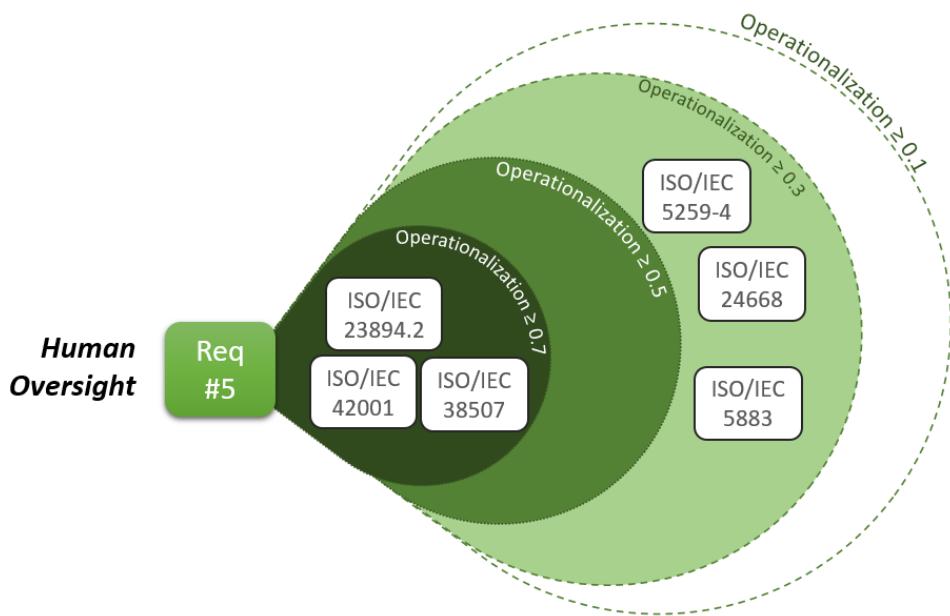


Figure 11. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Human Oversight"

## AI Standards space

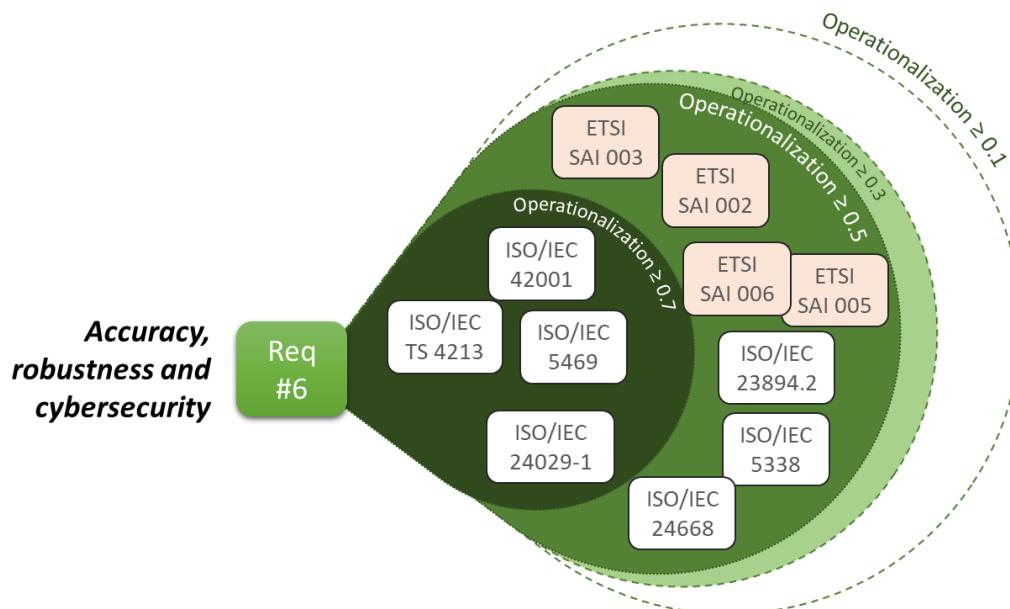


Figure 12. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement “Accuracy, robustness and cybersecurity” (ETSI standards are represented as pink boxes, while ISO/IEC standards have a white background)

## AI Standards space

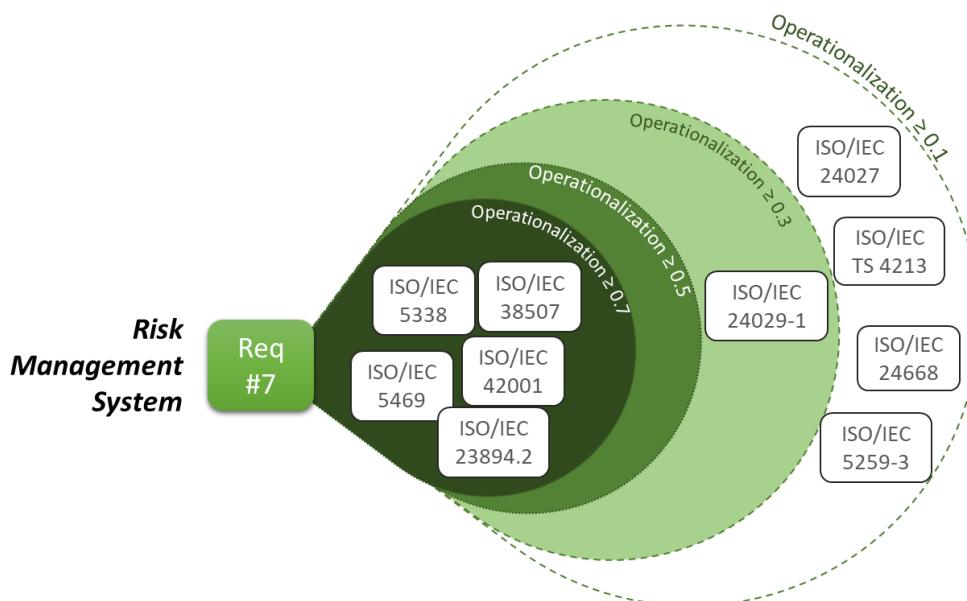
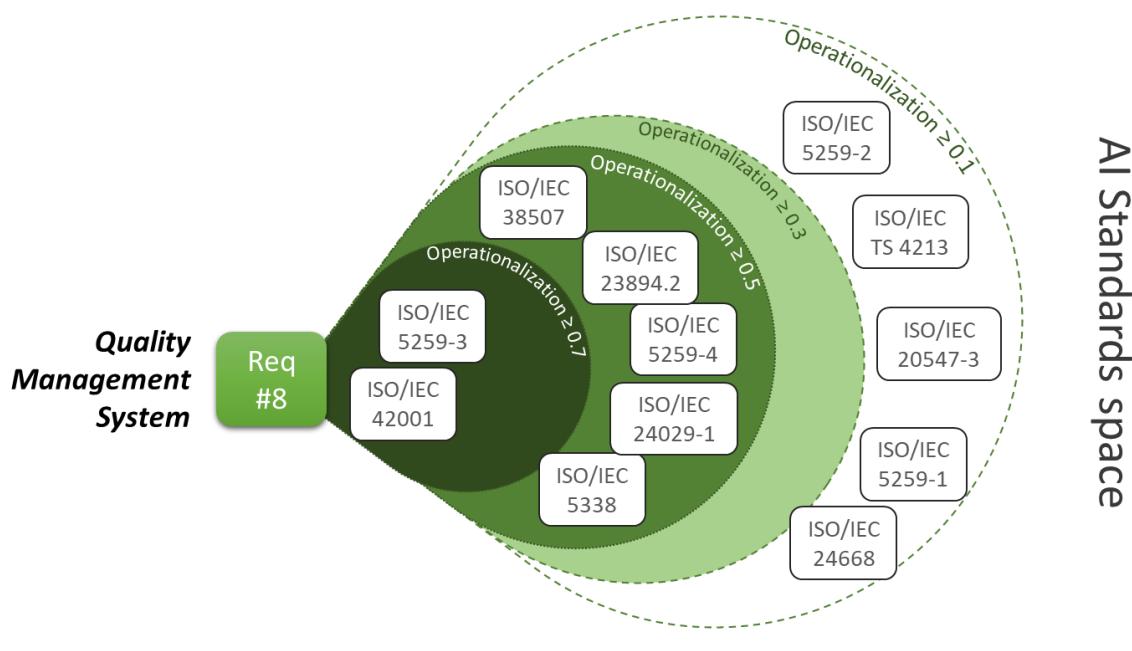


Figure 13. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement “Risk Management System”



*Figure 14. Radar diagram of the operationalisation levels characterizing the analysed standards, to support the AIA requirement "Quality Management System"*

### 8.3.1 Discussion

#### 8.3.1.1 General findings

We analysed in-depth 22 standards managed by ISO/IEC and ETSI; only three of them were assessed as irrelevant for operationalizing (one or more) AIA requirements. Fourteen standards performed well resulting with a high or very high operationalisation level for one AIA requirement, at least.

For five out of eight AIA requirements, the radar diagrams “detect” standards with a very high level of operationalisation (more or equal to 0.7). These requirements are: “Transparency and information to users”, “Human Oversight”, “Accuracy, robustness and cybersecurity”, “Risk Management System”, and “Quality Management System”.

For the remaining three requirements (i.e. “Data and Data Governance”, “Technical Documentation”, and “Record Keeping”) the diagrams detect standards with a high level of operationalisation (from 0.5 to 0.7).

All the standards with a very high operationalisation index are ISO/IEC specifications. The ETSI standards, characterized by a good value of operationalisation, interest principally a couple of requirements: “Data and Data Governance” and “Accuracy, robustness and cybersecurity”. This is consistent with the three key areas on which the ETSI SAI (Securing Artificial Intelligence) focus: using AI to enhance security, mitigating against attacks that leverage AI, and securing AI itself from attack.

Noteworthy, although for the standard ISO/IEC 24372 many relevant paragraphs were recognized, their content was not considered effective for operationalizing the AIA requirements. This is consistent with the typology and maturity of the document, which is a draft technical report.

Four standards are characterized by a very high operationalisation levels (ISO/IEC 5338; ISO/IEC 5469; ISO/IEC 4213; ISO/IEC 24029-1). In particular, ISO/IEC 5469 results extremely close to the objectives of two requirements: “Accuracy, Robustness, and

Cybersecurity" and "Risk Management System". Interestingly, ISO/IEC 24029-1 has a very high operationalisation value for the Requirement 6 "Accuracy, robustness and cybersecurity" but the total operationalisation index value is low because of its very low impact on all the other requirements.

Naturally, we do not expect to find a standard that covers all the requirements; therefore, standards with a high operationalisation for one requirement result extremely relevant for the AIA regulation. This consideration guided to the definition of the group of "operationalisation essential standards".

### 8.3.1.2 The group of operationalisation essential standards

Looking at the standard fiches (see Annexes G1 and G2), it is possible to recognize which standards have a very high operationalisation value for the single AIA requirements. It is useful to **recognizing a set of essential standards that provide a very high operationalisation value for at least one AIA requirement** (i.e. score  $\geq 5.5$ ):

- ISO/IEC 4213
- ISO/IEC 5259-3
- ISO/IEC 5338
- ISO/IEC 5469
- ISO/IEC 23894-2
- ISO/IEC 24027
- ISO IEC 24029-1
- ISO/IEC 38507
- ISO/IEC 42001

This set of standards (referred in the rest of the document as the **group of operationalisation essential standards**) provides the best baseline to operationalize the AIA requirements.

The **group of operationalisation essential standards does not cover the first three AIA requirements** (i.e. i.e. "Data and Data Governance", "Technical Documentation", and "Record Keeping"), as already discussed. This **can be recognized as a gap in the view of identifying future standardisation needs**.

*Table 20. Standards operationalisation values (score from 0 to 1) for each AIA requirements and the value resulting total operationalisation indexes (bold value are greater than 0.5).*

	Data and data governance	Technical documentation	Record keeping	Transparency and information to users	Human oversight	Accuracy, robustness, and cybersecurity	Risk management system	Quality management system	Total Operationalisation value
ISO/IEC TS 4213	0.5	0	0	0.25	0	<b>1</b>	0.16	0.5	<b>0.58</b>
ISO/IEC AWI 5259-1	0.25	0	0	0	0	0	0	0.25	0.25
ISO/IEC AWI 5259-2	0.5	0	0	0.25	0	0	0	0.5	0.41
ISO/IEC AWI 5259-3	0.5	0	0	0.25	0	0	0.16	<b>1</b>	0.48
ISO/IEC AWI 5259-4	0.5	0	0	0	0.33	0	0	0.5	0.44

ISO/IEC AWI 5338	0.5	0	0	0	0.33	0.5	<b>0.83</b>	0.5	<b>0.53</b>
ISO/IEC TR 5469	0.5	0	0	0.25	0	<b>1</b>	<b>0.83</b>	0	<b>0.64</b>
ISO/IEC 20547-3	0	0	0	0	0	0	0	0.25	0.25
ISO/IEC 23894-2	0.5	0.5	0.5	<b>1</b>	<b>1</b>	0.5	<b>0.83</b>	0.5	<b>0.66</b>
ISO/IEC 24027	0.5	0.5	0	<b>1</b>	0	0	0.16	0	<b>0.54</b>
ISO/IEC TR 24028	0	0	0	0.5	0.33	0	0	0	0.41
ISO IEC TR 24029-1	0.5	0	0	0.25	0	<b>1</b>	0.33	0.5	<b>0.51</b>
ISO/IEC DTR 24372	0	0	0	0	0	0	0	0	0
ISO/IEC CD 24668	0.5	0	0.25	0.12	0.33	0.5	0.16	0.25	0.30
ISO/IEC 38507	0.5	0	0	<b>1</b>	<b>1</b>	0	<b>0.83</b>	0.5	<b>0.76</b>
ISO/IEC 42001	0.5	0.5	0	<b>0.75</b>	<b>1</b>	<b>1</b>	<b>0.83</b>	<b>1</b>	<b>0.79</b>
ETSI GR SAI 001	0	0	0	0	0	0	0	0	0
ETSI GR SAI 002	0.5	0	0	0	0	0.5	0	0	<b>0.5</b>
ETSI GR SAI 003	0	0	0	0	0	0.5	0	0	<b>0.5</b>
ETSI GR SAI 004	0	0	0	0	0	0	0	0	0
ETSI GR SAI 005	0.5	0	0	0	0	0.5	0	0	<b>0.5</b>
ETSI GR SAI 006	0	0	0	0	0	0.5	0	0	<b>0.5</b>

At the requirement level, **the analysis showed the lack of high operationalisation standards for the first three AIA requirements**. However, at the sub-requirement level (see Table 19), the investigation outlined that **this is true only for some of their sub-requirements (clear gaps)**:

- (Req 1) Data and data governance:
  - SR.2: High-risk AI systems not using techniques involving models training
    - Management practices
    - Data governance practices
- (Req 2) Technical documentation:
  - SR.2: High-risk AI system
    - The existence of only one technical documentation file
- (Req 7) Risk management system
  - S.4: User's age
    - accessibility to children

A further discussion dealing with the single AIA requirements is the subject of the next paragraphs.

#### *8.3.1.3 “Technical documentation” and “Record keeping” requirements*

“Technical documentation” and “Record keeping” requirements have a low operationalisation, being operationalized by, respectively, three standards and two standards; furthermore, the sub-requirement 2 (SR.2) concerning the uniqueness of the technical documentation is not mentioned in any of the recognized specifications. However, as the AIA itself prescribes in detail the necessary elements of the technical documentation (by virtue of a dedicated annex) a specific standard capturing this requirement may not be necessary. This is in fact not a domain traditionally covered by standardisation in product legislation.

#### *8.3.1.4 “Accuracy, robustness and cybersecurity” and “Data and data governance” requirements*

These requirements are characterized by the highest number of standards within the High and Medium operationalisation categories: indeed “Accuracy, robustness and cybersecurity” and “Data and data governance” are, for AI systems, pivotal concepts and, therefore, a lot of standardisation work addresses them, directly or indirectly.

However, for “Data and data governance”, Table 19 shows how the sub-requirement 2 (SR.2), dealing with AI systems not requiring model training, is not mentioned in the analysed specifications. This is the reason for not having very high operation standards for this requirement. On the other hand, “Accuracy, robustness and cybersecurity” is very well operationalized, by four standards with operationalisation larger than 0.7.

#### *8.3.1.5 “Quality Management System” and “Risk management system” requirements*

Both “Risk Management Systems” (RMS) and “Quality management systems” (QMS) are very well covered, with respectively five and seven standards in the zone with operationalisation larger than 0.5.

This is not surprising as they build on the extensive pre-existing standardisation literature addressing RMS and QMS in the software and big data context, hence many of the analysed standards are a natural extension of them in the context of AI. It is, however, noteworthy that the sub-requirement 4 (SR.4) of RMS, dealing with children’s accessibility to AI products and services is absent from the analysed specifications.

Finally, in the case of QMS, while the sub-requirements SR.1.1 is well covered (12 standards), the more general and holistic requirement (SR.1) is covered partially only.

#### *8.3.1.6 “Human Oversight” requirement*

The “Human Oversight” is operationalized by three standards with operationalisation larger than 0.7. However, the recognized standards give mostly a broad guidance in carrying out such oversight, in line with the horizontality of the considered standards.

A higher degree of operationalisation for human oversight of an AI system may imply taking into account the specificities of the AI application, therefore involving more vertical considerations which could partially explain its relative limited coverage in our analysis, where we focused on horizontal standards. To address the operationalisation level required by the AI system developers, a set of vertical standards (addressing specific application domain and technological frameworks) might be required to be follow —see also one of the final recommendations.

### 8.3.2 Total Operationalisation index (southern hemisphere)

To calculate a unique and holistic operationalisation value that characterizes each standard, the eight operationalisation indicators are combined according to Equation (2) (see Section 8.3) determining the Total Operationalisation index (i.e. O<sub>i</sub>). According to our methodology, this parameter contributes to calculate the Suitability index of a given standard. The O<sub>i</sub> values (representing each standard) are reported in the last column of Table 20. According to this parameter, it is possible to distinguish three groups of standards:

- Standards with a High total operationalisation ( $\geq 0.7$ )
- Standards with a Medium total operationalisation ( $0.5 \leq O < 0.7$ )
- Standards with a Low total operationalisation ( $< 0.5$ )

It is worth noticing that our choice of normalization for the Total Operationalisation index avoids penalising standards with a high operationalisation score in just a subset of requirements: as it is possible to observe in Table 20, the Medium and High total operationalisation score correlates with having one or more requirements with a high operationalisation, with the sole exception of ISO/IEC 5259-3, which stands as an outlier.

Two standards are characterized by a high total operationalisation value (i.e. ISO/IEC 42001 and ISO/IEC 38507). Nine standards have a medium total operationalisation value, five from ISO/IEC and four from ETSI. Only three standards have a total operationalisation value equal to zero.

## 8.4 Suitability gaps

As discussed in section 6.1.2 (Suitability index methodology), the suitability index is the result of the (weighted) contribution of some traits characterizing the analysed standard; traits that are considered important for implementing the AIA. The total operational index is only one of these traits, although extremely important.

For each analysed standard, a spider diagram (introduced in Annexes G1 and G2) shows the value of the parameters contributing to the suitability index. For example, the spider diagram of the standard ISO/IEC 24668 is depicted in Figure 15.

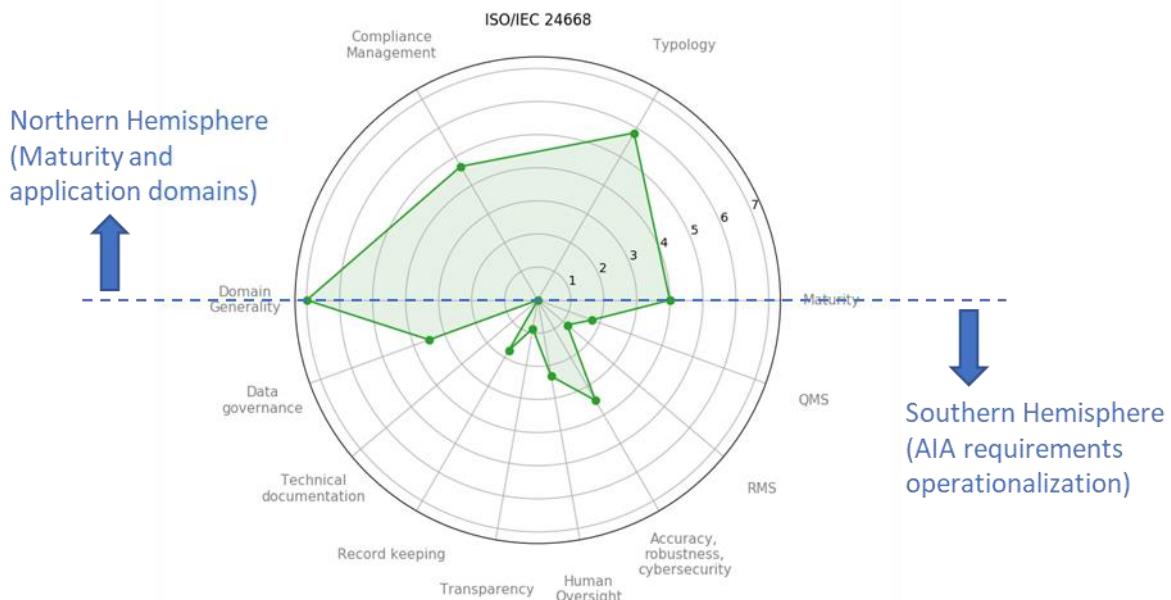


Figure 15. The spider diagram of standard ISO/IEC 24668, showing the values of the suitability index factors.

The northern hemisphere deals with the standard maturity, typology, and domain application aspects (see Section 6.1.2), while the southern hemisphere contains the operationalisation levels of the standard in respect to the eight AIA requirements —the combination of which generates the total operational index. The weighted combination of the values of the two hemisphere quantifies the suitability index.

The calculated suitability indicators can be plotted in a radar diagram, which shows the “proximity” (i.e. relevance) of each standard to the AIA objectives —see Figure 16 and Figure 17. The depicted radar diagrams distinguish among four “proximity” range categories, defining four corresponding groups of standards:

- Standards characterized by a **High suitability** level ( $Si \geq 0.5$ )
- Standards characterized by a **Medium suitability** level ( $0.5 < Si \leq 0.4$ )
- Standards characterized by a **Low suitability** level ( $0.4 < Si \leq 0.3$ )
- Standards characterized by a **Very Low suitability** level ( $0.3 < Si \leq 0.1$ )

### 8.4.1 Southern hemisphere contribution to the suitability index (the total operationalisation index)

The contribution of the southern hemisphere to the Suitability index is equal to the total operationalisation index. This complex indicator is calculated from the operationalisation indicators computed against the eight AIA requirements —see Equations (2), (3), (4).

To make the total operationalisation index meaningful and consistent with the requirements operationalisation indicators, it is important to note that:

- (a) The eight requirements are not independent each other, covering (in different combinations) common subjects. Therefore, it is common that a standard results relevant for more than one requirement.
- (b) If a given standard is associated to a high operationalisation indicator for one requirement, this value is effectively weighted in the calculation of the total operational index —by a specific normalization strategy.
- (c) Consistently, for the total operational index calculation, operationalisation indicators equal to zero are not considered —see Equation (2).

As a result, the total operationalisation indexes provide holistic values that are consistent with the operationalisation indicators discussed in the previous section.

The total operationalisation index is a key parameter for calculating the suitability index, thus, its (normalized) weighing factor is always assumed to be 1. In addition, where the total operationalisation index is equal to zero, also the suitability index must be considered equal to zero.

#### 8.4.2 Northern hemisphere contribution to the suitability index

It is reasonable to think of (and create) different suitability indexes considering the diverse concerns that distinguish the different stakeholders to ensure the development of a well-functioning internal market for AI systems, where both benefits and risks of AI are adequately addressed at Union level.

This is achieved by assigning different weight to the parameters belonging to the northern hemisphere —as anticipated the operational index weight is always taken equal to 1. In this document, we adopted the viewpoint of a couple of important (and broad) stakeholder categories and generated two different suitability indexes showed in the radar plots of Figure 16 and Figure 17.

#### 8.4.3 Viewpoint #1: EU regulatory framework implementers

These stakeholders are mainly concerned about the European and International standardisation process to underpin the regulatory framework and implement the AIA.

Considering that the AIA was released in April 2021, and the regulatory framework will likely not be adopted before 2023, it is reasonable to decide that the maturity level of the present standards (along with the existence of compliance tools) are not essential —according to ISO, “from first proposal to final publication, developing a standard usually takes about 3 years”.

This leads to assign the following values for calculating a suitability index that is much more concerned about the operationalisation level:

$$w1 = 1; w2=0.7/4; w3=0.5/4; w4=1/4; w5=0.3/4;$$

In a nutshell, the sum of all the (weighted) contributions belonging to the northern hemisphere would, at most, equal the total operationalisation contribution (i.e. the southern hemisphere part). The radar diagram showing the resulting suitability indexes is depicted in Figure 16.

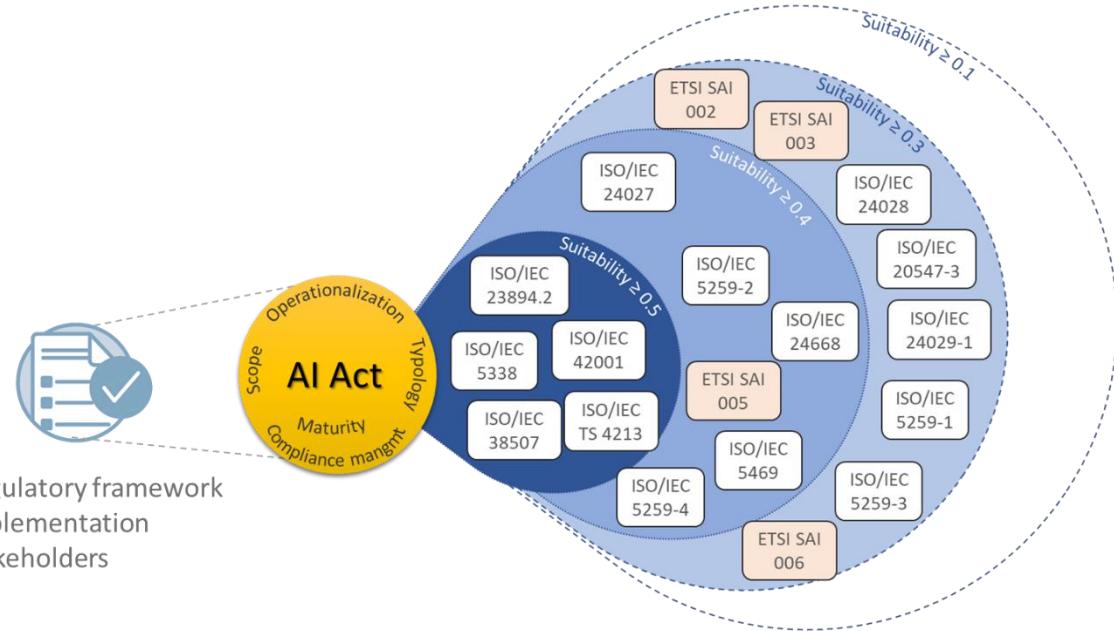


Figure 16. Radar diagram of the suitability levels characterizing the analysed standards, from the point of view of regulatory framework implementation stakeholders (ETSI standards are represented as pink boxes, while ISO/IEC standards have a white background)

#### 8.4.4 Viewpoint #2: AI system developers

The viewpoint of an AI system developer is concerned about finding an actual standard that is already mature and provides a good level of operationalisation of the AIA requirements, with which she/he wants to comply. Naturally, the existence of compliance instruments would be an important element to be considered, too.

To reflect these needs, the weighting values give more importance to the present maturity level, as long as the operationalisation value is acceptable:

$$w1 = 1; w2 = 0.7/0.25; w3 = 0.5/0.25; w4 = 1/0.25; w5 = 0.3/0.25;$$

In a nutshell, in the respect of the previous configuration, the contribution of the northern hemisphere is amplified (by a factor 4) compared to the southern one (i.e. the total operationalisation value). The radar diagram showing the resulting suitability indexes is depicted in Figure 17.

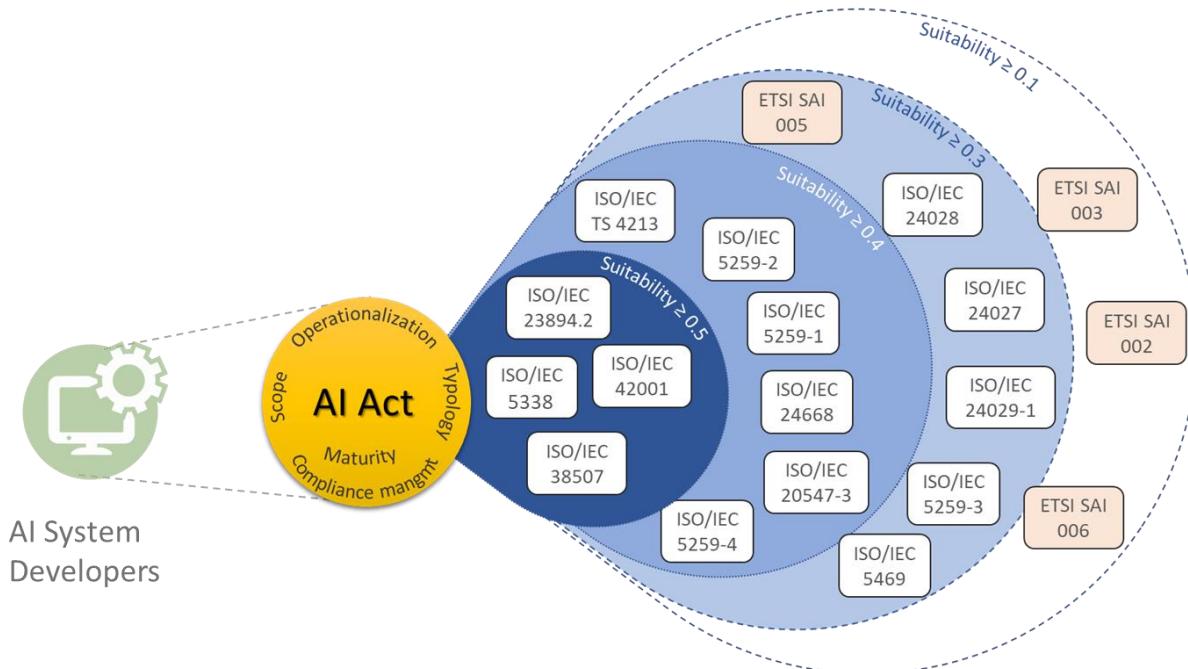


Figure 17. Radar diagram of the suitability levels characterizing the analysed standards, from the point of view of AI system developers (ETSI standards are represented as pink boxes, while ISO/IEC standards have a white background)

#### 8.4.5 Discussion

A couple of standards suitability maps were calculated by reflecting two important and different viewpoints. In both cases 19 (out of 22) standards are mapped.

In the perspective of who must implement the AIA reference framework, the 19 standards are in general more suitable (e.g. more standards with a high and medium suitability level and no standard with a very low suitability value) than in the view of AI system developers. In other words, in the radar map the standards are “closer” to the AI act gravitational point —this is due to the good values calculated for the total operationalisation index. While in the second radar map, the standards are more dispersed because of the diverse maturity levels associated to the standards.

It is worthy to note that in both cases (i.e. adopting two quite different point of views), the *high* suitability standards remain the same (with the only exception of ISO/IEC TS4313). A similar remark can be done for the *medium* suitability standards (with two exceptions, this time). This invariance suggests the opportunity to **recognizing a group of essential standards that result suitable, despite the viewpoint considered**:

- ISO/IEC 23894-2
- ISO/IEC 5338
- ISO/IEC 42001
- ISO/IEC 38507
- ISO/IEC 4213
- ISO/IEC 5259-2
- ISO/IEC 5259-4
- ISO/IEC 24668
- ISO/IEC 24027

This set of standards (referred in the rest of the document as the **group of suitability essential standards**) provides the best compromise between operationalisation and

maturity levels. The requirements and sub-requirements operationalisation provided by this group of important standards is represented in Tables 19 and 20.

With reference to Figure 18, both the groups of operationalisation and suitability essential standards consist of nine elements. The intersection of the two sets contains six common elements:

- ISO/IEC 4213
- ISO/IEC 5338
- ISO/IEC 23894-2
- ISO/IEC 24027
- ISO/IEC 38507
- ISO/IEC 42001

This group of standards may be indicated as the **group of core standards**

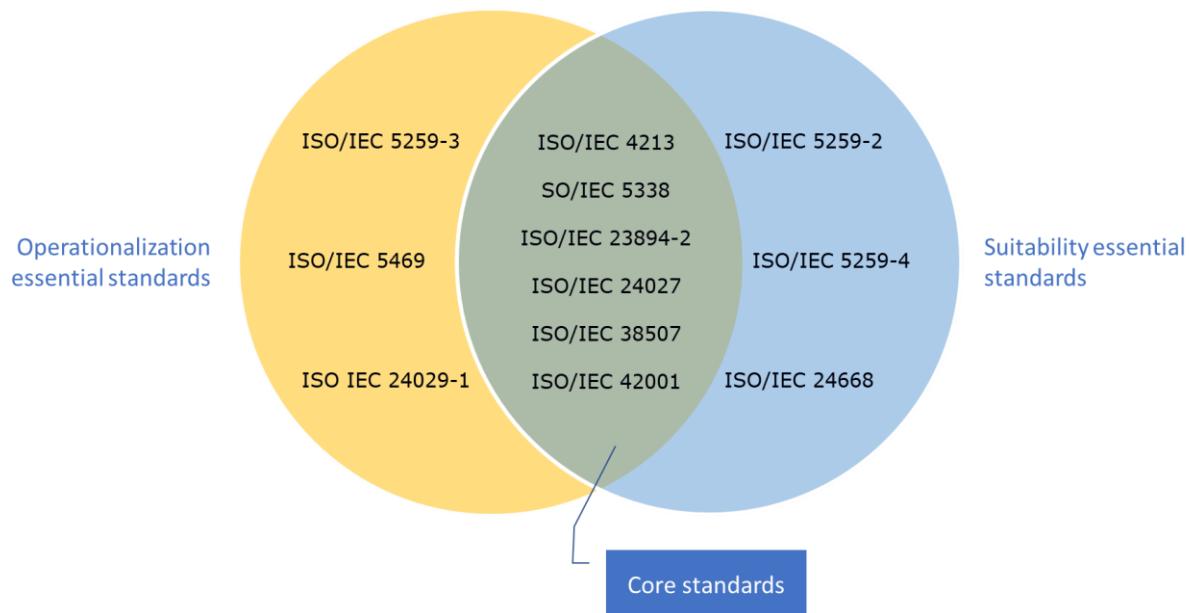


Figure 18. The relationship between the groups of operational/suitability essential standards and the core ones.

According to our study, these are the three groups of standards recognized as the most relevant ones, presently. Immediately after these standards, it is useful to also consider the standards (eight ones) that showed a medium operationalisation index —as documented in Table 20.

## 9 Conclusions and Recommendations

In this technical report an **overview of the present AI standards landscape** was briefly provided. A **high-level analysis was carried out to map the introduced standards**

**onto the eight requirements defined by the AIA<sup>2</sup>.** For this version of the report, only ISO/IEC JTC1-SC42 standards and ETSI SAI standards were analysed by the study.

To refine the mapping and understand possible gaps, an **in-depth analysis** was carried out using a **supervised analytical methodology to calculate the operationalisation and suitability level** of a set of international standards to implement the requirements introduced by the AIA.

The supervised analytical procedure allowed **to recognize the significant paragraphs connecting each analysed standard to the eight AIA requirements.**

Our analysis found that **many relevant standards exist (already published or in the pipeline).** Therefore, **the AIA requirement operationalisation can build on existing efforts.**

*Table 21. Summary of the relevant standards for the AIA key requirements (in bold, standards already published or in final draft status)*

Requirement	Very high/high operationalisation standards
<b>Data and data governance</b>	ISO/IEC TS 4213, ISO/IEC 5259-2, ISO/IEC 5259-3, ISO/IEC 5259-4, ISO/IEC 5338, ISO/IEC 5469, ISO/IEC 23894.2, ISO/IEC 24027, <b>ISO/IEC 24029-1</b> , ISO/IEC 24668, ISO/IEC 38507, ISO/IEC 42001, ETSI SAI 002, <b>ETSI SAI 005</b>
<b>Technical documentation</b>	ISO/IEC 23894.2, ISO/IEC 24027, ISO/IEC 42001
<b>Record keeping</b>	ISO/IEC 23894.2
<b>Transparency and information to users</b>	ISO/IEC 23894.2, ISO/IEC 24027, <b>ISO/IEC 24028</b> , ISO/IEC 38507, ISO/IEC 42001
<b>Human oversight</b>	ISO/IEC 23894.2, ISO/IEC 38507, ISO/IEC 42001
<b>Accuracy robustness and cybersecurity</b>	ISO/IEC TS 4213, ISO/IEC 5338, ISO/IEC 5469, ISO/IEC 23894.2, <b>ISO/IEC 24029-1</b> , ISO/IEC 24668, ISO/IEC 42001, ETSI SAI 002, ETSI SAI 003, <b>ETSI SAI 005</b> , ETSI SAI 006
<b>Risk management system</b>	ISO/IEC 5338, ISO/IEC 5469, ISO/IEC 23894.2, ISO/IEC 38507, ISO/IEC 42001
<b>Quality management system</b>	ISO/IEC 5259-3, ISO/IEC 5259-4, ISO/IEC 5338, ISO/IEC 23894.2, <b>ISO/IEC 24029-1</b> , ISO/IEC 38507, ISO/IEC 42001

<sup>2</sup> i.e. "Data and data governance", "Technical Documentation", "Record keeping", "Transparency and provision of information to users", "Human oversight", "Accuracy, robustness, and cybersecurity", "Risk management system", "Quality management system" (European Commission, 2021)

However, the calculation of **operationalisation indicators allowed to recognize significant gaps at the level of certain AIA sub-requirements**, notably for the following requirements: "Data and data governance", "Technical documentation", and "Risk system management". Three sub-requirements gaps were recognized:

- Req 1: Data and data governance → SR.2: High-risk AI systems not using techniques involving models training (i.e. management practices and data governance practices)
- Req 2: Technical documentation → SR.2: High-risk AI system (i.e. the existence of only one technical documentation file)
- Req 7: Risk management system → S.4: User's age (i.e. accessibility to children)

The analysis further identified a **group of twelve operationalisation/suitability essential standards relevant to the eight requirements constituting the AIA reference framework**. For the present purposes, an essential standard can be defined as a standard that contributes in a significant way the implementation of one or more AIA requirements, as currently expressed in the Commission's proposal.

**A core group of standards**, which includes six ISO/IEC standards, was then identified. It corresponds to the intersection of the sets constituting the suitability and operationalisation groups of essential standards. Presently, **these standards emerged as the most relevant working items to focus on, for implementing the AIA act and addressing the concerns of the different stakeholders**.

It should be noted that, for specific requirements or sub-requirements, standards (other than the essential ones) may also have a high/good operationalisation score; these latter standards stand in a non-trivial relationship with the set of recognized essential standards, since different specifications are usually developed independently. Thus, as they are not designed coherently, the essential standards may be locally overlapping with the less relevant ones but, also, they may present different facets of the same concept, being to some extent complementary.

**In the next iterations of this report, the group of essential standards will likely be complemented by others** (there are **about 50 AI standards to be published by the end of 2023**) which might contribute to cover some of the existing gaps. As already done with the high-level analysis and mapping, in the near future IEEE and ITU-T standards will be analysed in-depth.

Drawing from our analysis, the following broad recommendations may thus be formulated to the Commission in order to support the development of usable standards for AI:

- **Continuously monitor the development of relevant standardisation working items**, as identified in this study.
- **Engage and work together with the relevant standardisation organisations (noticeably the ESOs) and standard committees** identified in this study, especially for the purpose of improving the suitability of standards and address identified gaps, on the basis of the methodology and conclusions outlined in this report. In that context, specific attention should be paid to the following aspects:
  - the developments related to ongoing standardisation work on AI definition and terminology<sup>3</sup>;

---

<sup>3</sup> In particular, it is recommended to follow the development of the work managed by OECD on AI concepts and systems definition and of ISO/IEC DIS 22989 "Artificial intelligence concepts and terminology".

- the need for vertical standards (possibly selecting priority areas)<sup>4</sup>;
- the consideration of compliance management instruments. In doing that, it is recommended to introduce specific risk and management system requirements;
- the actual need and extent of standardisation activities with regard to technical documentation, taking into account the level of detail of the related provisions in the AIA and the experience in product legislation;
- the need for surveys and pre-standardisation activities, where existing sub-requirements gaps are recognized.
- **Update the present study regularly** to reflect ongoing AI standardisation developments and the evolution of the European AIA framework. It is recommended to apply the introduced in-depth methodology (noticeably, the developed supervised analytical procedure) to analyse the future development of the recognized standards — and assess the expected improvement, in terms of AIA act operationalisation.

Moreover, in order to support AI system developers, as well as other stakeholders dealing with the AIA, **analyse the network created by the multi-level connections of the first level standards** (i.e. the recognized core and essential standards) and **create a digital tool/framework**. This would help stakeholders to understand the connectivity and complexity of first-level standards implementation and the complementarity of different standards. If the framework covers different SDOs, it would also support stakeholders in recognizing consistency and/or overlaps characterizing standards managed by different SDOs, for implementing the AIA.

---

<sup>4</sup> In particular, it is expected that this investigation might play an important role in relation with the "Human oversight" requirement for two reasons: a) the small number of horizontal standards recognized to be relevant; b) the nature of the human supervision and intervention is mainly domain specific.

## Annex A. ETSI standards and initiatives description

Reference ID	
<b>DES/eHEALTH-008</b>	
	<i>Title</i>
eHEALTH Data recording requirements for eHealth	
	<i>Domain level</i>
Application	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
The aim of this work is to identify the requirements for recording eHealth events, i.e. those from ICT based eHealth devices and from health practitioners. On the understanding, as illustrated in the use case document and in the White Paper, that health records are subject to security and privacy constraints, but at the same time need to be available to many different stakeholders across time and space without pre-cognition of who those stakeholders are. The purpose of this technical specification is to very carefully specify at stage1 and stage 2 level the normative framework for ensuring events/transactions related to a patient are recorded accurately by identifiable entities (devices or health professionals) and made available with minimum delay to any other health professional (i.e. to ensure that actions taken by one health professional is visible to any other health professional irrespective of location without delay). The normative framework is intended to be adopted by all groups contributing to eHealth including CYBER, smartM2M, smartBAN	
<i>Maturity level</i>	
Early Draft	
	<i>Release time of specification/initiative outcome</i>
08/2021	
	<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56908">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56908</a>	

Reference ID	
<b>TR 103 821</b>	
	<i>Title</i>
Autonomic network engineering for the self-managing Future Internet (AFI); Artificial Intelligence (AI) in Test Systems and Testing AI models.	
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
This work item covers the following points:	
<ul style="list-style-type: none"> <li>• A general guide on the benefits of AI in Test Systems, with illustrations of AI in Test Systems</li> <li>• A general guide for testing AI Models in general, and the definitions of standardized metrics for measurements and assessments in Testing and Certification of AI Models, including certification of AI models of Autonomic Components/Systems</li> <li>• Testing ETSI GANA Models Cognitive Decision Elements (DEs) as AI Models for Autonomic (Closed-Loop) Network Automation, in the space of Autonomic Management &amp; Control (AMC) of Networks and Services, with illustrations of AI Models for Autonomic Management &amp; Control of 5G Network Slices</li> <li>• Generic Test Framework for Testing ETSI GANA Multi-Layer Autonomics &amp; their AI Algorithms for Closed-Loop Network Automation (see EG 203 341).</li> </ul>	

<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
01/2021	
<i>Useful Link</i>	
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58442">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58442</a>	

<i>Reference ID</i>	
<b>GS/ARF-003</b>	
<i>Title</i>	
Augmented Reality Framework (ARF); AR framework architecture	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Application	
<i>Main Objectives and Expected content</i>	
The document specifies a functional reference architecture for AR components, systems and services. The structure of this architecture and the functionalities of its components have been derived from a collection of use cases (ETSI GR ARF 002) and an overview of the current landscape of AR standards (ETSI GR ARF 001). The document introduces the characteristics of an AR system and describes the functional building blocks of the AR reference architecture and their mutual relationships. The generic nature of the architecture is validated by mapping the workflow of several use cases to the components of this framework architecture.	
<i>Maturity level</i>	
Published	
<i>Release time of specification/initiative outcome</i>	
03/2020	
<i>Useful Link</i>	
<a href="https://www.etsi.org/deliver/etsi_gs/ARF/001_099/003/01.01.01_60/gs_ARF003v0101_01p.pdf">https://www.etsi.org/deliver/etsi_gs/ARF/001_099/003/01.01.01_60/gs_ARF003v0101_01p.pdf</a>	

<i>Reference ID</i>	
<b>GS CIM 009 V1.2.1</b>	
<i>Title</i>	
Context Information Management (CIM); NGSI-LD API.	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
The purpose of the document is the definition of a standard API for Context Information Management (NGSI-LD API) enabling close to real-time access to information coming from many different sources (not only IoT data sources). The document defines how such an API enables applications to perform updates on context, register context providers which can be queried to get updates on context, query information on current and historic context information and subscribe to receive notifications of context changes. ISG CIM has not so far defined reference points specifically to higher-layer AI reasoning platforms. NGSI-LD API uses linked open data and property graphs to reference data definitions (ontologies) such as those in SAREF.	
<i>Maturity level</i>	

Published	<i>Release time of specification/initiative outcome</i>
10/2019	<i>Useful Link</i>
	<a href="https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.01_60/gs_CIM009v012_01p.pdf">https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.01_60/gs_CIM009v012_01p.pdf</a>

<i>Reference ID</i>
<b>GR CIM-007</b>
<i>Title</i>
Context Information Management (CIM): Security and Privacy
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
<i>Main Objectives and Expected content:</i> The purpose of this Work Item is to provide a state-of-the-art assessment of security and privacy issues associated with ISG CIM specifications, related to the API, Data Publishing Platforms and Data Model Work Items. Recommendations shall be accompanied by pro/con information with the intent to reference as much as possible existing widely supported concepts. There are several issues that need to be addressed, including but not limited to provenance of data, assuring privacy and security between stakeholders, assuring trust, understanding how to ensure the aggregation of data does not increase the attack space or compromise privacy. The work item will investigate items such as but not limited to; what should be connected via the information model and are there any particular lifecycle constraints that may be placed on data? The scope of this work is strictly limited to the CIM scope of work, e.g. device security is excluded. Where appropriate, it references existing work, specifications and standards.
<i>Maturity level</i>
In development (early draft)
<i>Release time of specification/initiative outcome</i>
01/2021
<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53370">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53370</a>

<i>Reference ID</i>
<b>GS ENI 001 v2.1.1</b>
<i>Title</i>
Experiential Networked Intelligence (ENI): ENI use cases
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The specification ETSI GS ENI 001 demonstrates several use cases on service assurance, fault management and self-healing, resource configuration, performance configuration, energy optimization, security and mobility management.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
09/2019

<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_gs/ENI/001_099/002/03.01.01_60/gs_ENI002v030101p.pdf">https://www.etsi.org/deliver/etsi_gs/ENI/001_099/002/03.01.01_60/gs_ENI002v030101p.pdf</a>

<i>Reference ID</i>
<b>GS ENI 005</b>
<i>Title</i>
Experiential Networked Intelligence (ENI); System Architecture
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The specification ETSI GS ENI 005 shows as a functional architecture how the data is collected, normalized and recursively processed to extract knowledge and wisdom from it. This data is used for decision-making and the results are returned to the network, where the behavior is continually monitored.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
09/2019
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_gs/ENI/001_099/002/03.01.01_60/gs_ENI002v030101p.pdf">https://www.etsi.org/deliver/etsi_gs/ENI/001_099/002/03.01.01_60/gs_ENI002v030101p.pdf</a>

<i>Reference ID</i>
<b>GR ENI 007</b>
<i>Title</i>
Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The document defines various categories for the level of application of Artificial Intelligence (AI) techniques to the management of the network, going from basic limited aspects, to the full use of AI techniques for performing network management. The requirements document ETSI GR ENI 007 on network classification of AI details the use of AI in a network into six stages, from "No AI" to "full AI" deployment.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
11/2019
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_gr/ENI/001_099/007/01.01.01_60/gr_ENI007v010101p.pdf">https://www.etsi.org/deliver/etsi_gr/ENI/001_099/007/01.01.01_60/gr_ENI007v010101p.pdf</a>

<i>Reference ID</i>
<b>GR NFV-IFA 041</b>
<i>Title</i>

Network Functions Virtualisation (NFV); Release 4 Management and Orchestration; Report on enabling autonomous management in NFV-MANO;
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The goal of the Work Item is to study and evaluate possible enhancements to NFV-MANO to improve its automation capabilities and introduce autonomous network mechanisms. This work will align with automation related work in organizations such as ETSI ISG ZSM, ETSI ISG ENI and 3GPP SA5. Recommendations for normative work to enable autonomous management in NFV-MANO will be made. Within ISG NFV (Network Function Virtualization), AI is being considered as a tool that eventually becomes part of the Management and Orchestration (MANO) stack. NFV virtualization is not explicitly considering AI, except in requirements to properly feed data and collect actions from AI modules.
<i>Maturity level</i>
In development (early draft)
<i>Release time of specification/initiative outcome</i>
03/2021
<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58467">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58467</a>

<i>Reference ID</i>
<b>DGR SAI-001</b>
<i>Title</i>
Securing Artificial Intelligence (SAI); AI Threat Ontology
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The purpose of this work item is to define what would be considered an AI threat and how it might differ from threats to traditional systems. The starting point that offers the rationale for this work is that currently, there is no common understanding of what constitutes an attack on AI and how it might be created, hosted and propagated. The AI Threat Ontology deliverable will seek to align terminology across the different stakeholders and multiple industries. This document will define what is meant by these terms in the context of cyber and physical security and with an accompanying narrative that should be readily accessible by both experts and less informed audiences across the multiple industries.
<i>Maturity level</i>
In development (stable draft)
<i>Release time of specification/initiative outcome</i>
05/2021
<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58856</a>

<i>Reference ID</i>
<b>DGR SAI-002</b>
<i>Title</i>
Securing Artificial Intelligence (SAI); Data Supply Chain Report.

<i>Domain level</i>	
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Data is a critical component in the development of AI systems. This includes raw data as well as information and feedback from other systems and humans in the loop, all of which can be used to change the function of the system by training and retraining the AI.	
However, access to suitable data is often limited causing a need to resort to less suitable sources of data. Compromising the integrity of training data has been demonstrated to be a viable attack vector against an AI system. This means that securing the supply chain of the data is an important step in securing the AI.	
The report will summarise the methods currently used to source data for training AI along with the regulations, standards and protocols that can control the handling and sharing of that data. It will then provide gap analysis on this information to scope possible requirements for standards for ensuring traceability and integrity in the data, associated attributes, information and feedback, as well as the confidentiality of these.	
<i>Maturity level</i>	
In development (early draft)	
	<i>Release time of specification/initiative outcome</i>
07/2021	
<i>Useful Link</i>	
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58857</a>	

<i>Reference ID</i>	
<b>DGS SAI-003</b>	
<i>Title</i>	
Securing Artificial Intelligence (SAI); Security Testing of AI.	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
The purpose of this work item is to identify objectives, methods and techniques that are appropriate for security testing of AI-based components. The overall goal is to have guidelines for security testing of AI and AI-based components considering of the different algorithms of symbolic and subsymbolic AI and addressing relevant threats from the work item "AI threat ontology".	
Security testing of AI has some commonalities with security testing of traditional systems but provides new challenges and requires different approaches, due to (a) significant differences between symbolic and subsymbolic AI and traditional systems that have strong implications on their security and on how to test their security properties, (b) non-determinism since AI-based systems may evolve over time (self-learning systems) and security properties may degrade, (c) test oracle problem, assigning a test verdict is different and more difficult for AI-based systems since not all expected results are known a priori, and (d) data-driven algorithms: in contrast to traditional systems, (training) data forms the behaviour of subsymbolic AI.	
<i>Maturity level</i>	
In development (early draft)	
	<i>Release time of specification/initiative outcome</i>
05/2021	
<i>Useful Link</i>	

[https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=58860](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58860)

<i>Reference ID</i>	
<b>GR SAI 004</b>	<i>Title</i>
Securing Artificial Intelligence (SAI); Problem Statement	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
This work item describes the challenges of securing AI-based systems and solutions, including challenges relating to data, algorithms and models in both training and implementation environments. The focus will be on challenges which are specific to AI-based systems, including poisoning and evasion.	
In development (draft)	<i>Maturity level</i>
12/2020	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59209">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59209</a>	

<i>Reference ID</i>	
<b>DGR SAI-005</b>	<i>Title</i>
Securing Artificial Intelligence (SAI); Mitigation Strategy Report.	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
This work item aims to summarize and analyze existing and potential mitigation against threats for AI-based systems. The goal is to have guidelines for mitigating against threats introduced by adopting AI into systems. These guidelines will shed light baselines of securing AI-based systems by mitigating against known or potential security threats. They also address security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases.	
In development (early draft)	<i>Maturity level</i>
03/2021	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59214">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59214</a>	

<i>Reference ID</i>	
<b>ETSI TS 103 327 V1.1.1</b>	<i>Title</i>
Smart Body Area Networks (SmartBAN); Service and application standardized enablers and interfaces, APIs and infrastructure for interoperability management.	<i>Domain level</i>
Application	

<i>Type of initiative</i>	
Standard	<i>Main Objectives and Expected content</i>
TC SmartBAN considers interfaces which would allow semantic interoperability of eHealth sensors with external systems (including by default AI).	
	<i>Maturity level</i>
Published	<i>Release time of specification/initiative outcome</i>
04/2019	<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327_v010101p.pdf">https://www.etsi.org/deliver/etsi_ts/103300_103399/103327/01.01.01_60/ts_103327_v010101p.pdf</a>	

<i>Reference ID</i>	
<b>GS ZSM 002</b>	<i>Title</i>
Zero-touch network and Service Management (ZSM); Reference Architecture.	
	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
The document defines and describes the reference architecture for the end-to-end Zero-touch network and Service Management (ZSM) framework based on a set of user scenarios and requirements documented in ETSI GS ZSM 001. ISG ZSM (ISG Zero-touch Network and Service Management), was formed with the goal to introduce a new end-to-end architecture and related solutions that will enable automation at scale and at the required minimal total cost of ownership (TCO), as well as to foster a larger utilization of AI technologies. The ZSM end-to-end architecture framework has been designed for closed-loop automation and optimized for data-driven machine learning and AI algorithms.	
	<i>Maturity level</i>
Published	<i>Release time of specification/initiative outcome</i>
08/2019	<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010_101p.pdf">https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010_101p.pdf</a>	

<i>Reference ID</i>	
<b>Smart Applications REference (SAREF) ontology</b>	<i>Title</i>
Smart Applications REference ontology	
	<i>Domain level</i>
Application	<i>Type of initiative</i>
Ontology	<i>Main Objectives and Expected content</i>
An enhancement of the SAREF portal, being finalized in 2020, concerns the double role of AI in semantics as a facilitator of the development and alignment of ontologies and semantics meanings, supporting human experts. The SAREF family of ontologies also supports IoT information discovery, enrichment and validation, therefore enabling the provision of AI services to support IoT semantic	

interoperability, based on a common understanding of IoT information (both for people and machines).	<i>Maturity level</i>
Published	<i>Release time of specification/initiative outcome</i>
2020	<i>Useful Link</i>
	<a href="https://saref.etsi.org/index.html">https://saref.etsi.org/index.html</a>

<i>Reference ID</i>	
<b>TR 103 674</b>	<i>Title</i>
SmartM2M: Artificial Intelligence and the oneM2M architecture	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Detailed description of selected use cases and identification of architectural evolutions (components, required mappings, etc.) to the oneM2M framework. It addresses the introduction of AI/ML into IoT systems and the opportunities for improving AI/ML performance through use of the horizontal oneM2M standard and its family of common service functions (CSFs).	
	<i>Maturity level</i>
In development	<i>Release time of specification/initiative outcome</i>
12/2020	<i>Useful Link</i>
	<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57866">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57866</a>

<i>Reference ID</i>	
<b>TR 103 675</b>	<i>Title</i>
SmartM2M AI for IoT: A Proof of Concept	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Detailed description of the use cases design and implementation; instructions for the (re-)creation of the prototypes from the selected framework and components; lessons learned. improving AI/ML performance through use of the horizontal oneM2M standard and its family of common service functions (CSFs). Its aim is to build and test a proof of concept that targets two technical innovations. One innovation involves extensions of existing CSFs to support new AI/ML-related functional requirements. The second innovation is to test the concept of new CSFs that offer AI/ML capabilities on an "as-a-service" basis. This could take the form of a configurable classification algorithm, for example, that one or more IoT solutions could access on a oneM2M-compliant IoT platform.	
	<i>Maturity level</i>
In development (draft)	<i>Release time of specification/initiative outcome</i>
12/2020	

<i>Useful Link</i>
<a href="https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=5786Z">https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=5786Z</a>

<i>Reference ID</i>
<b>TS 102 181 v1.3.1</b>
<i>Title</i>
Emergency Communications (EMTEL); Requirements for communication between authorities/organizations during emergencies.
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The specification describes requirements for communications from authorities/organizations to individuals, groups or the general public in emergency situations. It describes the functional requirements for communications between the authorized representatives involved in the responses and actions when handling an emergency. The level of precision has been chosen to avoid interaction with the specific local, regional or national organizations and diagrams of relations between authorized representatives. It follows from this that adaptations will have to be done when implementing the present document at a local level. The scope of the document also encompasses various types of services that can bring an added value to this basic scenario or add new scenarios, such as the services brought by other technologies e.g. IoT devices that support communications between authorities during emergencies.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
06/2020
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_ts/102100_102199/102181/01.03.01_60/ts_102181_v010301p.pdf">https://www.etsi.org/deliver/etsi_ts/102100_102199/102181/01.03.01_60/ts_102181_v010301p.pdf</a>

<i>Reference ID</i>
<b>TS 102 182 v1.5.1</b>
<i>Title</i>
Emergency Communications (EMTEL); Requirements for communications from authorities/organizations to individuals, groups or the general public during emergencies.
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The present document gives an overview of the requirements for communication from authorities/organizations to citizens in all types of emergencies. It collects operational and organizational requirements as a basis for a common notification service, including targeting of the area to be notified. Although many of the requirements relate to national public policies and regulation, there are several service and technical aspects which are better dealt with on the European level to ensure harmonized access and services over Europe and service effectiveness through increased user awareness by using standardized solutions.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>

07/2020
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_ts/102100_102199/102182/01.05.01_60/ts_102182v010501p.pdf">https://www.etsi.org/deliver/etsi_ts/102100_102199/102182/01.05.01_60/ts_102182v010501p.pdf</a>

<i>Reference ID</i>
<b>TS 103 194</b>
<i>Title</i>
Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The document contains a description of scenarios, use cases, and definition of requirements for the autonomic/self-managing future internet. Scenarios and use cases selected in the present document reflect real-world problems which can benefit from the application of autonomic/self-management principles.
TC INT specifications consider events that can trigger a network to dynamically change network properties. Events vary depending on the specific AI systems deployed in the network and the level where they operate, external or internal to the network. These events can occur in a chain-like fashion, e.g. policy change can trigger several secondary events in lower-level functional units.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
10/2014
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ts_103194v010101p.pdf">https://www.etsi.org/deliver/etsi_ts/103100_103199/103194/01.01.01_60/ts_103194v010101p.pdf</a>

<i>Reference ID</i>
<b>TS 103.195-2</b>
<i>Title</i>
Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management.
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The scope of the document is to provide the definition of the Generic Autonomic Network Architecture (GANA) as an architectural reference model for autonomic networking, cognitive networking and self-management that addresses the requirements defined in ETSI TS 103 194 - a compilation of example requirements which reflect real-world problems that benefit from the application of automated management, autonomic management and self-management principles for networks and services delivered by the network to applications.
The objective of the document is to describe the GANA reference model with its associated Functional Blocks (FBs) and their associated reference points that can be instantiated onto target currently existing, emerging or future reference network

architectures (including their management and control architectures) to create autonomics-enabled reference network architectures and their associated management and control architectures.
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
05/2018
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf">https://www.etsi.org/deliver/etsi_ts/103100_103199/10319502/01.01.01_60/ts_10319502v010101p.pdf</a>

<i>Reference ID</i>
<b>EG 203 341 V1.1.1</b>
<i>Title</i>
<b>Core Network and Interoperability Testing (INT): Approaches for Testing Adaptive Network.</b>
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The document, "Approaches for Testing Adaptive Networks" defines a framework of testing principles and guidelines that may be used to test networks that exhibit some form of autonomic adaptive behavior, which allows them to dynamically change their configuration, structure or operational parameters. The (re)-configuration is performed in response to stimuli such as changes in workload, operator policies that govern their operation, context (the network is context-aware and may have a degree of self-awareness); and challenges in the environment (i.e. conditions under which the network is operating, e.g. manifestations of faults, errors, failures in various parts of the network and its hardware and software components).
<i>Maturity level</i>
Published
<i>Release time of specification/initiative outcome</i>
10/2016
<i>Useful Link</i>
<a href="https://www.etsi.org/deliver/etsi_eg/203300_203399/203341/01.01.01_60/eg_203341v010101p.pdf">https://www.etsi.org/deliver/etsi_eg/203300_203399/203341/01.01.01_60/eg_203341v010101p.pdf</a>

## Annex B. ISO and ISO/IEC standards and initiatives description

At the outset, each ISO deliverable is assigned to a standards development track. This track determines the timeframe of the project (12, 24, or 36 months) as it passes through the various stages to publication (ISO, 2020).

For a given specification, the “Maturity level” field makes reference to the present stage according to the ISO life cycle, see Figure 19, where main stages are encoded as reported in Table 22 (ISO, 2020).

Table 22. ISO maturity level codes

STAGE Code	MEANING
00	PRELIMINARY
10	PROPOSAL
20	PREPARATORY
30	COMMITTEE
40	ENQUIRY
50	APPROVAL
60	PUBLICATION
90	REVIEW
95	WITHDRAWAL

### LIFE CYCLE

A standard is reviewed every 5 years



Figure 19. ISO life cycle of a specification (source: ISO Website, [www.iso.org](http://www.iso.org))

Reference ID
<b>ISO/IEC 25024:2015</b>
<i>Title</i>
Systems and software engineering — Systems and software Quality Requirements and Evaluation (SquaRE)
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
ISO IEC 25024 2015 contains the following (a) a basic set of data quality measures for each characteristic; (b) a basic set of target entities to which the quality measures are applied during the data-life-cycle; (c) an explanation of how to apply data quality measures; (d) a guidance for organizations defining their own measures for data quality requirements and evaluation. It includes, as informative annexes, a synoptic table of quality measure elements defined in this International standard (Annex A), a table of quality measures associated to each quality measure element and target entity (Annex B), considerations about specific quality measure elements (Annex C), a list of quality

measures in alphabetic order (Annex D), and a table of quality measures grouped by characteristics and target entities (Annex E).

	<i>Maturity level</i>
Review	
	<i>Release time of specification/initiative outcome</i>
Published	
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/35749.html">https://www.iso.org/standard/35749.html</a>	

	<i>Reference ID</i>
<b>ISO/IEC TR 24027</b>	
	<i>Title</i>
	Information technology - Artificial Intelligence (AI) – Bias in AI systems and AI-aided decision making
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Technical report	
	<i>Main Objectives and Expected content</i>
To address bias in relation to AI systems, especially with regards to AI-aided decision making. To provide measurement techniques and methods for assessing bias, with the aim to address and treat bias-related vulnerabilities. All AI system lifecycle phases are in scope, including but not limited to data collection, training, continual learning, design, testing, evaluation, and use.	
	<i>Maturity level</i>
Committee (under development)	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/77607.html?browse=tc">https://www.iso.org/standard/77607.html?browse=tc</a>	

	<i>Reference ID</i>
<b>SO/IEC TR 24028:2020</b>	
	<i>Title</i>
	Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Technical report	
	<i>Main Objectives and Expected content</i>
This document surveys topics related to trustworthiness in AI systems, including the following:	

- approaches to establish trust in AI systems through transparency, explainability, controllability, etc.;
- engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and
- approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.

The specification of levels of trustworthiness for AI systems is out of the scope of this document.

	<i>Maturity level</i>
Publication	
	<i>Release time of specification/initiative outcome</i>
2020	
	<i>Useful Link</i>
	<a href="https://www.iso.org/standard/77608.html">https://www.iso.org/standard/77608.html</a>

	<i>Reference ID</i>
<b>ISO/IEC DTR 24029-1</b>	
	<i>Title</i>
Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview	
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
To provide background about the existing methods to assess the robustness of neural networks.	
	<i>Maturity level</i>
Committee (under development)	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
	<a href="https://www.iso.org/standard/77609.html">https://www.iso.org/standard/77609.html</a>

	<i>Reference ID</i>
<b>ISO/IEC AWI 24029-2</b>	
	<i>Title</i>
Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods	
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>

To provide guidelines on the use of formal methods to assess robustness properties of neural networks.

<i>Maturity level</i>	
Proposal	<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>	
<a href="https://www.iso.org/standard/79804.html">https://www.iso.org/standard/79804.html</a>	

<i>Reference ID</i>	
<b>ISO/IEC WD 5259-1</b>	
<i>Title</i>	
Data quality for analytics and ML — Part 1: Overview, terminology, and examples	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
To provide the landscape for understanding and associating of data quality for analytics and ML series and guides the foundational concepts regarding data quality for analytics and AI.	
<i>Maturity level</i>	
Preparatory	
<i>Release time of specification/initiative outcome</i>	
<i>Useful Link</i>	
<a href="https://www.iso.org/standard/81088.html">https://www.iso.org/standard/81088.html</a>	

<i>Reference ID</i>	
<b>ISO/IEC WD 5259-2</b>	
<i>Title</i>	
Data quality for analytics and ML — Part 2: Data quality measures	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
To provide a data quality model, data quality measures, and guidance on reporting data quality in the context of analytics and machine learning (ML).	
<i>Maturity level</i>	
Preparatory	
<i>Release time of specification/initiative outcome</i>	

<i>Useful Link</i>

<i>Reference ID</i>
<b>ISO/IEC WD 5259-3</b>
<i>Title</i>
Data quality for analytics and ML — Part 3: Data quality management requirements and guidelines.
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
To provide requirements and guidance for establishing, implementing, maintaining and continually improving the quality for data used in the areas of analytics and ML.
<i>Maturity level</i>
Preparatory
<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>
<a href="https://www.iso.org/standard/81092.html">https://www.iso.org/standard/81092.html</a>

<i>Reference ID</i>
<b>ISO/IEC WD 5259-4</b>
<i>Title</i>
Data quality for analytics and ML — Part 4: Data quality process framework
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
To provide general common organizational approaches, regardless of type, size or nature of the applying organization, to ensure data quality for training and evaluation in analytics and ML.
<i>Maturity level</i>
Preparatory
<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>
<a href="https://www.iso.org/standard/81093.html">https://www.iso.org/standard/81093.html</a>

<i>Reference ID</i>
<b>ISO/IEC WD 5338</b>

<i>Title</i>	
Information technology — Artificial intelligence — AI system life cycle processes	
<i>Domain level</i>	
General	
Standard	<i>Type of initiative</i>
	<i>Main Objectives and Expected content</i>
To provide processes that support the definition, control and improvement of AI system life cycle processes used within an organization or a project. Organizations and projects can use these processes when developing or acquiring AI systems.	
<i>Maturity level</i>	
Preparatory	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/81118.html?browse=tc">https://www.iso.org/standard/81118.html?browse=tc</a>	

<i>Reference ID</i>	
<b>ISO/IEC AWI TR 5469</b>	
<i>Title</i>	
Artificial intelligence — Functional safety and AI systems	
<i>Domain level</i>	
General	
Technical report	<i>Type of initiative</i>
	<i>Main Objectives and Expected content</i>
to describe properties, relevant risk factors, usable methods and processes for the application of AI in safety-relevant functions, for the application of safety-relevant functions for the control of AI systems and for the application of AI in the development of safety-relevant functions.	
<i>Maturity level</i>	
Proposal	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/81283.html?browse=tc">https://www.iso.org/standard/81283.html?browse=tc</a>	

<i>Reference ID</i>	
<b>ISO/IEC AWI TR 24368</b>	
<i>Title</i>	
Information technology — Artificial intelligence — Overview of ethical and societal concerns	
<i>Domain level</i>	

General	<i>Type of initiative</i>
Technical report	<i>Main Objectives and Expected content</i>
	<i>Maturity level</i>
Preparatory	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/78507.html?browse=tc">https://www.iso.org/standard/78507.html?browse=tc</a>	

	<i>Reference ID</i>
<b>ISO/IEC AWI TR 24372</b>	
	<i>Title</i>
Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems	
	<i>Domain level</i>
General	<i>Type of initiative</i>
Technical report	<i>Main Objectives and Expected content</i>
to provide an overview of the state of the art of computational approaches for AI systems, by describing: a) main computational characteristics of AI systems; b) main algorithms and approaches used in AI systems, referencing use cases contained in ISO/IEC TR 24030.	
	<i>Maturity level</i>
Preparatory	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.iso.org/standard/78508.html?browse=tc">https://www.iso.org/standard/78508.html?browse=tc</a>	

	<i>Reference ID</i>
<b>ISO/IEC CD 24668</b>	
	<i>Title</i>
Information technology — Artificial intelligence — Process management framework for Big data analytics	
	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
to provide a process management framework to effectively leverage big data analytics across the organization irrespective of the industries/sectors. This document specifies	

the process reference model for big data analytics with its process groups considered along with their interconnectivity, and the process assessment model that provides a common basis for performing assessments on big data processes.

	<i>Maturity level</i>
Committee	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
	<a href="https://www.iso.org/standard/78368.html?browse=tc">https://www.iso.org/standard/78368.html?browse=tc</a>

	<i>Reference ID</i>
<b>ISO/IEC 25012:2008</b>	
	<i>Title</i>
	Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model
	<i>Domain level</i>
General	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
	To define a general data quality model for data retained in a structured format within a computer system. ISO/IEC 25012:2008 can be used to establish data quality requirements, define data quality measures, or plan and perform data quality evaluations. It could be used, for example,
	<ul style="list-style-type: none"> <li>• to define and evaluate data quality requirements in data production, acquisition and integration processes,</li> <li>• to identify data quality assurance criteria, also useful for re-engineering, assessment and improvement of data,</li> <li>• to evaluate the compliance of data with legislation and/or requirements.</li> </ul>
	ISO/IEC 25012:2008 categorizes quality attributes into fifteen characteristics considered by two points of view: inherent and system dependent. Data quality characteristics will be of varying importance and priority to different stakeholders. ISO/IEC 25012:2008 is intended to be used in conjunction with the other parts of the SQuaRE series of International Standards, and with ISO/IEC 9126-1 until superseded by ISO/IEC 25010. THIS STANDARD WAS LAST REVIEWED AND CONFIRMED IN 2019. THEREFORE, THIS VERSION REMAINS CURRENT.
	<i>Maturity level</i>
Published	
	<i>Release time of specification/initiative outcome</i>
2019	
	<i>Useful Link</i>

	<i>Reference ID</i>
<b>ISO/IEC WD TS 4213</b>	

<i>Title</i>
Information technology — Artificial Intelligence — Assessment of machine learning classification performance
<i>Domain level</i>
General
<i>Type of initiative</i>
Technical specification
<i>Main Objectives and Expected content</i>
to specify methodologies for measuring classification performance of machine learning models, systems and algorithms.
<i>Maturity level</i>
Preparatory
<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>
<a href="https://www.iso.org/standard/79799.html">https://www.iso.org/standard/79799.html</a>

<i>Reference ID</i>
<b>ISO/IEC 23894</b>
<i>Title</i>
Information Technology – Artificial Intelligence – Risk Management
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
To provide guidelines on managing risk faced by organizations during the development and application of artificial intelligence (AI) techniques and systems. The guidelines also aim to assist organizations to integrate risk management into their AI-related activities and functions. It moreover describes processes for the effective implementation and integration of AI risk management. The application of these guidelines can be customized to any organization and its context.
<i>Maturity level</i>
Committee
<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>
<a href="https://www.iso.org/standard/77304.html?browse=tc">https://www.iso.org/standard/77304.html?browse=tc</a>

<i>Reference ID</i>
<b>ISO/IEC CD 38507</b>
<i>Title</i>
Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations

<i>Domain level</i>	
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
To provide guidance for governing bodies of organizations that are using – or considering the use of - tools or systems that incorporate artificial intelligence. This document is a high level, principles-based advisory standard. In addition to providing broad guidance on the role of a governing body, it encourages organizations to use appropriate standards to underpin their governance of information technology – including the use of artificial intelligence (AI).	
<i>Maturity level</i>	
Committee	<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>	
<a href="https://www.iso.org/standard/56641.html?browse=tc">https://www.iso.org/standard/56641.html?browse=tc</a>	

<i>Reference ID</i>	
<b>ISO/IEC WD 42001</b>	
<i>Title</i>	
Information Technology — Artificial intelligence — Management system	
<i>Domain level</i>	
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
to provide the requirements and provides guidance for establishing, implementing, maintaining and continually improving an artificial intelligence management system within the context of an organization.	
<i>Maturity level</i>	
Preparatory	<i>Release time of specification/initiative outcome</i>
<i>Useful Link</i>	
<a href="https://www.iso.org/standard/81230.html?browse=tc">https://www.iso.org/standard/81230.html?browse=tc</a>	

<i>Reference ID</i>	
<b>ISO/IEC AWI 25059</b>	
<i>Title</i>	
Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI-based systems.	
<i>Domain level</i>	

General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
	to introduce a quality model for AI systems. It is an application-specific extension to the SQuaRE series. The model characteristics provide a consistent terminology for specifying, measuring and evaluating AI system quality.
	<i>Maturity level</i>
Preparatory	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
	<a href="https://www.iso.org/standard/80655.html">https://www.iso.org/standard/80655.html</a>

## Annex C. ITU-T standards and initiatives description

<i>Reference ID</i>	
<b>ITU-T Y.3170</b>	
	<i>Title</i>
Requirements for machine learning-based quality of service assurance for the IMT-2020 network	
	<i>Domain level</i>
Application	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
This recommendation specifies requirements of machine learning based QoS assurance for the international mobile telecommunications 2020 (IMT-2020) network. This recommendation provides an overview of machine learning based QoS assurance for IMT-2020 network. It describes capabilities for QoS anomaly detection and prediction using machine learning. In addition, recommendation describes a functional model of machine learning based QoS assurance which includes functional components such as QoS data collection, data pre-processing, data storage, modelling and training, QoS anomaly detection and prediction, QoS policy decision making, enforcement and reporting. Based on the capabilities and functionalities described in the functional model, this recommendation specifies the high-level requirements and functional requirements of machine learning based QoS assurance for IMT-2020 network.	
	<i>Maturity level</i>
Published	
	<i>Release time of specification/initiative outcome</i>
09/2018	
	<i>Useful Link</i>
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14278">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14278</a>	

<i>Reference ID</i>	
<b>ITU-T Y.qos-ml-arc</b>	
	<i>Title</i>
Architecture of machine learning based QoS assurance for IMT-2020 network.	
	<i>Domain level</i>
Application	
	<i>Type of initiative</i>
Standard	
	<i>Main Objectives and Expected content</i>
This recommendation specifies architecture of machine learning based QoS assurance for the international mobile telecommunications 2020 (IMT-2020) network. It provides an overview of unified architecture for ML in 5G and future networks. In addition, it describes the architecture of machine learning based QoS assurance. Based on the architecture, this recommendation specifies the procedures of machine learning based QoS assurance for IMT-2020 network.	
	<i>Maturity level</i>
In development (initial draft)	
	<i>Release time of specification/initiative outcome</i>
	<i>Useful Link</i>
<a href="https://www.itu.int/md/T17-SG13-181102-TD-WP1-0276/en">https://www.itu.int/md/T17-SG13-181102-TD-WP1-0276/en</a>	

<i>Reference ID</i>	
<b>ITU-T Y.MecTa-ML</b>	
<i>Title</i>	
Mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning	
<i>Domain level</i>	
Application	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
<p>Application-descriptor-agnostic traffic is the traffic which cannot be identified by an application descriptor. On the one hand, traditional traffic awareness technologies such as deep packet inspection are not highly effective when they are applied to application-descriptor-agnostic traffic. On the other hand, with development of the artificial intelligence, many related technologies are emerging and applied in various areas. Compared to traditional traffic methods, traffic awareness method combining with machine learning based technologies will be more effective when it is used to process other application-descriptor-agnostic. Therefore, it is time to study mechanism and methods to implement application-descriptor-agnostic traffic awareness functions based on machine learning. This Recommendation specifies the mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning.</p>	
<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
07/2021	
<i>Useful Link</i>	
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14619">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14619</a>	

<i>Reference ID</i>	
<b>ITU-T Y.3531</b>	
<i>Title</i>	
Cloud computing- functional requirements for machine learning as a service	
<i>Domain level</i>	
Application	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
<p>This Recommendation provides cloud computing requirements for machine learning as a service, which addresses requirements from use cases. Machine learning as a service (MLaaS) is a cloud service category to support the development and applications of machine learning in the cloud computing environments. On the perspective of cloud computing service provisioning, this Recommendation defines the functional requirements for MLaaS to identify functionalities such as data gathering, machine learning modelling and computing resources, etc. Also, this draft Recommendation aligned with the cloud computing reference architecture of ITU-T Y.3502. Developments of machine learning algorithms and methodology are out of the scope on this Recommendation.</p>	
<i>Maturity level</i>	
Approved	
<i>Release time of specification/initiative outcome</i>	
09/2020	
<i>Useful Link</i>	

[https://www.itu.int/itu-t/workprog/wp\\_item.aspx?isn=14484](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14484)

<i>Reference ID</i>	
<b>ITU-T Y.3172</b>	<i>Title</i>
Architectural framework for machine learning in future networks including IMT-2020	
	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
This document specifies an architectural framework for machine learning (ML) in future networks including IMT-2020. A set of architectural requirements and specific architectural components needed to satisfy these requirements are presented. These components include, but are not limited to, ML pipeline and ML management and orchestration functionalities. The integration of such components into future networks including IMT-2020 and guidelines for applying this architectural framework in a variety of technology-specific underlying networks are also described.	
	<i>Maturity level</i>
Approved	<i>Release time of specification/initiative outcome</i>
06/2019	
	<i>Useful Link</i>
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15020">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15020</a>	

<i>Reference ID</i>	
<b>ITU-T H.CUAV-AIF</b>	<i>Title</i>
Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence.	
	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
This recommendation provides framework and requirements for civilian unmanned aerial vehicle (CUAV) flight control using artificial intelligence. Currently, the CUAV has been widely used in industry and consumption areas, there are also problems in the development of CUAVs. In addition to the policy and legal supervision, the other problem is how CUAVs avoid obstacles during the flight, and how the CUAVs applied in a specific industry can automatically navigate, track or fly along a specific area according to the mission requirements. This draft Recommendation provides a framework of civilian unmanned aerial vehicle flight control using Artificial Intelligence, including the flight navigation control of a CUAV itself (including avoiding obstacles, normal take-off and landing) and the specific flight control (including automatic navigation, tracking, or along a regular direction or specific area) based on the specific industry application requirements. This framework is not a specific implementation case, but it provides a framework and capability requirements for each specific implementation, and the product and system integrators can design and produce specific products and systems according to this framework.	
	<i>Maturity level</i>
In development	<i>Release time of specification/initiative outcome</i>
2021	

<i>Useful Link</i>
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14760">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14760</a>

<i>Reference ID</i>
<b>ITU-T F.VS-AIMC</b>
<i>Title</i>
Use cases and requirements for multimedia communication enabled vehicle systems using artificial intelligence.
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
This recommendation specifies use cases and requirements of artificial intelligence for ICT-enabled autonomous vehicle systems. This draft Recommendation covers the followings: <ul style="list-style-type: none"> <li>• Use cases: to identify the use cases of artificial intelligence applied to the ICT-based autonomous vehicle systems, e.g. situational awareness, route planning, driving behavior decision and human-computer interaction;</li> <li>• Requirements: to identify the service and network requirements, functional requirements and non-functional requirements of the ICT-based autonomous vehicle systems .</li> </ul>
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
2020
<i>Useful Link</i>
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14767">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14767</a>

<i>Reference ID</i>
<b>ITU-T Y. 4470</b>
<i>Title</i>
Reference architecture of artificial intelligence service exposure for smart sustainable cities
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
This recommendation introduces the artificial intelligence service exposure (AISE) for smart sustainable cities (SSC), analyses common characteristics and high-level requirements of AISE, brings a reference architecture of AISE and relevant common capabilities. The AISE is one of the bases, supporting functional entities for smart sustainable cities, with which the SSC services can use the uniform interfaces (exposed by the AISE) to integrate and access the AI capabilities (functionalities) of AI services (e.g., machine learning services for video/audio/picture recognition, natural language processing services, traffic prediction services etc.). The AISE can leverage the AI capabilities developed and exposed by AI service providers for SSC services, and can support the SSC service providers to integrate and access the exposed AI capabilities. The AISE can provide security and privacy mechanism on the SSC data. The AISE can support the AI service providers to design and train AI capabilities with local SSC data on AISE in SSCs, and can support the SSC services to integrate and access AI capabilities.

<i>Maturity level</i>	
Approved	
<i>Release time of specification/initiative outcome</i>	
08/2020	
<i>Useful Link</i>	
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14503">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14503</a>	

<i>Reference ID</i>	
<b>Y.Suppl.63 to ITU-T Y.4000 series</b>	
<i>Title</i>	
Unlocking Internet of things with artificial intelligence: Where we are and where we could be.	
<i>Domain level</i>	
Application	
<i>Type of initiative</i>	
Supplement to standard	
<i>Main Objectives and Expected content</i>	
<p>As the IoT system seeks to spread within the urban realm in keeping with smart and sustainable city aspirations, the need to manage the burgeoning big data and establishing a self-sustaining urban ecosystem is at the fore-front. Accordingly, this Technical Report examines how artificial intelligence could step in as the saviour and bolster the intent of urban stakeholders to deploy IoT technologies and eventually transition to smart cities. This Technical Report includes:</p> <ul style="list-style-type: none"> <li>- The various technologies from AI which will help cater to urbanization and facilitate smart city transformations;</li> <li>- The role played by AI in managing the data generated within the IoT realm;</li> <li>- The main benefits of adopting AI and delving into how this technology could be leveraged to attain the targets stipulated in the recently established Sustainable Development Goals (SDGs).</li> </ul>	
<i>Maturity level</i>	
Approved	
<i>Release time of specification/initiative outcome</i>	
07/2020	
<i>Useful Link</i>	
<a href="https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14103">https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14103</a>	

## Annex D. IEEE standards and initiatives description

<i>Reference ID</i>	
<b>IEEE – ECPAIS</b>	
<i>Title</i>	
Ethics Certification Program for Autonomous and Intelligent Systems	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Training program	
<i>Main Objectives and Expected content</i>	
<p>The ECPAIS program is meant to create specifications for certification and marking processes that advance transparency, accountability, and reduction in algorithmic bias in autonomous and intelligent systems. ECPAIS intends to offer a process and define a series of marks by which organizations can seek certifications for their processes around the A/IS products, systems, and services they provide.</p> <p>ECPAIS's goal is to enable work in cycles of development and industry validation, and deliver the following outcomes:</p> <ul style="list-style-type: none"> <li>• Criteria and process for a Certification / mark focused on Transparency in AIS</li> <li>• Criteria and process for a Certification / mark focused on Accountability in AIS</li> <li>• Criteria and process for a Certification / mark focused on Algorithmic Bias in AIS</li> </ul>	
<i>Maturity level</i>	
ECPAIS Certification Criteria (ECC) programmes are finalized and the reports have been issued.	
<i>Release time of specification/initiative outcome</i>	
Fall 2020	
<i>Useful Link</i>	
<a href="https://standards.ieee.org/industry-connections/ecpais.html">https://standards.ieee.org/industry-connections/ecpais.html</a>	

<i>Reference ID</i>	
<b>IEEE P7000™</b>	
<i>Title</i>	
Draft Model Process for Addressing Ethical Concerns During System Design	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
<p>This standard outlines an approach for identifying and analyzing potential ethical issues in a system or software program from the onset of the effort. The values-based system design methods address ethical considerations at each stage of development to help avoid negative unintended consequences while increasing innovation.</p>	
<i>Maturity level</i>	
In development	

<i>Release time of specification/initiative outcome</i>
September 2021
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7000.html">https://standards.ieee.org/project/7000.html</a>

<i>Reference ID</i>
<b>IEEE P7001™</b>
<i>Title</i>
Transparency of Autonomous Systems
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The standard concerns developing autonomous technologies that can assess their own actions and help users understand why a technology makes certain decisions in different situations. The project also offers ways to provide transparency and accountability for a system to help guide and improve it, such as incorporating an event data recorder in a self-driving car or accessing data from a device's sensors.
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2021
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7001.html">https://standards.ieee.org/project/7001.html</a>

<i>Reference ID</i>
<b>IEEE P7002™</b>
<i>Title</i>
Data Privacy Process
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
Data Privacy Process specifies how to manage privacy issues for systems or software that collect personal data. It will do so by defining requirements that cover corporate data collection policies and quality assurance. It also includes a use case and data model for organizations developing applications involving personal information. The standard will help designers by providing ways to identify and measure privacy controls in their systems utilizing privacy impact assessments.
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2021
<i>Useful Link</i>

<https://standards.ieee.org/project/7002.html>

<i>Reference ID</i>	
<b>IEEE P7003™</b>	
<i>Title</i>	
Algorithmic Bias Considerations	
<i>Domain level</i>	
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Algorithmic Bias Considerations provides developers of algorithms for autonomous or intelligent systems with protocols to avoid negative bias in their code. Bias could include the use of subjective or incorrect interpretations of data like mistaking correlation with causation. The project offers specific steps to take for eliminating issues of negative bias in the creation of algorithms. The standard will also include benchmarking procedures and criteria for selecting validation data sets, establishing and communicating the application boundaries for which the algorithm has been designed, and guarding against unintended consequences.	
<i>Maturity level</i>	
In development	<i>Release time of specification/initiative outcome</i>
December 2021	<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7003.html">https://standards.ieee.org/project/7003.html</a>	

<i>Reference ID</i>	
<b>IEEE P7004™</b>	
<i>Title</i>	
Standard on Child and Student Data Governance	
<i>Domain level</i>	
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Standard that provides processes and certifications for transparency and accountability for educational institutions that handle data meant to ensure the safety of students. The standard defines how to access, collect, share, and remove data related to children and students in any educational or institutional setting where their information will be accessed, stored, or shared.	
<i>Maturity level</i>	
In development	<i>Release time of specification/initiative outcome</i>
December 2021	

<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7004.html">https://standards.ieee.org/project/7004.html</a>

<i>Reference ID</i>
<b>IEEE P7005™</b>
<i>Title</i>
Standard on Employer Data Governance
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The standard provides guidelines and certifications on storing, protecting, and using employee data in an ethical and transparent way. The project recommends tools and services that help employees make informed decisions with their personal information. The standard will help provide clarity and recommendations both for how employees can share their information in a safe and trusted environment as well as how employers can align with employees in this process while still utilizing information needed for regular work flows.
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2021
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7005.html">https://standards.ieee.org/project/7005.html</a>

<i>Reference ID</i>
<b>IEEE P7006™</b>
<i>Title</i>
Standard on Personal Data AI Agent Working Group
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
The standard addresses concerns raised about machines making decisions without human input. This standard hopes to educate government and industry on why it is best to put mechanisms into place to enable the design of systems that will mitigate the ethical concerns when AI systems can organize and share personal information on their own. Designed as a tool to allow any individual to essentially create their own personal "terms and conditions" for their data, the AI Agent will provide a technological tool for individuals to manage and control their identity in the digital and virtual world.
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2022
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7006.html">https://standards.ieee.org/project/7006.html</a>

<i>Reference ID</i>	
<b>IEEE P7007™</b>	
<i>Title</i>	
ONTOLOGICAL STANDARD FOR ETHICALLY DRIVEN ROBOTICS AND AUTOMATION SYSTEMS	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
Ontological Standard for Ethically driven Robotics and Automation Systems establishes a set of ontologies with different abstraction levels that contain concepts, definitions and axioms that are necessary to establish ethically driven methodologies for the design of Robots and Automation Systems.	
<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
December 2021	
<i>Useful Link</i>	
<a href="https://standards.ieee.org/project/7007.html">https://standards.ieee.org/project/7007.html</a>	

<i>Reference ID</i>	
<b>IEEE P7008™</b>	
<i>Title</i>	
Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
This standard establishes a delineation of typical nudges (currently in use or that could be created) that contains concepts, functions and benefits necessary to establish and ensure ethically driven methodologies for the design of the robotic, intelligent and autonomous systems that incorporate them. "Nudges" as exhibited by robotic, intelligent or autonomous systems are defined as overt or hidden suggestions or manipulations designed to influence the behavior or emotions of a user.	
<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
December 2022	
<i>Useful Link</i>	
<a href="https://standards.ieee.org/project/7008.html">https://standards.ieee.org/project/7008.html</a>	

<i>Reference ID</i>	
<b>IEEE P7009™</b>	
<i>Title</i>	

STANDARD FOR FAIL-SAFE DESIGN OF AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS	
	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
	Standard that establishes a practical, technical baseline of specific methodologies and tools for the development, implementation, and use of effective fail-safe mechanisms in autonomous and semi-autonomous systems. The standard includes (but is not limited to): clear procedures for measuring, testing, and certifying a system's ability to fail safely on a scale from weak to strong, and instructions for improvement in the case of unsatisfactory performance. The standard serves as the basis for developers, as well as users and regulators, to design fail-safe mechanisms in a robust, transparent, and accountable manner.
	<i>Maturity level</i>
In development	<i>Release time of specification/initiative outcome</i>
December 2022	<i>Useful Link</i>
	<a href="https://standards.ieee.org/project/7009.html">https://standards.ieee.org/project/7009.html</a>

<i>Reference ID</i>	
<b>IEEE 7010™ -2020</b>	<i>Title</i>
	IEEE RECOMMENDED PRACTICE FOR ASSESSING THE IMPACT OF AUTONOMOUS AND INTELLIGENT SYSTEMS ON HUMAN WELL-BEING
	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
	The impact of artificial intelligence or autonomous and intelligent systems (A/IS) on humans is measured by this standard. The positive outcome of A/IS on human well-being is the overall intent of this standard. Scientifically valid well-being indices currently in use and based on a stakeholder engagement process ground this standard. Product development guidance, identification of areas for improvement, risk management, performance assessment, and the identification of intended and unintended users, uses and impacts on human well-being of A/IS are the intents of this standard.
	<i>Maturity level</i>
Published	<i>Release time of specification/initiative outcome</i>
05/2020	<i>Useful Link</i>
	<a href="https://standards.ieee.org/standard/7010-2020.html">https://standards.ieee.org/standard/7010-2020.html</a>

<i>Reference ID</i>	
<b>IEEE P7011™</b>	<i>Title</i>

STANDARD FOR THE PROCESS OF IDENTIFYING & RATING THE TRUST-WORTHINESS OF NEWS SOURCES	
	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
<p>Standard for the Process of Identifying &amp; Rating the Trustworthiness of News Sources will address the negative impacts of the unchecked proliferation of fake news by providing an open system of easy-to-understand ratings. In so doing, it shall assist in the restoration of trust in some purveyors, appropriately discredit other purveyors, provide a disincentive for the publication of fake news, and promote a path of improvement for purveyors wishing to do so. The standards shall target a representative sample set of news stories in order to provide a meaningful and accurate rating scorecard.</p>	
	<i>Maturity level</i>
In development	<i>Release time of specification/initiative outcome</i>
December 2022	<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7011.html">https://standards.ieee.org/project/7011.html</a>	

Reference ID	
<b>IEEE P7012™</b>	
Title	
STANDARD FOR MACHINE READABLE PERSONAL PRIVACY TERMS	
	<i>Domain level</i>
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
<p>Standard for Machine Readable Personal Privacy Terms will provide individuals with means to proffer their own terms respecting personal privacy, in ways that can be read, acknowledged and agreed to by machines operated by others in the networked world. In a more formal sense, the purpose of the standard is to enable individuals to operate as first parties in agreements with others—mostly companies—operating as second parties. Note that the purpose of this standard is not to address privacy policies, since these are one-sided and need no agreement. (Terms require agreement; privacy policies do not.)</p>	
	<i>Maturity level</i>
In development	<i>Release time of specification/initiative outcome</i>
December 2022	<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7012.html">https://standards.ieee.org/project/7012.html</a>	

Reference ID	
<b>IEEE P7014™</b>	<i>Title</i>
STANDARD FOR EMULATED EMPATHY IN AUTONOMOUS AND INTELLIGENT SYSTEMS AND INTELLIGENT SYSTEMS	
<i>Domain level</i>	
General	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Defines a model for ethical considerations and practices in the design, creation and use of empathic technology, incorporating systems that have the capacity to identify, quantify, respond to, or simulate affective states.	
<i>Maturity level</i>	
In development	<i>Release time of specification/initiative outcome</i>
December 2023	<i>Useful Link</i>
<a href="https://standards.ieee.org/project/7014.html">https://standards.ieee.org/project/7014.html</a>	

Reference ID	
<b>IEEE 2801</b>	<i>Title</i>
Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence	
<i>Domain level</i>	
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
The standard identifies best practices for establishing a quality management system for datasets used for artificial intelligence medical device. The recommended practice covers a full cycle of dataset management, including items such as but not limited to data collection, transfer, utilization, storage, maintenance and update. The recommended practice recommends a list of critical factors that impact the quality of datasets, such as but not limited to data sources, data quality, annotation, privacy protection, personnel qualification/training/evaluation, tools, equipment, environment, process control and documentation.	
<i>Maturity level</i>	
In development	<i>Release time of specification/initiative outcome</i>
May 2022	<i>Useful Link</i>
<a href="https://standards.ieee.org/project/2801.html">https://standards.ieee.org/project/2801.html</a>	

Reference ID	
<b>IEEE P2802</b>	<i>Title</i>

Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology	<i>Domain level</i>
Application	<i>Type of initiative</i>
Standard	<i>Main Objectives and Expected content</i>
Establishes terminology used in artificial intelligence medical device, including definitions of fundamental concepts and methodology that describe the safety, effectiveness, risks and quality management of artificial intelligence medical device.	
<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
December 2022	
<i>Useful Link</i>	
<a href="https://standards.ieee.org/project/2802.html">https://standards.ieee.org/project/2802.html</a>	

<i>Reference ID</i>	
<b>IEEE P2807.1™</b>	
<i>Title</i>	
Knowledge Graph Testing	
<i>Domain level</i>	
General	
<i>Type of initiative</i>	
Standard	
<i>Main Objectives and Expected content</i>	
This standard defines technical requirements, performance metrics, evaluation criteria and test cases for knowledge graphs. The mandatory test cases include data input, metadata, data extraction, data fusion, data storage and retrieval, inference and analysis, and knowledge graph display.	
<i>Maturity level</i>	
In development	
<i>Release time of specification/initiative outcome</i>	
December 2023	
<i>Useful Link</i>	
<a href="https://standards.ieee.org/project/2807_1.html">https://standards.ieee.org/project/2807_1.html</a>	

<i>Reference ID</i>
<b>IEEE P2846™</b>
<i>Title</i>
A FORMAL MODEL FOR SAFETY CONSIDERATIONS IN AUTOMATED VEHICLE DECISION MAKING
<i>Domain level</i>
Application
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>

This standard defines a formal rules-based mathematical model for automated vehicle decision making using discrete mathematics and logic. The model applies to the planning and decision-making functions of an SAE Level 3-5 automated vehicle. The model is formally verifiable, technology neutral, and parameterized to allow for regional customization by governments as desired. The standard applies to specified driving scenarios and cases, which do not eliminate all hazards but balance safety with practicability. For example, some scenarios include highway driving and potentially full urban driving. The standard also describes a test methodology and tools necessary to perform verification of an automated vehicle to assess conformance with the standard. The proposed standard does not address the host vehicle navigation system implementing the logic or anything relating to perception, object detection, recognition, verification and/or classification, free space detection, etc.

<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2021
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/2846.html">https://standards.ieee.org/project/2846.html</a>

<i>Reference ID</i>
<b>IEEE P2863™</b>
<i>Title</i>
Recommended Practice for Organizational Governance of Artificial Intelligence
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
This recommended practice specifies governance criteria such as safety, transparency, accountability, responsibility and minimizing bias, and process steps for effective implementation, performance auditing, training and compliance in the development or use of artificial intelligence within organizations.
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2022
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/2863.html">https://standards.ieee.org/project/2863.html</a>

<i>Reference ID</i>
<b>IEEE P3652.1-2020™</b>
<i>Title</i>
Guide for Architectural Framework and Application of Federated Machine Learning
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>

Provides a blueprint for data usage and model building across organizations while meeting applicable privacy, security and regulatory requirements. It defines the architectural framework and application guidelines for federated machine learning, including: 1) description and definition of federated learning, 2) the types of federated learning and the application scenarios to which each type applies, 3) performance evaluation of federated learning, and 4) associated regulatory requirements.

<i>Maturity level</i>
Approved draft
<i>Release time of specification/initiative outcome</i>
December 2022
<i>Useful Link</i>
<a href="https://standards.ieee.org/standard/3652_1-2020.html">https://standards.ieee.org/standard/3652_1-2020.html</a>

<i>Reference ID</i>
<b>IEEE P3333.1.3</b>
<i>Title</i>
STANDARD FOR THE DEEP LEARNING-BASED ASSESSMENT OF VISUAL EXPERIENCE BASED ON HUMAN FACTORS
<i>Domain level</i>
General
<i>Type of initiative</i>
Standard
<i>Main Objectives and Expected content</i>
This standard defines deep learning-based metrics of content analysis and quality of experience (QoE) assessment for visual contents, which is an extension of Standard for the Quality of Experience (QoE) and Visual-Comfort Assessments of Three-Dimensional (3D) Contents Based on Psychophysical Studies (IEEE STD 3333.1.1)) and Standard for the Perceptual Quality Assessment of Three Dimensional (3D) and Ultra High Definition (UHD) Contents (IEEE 3333.1.2). The scope covers the following:
<ul style="list-style-type: none"> <li>* Deep learning models for QoE assessment (multilayer perceptrons, convolutional neural networks, deep generative models)</li> <li>* Deep metrics of visual experience from High Definition (HD), UHD, 3D, High Dynamic Range (HDR), Virtual Reality (VR) and Mixed Reality (MR) contents</li> <li>* Deep analysis of clinical (electroencephalogram (EEG), electrocardiogram (ECG), electrooculography (EOG), and so on) and psychophysical (subjective test and simulator sickness questionnaire (SSQ)) data for QoE assessment</li> <li>* Deep personalized preference assessment of visual contents</li> <li>* Building image and video databases for performance benchmarking purpose if necessary.</li> </ul>
<i>Maturity level</i>
In development
<i>Release time of specification/initiative outcome</i>
December 2021
<i>Useful Link</i>
<a href="https://standards.ieee.org/project/3333_1_3.html">https://standards.ieee.org/project/3333_1_3.html</a>

## Annex E Standards mapping per Requirement



### Data and data governance

The most relevant standards regarding data and data governance for AI risk systems are summarized in Table 23.

Table 23. Relevant standards for the requirement: "Data and data governance"

SDO	Relevant standards
IEEE	ECPAIS Bias – Data consistency and evaluation; IEEE P7002; P7003; P7004; P7005; P7006; P7009; IEEE P2801; P2807; P2863.
ETSI	DES/eHEALTH-008; GS CIM 009; ENI GS 001; ENI GS 005; GR NFV-IFA 041; DGR SAI 002; TR 103 675; TR 103 674; TS 101 182; TS 103 327; TS 103 194; TS 103 195.2
ISO/IEC JTC1	ISO/IEC 25024; ISO/IEC 5259; ISO/IEC 24668; ISO/IEC 25012
ITU-T	ITU-T Y.3170 ; ITU-T Y.MecTa-ML ; ITU-T Y.3531 ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU-T Y.4470 : Y.Supp.63 to ITU-T Y.4000 series



### Record-keeping and Technical Data

The most relevant standards regarding record-keeping and technical data needs are summarized in Table 24**Error! Reference source not found..**

Table 24. Relevant standards for the requirement: "Record-keeping" and "Technical Data"

SDO	Relevant standards
IEEE	ECPAIS Transparency – Understanding System Design; IEEE P7000, P7001, P7006; IEEE P2801, P2802, P2807, P2863, P3333.1.3;
ETSI	DGR SAI 002, ISG ZSM 002, ISG CIM 009, SAREF Ontologies;
ISO/IEC JTC1	ISO/IEC 5338; ISO/IEC 5469; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668; ISO/IEC 25012
ITU-T	



### Transparency and provision of information to users

The most relevant standards regarding transparency and provision of information to users are summarized in Table 25**Error! Reference source not found..**

*Table 25. Relevant standards for the requirement: "Transparency and provision of information to users"*

SDO	Relevant standards	
IEEE	ECPAIS Transparency – Confidence in System Behaviour, Understandability of Presentation, ECPAIS-Accountability, ECPAIS-Bias; IEEE P7001, P7008, P7012, P3652.1, P7000, P7003, P7004, P7005, P7007, P7009, P7011, P7014, P2863;	
ETSI	DES/eHEALTH-008; GS CIM 009; DGR SAI 002; SAREF Ontologies	
ISO/IEC JTC1	ISO/IEC 24027; ISO/IEC 24028; ISO/IEC 5338; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668; ISO/IEC 4213	
ITU-T	ITU-T Y.4470	

## Human oversight

The most relevant standards regarding human oversight are summarized in Table 26**Error! Reference source not found..**

*Table 26. Relevant standards for the requirement: "Human oversight"*

SDO	Relevant standards	
IEEE	ECPAIS Accountability – Human Oversight (G3), Adequate Quality of Understanding (G3.1.2); IEEE P7000, P7006, 7010, P7014, P2863;	
ETSI	DES/eHEALTH-008; DGR SAI 005; ENI 008;	
ISO/IEC JTC1		
ITU-T		

## Accuracy, robustness, and cybersecurity

The most relevant standards regarding the topics of robustness, accuracy and cybersecurity are summarized in Table 27**Error! Reference source not found..**

*Table 27. Relevant standards for the requirement: "Accuracy, robustness, and cybersecurity"*

SDO	Relevant standards	
IEEE	ECPAIS Transparency – Confidence in System Behaviour, Immutable Architecture; IEEE P7003; P7007, P7009, P7011, P7012; IEEE P2802, P 2807, P2846, P2863, P3333.1.3;	
ETSI	GS ARF 003; GR CIM 007; ENI GS 001; ENI GR 007; DGR SAI 001; DGR SAI 002; DGS SAI 003; GR SAI 004; DGR SAI 005; GS ZSM 002; TS 102 181; TS 101 182; TR 103 674; TR 103 675; TS 103 327; ENI GR 10	
ISO/IEC JTC1	ISO/IEC 24027; ISO/IEC 24028; ISO/IEC 24029; ISO/IEC 5469	
ITU-T	ITU-T Y.3170 ; ITU-T Y.qos-ml-arc ; ITU-T Y.MecTa-ML ; ITU-T Y.3531 ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU- T Y.4470	



## Quality Management System

The most relevant standards regarding quality management system are summarized in Table 28**Error! Reference source not found..**

Table 28. Relevant standards for Quality Management system

SDO	Relevant standards	
IEEE	IEEE P2801; IEEE P2863, IEEE P7000;	
ETSI	TR 103 748, TR 103 749	
ISO	ISO/IEC 25059; ISO/IEC 2867; ISO/IEC 38507; ISO/IEC 42001;	
ITU-T		

### **Box 1. ISO 9000 standard family for Quality Management Systems**

Although it does not concern AI per se, a fundamental set of standards for Quality Management Systems (QMS) is the ISO 9000 series.

The standards in the ISO 9000 series provide organizations with a number of quality management principles, including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement.

In particular, ISO 9000 outlines the seven quality management principles underlying the family of standards, while ISO 9001 details the requirements to be fulfilled by organizations in order to comply with the standard.

ISO 9001 is the only standard in the family that can be certified to. It can be used independently from the organization size and its field of activity. Thus, it is a widely used tool for management, with over one million companies and organizations in over 170 countries certified to ISO 9001 (ISO, 2014).



### Risk Management System

The most relevant standards regarding risk management system (including testing for conformity assessment) are summarized in Table 29**Error! Reference source not found..**

*Table 29. Relevant standards for Risk Management system (including testing for conformity assessment)*

SDO	Relevant standards	
IEEE	IEEE P2863; IEEE P7009; IEEE P2807; IEEE P2846	
ETSI	TR 103 821; GS ARF 003; CIM GR 007; ENI GS 005; GR NFV-IFA 041; DGS SAI 003; EG 203 341; TS 103 194; TS 103 195.2; TR 103 748; TR 103 749;	
ISO/IEC JTC1	ISO/IEC 23894; ISO/IEC 5469; ISO/IEC 4213; ISO/IEC 25059; ISO/IEC 24029-2	
ITU-T	ITU-T Y.qos-ml-arc ; ITU-T Y.3172 ; ITU-T H.CUAV-AIF ; ITU-T F.VS-AIMC ; ITU-T Y.4470	

## Annex F. Standards mapping per SDO

### CEN/CENELEC Focus Group on AI and future JTC

CEN and CENELEC aim to work as the interface between international standardisation and the European market needs (business, policy, and regulatory contexts).

In 2020, CEN/CENELEC established a Focus Group on AI to recognize the European needs for AI standardisation and support future EU (horizontal and vertical) regulations on AI. The Focus Group worked out a road map analysis, building on a strong consensus of over 80 experts (CEN/CENELEC, 2020).

Implementing one of the Focus Group recommendations, in June 2021, CEN-CENELEC established the JTC21 on "Artificial Intelligence". The scope of this committee is:

To "... produce standardisation deliverables in the field of Artificial Intelligence (AI) and related use of data, as well as provide guidance to other technical committees concerned with Artificial Intelligence. The JTC shall also consider the adoption of relevant international standards and standards from other relevant organisations, like ISO/IEC JTC 1 and its subcommittees, such as SC 42 (Artificial Intelligence). The JTC shall produce standardisation deliverables to address European market and societal needs and to underpin primarily EU legislation, policies, principles, and values (CEN-CENELEC, 2021).

### ETSI standards and initiatives

In this section, we review the standards and initiatives by ETSI that are relevant with respect to the recognized AI requirements. In Table 30**Error! Reference source not found.**, we give an overview on the alignment between each specification and the requirements set out by the European Commission (European Commission, 2020).

*Table 30. Overview of standards and initiatives by ETSI and their alignment with the EC requirements.*

Title	Data and data governance	Quality management system	Technical data and Record keeping	Transparency and information to users	Human oversight	Robustness accuracy, and cybersecurity	Risk management system
DES/eHEALTH-008	X		X	X		X	
TR 103 821							X
GS ARF 003					X		X
CIM GR 007					X		X
GS CIM 009	X			X			
ENI GS 001	X				X		
ENI GS 005	X						X
ENI GR 007					X		
GR NFV-IFA 041	X						X
DGR SAI 001					X		
DGR SAI 002	X		X	X	X		
DGS SAI 003					X		X
GR SAI 004					X		
DGR SAI 005					X		X
GS ZSM 002					X		
TS 102 181					X		
TS 101 182	X				X		X
EG 203 341							X
SAREF Ontology				X		X	
TR 103 674	X				X		

TR 103 675	X				X		
TR 103748		X					X
TR 103749		X					X
TR 103821							
TS 103 327	X				X		
TS 103 194	X						X
TS 103 195.2	X						X

Each standard and initiative is briefly introduced in “Annex A. ETSI standards and initiatives description”.

## ISO/IEC JTC1 standards and initiatives

In this section, we review the standards and initiatives by ISO/IEC JTC1 that are relevant with respect to AI requirements. In Table 31**Error! Reference source not found.**, we give an overview on the alignment between each specification and the requirements set out by the European Commission (European Commission, 2020).

*Table 31. Overview of standards and initiatives by ISO/IEC JTC1 and their alignment with the EC requirements.*

Title	Data and data governance	Quality management system	Technical data and Record keeping	Transparency and information to users	Human oversight	Robustness accuracy, and cybersecurity	Risk management systems
ISO/IEC 4213				X			X
ISO/IEC 5259	X						
ISO/IEC 5338			X	X			
ISO/IEC 5469			X			X	
ISO 9000:2015							X
ISO 9001:2015							X
ISO 9004:2018							X
ISO/IEC 23894							X
ISO/IEC 24027				X		X	
ISO/IEC 24028				X		X	
ISO/IEC 24029-2						X	X
ISO/IEC 24368			X	X			
ISO/IEC 24372			X	X			
ISO/IEC 23894							X
ISO/IEC 24668	X		X	X			
ISO/IEC 25012	X		X				
ISO/IEC 25024	X						
ISO/IEC 25059		X					X
ISO/IEC 2867	X						
ISO/IEC 29119							
ISO/IEC 38507		X					
ISO/IEC 42001		X					

Each standard and initiative is briefly introduced in “Annex B. ISO and ISO/IEC standards and initiatives description”.

## ITU-T standards and initiatives

In this section, we review the standards and initiatives by ITU-T that are relevant with respect to the proposed AI requirements. In Table 32**Error! Reference source not found.**, we give an overview of the alignment between each specification and the requirements set out by the European Commission (European Commission, 2021).

*Table 32 Overview of standards and initiatives by ITU-T and their alignment with the EC requirements.*

Title	Data and data governance	Quality management system	Technical data and Record keeping	Transparency and information to users	Human oversight	Robustness accuracy, and cybersecurity	Risk management system
ITU-T Y.3170	X				X		
ITU-T Y.qos-ml-arc					X		X
ITU-T Y.MecTa-ML	X				X		
ITU-T Y.3531	X				X		
ITU-T Y.3172	X				X		X
ITU-T H.CUAV-AIF	X				X		X
ITU-T F.VS-AIMC	X				X		X
ITU-T Y.4470	X			X	X		X
Y.Supp.63 to ITU-T Y.4000 series	X						

Each standard and initiative is briefly introduced in “Annex C. ITU-T standards and initiatives description”.

## IEEE standards and initiatives

In this section, we review the standards and initiatives by IEEE that are relevant with respect to the introduced AI requirements. In Table 33**Error! Reference source not found.**, we provide a mapping between existing IEEE work and the requirements set out by the European Commission (European Commission, 2020).

*Table 33. Overview of standards and initiatives by IEEE and their alignment with the EC requirements.*

Title	Data and data governance	Quality management system	Technical data and Record keeping	Transparency and information to users	Human oversight	Robustness accuracy, and cybersecurity	Risk management system
-------	--------------------------	---------------------------	-----------------------------------	---------------------------------------	-----------------	--	------------------------

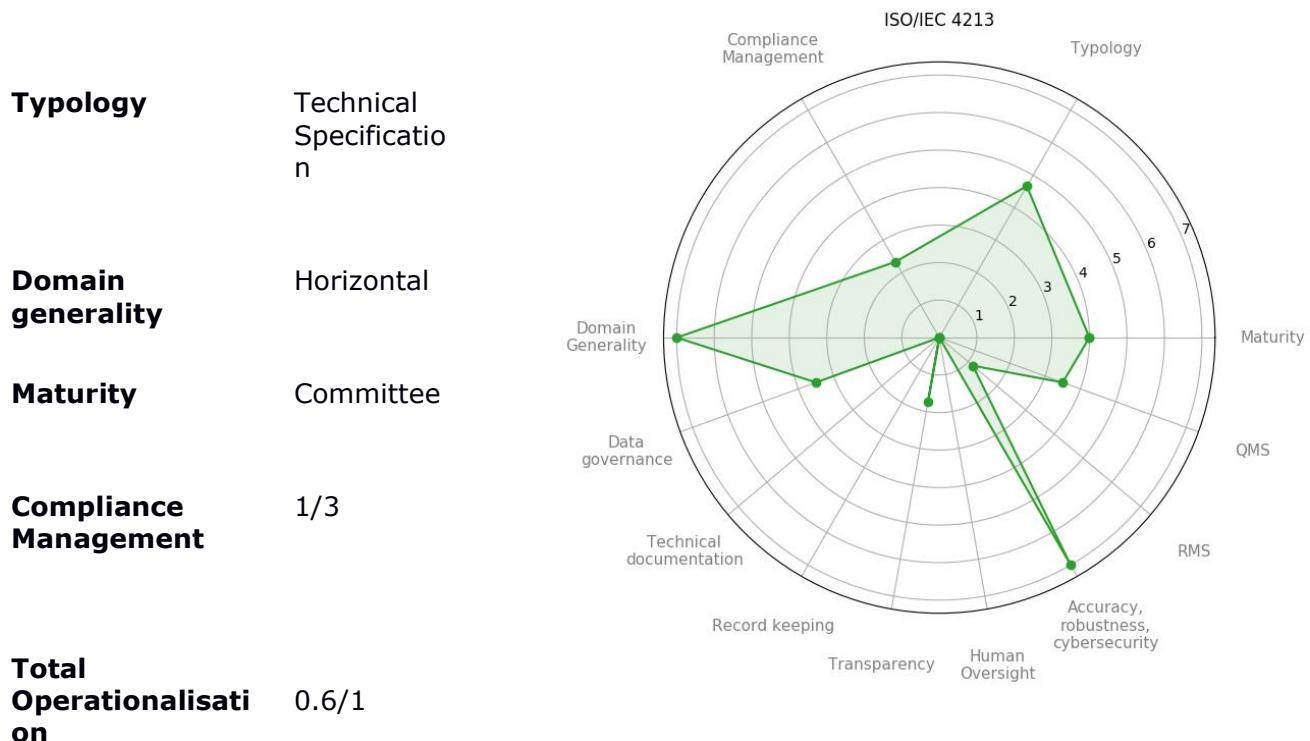
ECPAIS Bias	X			X			
ECPAIS Transparency			X	X	X		
ECPAIS Accountability				X		X	
IEEE P7000			X			X	
IEEE P7001			X	X			
IEEE P7002	X						
IEEE P7003	X			X	X		
IEEE P7004	X			X			
IEEE P7005	X			X			
IEEE P7006	X		X			X	
IEEE P7007				X	X		
IEEE P7008				X			
IEEE P7009	X			X	X		X
IEEE 7010						X	
IEEE P7011				X	X		
IEEE P7012				X		X	
IEEE P7014				X		X	
IEEE P2801	X		X				
IEEE P2802			X		X		
IEEE P2807	X		X		X		X
IEEE P2846					X		X
IEEE P2863	X		X	X	X	X	X
IEEE P3652.1				X			
IEEE P3333.1.3			X		X		
IEEE 2801		X					X

Each standard is briefly introduced in “Annex D. IEEE standards and initiatives description”.

## Annex G1. Fiches generated by the detailed analysis for ISO/IEC standards

ISO/IEC TS 4213 - Information Technology — Artificial Intelligence — Assessment of machine learning classification performance

### Overview



### Operationalisation score

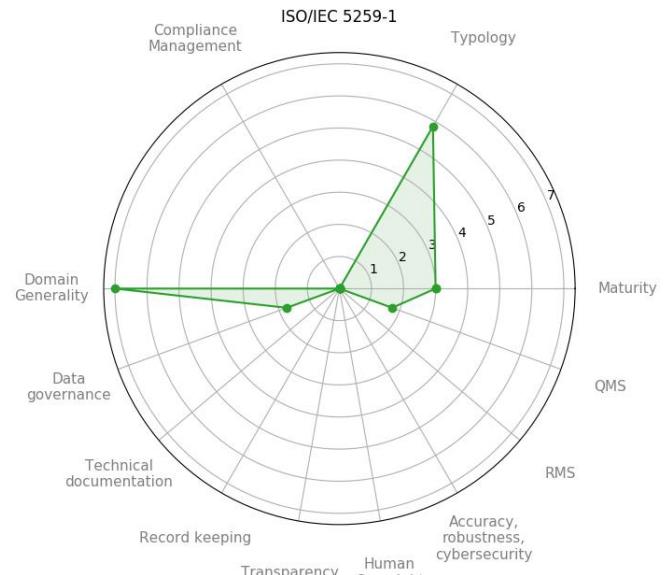
ISO IEC TS 4213	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R4. Transparency and information to users</b>
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR1.</b> Levels of accuracy and accuracy metrics
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies
	<b>R7. Risk management system</b>

	<b>SR3</b> Testing of AI system
<b>R8. Quality management system</b>	
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

ISO/IEC AWI 5259-1 Data quality for analytics and ML — Part 1: Overview, terminology, and examples

## Overview

<b>Typology</b>	International Standard
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Preparatory
<b>Compliance Management</b>	0/3
<b>Total Operationalisation</b>	0.25/1



## Operationalisation score

ISO IEC 5259-1	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R8. Quality management system</b>
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

## ISO/IEC AWI 5259-2 - Data quality for analytics and ML — Part 2: Data quality measures

### Overview

#### Typology

International Standard

#### Domain generality

Horizontal

#### Maturity

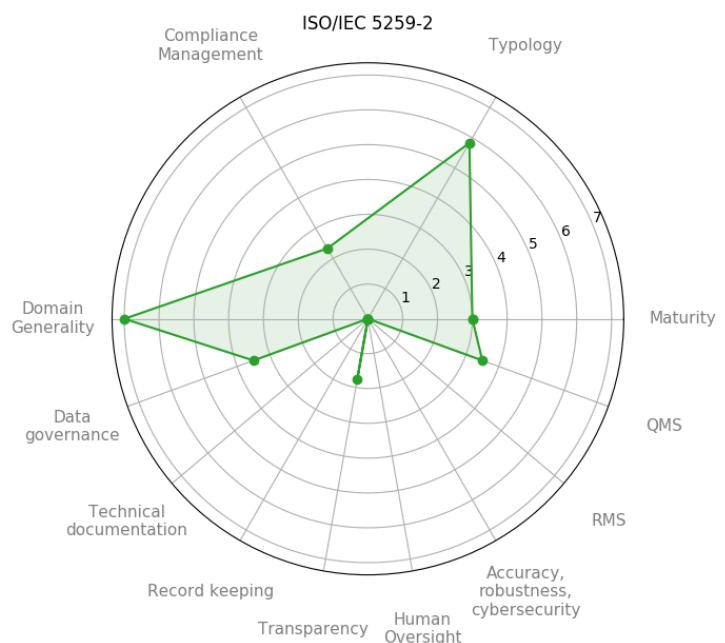
Preparatory

#### Compliance Management

1/3

#### Total Operationalisation

0.41  
n



### Operationalisation score

ISO IEC 5259-2	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R4. Transparency and information to users</b>
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>R8. Quality management system</b>
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

---

## ISO/IEC 5259-3 Data quality for analytics and ML — Part 3: Data quality management requirements and guidelines

### Overview

#### Typology

International  
Standard

#### Domain generality

Horizontal

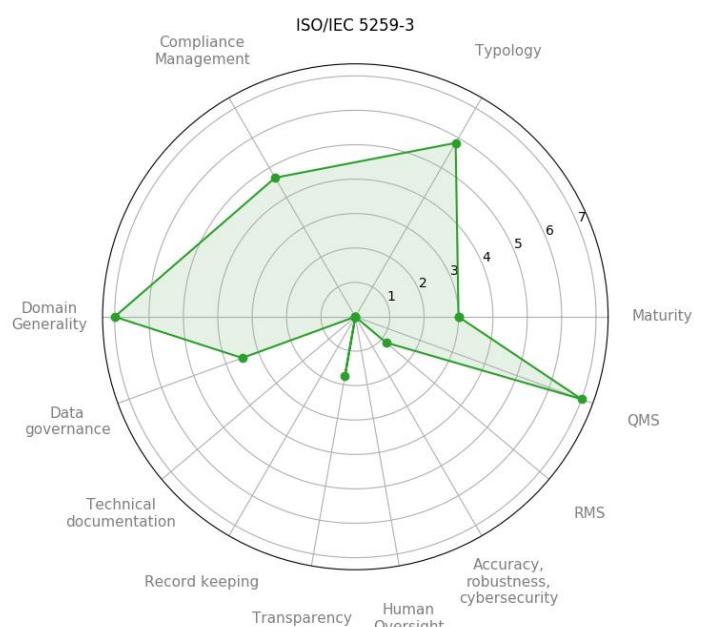
#### Maturity

Preparatory

#### Compliance Management

2/3

**Total Operationalisation** 0.47/1  
**n**



### Operationalisation score

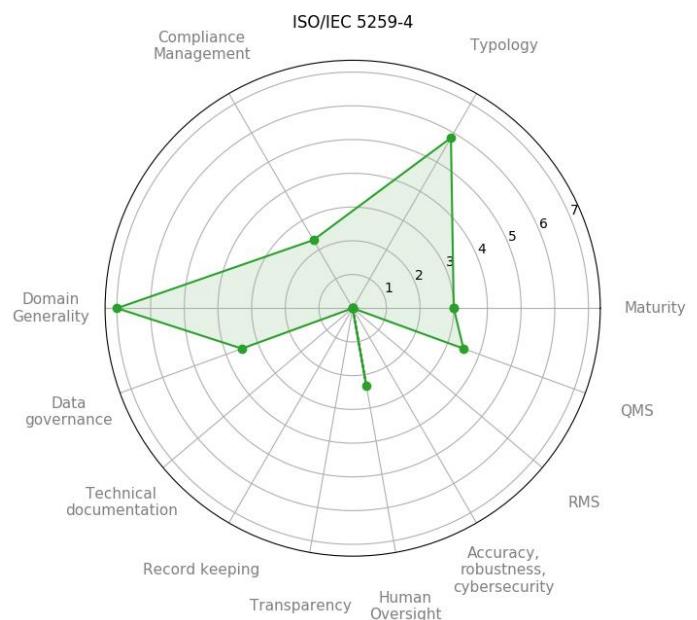
ISO IEC 5259-3	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R4. Transparency and information to users</b>
	<b>SR1.1.</b> Instruction for use and operations documentation
	<b>R7. Risk management system</b>
	<b>SR1.1.</b> Risk management process
	<b>R8. Quality management system</b>

	<b>SR1.</b> Quality management system (written) description <b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)
--	--

ISO/IEC AWI 5259-4 - Data quality for analytics and ML — Part 4: Data quality process framework

## Overview

<b>Typology</b>	International Standard
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Preparatory
<b>Compliance Management</b>	1/3
<b>Total Operationalisation</b>	0.44



## Operationalisation score

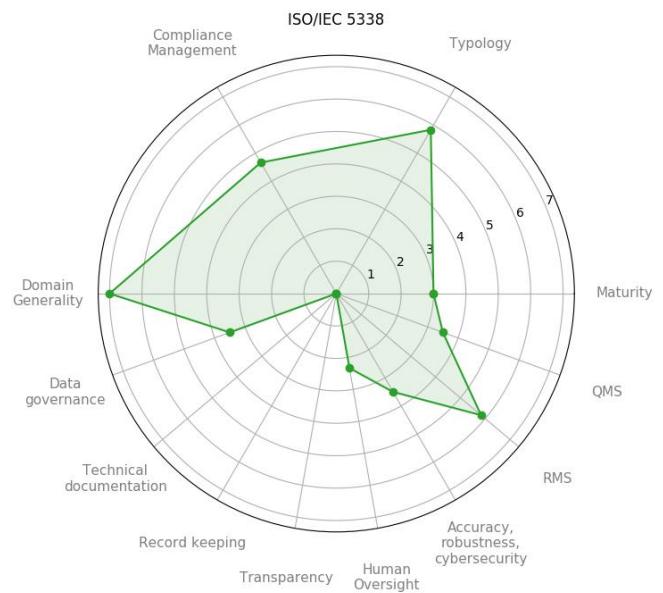
<b>ISO IEC 5259-4</b>	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R5. Human oversight</b>
	<b>SR1.1</b> Human oversight measures
	<b>R8. Quality management system</b>
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

---

## ISO/IEC AWI 5338 Information technology — Artificial intelligence — AI system life cycle processes

### Overview

<b>Typology</b>	International Standard
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Preparatory
<b>Compliance Management</b>	2/3
<b>Total Operationalisation</b>	0.53



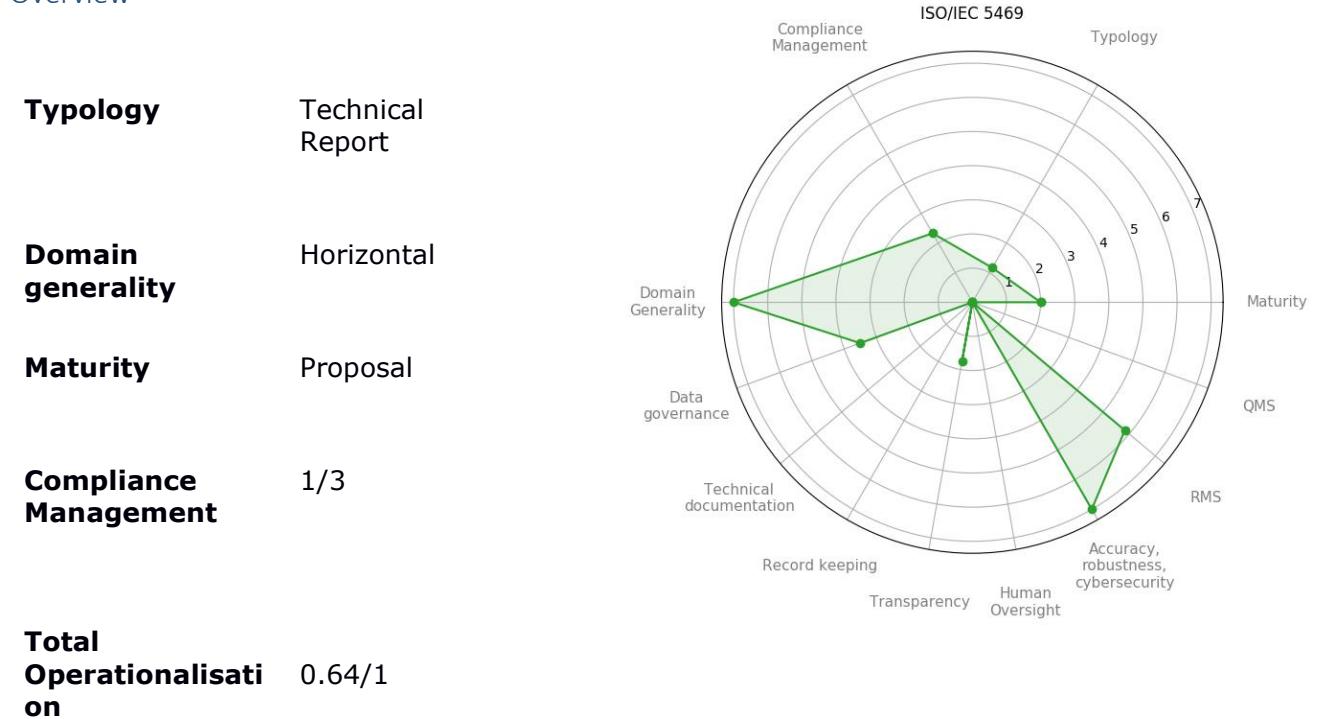
### Operationalisation score

<b>ISO IEC 5338</b>	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R5. Human oversight</b>
	<b>SR1.1</b> Human oversight measures
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR1.</b> Levels of accuracy and accuracy metric
	<b>R7. Risk management system</b>
	<b>SR1.</b> Risk management system characterizing AI system

	<p><b>SR1.1.</b> Risk management process</p> <p><b>SR1.2</b> Risk management measures to eliminate or reduce risks</p> <p><b>SR2</b> Required pre-conditions to operate the AI system</p> <p><b>SR3</b> Testing of AI system</p>
<b>R8. Quality management system</b>	
	<p><b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)</p>

## ISO/IEC TR 5469 - Artificial intelligence — Functional safety and AI systems

### Overview



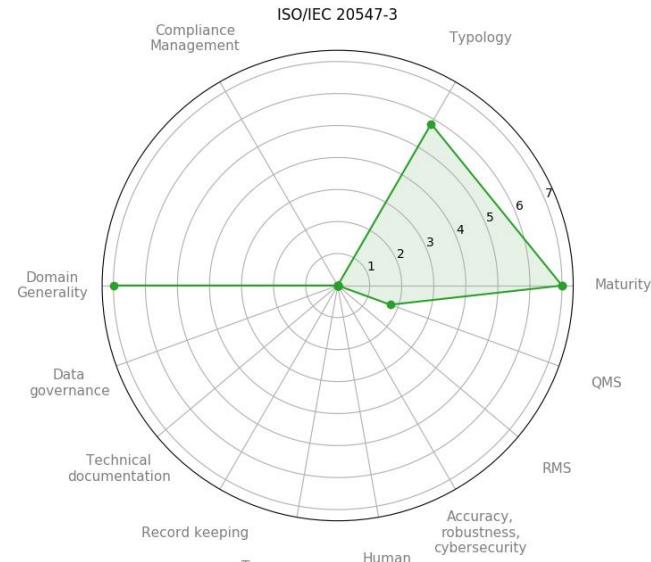
### Operationalisation score

ISO IEC IEC TR 5469	<b>R1. Data and data governance</b> <b>SR1.</b> Training, validation, and testing datasets
------------------------------	---

	<b>R4. Transparency and information to users</b>
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR1.</b> Levels of accuracy and accuracy metrics
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies
	<b>R7. Risk management system</b>
	<b>SR1.</b> Risk management system characterizing AI system
	<b>SR1.1.</b> Risk management process
	<b>SR1.2</b> Risk management measures to eliminate or reduce risks
	<b>SR2</b> Required pre-conditions to operate the AI system
	<b>SR3</b> Testing of AI system

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

## Overview

Typology	International Standard	
Domain generality	Horizontal	
Maturity	Published	
Compliance Management	0/3	
Total Operationalisation	0.25	

Operationalisation score

ISO IEC 20547.3	<b>R8. Quality Management System</b>
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality) compliance strategy applied technical specifications (including standards) data management (including: data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention)

---

ISO/IEC 23894.2 - Information Technology — Artificial Intelligence — Risk Management

Overview

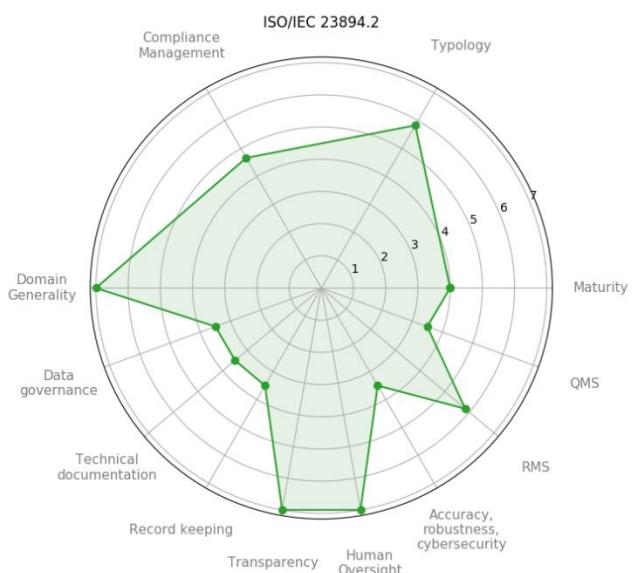
### Typology

**Domain generality**    Horizontal

**Maturity**                  Committee

**Compliance Management**      2/3

**Total Operationalisation**      0.66/1



Operationalisation score

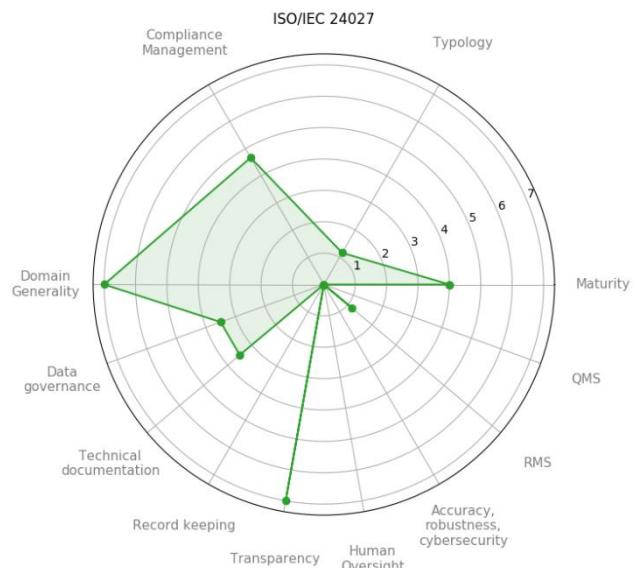
### ISO IEC R1. Data and data governance

	<b>SR1.</b> Training, validation, and testing datasets
	<b>R2. Technical documentation</b>
	<b>SR1.</b> Technical documentation of the high-risk AI system
	<b>R3. Record keeping</b>
	<b>SR1.</b> High-risk system automatic logging capability (the automatic recording of events while the high-risk AI systems is operating)
	<b>R4. Transparency and information to users</b>
	<b>SR1.</b> Documentation existence (High-risk AI System Operations Transparency)
	<b>SR1.1.</b> Instruction for use and operations documentation
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>SR1.2.</b> Instruction for use and operations documentation
	<b>R5. Human oversight</b>
	<b>SR1.</b> Human oversight to preventing or minimize risks
	<b>SR1.1</b> Human oversight measures
	<b>SR1.2</b> Human oversight understanding and/or interpretation
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies
	<b>R7. Risk management system</b>
	<b>SR1.</b> Risk management system characterizing AI system
	<b>SR1.1.</b> Risk management process
	<b>SR1.2</b> Risk management measures to eliminate or reduce risks
	<b>SR2</b> Required pre-conditions to operate the AI system
	<b>SR3</b> Testing of AI system
	<b>R8. Quality management system</b>
	<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

# ISO/IEC TR 24027 Information technology — Artificial Intelligence (AI) — Bias in AI systems and AI aided decision making

## Overview

<b>Typology</b>	Technical Report
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Committee
<b>Compliance Management</b>	2/3
<b>Total Operationalisation</b>	0.54/1



## Operationalisation score

ISO IEC TR 24027	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R2. Technical documentation</b>
	<b>SR1.</b> Technical documentation of the high-risk AI system
	<b>R4. Transparency and information to users</b>
	<b>SR1.</b> Documentation existence (High-risk AI System Operations Transparency)
	<b>SR1.1.</b> Instruction for use and operations documentation
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>SR1.2.</b> Instruction for use and operations documentation
	<b>R7. Risk management system</b>
	<b>SR1.2</b> Risk management measures to eliminate or reduce risks

---

## ISO/IEC TR 24028:2020 Information technology — Artificial Intelligence (AI) — Bias in AI systems and AI aided decision making

### Overview

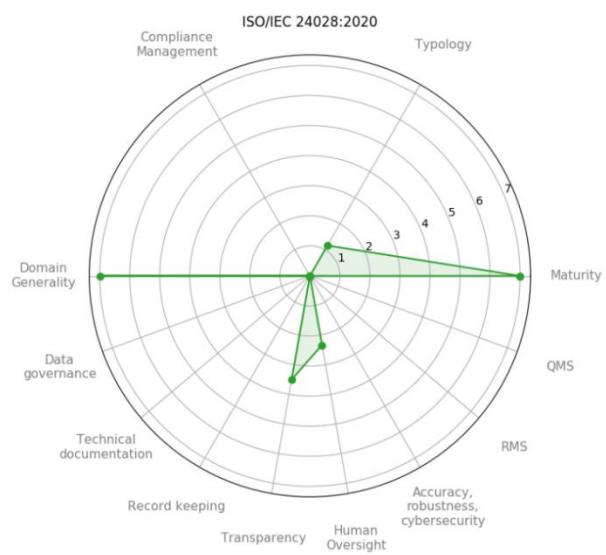
**Typology** Technical Report

**Domain generality** Horizontal

**Maturity** Published

**Compliance Management** 0/3

**Total Operationalisation** 0.41



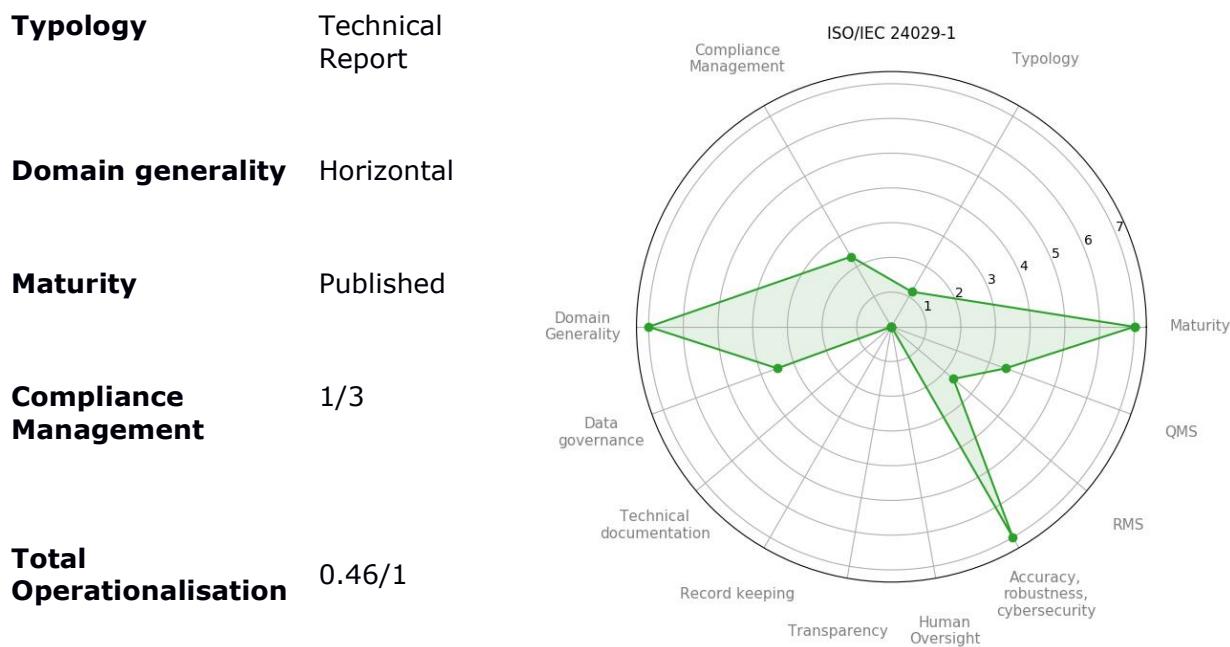
### Operationalisation score

	<b>R4. Transparency and information to users</b>
	<b>SR1.1.</b> Instruction for use and operations documentation
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>R5. Human oversight</b>
	<b>SR1.1</b> Human oversight measures

---

## ISO IEC TR 24029-1 Assessment of the robustness of neural networks - Part 1: Overview

### Overview



Operationalisation score

ISO IEC TR 24029-1	<b>Requirement 6: Accuracy, robustness and cybersecurity</b> <ul style="list-style-type: none"> <li><b>SR1.</b> Levels of accuracy and accuracy metrics      Declaration (in the instructions of use)</li> <li><b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies           <ul style="list-style-type: none"> <li>System vulnerabilities exploitation</li> <li>Training datasets manipulations (e.g. 'data poisoning', and 'adversarial examples')</li> </ul> </li> </ul>
	<b>Requirement 4: Transparency and provision of information to users</b> <ul style="list-style-type: none"> <li><b>SR1.</b> Documentation existence           <p>documentation that includes (concise, complete, correct and clear) information that is relevant, accessible and comprehensible to users</p> </li> </ul>
	<b>R1. Data and data governance</b> <ul style="list-style-type: none"> <li><b>SR1.</b> Training, validation, and testing datasets           <ul style="list-style-type: none"> <li>Quality Criteria</li> <li>Management practices</li> </ul> </li> </ul>

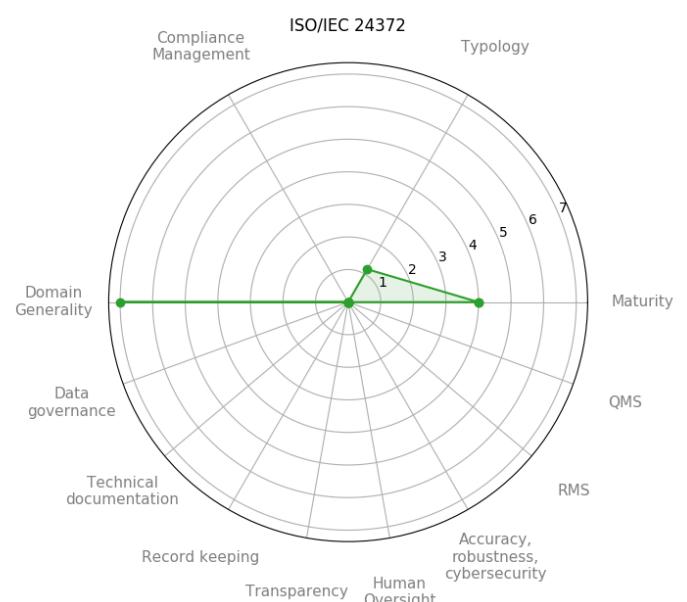
	<b>R7. Risk management system</b>
	<p><b>SR2.1</b> Risk management measures to eliminate or reduce risks</p> <ul style="list-style-type: none"> <li>adequate design and development</li> <li>user training</li> </ul>
	<p><b>SR2.</b> Required pre-conditions to operate the AI system</p> <ul style="list-style-type: none"> <li>user's capacities (e.g. technical knowledge, experience, education, training)</li> </ul>
	<b>R8. Quality management system</b>
	<p><b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)      compliance strategy</p> <ul style="list-style-type: none"> <li>applied technical specifications (including standards)</li> <li>data management (including: data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention)</li> </ul>

---

ISO/IEC TR 24372 Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems

## Overview

<b>Typology</b>	Technical Report
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Committee
<b>Compliance Management</b>	0/3
<b>Total Operationalisation</b>	0.0



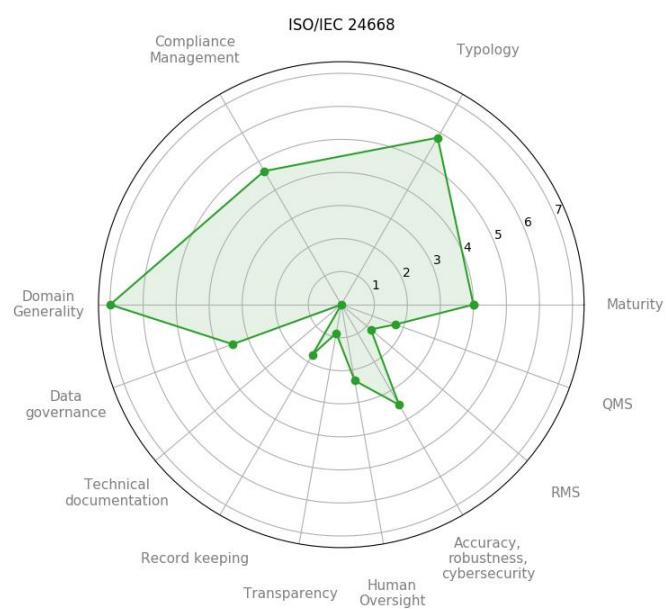
## Operationalisation score

ISO IEC TR 24372	<b>R1. Data and data governance</b> <b>R2. Technical documentation</b> <b>R3. Record keeping</b> <b>R4. Transparency and information to users</b> <b>R5. Human oversight</b> <b>R6. Accuracy, robustness, cybersecurity</b> <b>R7. Risk management system</b> <b>R8. Quality management system</b>
------------------	---

## ISO/IEC CD 24668 Information technology — Artificial intelligence — Process management framework for Big data analytics

### Overview

<b>Typology</b>	International Standard
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Committee
<b>Compliance Management</b>	2/3
<b>Total Operationalisation</b>	0.30

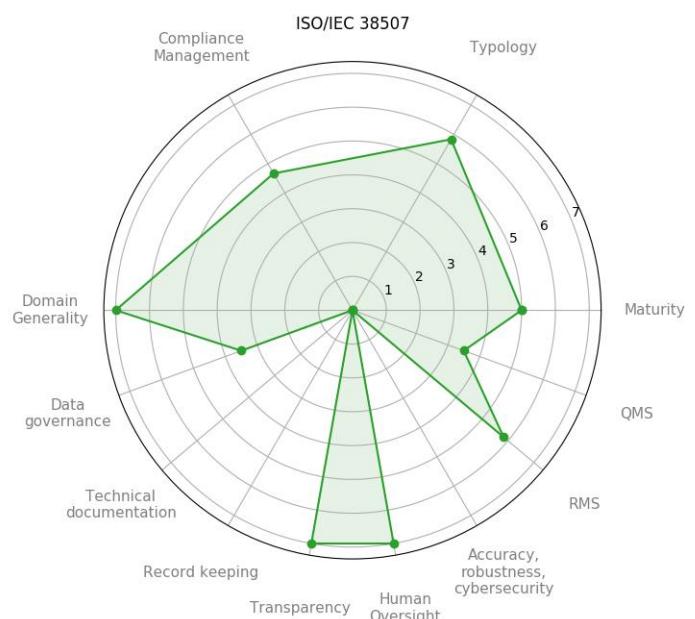


## Operationalisation score

<b>R1. Data and data governance</b>
<b>SR1.</b> Training, validation, and testing datasets
<b>R3. Record keeping</b>
<b>SR1.</b> High-risk system automatic logging capability (the automatic recording of events while the high-risk AI systems is operating)
<b>SR2.</b> High-risk system automatic logs content
<b>R4. Transparency and information to users</b>
<b>SR1.</b> Documentation existence (High-risk AI System Operations Transparency)
<b>SR1.1.</b> Instruction for use and operations documentation
<b>SR1.1.1.</b> Instruction and documentation content
<b>SR1.2.</b> Instruction for use and operations documentation
<b>R5. Human oversight</b>
<b>SR1.</b> Human oversight to preventing or minimize risks
<b>SR1.1</b> Human oversight measures
<b>SR1.2</b> Human oversight understanding and/or interpretation
<b>R6. Accuracy, robustness, cybersecurity</b>
<b>SR1.</b> Levels of accuracy and accuracy metrics
<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies
<b>R7. Risk management system</b>
<b>SR1.1.</b> Risk management process
<b>SR1.2</b> Risk management measures to eliminate or reduce risks
<b>R8. Quality management system</b>
<b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)

## Overview

<b>Typology</b>	International Standard
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Enquiry
<b>Compliance Management</b>	2/3
<b>Total Operationalisation</b>	0.76



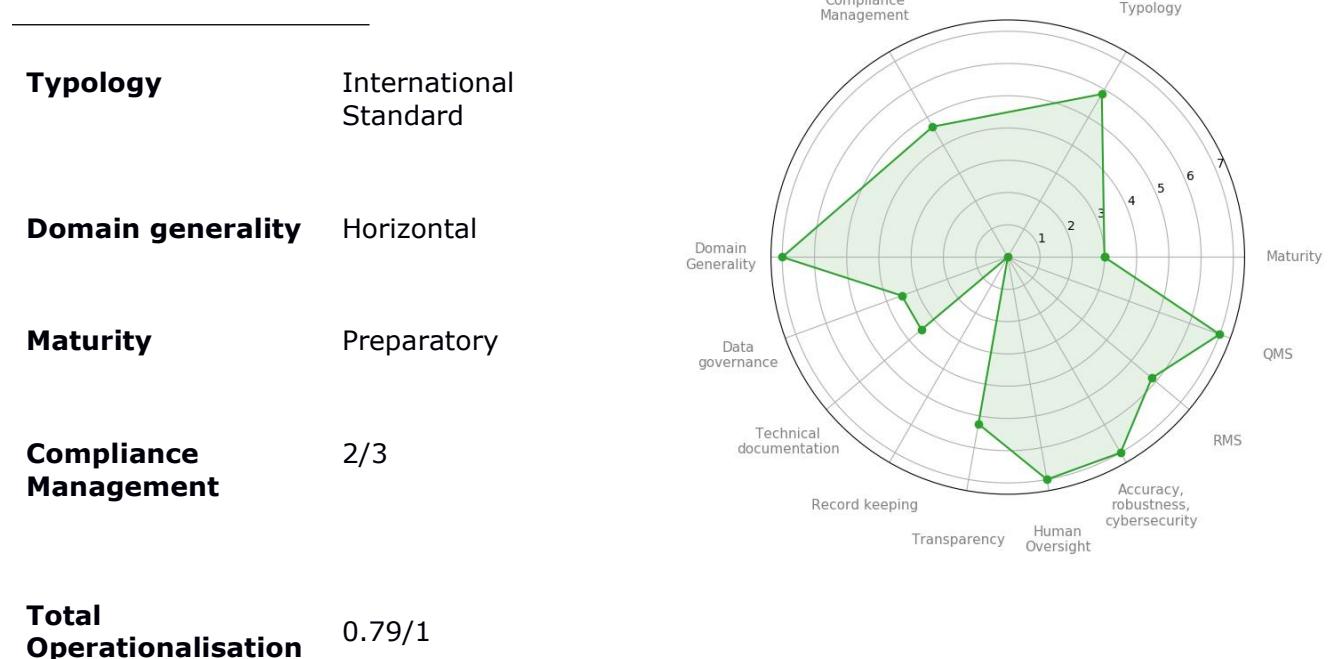
## Operationalisation score

<b>ISO IEC 38507</b>	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R4. Transparency and information to users</b>
	<b>SR1.</b> Documentation existence (High-risk AI System Operations Transparency)
	<b>SR1.1.</b> Instruction for use and operations documentation
	<b>SR1.1.1.</b> Instruction and documentation content
	<b>SR1.2.</b> Instruction for use and operations documentation
	<b>R5. Human oversight</b>
	<b>SR1.</b> Human oversight to preventing or minimize risks
	<b>SR1.1</b> Human oversight measures
	<b>SR1.2</b> Human oversight understanding and/or interpretation
	<b>R7. Risk management system</b>
	<b>SR1.</b> Risk management system characterizing AI system
	<b>SR1.1.</b> Risk management process

	<p><b>SR1.2</b> Risk management measures to eliminate or reduce risks</p> <p><b>SR2</b> Required pre-conditions to operate the AI system</p> <p><b>SR3</b> Testing of AI system</p>
<b>R8. Quality management system</b>	
	<p><b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)</p>

## ISO/IEC AWI 42001 Information Technology — Artificial intelligence — Management system

### Overview



### Operationalisation score

ISO IEC 42001	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R2. Technical documentation</b>
	<b>SR1.</b> Technical documentation of the high-risk AI system

	<b>R4. Transparency and information to users</b>
	<p><b>SR1.</b> Documentation existence (High-risk AI System Operations Transparency)</p> <p><b>SR1.1.</b> Instruction for use and operations documentation</p> <p><b>SR1.1.1.</b> Instruction and documentation content</p>
	<b>R5. Human oversight</b>
	<p><b>SR1.</b> Human oversight to preventing or minimize risks</p> <p><b>SR1.1</b> Human oversight measures</p> <p><b>SR1.2</b> Human oversight understanding and/or interpretation</p>
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<p><b>SR1.</b> Levels of accuracy and accuracy metrics</p> <p><b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies</p>
	<b>R7. Risk management system</b>
	<p><b>SR1.</b> Risk management system characterizing AI system</p> <p><b>SR1.1.</b> Risk management process</p> <p><b>SR1.2</b> Risk management measures to eliminate or reduce risks</p> <p><b>SR2</b> Required pre-conditions to operate the AI system</p> <p><b>SR3</b> Testing of AI system</p>
	<b>R8. Quality management system</b>
	<p><b>SR1.</b> Quality management system (written) description</p> <p><b>SR1.1.</b> Set of techniques, processes, and procedures (put in place to ensure quality)</p>

## Annex G2. Fiches generated by the detailed analysis for ETSI standards

### ETSI GR SAI 001 – AI Threat Ontology

#### Overview

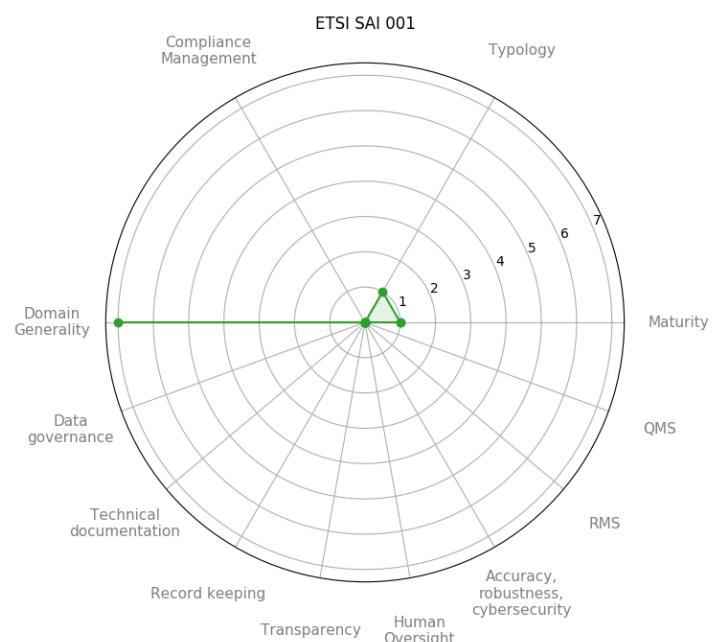
**Typology** Group Report

**Domain generality** Horizontal

**Maturity** Draft

**Compliance Management** 0/3

**Total Operationalisation** 0/1



#### Operationalisation score

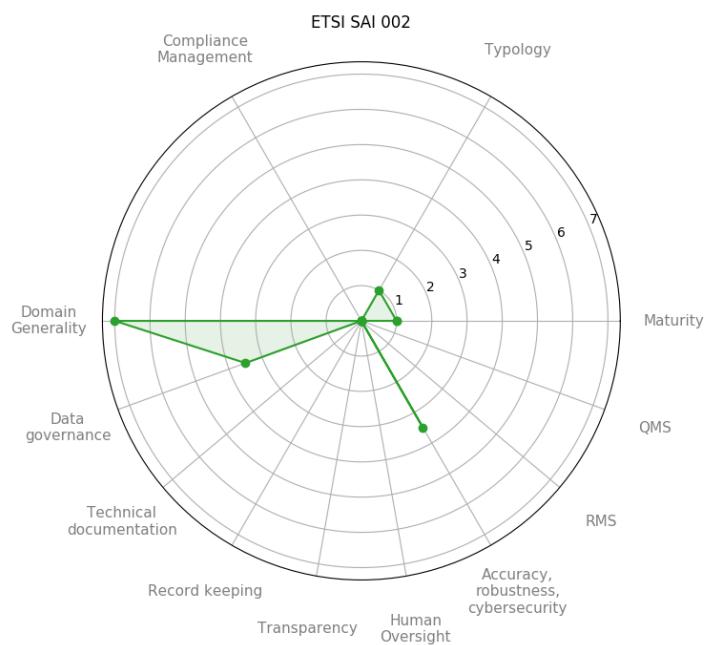
ETSI GR SAI 001	<b>R1. Data and data governance</b>
	<b>R2. Technical documentation</b>
	<b>R3. Record keeping</b>
	<b>R4. Transparency and information to users</b>
	<b>R5. Human oversight</b>
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>R7. Risk management system</b>
	<b>R8. Quality management system</b>

---

## ETSI GR SAI 002 – Data Supply Chain Methodology

### Overview

<b>Typology</b>	Group Report
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Draft
<b>Compliance Management</b>	0/3
<b>Total Operationalisation</b>	0.5/1



### Operationalisation score

ETSI GR SAI 002	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies

---

## ETSI GR SAI 003 – Securing Artificial Intelligence (SAI) - Security Testing of AI

## Overview

### **Typology**

Group Report

### **Domain generality**

Horizontal

### **Maturity**

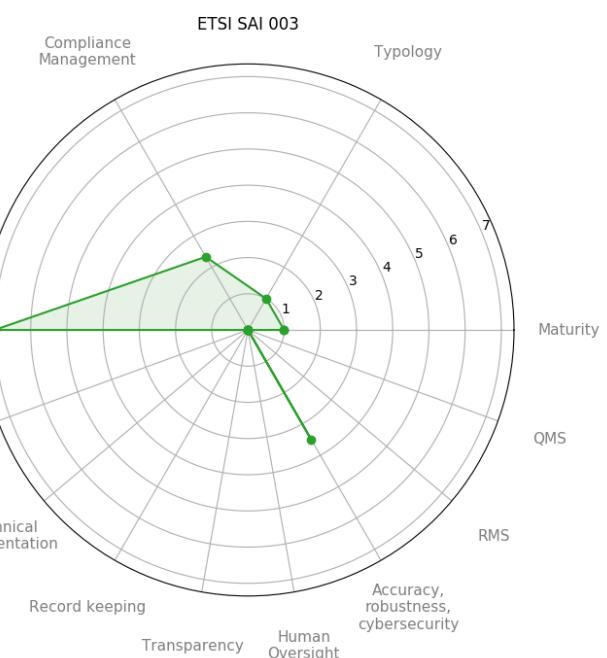
Draft

### **Compliance Management**

1/3

### **Total Operationalisation**

0.5/1

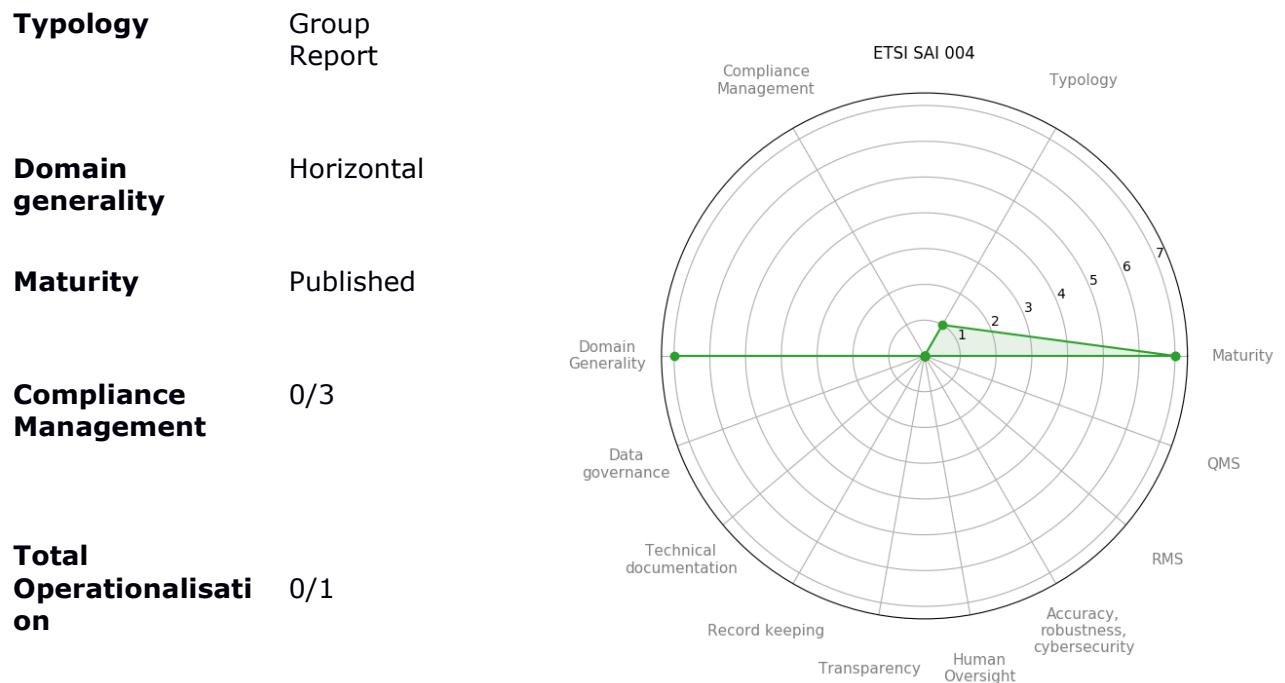


## Operationalisation score

<b>ETSI SAI 003</b>	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies

## ETSI SAI 004 - Securing Artificial Intelligence (SAI); Problem Statement

## Overview



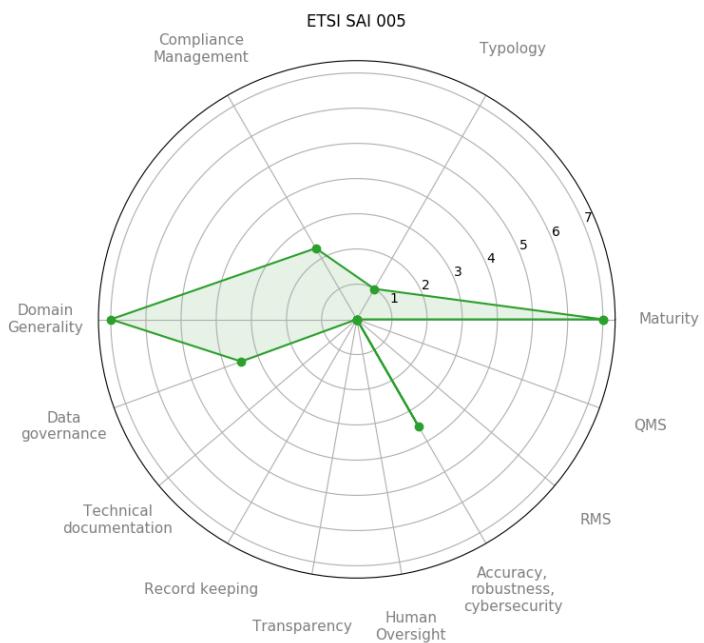
## Operationalisation score

<b>ETSI SAI 004</b>	<b>R1. Data and data governance</b>
	<b>R2. Technical documentation</b>
	<b>R3. Record keeping</b>
	<b>R4. Transparency and information to users</b>
	<b>R5. Human oversight</b>
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>R7. Risk management system</b>
	<b>R8. Quality management system</b>

ETSI GR SAI 005 - Securing Artificial Intelligence (SAI); Mitigation Strategy Report

## Overview

<b>Typology</b>	Group Report
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Published
<b>Compliance Management</b>	1/3
<b>Total Operationalisation</b>	0.5/1



## Operationalisation score

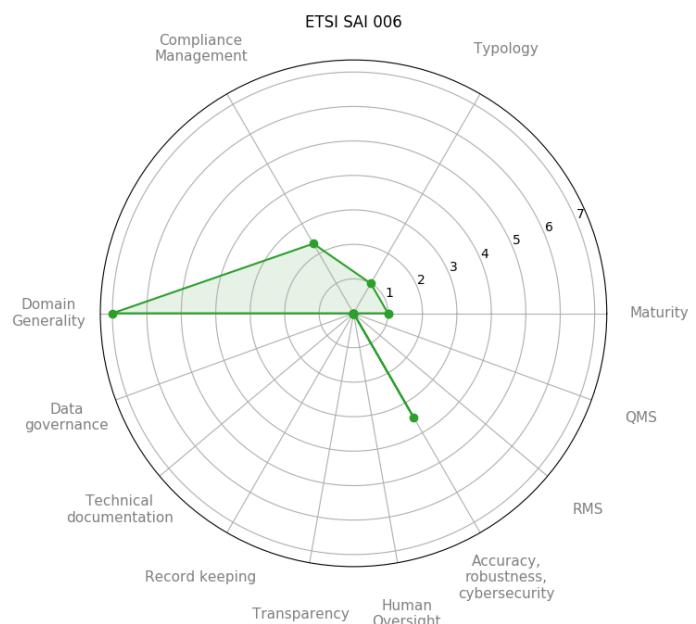
<b>ETSI SAI 005</b>	<b>R1. Data and data governance</b>
	<b>SR1.</b> Training, validation, and testing datasets
	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies

---

ETSI GR SAI 006 – Securing Artificial Intelligence (SAI); The role of hardware in security of AI

## Overview

<b>Typology</b>	Group Report
<b>Domain generality</b>	Horizontal
<b>Maturity</b>	Draft
<b>Compliance Management</b>	1/3
<b>Total Operationalisation</b>	0.5/1



## Operationalisation score

<b>ETSI SAI 006</b>	<b>R6. Accuracy, robustness, cybersecurity</b>
	<b>SR2.</b> Resilience/robustness as regards errors, faults or inconsistencies

## Annex H. Terms definition

Term	Definition	Source
artificial intelligence system (AI system)	software that is developed with one or more of the techniques and approaches listed in Annex I of AIA and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with	AIA
biometric data	personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data	AIA
common specifications	a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under this Regulation	AIA
conformity assessment	the process of verifying whether the requirements (e.g. defined by AIA) relating to an AI system have been fulfilled	AIA
conformity assessment body	a body that performs third-party conformity assessment activities, including testing, certification and inspection.	AIA
input data	data provided to or directly acquired by an AI system on the basis of which the system produces an output	AIA
instructions for use	the information provided by the provider to inform the user of in particular an AI system's intended purpose and proper use, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used;	AIA
intended purpose	the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation	AIA

harmonised standard	a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012	AIA
performance of an AI system	the ability of an AI system to achieve its intended purpose	AIA
provider	natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge	AIA
reasonably foreseeable misuse	the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems	AIA
testing data	data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service	AIA
training data	data used for training an AI system through fitting its learnable parameters, including the weights of a neural network	AIA
user	any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity	AIA
validation data	data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split	AIA

## 10 References

- Bartram, R. (2018, 10 18). THE NEW FRONTIER FOR ARTIFICIAL INTELLIGENCE. Retrieved from ISO.org: <https://www.iso.org/news/ref2336.html>
- Carpenter, T. (2012). Electronic publishing standards, Academic and professional publishing, Chandos publishing, pg. 215-241.
- CEN-CENELEC. (2021). *CEN/CLC/JTC 21 N 32*. Brussels: CEN-CENELEC.
- De Vries, H.J. (1998). The classification of standards. *Knowledge Organization*, 25(3), pg. 79-89.
- ETSI. (2021). *Types of standards*. Retrieved from ETSI: <https://www.etsi.org/standards/types-of-standards?jjj=1620577184012>
- European Commission. (1998). DIRECTIVE 98/34/EC (CELEX 31998L0034): laying down a procedure for the provision of information in the field of technical standards and. Luxembourg: Official Journal of the European Communities.
- European Commission. (2020). COM(2020) 65 final. WHITE PAPER: On Artificial Intelligence - A European approach to excellence and trust. Luxembourg: European Commission.
- European Commission. (2021, April 21). *Proposal for a Regulation laying down harmonised rules on artificial intelligence*. Retrieved from European Commission: <https://ec.europa.eu/newsroom/dae/redirection/document/75788>
- European Commission. (2021, April 21). Impact Assessment of the Regulation on Artificial intelligence. Retrieved from European Commission: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence>
- European Union. (2012). Regulation (eu) no 1025/2012 of the european parliament and of the council on European standardisation,. Brussels: European Union.
- High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for for trustworthy AI. Luxembourg: European Commission.
- IEC. (2021). *Terms and Definitions*. Retrieved from International Electrotechnical Commission: [https://www.iec.ch/standardsdev/resources/draftingpublications/directives/introductory/terms\\_and\\_definitions.htm](https://www.iec.ch/standardsdev/resources/draftingpublications/directives/introductory/terms_and_definitions.htm)
- IEEE Standards University. (2016, 09 23). STANDARDS GLOSSARY. Retrieved from IEEE.org: <https://www.standardsuniversity.org/article/standards-glossary/#D>
- ISO. (2021). *THE DIFFERENT TYPES OF ISO PUBLICATIONS*. Retrieved from Developin Standards: deliverables: <https://www.iso.org/deliverables-all.html>
- ISO. (2020). *Stages and Resources for Standards Development*. Retrieved from ISO: Resources: <https://www.iso.org/stages-and-resources-for-standards-development.html#:~:text=At%20the%20outset%2C%20each%20ISO,ISO%20standard%20follows%20defined%20stages>
- ISO. (2020, 12 14). INTERNATIONAL HARMONIZED STAGE CODES. Retrieved from www.iso.org: <https://www.iso.org/stage-codes.html>
- ISO, The ISO Survey of Management System Standard Certifications, 2014.
- OGC. (2020, 12 12). OGC Standards. Retrieved from OGC.org: <https://www.ogc.org/docs/is>
- Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC,

2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.

European Commission, Vademecum on European standardisation in support of Union legislation and policies, SWD(2015) 205 final of 27/10/2015.

Vaughan-Nichols S.J. (2010). Will HTML5 restandardize the web?. Computer 43(4), pg.13-15.

von der Leyen, U. (2019). *A Union that strives for more: my agenda for Europe*. Retrieved from POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2019-2024: [https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission\\_en\\_0.pdf](https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf)

## 11 List of Tables

TABLE 1. OVERALL REPRESENTATION OF MAPPED STANDARDS (ALREADY PUBLISHED STANDARDS ARE IN BOLD) .....	20
TABLE 2. DOMAIN GENERALITY OF AN IMPLEMENTATION STANDARD: POSSIBLE TOPICAL CASES.....	27
TABLE 3. EXECUTIVE VERSION OF THE “DATA AND DATA GOVERNANCE” REQUIREMENT .....	29
TABLE 4. KEYWORDS ASSOCIATED TO THE “DATA AND DATA GOVERNANCE” REQUIREMENT .....	30
TABLE 5. EXECUTIVE VERSION OF THE “TECHNICAL DOCUMENTATION” REQUIREMENT .....	30
<i>TABLE 6. KEYWORDS ASSOCIATED TO THE “TECHNICAL DOCUMENTATION” REQUIREMENT .....</i>	30
TABLE 7. EXECUTIVE VERSION OF THE “RECORD-KEEPING” REQUIREMENT .....	30
<i>TABLE 8. KEYWORDS ASSOCIATED TO THE “RECORD-KEEPING” REQUIREMENT .....</i>	31
TABLE 9. EXECUTIVE VERSION OF THE “TRANSPARENCY AND PROVISION OF INFORMATION TO USERS” REQUIREMENT .....	31
<i>TABLE 10. KEYWORDS ASSOCIATED TO THE “TRANSPARENCY AND PROVISION OF INFORMATION TO USERS” REQUIREMENT .....</i>	32
TABLE 11. EXECUTIVE VERSION OF THE “HUMAN OVERSIGHT” REQUIREMENT.....	32
<i>TABLE 12. KEYWORDS ASSOCIATED TO THE “HUMAN OVERSIGHT” REQUIREMENT.....</i>	32
TABLE 13. EXECUTIVE VERSION OF THE “ACCURACY, ROBUSTNESS AND CYBERSECURITY” REQUIREMENT .....	32
<i>TABLE 14. KEYWORDS ASSOCIATED TO THE “ACCURACY, ROBUSTNESS AND CYBERSECURITY” REQUIREMENT .....</i>	33
TABLE 15. EXECUTIVE VERSION OF THE “RISK MANAGEMENT SYSTEM” REQUIREMENT .....	33
<i>TABLE 16. KEYWORDS ASSOCIATED TO THE “RISK MANAGEMENT SYSTEM” REQUIREMENT .....</i>	34
TABLE 17. EXECUTIVE VERSION OF THE “QUALITY MANAGEMENT SYSTEM” REQUIREMENT .....	34
<i>TABLE 18. KEYWORDS ASSOCIATED TO THE “QUALITY MANAGEMENT SYSTEM” REQUIREMENT .....</i>	34
TABLE 19. ROLE OF THE ANALYSED STANDARDS IN OPERATIONALISATION THE AIA SUB-REQUIREMENTS. THE OUTLINED COLUMNS (WITH A PINK BACKGROUND) SHOWS THE EVIDENT GAPS, AT THE SUB-REQUIREMENTS LEVEL.....	37
TABLE 20. STANDARDS OPERATIONALISATION VALUES (SCORE FROM 0 TO 1) FOR EACH AIA REQUIREMENTS AND THE VALUE RESULTING TOTAL OPERATIONALISATION INDEXES (BOLD VALUE ARE GREATER THAN 0.5). .....	44
TABLE 21. SUMMARY OF THE RELEVANT STANDARDS FOR THE AIA KEY REQUIREMENTS (IN BOLD, STANDARDS ALREADY PUBLISHED OR IN FINAL DRAFT STATUS) .....	53
TABLE 22. ISO MATURITY LEVEL CODES.....	68
TABLE 23. RELEVANT STANDARDS FOR THE REQUIREMENT: “DATA AND DATA GOVERNANCE” .....	95
TABLE 24. RELEVANT STANDARDS FOR THE REQUIREMENT: “RECORD-KEEPING” AND “TECHNICAL DATA” .....	95
TABLE 25. RELEVANT STANDARDS FOR THE REQUIREMENT: “TRANSPARENCY AND PROVISION OF INFORMATION TO USERS” .....	96
TABLE 26. RELEVANT STANDARDS FOR THE REQUIREMENT: “HUMAN OVERSIGHT” .....	96
TABLE 27. RELEVANT STANDARDS FOR THE REQUIREMENT: “ACCURACY, ROBUSTNESS, AND CYBERSECURITY” .....	96
TABLE 28. RELEVANT STANDARDS FOR QUALITY MANAGEMENT SYSTEM .....	97
TABLE 29. RELEVANT STANDARDS FOR RISK MANAGEMENT SYSTEM (INCLUDING TESTING FOR CONFORMITY ASSESSMENT) .....	98
TABLE 30. OVERVIEW OF STANDARDS AND INITIATIVES BY ETSI AND THEIR ALIGNMENT WITH THE EC REQUIREMENTS.....	99
TABLE 31. OVERVIEW OF STANDARDS AND INITIATIVES BY ISO/IEC JTC1 AND THEIR ALIGNMENT WITH THE EC REQUIREMENTS....	100
TABLE 32 OVERVIEW OF STANDARDS AND INITIATIVES BY ITU-T AND THEIR ALIGNMENT WITH THE EC REQUIREMENTS .....	101
TABLE 33. OVERVIEW OF STANDARDS AND INITIATIVES BY IEEE AND THEIR ALIGNMENT WITH THE EC REQUIREMENTS.....	101

## 12 List of Figures

FIGURE 1. EXAMPLE OF FIRST-LEVEL STANDARD AND ITS CONNECTED/REFERENCED SECOND-LEVEL ONES .....	12
FIGURE 2. OVERALL METHODOLOGY ADOPTED TO IDENTIFY MOST RELEVANT STANDARDS, RECOGNIZE GAPS, AND PROVIDE RECOMMENDATIONS.....	14
FIGURE 3. AI-RELATED GENERAL STANDARDS POPULATION, OBTAINED AS THE OUTCOME OF STEP 1 AND CATEGORIZED ACCORDING THE TWO DIMENSIONS HORIZONTAL/VERTICAL AND FOUNDATIONAL/IMPLEMENTATION.....	16
FIGURE 4: YEARLY DISTRIBUTION OF STANDARD PUBLICATION OR EXPECTED PUBLICATION. THE NUMBERS FOR YEARS 2021-2024 ARE PROVISIONAL, BASED ON THE SPECIFICATIONS' METADATA.....	21
FIGURE 5. METHODOLOGY TO ANALYSE THE OPERATIONALISATION AND THEN THE SUITABILITY INDEXES CHARACTERIZING THE AI STANDARDS RECOGNIZED IN THE HIGH-LEVEL MAPPING .....	24
FIGURE 6. SEMI-STRUCTURED MODEL APPLIED TO GENERATE THE EXECUTIVE VERSION OF THE AIA REQUIREMENTS .....	29
FIGURE 7. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "DATA AND DATA GOVERNANCE" (ETSI STANDARDS ARE REPRESENTED AS PINK BOXES, WHILE ISO/IEC STANDARDS HAVE A WHITE BACKGROUND) .....	39
FIGURE 8. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "TECHNICAL DOCUMENTATION" .....	40
FIGURE 9. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "RECORD KEEPING" .....	40
FIGURE 10. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "TRANSPARENCY AND INFORMATION TO USERS" .....	41
FIGURE 11. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "HUMAN OVERSIGHT" .....	41
FIGURE 12. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "ACCURACY, ROBUSTNESS AND CYBERSECURITY" (ETSI STANDARDS ARE REPRESENTED AS PINK BOXES, WHILE ISO/IEC STANDARDS HAVE A WHITE BACKGROUND) .....	42
FIGURE 13. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "RISK MANAGEMENT SYSTEM" .....	42
FIGURE 14. RADAR DIAGRAM OF THE OPERATIONALISATION LEVELS CHARACTERIZING THE ANALYSED STANDARDS, TO SUPPORT THE AIA REQUIREMENT "QUALITY MANAGEMENT SYSTEM" .....	43
FIGURE 15. THE SPIDER DIAGRAM OF STANDARD ISO/IEC 24668, SHOWING THE VALUES OF THE SUITABILITY INDEX FACTORS. ....	48
FIGURE 16. RADAR DIAGRAM OF THE SUITABILITY LEVELS CHARACTERIZING THE ANALYSED STANDARDS, FROM THE POINT OF VIEW OF REGULATORY FRAMEWORK IMPLEMENTATION STAKEHOLDERS (ETSI STANDARDS ARE REPRESENTED AS PINK BOXES, WHILE ISO/IEC STANDARDS HAVE A WHITE BACKGROUND) .....	50
FIGURE 17. RADAR DIAGRAM OF THE SUITABILITY LEVELS CHARACTERIZING THE ANALYSED STANDARDS, FROM THE POINT OF VIEW OF AI SYSTEM DEVELOPERS (ETSI STANDARDS ARE REPRESENTED AS PINK BOXES, WHILE ISO/IEC STANDARDS HAVE A WHITE BACKGROUND) .....	51
FIGURE 18. THE RELATIONSHIP BETWEEN THE GROUPS OF OPERATIONAL/SUITABILITY ESSENTIAL STANDARDS AND THE CORE ONES... ..	52
FIGURE 19. ISO LIFE CYCLE OF A SPECIFICATION (SOURCE: ISO WEBSITE, WWW.ISO.ORG) .....	68

## 13 Glossary

AI	Artificial Intelligence
AWI	Approved Work Item
CD	Committee Draft
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
DIN	Deutsches Institut für Normung (German Institute for Standardisation)
DIS	Draft International Standard (Enquiry draft)
EC	European Commission
ETSI	European Telecommunications Standards Institute
EU	European Union
FDIS	Final Draft International Standard
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
ML	Machine Learning
NSO	National Standards Organizations
OGC	Open Geospatial Consortium
PWI	Preliminary work item
QMS	Quality Management System
RMS	Risk Management System
SDOs	Standards Development Organizations
WD	Working draft

## **GETTING IN TOUCH WITH THE EU**

### **In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

### **On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## **FINDING INFORMATION ABOUT THE EU**

### **Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### **EU publications**

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).

The European Commission's  
science and knowledge service  
Joint Research Centre

**JRC Mission**

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**

[ec.europa.eu/jrc](http://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub



Publications Office  
of the European Union

doi:10.2760/376602

ISBN 978-92-76-40325-8