Contribution ID: 4321f98b-5ece-453d-8c6e-a7c3ffa6c3f5
Date: 05/04/2022 19:16:11

CAMSS
COMMON
ASSESSMENT
METHOD FOR
STANDARDS AND
SPECIFICATIONS

CAMSS Assessment EIF Scenario v5.0.0

Fields marked with * are mandatory.

CAMSS Assessment EIF Scenario v5.0.0

CAMSS
SOLUTION

ASSESSMENT
EIF Scenario

Release Date: 31/01/2022

Scenario Version: 5.0.0

INTRODUCTION

CAMSS

COMMON
ASSESSMENT
METHOD FOR
STANDARDS AND
SPECIFICATIONS

EIF Scenario

The European Interoperability Framework (EIF) provides guidance to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

This CAMSS Scenario allows to assess the compliance of **interoperability specifications** with the EIF. The objective of the obtained assessment is to determine the suitability of the assessed interoperability specification for the delivery of interoperable European public services.

Background

CAMSS is the European guide for assessing and selecting standards and specifications for an eGovernment project, a reference when building an architecture, and an enabler for justifying the choice of standards and specifications in terms of interoperability needs and requirements. It is fully aligned with the European Standardisation Regulation 1025/2012.
The main objective of CAMSS is achieving interoperability and avoiding vendor lock-in by establishing a neutral and unbiased method for the assessment of technical specifications and standards in the field of ICT. This method will be compliant with Regulation 1025/2012 on European Standardisation.
While ICT solutions have specific characteristics at the political, legal, and organisational levels; semantic and technical interoperability are based mostly on technical specifications or standards. Within the context of the elaboration of their National Interoperability Frameworks, Member States organise the assessment of technical specifications or standards, in order to establish their national recommendations. Deciding on the recommended technical specifications or standards often calls for a resource-intensive and time-consuming assessment. In order to tackle this, the Digital Europe Programme (DEP) defines an action focused on the development of a common assessment method for standards and specifications (CAMSS).

The purpose of CAMSS is:

- to ensure that assessments of technical ICT specifications or standards and interoperability profiles are performed according to high and consistent standards;

- to ensure that assessments will contribute significantly to the confidence in the interoperability of systems implementing these specifications and profiles;
- to enable the reuse, in whole or in part, of such assessments;
- to continuously improve the efficiency and effectiveness of the assessment process for ICT technical specifications, standards, and interoperability profiles.

The expected benefits of the CAMSS are:

- Ensuring greater transparency throughout the selection of standards in the context of ICT strategies, architectures, and interoperability frameworks. This will be achieved through the establishment of a commonly agreed assessment method, assessment process, and a list of assessment attributes.

- Reducing resource and time requirements and avoiding duplication of efforts. (Partial) sharing of finalised assessments of standards and specifications.

- Allowing easier and faster assessments, and reusing the ones already performed through the creation and maintenance of a library of standards.

Your compliance level of the specification assessed depends on the scores you achieved in each section of the survey. Please see below the survey score conversion table below for guidance.

			Compliance Level		
Section	**Ad-hoc**	**Opportunistic**	**Essential**	**Sustainable**	**Seamless**
Principles setting the context for EU Actions on Interoperability	20	40	50	80	90
EIF Core Interoperability Principles	0 to 440	441 to 880	881 to 1320	1321 to 1760	1761 to 2200
EIF Principles Related to generic user needs and expectations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500
EIF Foundation principles for cooperation among public	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500

administrations					
EIF Interoperability Layers	0 to 220	221 to 440	441 to 660	661 to 880	881 to 1100

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

Compliance Level	Description
Ad-hoc	Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area.
Opportunistic	Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area.
Essential	Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirement and recommendations from the European Interoperability Framework.
Sustainable	Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area.
Seamless	Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.

Contact: For any general or technical questions, please send an email to DIGIT-CAMSS@ec.europa.eu. Follow all activities related to the CAMSS on our CAMSS community page.

USER CONSENT

Disclaimer:
By no means will the Interoperability Specification assessment imply any endorsement of the EC to the assessed specification. Likewise, The use of CAMSS Tool implies that the user accepts that the EC is not liable on the assessment nor on any direct or indirect consequence/decision of such assesment.

CAMSS Tools are based on EU Survey, by accepting the CAMSS Privacy Statment the user also accepts EU Survey Privacy Statement and the Terms of use.

* Please, fill in the mandatory* information to start the assessment

- ☑ *I have read and agreed to the following CAMSS Privacy Statement: here
- ☑ I agree to be contacted for evaluation purposes, namely to share my feedback on specific DEP solutions and actions and on the DEP programme and the European Interoperability Framework in general.

This assessment tool is licensed under the European Union Public License (EUPL)

IDENTIFICATION

Information on the information provider

Your Last name

CAMSS Team

Your First Name

Your Position / Role

* Your Organisation

European Commission DG DIGIT

Your Contact phone number

* Would you like to be contacted for evaluation purposes in the context of your assessment? To see how your data is handled, please check again the Privacy statement here

In case you would like to be contacted, please select "yes" and provide your email.

- ● Yes
- ○ No

Contact Email

* Where did you learn about CAMSS?

- ○ DEP Programme (DEP website, DEP social media)
- ● Joinup (e.g., CAMSS Collection, Joinup social media)
- ○ European Commission
- ○ Public Administrations at national, regional or local level
- ○ Standards Developing Organizations (SDOs)
- ○ Other

If you answered "Other" in the previous question, please specify how:

Information on the specification

* Specificaton type

○ Specification
● Standard
○ Application Profile
○ Family of Specification

* Title of the specification

ISO/IEC 27001 Information Security Management

* Version of the specification

2.0

* Description of the specification

ISO/IEC 27001 is an international standard on how to manage information security. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS).

* URL from where the specification is distributed

https://www.iso.org/standard/54534.html

* Name and website of the standard developing/setting organisation (SDO/SSO) of the specification

○ W3C (https://www.w3.org)
○ OASIS (https://www.oasis-open.org/)
○ IEEE (https://standards.ieee.org/)
○ ETSI (https://www.etsi.org/)
○ GS1 (https://www.gs1.fr/)
○ openEHR (https://www.openehr.org/)
○ IETF (https://www.ietf.org/)
● Other (SDO/SSO)

* In case of Other SDO, please, provide its name:

ISO

* and, provide its URL:

https://www.iso.org/home.html

Contact information/contact person of the SDO
a) for the organisation
b) for the specification submitted

Information on the assessment of the specification

Reason for the submission, the need and intended use for the specification

If any other evaluation of this specification is known, e.g. by member states or European Commission projects, provide a link to this evaluation.

Considerations

Is the functional area of application for the formal specification addressing interoperability and eGovernment?

● YES
○ NO

Additional Info

EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

This category is related to the first underlying principle (UP) of the EIF Subsidiarity and Proportionality (UP1). The basis of this principle is to ensure that the EU Actions are taken or stated to improve national actions or decisions. Specifically, it aims to know if National Interoperability Frameworks are aligned with the EIF.

Please note that some of the questions have a prefilled answer depending on the SDO. To ensure it, please see that these questions include a help message that remarks it.

Subsidiarity and Proportionality

* **A1 - To what extent has the specification been included in a national catalogue from a Member State whose National Interoperability Framework has a high performance on interoperability according to National Interoperability Framework Observatory factsheets?**

EIF Recommendation 1: Ensure that national interoperability frameworks and interoperability strategies are aligned with the EIF and, if needed, tailor and extend them to address the national context and needs.

This criterion assesses if the specifications have been included within the National Catalogues of Specifications of the Member States that are highly aligned with the higher level of performance in terms of interoperability.

The Digital Public Administration Factsheets uses three categories to evaluate the level of National Interoperability frameworks in accordance with the EIF. The three categories are 1. CONCEPTUAL MODEL FOR INTEGRATED PUBLIC SERVICES PROVISION; 2 INTEROPERABILITY LAYERS, and 3. INTEROPERABILITY PRINCIPLES. National Interoperability Frameworks reports can be found here: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2020

○ Not Answered

○ Not Applicable

○ The specification has not been included within the catalogue of any Member State.

○ The specification has been included within the catalogue of a Member State with a lower performance than stated in the Digital Public Administration Factsheets from the NIFO.

○ The specification has been included within the catalogue of a Member State with a middel-lower performance than stated in the Digital Public Administration Factsheets from the NIFO.

○ The specification has been included within the catalogue of a Member State with a middle-upper performance than stated in the Digital Public Administration Factsheets from the NIFO.

● The specification has been included within the catalogue of a Member State with a higher performance than stated in the Digital Public Administration Factsheets from the NIFO.

* Justification

ISO/IEC 27001 is included in a national catalogue of recommended specifications, the Norway ICT Catalogue. The National Interoperability Framework (NIF) of this Member State is fully aligned with the European Interoperability Framework (EIF) according to the National Interoperability Framework Observatory (NIFO) factsheets, with a performance above the EU average.

Norway catalogue of standards:
https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder

NIFO factsheets:
https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets-2021

EIF CORE INTEROPERABILITY PRINCIPLES

In this category, elements related to the core interoperability principles (UP) are encompassed, which are: openness (UP 2), transparency (UP3), reusability (UP4), technological neutrality, and data portability (UP5).

Openness

*** A2 - Does the specification facilitate the publication of open data?**

EIF Recommendation 2: Publish the data you own as open data unless certain restrictions apply

Relates to the ability of the specification to publish data as open data or not.

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

According to the Tim Berners-Lee 5-star, ISO/IEC 27001 cannot be considered as a facilitator of open data as the standard does not make its content publicly available on the web; therefore, the standard does not facilitate the publication of open data.

Berners-Lee website:
https://5stardata.info/en/

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

*** A3 - To what extent do stakeholders have the opportunity to contribute to the development of the specification?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Relates to in which measure the different stakeholders that a specification can benefit have the opportunity to participate in the working groups focused on the development of certain specifications.

○ Not Answered
○ Not Applicable
○ There is no information on the working group of the specification.
● The working group is open to participation by any stakeholder but requires registration, fees, and membership approval.
○ The working group is open to participation by any stakeholder but requires fees and membership approval.
○ The working group is open to participation following a registration process.
○ The working group is open to all without specific fees, registration, or other conditions.

* Justification

ISO/IEC 27001 was developed by the ISO/IEC joint technical committee JTC 1. The access to JTC 1 working area is restricted, and individuals or companies are not eligible as members of ISO. ISO has defined a clear procedure to develop its standards. It consists in a 6-steps process where everyone who is interested can participate. However, if you want to participate, you have to contact your national standards body and you have to be approved for joining the Technical committee (TC) who will develop the standard. ISO has defined the roadmap of standards, it is composed of 6 steps as before said. For the approval of a standard the two-thirds majority of P-members of TC is needed. If the result is negative, the document is returned to TC/SC to be further studied.

The ISO standardization process:
https://www.iso.org/stages-and-resources-for-standards-development.html

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

ISO membership reference:
https://www.iso.org/get-involved.html

*** A4 - To what extent is a public review part of the release lifecycle?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

A public review consists of the public availability of the specification's draft for stakeholders to provide inputs for the improvement and fix of possible bugs.

- ○ Not Answered
- ○ Not Applicable
- ● Specification releases do not foresee public reviews.
- ○ Public review is applied to certain releases depending on the involved changes.
- ○ All major releases foresee a public review.
- ○ All major and minor releases foresee a public review but, during which, collected feedback is not publicly visible.
- ○ All major and minor releases foresee a public review during which collected feedback is publicly visible.

* Justification

Every five years, ISO standards go through a systematic review process during which the members assess and propose updatings.

ISO public review guide:
https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100413.pdf

*** A5 - Is the specification available with any restrictions related to Fair, Reasonable, and Non-Discriminatory ((F)RAND)?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

The FRAND basis relates to fair, reasonable, and non-discriminatory IPR disclosures.

- ○ Not Answered
- ○ Not Applicable
- ● NO

○ YES

* Justification

ISO 27001 has restricted IPR disclosures and requires payment to access it.

ISO 27001 foreword:
https://www.iso.org/obp/ui/#iso:std:54534:en

*** A6 - Is the specification licensed on a royalty-free basis?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Additionally to the EIF's recommendation that refers to open-source software it applies to a specification in itself at any interoperability level (legal, organisational, semantic, or technical)

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

ISO standards are not licensed on a royalty-free basis since they require an initial payment for accessing it and using it. Moreover, conformance testing requires payment in some cases.

ISO 27001 foreword:
https://www.iso.org/obp/ui/#iso:std:54534:en

*** A7 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?**

EIF Recommendation 4: Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Maturity related to the stability of the specification, meaning that it has been evolved enough and mechanisms for its development have been put in place (Change Management processes, monitoring, etc.)

○ Not Answered
○ Not Applicable
○ The specification has no published releases and no publicly accessible information on its development state.
○ The specification is under development without published releases.
○ The specification is under development with published preview releases.
● The specification has published major releases but without public documentation on its supporting processes (e.g. change management and release management).
○ The specification, in addition to having major releases available, has published documentation on its supporting processes (e.g. change management and release management).

* Justification

ISO/IEC 27001 was published back in 2005 and has undergone several changes, being last modified in 2015. Although Draft versions are publicly available, change management and release management processes are not open to the public.

ISO/IEC 27001 foreword:
https://www.iso.org/obp/ui/#iso:std:54534:en

ENISA-ISO/IEC 27001 reference:
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001?msclkid=81681be8affa11ecb89769e4176d852c

* **A8 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?**

EIF Recommendation 4: Give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support, and innovation.

Relates to how the specification is supported by the market, taking as a reference whether or not the specifications are widely used or implemented. There is an exception, and it is when the specification is being used to create innovative solutions.

○ Not Answered
○ Not Applicable - The specification does not have market acceptance because it is directly used to create innovative solutions.
○ There is no information about the specification's market uptake.
○ The specification has known implementations but not enough to indicate market acceptance.
○ The specification has widespread use indicating market acceptance.
○ The specification has widespread use and relevant independent reports proving its market acceptance.
● The specification has widespread use, indicating market acceptance.

* Justification

ISO/IEC 27001 can be considered a defacto standard for security and risk management in IT systems. The specification is a common method to ensure securing information and data in IT systems.

ISO/IEC 27001 foreword:
https://www.iso.org/obp/ui/#iso:std:54534:en

* **A9 - To what extent has the specification support from at least one community?**

EIF Recommendation 3: Ensure a level playing field for open-source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.

Related to whether or not communities are surrounding the specification at any level legal, organisational, semantic, or technical contributions to its enhancement and development.

○ Not Answered
○ Not Applicable
○ There is no community linked to the specification.

○ Specification support is available but as part of a closed community requiring registration and possibly fees.
○ There is no specific community to support the specification but there are public channels for the exchange of help and knowledge among its users.
○ There is a community providing public support linked to the specification but in a best-effort manner.
● There is a community tasked to provide public support linked to the specification and manage its maintenance.

* Justification

The ISO community, brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. All of ISO's technical work, including the technical committees, is managed by the Technical Management Board (TMB). Some of the TMB's tasks include setting up technical committees, appointing chairs and monitoring the progress of technical work.

ISO developing standards:
https://www.iso.org/who-develops-standards.html

Transparency

*** A10 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

○ Not Answered
○ Not Applicable
○ The specification hinders visibility.
○ The specification neither promotes nor hinders visibility.
○ The specification can contribute and promote the visibility of administrations, but it is not its main purpose.
○ The specification can enable the visibility of administrations if combined with other specifications.
● The specification actively promotes and supports visibility.

* Justification

By helping administrations to identify and manage possible risks, ISO/IEC 27001 ensures and fosters the continuous availability of administrations data and information. In the following link you can see an example of audits in public administration. Financial audits require the review of the IT part and with it the ISO/IEC 27001.

Application of ISO/IEC 27001 in public administration:
https://core.ac.uk/display/196275557

*** A11 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

○ Not Answered
○ Not Applicable

○ The specification hinders comprehensibility.

○ The specification neither promotes nor hinders comprehensibility.

○ The specification can contribute and promote the comprehensibility of administrations, but it is not its main purpose.

○ The specification can scope the comprehensibility of administrations if combined with other specifications.

● The specification actively promotes and supports comprehensibility.

* Justification

By helping administrations to identify and manage possible risks, ISO/IEC 27001 ensures and fosters the continuous availability of administration's data and information.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* **A12 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

Relates to ensuring availability of interfaces with internal information systems. As the EIF defines: *Public administrations operate a large number of what are often heterogeneous and disparate information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates the reuse of systems and data and enables these to be integrated into larger systems.*

○ Not Answered

● Not Applicable

○ The specification prevents the exposure of such interfaces.

○ The specification neither promotes nor hinders the exposure of such interfaces.

○ The specification can contribute to the exposure of interfaces, but it is not its main purpose.

○ The specification can enable the exposure of interfaces if combined with other specifications.

○ The specification enables exposure of such interfaces.

* Justification

The specification is focused on the preservation of confidential data and its availability. Therefore this criterion is not applicable to this specification.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* **A13 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?**

EIF Recommendation 5: Ensure internal visibility and provide external interfaces for European public services.

Securing the right to the protection of personal data, by respecting the applicable legal framework for the large volumes of personal data of citizens, held and managed by Public administrations.

○ Not Answered

○ Not Applicable

○ The specification hinders the protection of personal data.
○ The specification does not address the protection of personal data but neither prevents it.
○ The specification includes certain data protection considerations but without being exhaustive.
○ The specification explicitly addresses data protection but without referring to relevant regulations.
● The specification explicitly addresses data protection and its alignment to relevant regulations.

* Justification

ISO/IEC 27001 is a security standard that formally specifies an Information Security Management system (ISMS) designed to keep information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain and continually improve the ISMS. It also indicates a set of recommended practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, corrective and preventive measures. Certification to ISO/IEC 27001 helps organisations comply with numerous regulatory and legal provisions related to information security.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Reusability

*** A14 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?**

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Relates to the use of the specification beyond a specific business domain. E.g. a specification developed under the eHealth domain that can be used in other domains or not.

○ Not Answered
○ Not Applicable
○ The specification is tied to a specific domain and is restricted from being used in other domains.
○ The specification is associated with a specific domain but its use in other domains is difficult.
○ The specification is associated with a specific domain but could be partially used in other domains.
○ The specification is associated with a specific domain but could be used 'as-is' to other domains.
● The specification is domain-agnostic, designed to be used in any domain.

* Justification

The specification is focused on the preservation of confidential data and its availability. The business domain is security, even though it can be implemented in any sector (e.g. eHealth).

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

*** A15 - To what extent is the specification usable beyond the business-specific domain, allowing its implementation across business domains?**

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

Relates to the use of the specification beyond a specific business domain. E.g. a specification developed under the eHealth domain that can be used in other domains or not.

- ○ Not Answered
- ○ Not Applicable
- ○ The specification is tied to a specific domain and is restricted from being implemented in other domains.
- ○ The specification is associated with a specific domain but its implementation in other domains is difficult.
- ○ The specification is associated with a specific domain but could be partially implemented in other domains.
- ○ The specification is associated with a specific domain but could be implemented 'as-is' to other domains.
- ● The specification is domain-agnostic, designed to be implemented in any domain.

* Justification

The specification is focused on the preservation of confidential data and its availability. The business domain is security, even though it can be implemented in any sector (e.g. eHealth).

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Technological Neutrality and Data Portability

*** A16 - Is the specification technology agnostic?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs

Relates to the dependency of the specification to be implemented without relying on specific technologies or platforms.

- ○ Not Answered
- ○ Not Applicable
- ○ NO
- ● YES

* Justification

ISO/IEC 27001 does not depend on other standards such as ISO/IEC 27002. Moreover, it can be implemented without relying on specific technologies, as ISO/IEC 27001 comprises a set of requirements that ensure the compliance with ISMS.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

*** A17 - Is the specification platform agnostic?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs

Relates to the dependency of the specification to be implemented without relying on specific technologies or platforms.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

ISO/IEC 27001 is structured to be compatible with other management system standards, such as ISO 9001 and is technology and vendor neutral, meaning that it is completely independent of the IT platform.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

*** A18 - To what extent does the specification allow for partial implementations?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

Partial implementations refer to the application of specifications, not in their whole, but part of the requirements or features it defines in the text.

It can also be understood as the implementation of different profiles, which is also related to a certain set of requirements depending on the context of implementation.

○ Not Answered
○ Not Applicable
○ The specification is only meant to be used as a whole.
○ The specification could be partially implemented but does not make specific provisions towards this.
○ The specification could be partially implemented but includes only guidelines towards this rather than sets of requirements.
● The specification explicitly foresees sets of requirements that can be implemented incrementally.
○ The specification explicitly foresees sets of requirements that can be implemented incrementally or separately.

* Justification

ISO/IEC 27001 includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

*** A19 - Does the specification allow customisation?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of customizations is Core Vocabularies, which define a set of general requirements that could fit in any context and allow for the customization to fit specific business requirements in the implementation.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

The establishment and implementation of an organization’s information security management system is influenced by the organization’s needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. All of these influencing factors are expected to change over time. ISO/IEC 27001, therefore, is designed to be implemented in accordance of any given organization's needs, allowing its customisation.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

*** A20 - Does the specification allow extension?**

EIF Recommendation 8: Do not impose any technological solutions on citizens, businesses, and other administrations that are technology-specific or disproportionate to their real needs.

A clear example of customizations is Core Vocabularies, which define a set of general requirements that could fit in any context and allow for the customization to fit specific business requirements in the implementation.

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

ISO/IEC 27001 is presented as an exhaustive set of requirements to be applied in any given Information Security Management system (ISMS), therefore, it does not allow extension.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

*** A21 - To what extent does the specification enable data portability between systems/applications supporting the implementation of European public services?**

EIF Recommendation 9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support data portability.
○ The specification neither addresses data portability nor prevents it.
○ The specification addresses data portability but without specific provisions to enable it.
○ The specification introduces certain aspects that can contribute to enabling data portability.

● The specification explicitly addresses and enables data portability.

* Justification

By using ISO/IEC 27001, administrations can ensure that, when needed, data portability can be done ensuring the integrity of data and preserving the confidentiality of the information being exchanged.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

* **A22 - To what extent does the specification enable data portability between systems/applications supporting the evolution of European public services?**

EIF Recommendation 9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support data portability.
○ The specification neither addresses data portability nor prevents it.
○ The specification addresses data portability but without specific provisions to enable it.
○ The specification introduces certain aspects that can contribute to enabling data portability.
● The specification explicitly addresses and enables data portability.

* Justification

The main purpose of the ISO/IEC 27001 is to preserve the confidentiality, integrity and availability of information by applying a risk management process and to give confidence to interested parties that risks are adequately managed. Following the requirements set by ISO/IEC 27001 secures data portability between systems, and its scalable approach supports the evolution of european public services.

ISO 27001 reference:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

This category includes all underlying principles from the EIF which are related to user needs. Principles included here are user-centricity (UP6), inclusion and accessibility (UP7), security and privacy (UP8), and multilingualism (UP9).

User-Centricity

* **A23 - To what extent does the specification allow relevant information to be reused when needed?**

EIF Recommendation 13: As far as possible under the legislation in force, ask users of European public services once-only and relevant-only information.

The Once-Only Principle is related to making the operations or transactions between administrations and stakeholders more efficient. It implies avoiding the provision of certain data or information twice or more when this information is already available for public administrations.
Additional and relevant information can be found here: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle

- ○ Not Answered
- ○ Not Applicable
- ○ Information needs to be provided whenever this is needed.
- ○ There is limited reuse of provided information.
- ○ Provided information is reused, but this is not consistently done.
- ○ Provided information is reused, but not in all scenarios.
- ● Information is provided once-only and reused as needed.

* Justification

The specification can contribute to the implementation of the once-only principle by setting the principles to manage and reduce the risk related to the information being exchanged between parties. In this sense, by securing and establishing the methods to control and reduce risks when treating sensitive information the specification can contribute, enhance and enable the implementation of the once-only principle.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Inclusion and Accessibility

*** A24 - To what extent does the specification enable the e-accessibility?**

EIF Recommendation 14: Ensure that all European public services are accessible to all citizens, including persons with disabilities, the elderly, and other disadvantaged groups. For digital public services, public administrations should comply with e-accessibility specifications that are widely recognised at the European or international level.

Examples of specifications addressing e-accessibility are, for instance, WAI-ARIA (https://www.w3.org/WAI/standards-guidelines/aria/) included within Web Content Accessibility Guidelines (WCAG) Overview (https://www.w3.org/WAI/standards-guidelines/wcag/).

- ○ Not Answered
- ● Not Applicable
- ○ The specification prevents or does not support e-accessibility.
- ○ The specification neither addresses e-accessibility nor prevents it.
- ○ The specification can contribute and promote e-accessibility, but it is not its main purpose.
- ○ The specification can enable e-accessibility if combined with other specifications.
- ○ The specification explicitly addresses and enables e-accessibility.

* Justification

The specification is focused on ensuring risk management regarding the security of information, therefore, this criterion does not apply due to the scope of the specification.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Security and Privacy

* **A25 - To what extent does the specification enable the secure exchange of data?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support the secure and trustworthy exchange of data.
○ The specification introduces certain aspects that can contribute to enabling the secure exchange of data.
○ The specification addresses data security and trustworthy data exchange but does not foresee specific provisions to enable them.
○ The specification addresses data security and trustworthy data exchange but specific provisions to enable them are limited.
● The specification explicitly addresses and enables the secure and trustworthy exchange of data.

* Justification

ISO/IEC 27001 is an international information security standard that aims to ensure the confidentiality, integrity and availability of the information of an organization and of the systems and applications that treat it.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* **A26 - To what extent does the specification enable the secure processing of data?**

EIF Recommendation 15: Define common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

Relates to the actions that Public Administrations establish concerning sensitive information for the proper delivery of public services. The different actions imply the reception, classification, and exchange of such information.

○ Not Answered
○ Not Applicable
○ The specification prevents or does not support the secure and trustworthy processing of data.
○ The specification introduces certain aspects that can contribute to enabling the secure processing of data.
○ The specification addresses data security and trustworthy data processing but does not foresee specific provisions to enable them.

○ The specification addresses data security and trustworthy data processing but specific provisions to enable them are limited.

● The specification explicitly addresses and enables the secure and trustworthy processing of data.

* Justification

ISO/IEC 27001 is an international information security standard that aims to ensure the confidentiality, integrity and availability of the information of an organization and of the systems and applications that treat it.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Multilingualism

*** A27 - To what extent could the specification be used in a multilingual context?**

EIF Recommendation 16: Use information systems and technical architectures that cater to multilingualism when establishing a European public service. Decide on the level of multilingualism support based on the needs of the expected users.

○ Not Answered

● Not Applicable

○ The specification cannot be used in a multilingual context.

○ The specification could be used in a multilingual context but has no specific provisions to facilitate this.

○ The specification foresees limited support for multilingualism.

○ The specification foresees support for multilingualism but this is not complete.

○ The specification is designed to fully support multilingualism.

* Justification

The specification is focused on ensuring risk management regarding the security of information, therefore, this criterion does not apply due to the scope of the specification.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

This category includes the criteria aiming to evaluate principles related to collaboration amongst public organisations, business, and citizens. This is related to the underlying principles of administrative simplification (UP10), preservation of information (UP11), and assessment of effectiveness and efficiency (UP12).

Administrative Simplification

* **A28 - Does the specification simplify the delivery of European public services?**

EIF Recommendation 17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

Being an international standard that encompasses the internal security framework of all private and public administrations, ISO/IEC 27001 helps to create digitally by default services that reduce the administrative burden on both sides, public administrations and stakeholders.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* **A29 - Does the specification enable digital service delivery channels?**

EIF Recommendation 17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.

○ Not Answered
● Not Applicable
○ NO
○ YES

* Justification

The purpose of ISO/IEC 27001 is other than enabling digital service delivery channels, therefore, this criterion is not applicable to this specification.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Preservation of Information

* **A30 - To what extent does the specification enable the long-term preservation of data/information /knowledge (electronic records included)?**

EIF Recommendation 18: Formulate a long-term preservation policy for information related to European public services and especially for information that is exchanged across borders.

Relates to the capacity of the specification to contribute to the long-term preservation of information.

○ Not Answered
○ Not Applicable

○ The specification prevents or does not support long-term preservation.
○ The specification neither addresses the long-term preservation nor prevents it.
○ The specification addresses the long-term preservation of electronic resources (information, data, etc) in a limited manner.
○ The specification addresses long-term preservation of electronic resources (information, data, etc), but not in a complete manner.
● The specification explicitly addresses and enables long-term preservation.

* Justification

In order to maintain the confidentiality, integrity and availability of information, ISO/IEC 27001 defines the standards on which the long-term preservation of data must be carried out so that it is stored in a secure manner in accordance with information security management systems.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Assessment of Effectiveness and Efficiency

* **A31 - To what extent are there assessments of the specification's effectiveness?**

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the degree to which the specification is effective while using it. There are indirect methods to determine that the specification is effective, for instance then a solution that has an effective performance and uses the specification to deliver the expected service.

Effectiveness: *the extent to which the specifications reach the expected action according to its purpose.*

○ Not Answered
○ Not Applicable
○ There are no such assessments.
○ There are such assessments that indirectly address the specification.
○ There are such assessments evaluating digital solutions' effectiveness that involve the specification.
○ There are such assessments addressing the specification and its effectiveness together with other specifications.
● There are such assessments directly addressing the specification.

* Justification

There are already existing assessments assessing the efficiency and effectiveness of the ISO/IEC 27001. An example of such assessment can be viewed on the following link.

ISO/IEC 27001 assessment:
https://www.researchgate.net/publication
/286651142_Evaluating_the_Effectiveness_of_ISO_27001_2013_Based_on_Annex_A

* **A32 - To what extent are there assessments of the specification's efficiency?**

EIF Recommendation 19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality, and balance between costs and benefits.

Related to the good use of time and resources not wasted unnecessarily by a specification being used. There are indirect methods to determine that the specification is efficient, for instance, a solution delivering a service with an efficient performance that uses the specification.

Efficiency: times and means needed to achieve the results using the specification.

○ Not Answered
○ Not Applicable
○ There are no such assessments.
○ There are such assessments that indirectly address the specification.
○ There are assessments evaluating digital solutions' efficiency that involve the specification.
○ There are such assessments addressing the specification and its efficiency together with other specifications.
● There are such assessments directly addressing the specification.

* Justification

There are already existing assessments assessing the efficiency and effectiveness of the ISO27001. An example of such assessment can be viewed on the following link.

ISO/IEC 27001 assessment:
https://www.researchgate.net/publication/286651142_Evaluating_the_Effectiveness_of_ISO_27001_2013_Based_on_Annex_A

EIF INTEROPERABILITY LAYERS

This category is aligned with the related interoperability models described in the EIF and apply to all the public services. It includes six layers: interoperability governance, integrated public service governance, legal interoperability, organisational interoperability, semantic interoperability, and technical interoperability covered by criteria A2 to A10 under the Openness category.

Interoperability Governance

* **A33 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?**

EIF Recommendation 20: Ensure holistic governance of interoperability activities across administrative levels and sectors.

The EIRA defines the required capabilities for promoting interoperability as a set of Architecture Building Blocks (ABBs). The association of specification to these ABBs means the capacity to enable Legal, Organisational, Semantic, or Technical aspects needed for the development of interoperable public services. This association can be taken from ELIS the EIRA Library of Interoperability Specifications (ELIS) but also can be established ad-hoc.

○ Not Answered
○ Not Applicable

○ NO
● YES

* Justification

ISO/IEC 27001 can be found in the EIRA Library of Interoperable Specifications (ELIS), more specifically to the "Security Framework" ABB in the Organizational view.

ELIS referenece:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elis/release/v110

*** A34 - To what extent can the conformance of the specification's implementations be assessed?**

EIF Recommendation 21: Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability.

Relates to the implementation of the specification being conformant with the requirements established in the text of the specification. There are different methods to ensure the conformance of an implementation: check manually if the implementation meets the requirements in the specification text (if any), use additional methods or resources provided to this purpose or use specific tools provided by the SDO developing the specification.

○ Not Answered
○ Not Applicable
○ The specification does not include a definition of conformance.
○ The specification defines conformance but not as a set of measurable requirements.
○ The specification defines conformance as requirements that can be measured manually.
● The specification defines conformance as requirements with resources to enable automated measurement.
○ The specification is complemented by a conformance testing platform to allow testing of implementations.

* Justification

ISO/IEC 27001 in itself is a method to audit the information systems. However, the specification does not publicly provide conformance testing requirements, and both testing techniques and auditing services require payment to third parties. There are, nevertheless, companies such as Vanta, which provide a resource to enable automated measurement of the compliance with ISO 27001 standard.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Vanta website:
https://www.vanta.com/products/iso-27001?utm_source=bing&utm_medium=paid&utm_campaign=iso27001_rsu_Spain&utm_term=iso%2027001&utm_campaign=ISO+27001+(RSU)+Spain&utm_source=bing&utm_medium=ppc&utm_adgroup=ISO%2027001%20Head%20Term&hsa_acc=4880914058&hsa_cam=15789616753&hsa_grp=1332609418067234&hsa_ad=&hsa_src=o&hsa_tgt=kwd-83288948889188:loc-170&hsa_kw=iso%2027001&hsa_mt=p&hsa_net=adwords&hsa_ver=3&msclkid=fc00bbfdb553107674c4d9b99642b779

*** A35 - Is the specification recommended by an European Member State?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

Recommended specifications are these specifications that the Member States provide as examples for the implementation of certain digital public services or for being used when procuring these digital public services or solutions.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

> ISO/IEC 27001 is included in the Catalogue of standards of Norway.
>
> Norway catalogue of standards:
> https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

*** A36 - Is the specification selected for its use in an European Cross-border project/initiative?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

The European Commission set up a process for the identification and assessment of specifications for its use in the development of IT solutions and also when procuring them. Find here the commission implementing decisions that include the specifications identified by the European Commission: https://ec.europa.eu/growth/single-market/european-standards/ict-standardisation/ict-technical-specifications_en

Additionally, there could be other situations where a specification can be selected for European projects or initiatives out of the scope of the above-mentioned context. These specifications can be considered positively in this assessment.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

> The European Space Agency is implementing ISO/IEC 27001 to ensure its data is protected and properly managed to reduce ISMS risks.
>
> European Space Agency case study:
> https://publicsectorassurance.org/case-study/european-space-agency-uses-iso-27001-to-protect-its-data/

*** A37 - Is the specification included in an open repository/catalogue of standards at national level?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

ISO/IEC 27001 is included in the Catalogue of standards of Norway.

Norway catalogue of standards:
https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

*** A38 - Is the specification included in an open repository/catalogue of standards at European level?**

EIF Recommendation 23: Consult relevant catalogues of standards, specifications, and guidelines at the national and EU level, in accordance with your NIF and relevant DIFs, when procuring and developing ICT solutions.

EIF Recommendation 6: Reuse and share solutions, and cooperate in the development of joint solutions when implementing European public services.

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

After checking the different standard catalogues at supra-national level, there is no evidence of the inclusion of ISO/IEC 27001 within any European catalogue of standards.

ICT technical specifications:
https://ec.europa.eu/growth/industry/policy/ict-standardisation/ict-technical-specifications_en

CEN search tool catalogue:
https://standards.cen.eu/dyn/www/f?p=CENWEB:105::RESET::::

CENELEC search tool catalogue:
https://www.cenelec.eu/dyn/www/f?p=104:107:0::::FSP_LANG_ID:25

Legal Interoperability

*** A39 - Is the specification a European Standard?**

EIF Recommendation 27: Ensure that legislation is screened by means of ‘interoperability checks’, to identify any barriers to interoperability. When drafting legislation to establish a European public service, seek to make it consistent with relevant legislation, perform a ‘digital check’, and consider data protection requirements.

European Standards are those standards developed by certain organisations dedicated to this purpose. CEN, CENELEC, and ETSI are the principal organisations and all of them are developing their standards under the basis of meeting the requirements established within the European Standardisation Regulation. CEN-CENELEC homepage: https://www.cencenelec.eu/

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

After checking the different standard catalogues at supra-national level, there is no evidence of the inclusion of ISO/IEC 27001 within any European catalogue of standards.

ICT technical specifications:
https://ec.europa.eu/growth/industry/policy/ict-standardisation/ict-technical-specifications_en

CEN search tool catalogue:
https://standards.cen.eu/dyn/www/f?p=CENWEB:105::RESET::::

CENELEC search tool catalogue:
https://www.cenelec.eu/dyn/www/f?p=104:107:0::::FSP_LANG_ID:25

Organisational Interoperability

* A40 - Does the specification facilitate the modelling of business processes?

EIF Recommendation 28: Document your business processes using commonly accepted modelling techniques and agree on how these processes should be aligned to deliver a European public service.

○ Not Answered
○ Not Applicable
○ NO
● YES

* Justification

ISO/IEC 27001 defines security aspects for information in IT systems, it is a key element when designing business processes and the requirements that the system and the organisation will need to meet.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* A41 - To what extent does the specification facilitate organisational interoperability agreements?

EIF Recommendation 29: Clarify and formalise your organisational relationships for establishing and operating European public services.

Relates to specifications' capacities to help and ease the creation and formalisation of Interoperability agreements. E.g. Memorandums of Understanding (MoUs), Services Level Agreements (SLAs).

○ Not Answered
○ Not Applicable
○ The specification's definition hinders the drafting of such agreements.
○ The specification makes no provisions that would facilitate the drafting of such agreements.
○ The specification defines certain elements to facilitate such agreements.
○ The specification defines most elements to facilitate such agreements.
● The specification explicitly identifies all elements to be used in drafting such agreements.

* Justification

The specification can help to define the framework for working within the organisation regarding data and information security. It also can help to establish a common view and method between administrations providing public services to ensure the proper treatment of information and how it should be done.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

ENISA reference:
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-27001

Semantic Interoperability

* **A42 - Does the specification encourage the creation of communities along with the sharing of their data and results on national platforms?**

EIF Recommendation 32: Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.

Relates to specifications that are narrowly related to the data/information being exchanged, its format, and structure. It would allow a common method/mechanism to improve its reuse and exchange removing possible limitations. An example of it could be RDF, which is used to describe information and its metadata using specific syntax and serialisation.

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

No communities have been found created to share data and results of the implementation of ISO 27001 on national platforms.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

* **A43 - Does the specification encourage the creation of communities along with the sharing of their data and results on European platforms?**

EIF Recommendation 32: Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.

Relates to specifications that are narrowly related to the data/information being exchanged, its format, and structure. It would allow a common method/mechanism to improve its reuse and exchange removing possible limitations. An example of it could be RDF, which is used to describe information and its metadata using specific syntax and serialisation.

○ Not Answered
○ Not Applicable
● NO
○ YES

* Justification

No communities have been found created to share data and results of the implementation of ISO 27001 on European platforms.

ISO/IEC 27001 reference website:
https://www.iso.org/standard/54534.html

Useful links

CAMSS Joinup Page (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss)

CAMSS Library of Assessments (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-assessments-library)

CAMSS Assessment EIF Scenario - User Guide (https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/camss-assessment-eif-scenario-quick-user-guide)

Contact

DIGIT-CAMSS@ec.europa.eu

CAMSS Assessment EIF Scenario v5.0.0 - Results

CAMSS Assessment Result

Thank you for your contribution.

The score of the specification related to the scenario under which it is being evaluated depends on the scores achieved in each section of the survey. Please see the example below for guidance.

The following table shows the 'compliance levels' that a specification can reach depending on the assessment score.

EIF Scenario Compliance Level Conversion Table

			Compliance Level		
Section	**Ad-hoc**	**Opportunistic**	**Essential**	**Sustainable**	**Seamless**
Principles setting the context for EU Actions on Interoperability	20	40	50	80	90
EIF Core Interoperability Principles	0 to 440	441 to 880	881 to 1320	1321 to 1760	1761 to 2200
EIF Principles Related to generic user needs and expectations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500

EIF Foundation principles for cooperation among public administrations	0 to 100	101 to 200	201 to 300	301 to 400	401 to 500
EIF Interoperability Layers	0 to 220	221 to 440	441 to 660	661 to 880	881 to 1100

The table below expresses the range of the score per section. When used in combination with the table above, the total score can be interpreted. See the example below for guidance.

Section Compliance Conversion Table

Compliance Level	Description
Ad-hoc	Poor level of conformance with the EIF - The specification does not cover the requirements and recommendations set out by the EIF in this area.
Opportunistic	Fair level of conformance with the EIF - The specification barely covers the requirements and recommendations set out by the European Interoperability Framework in this area.
Essential	Essential level of conformance with the EIF - The specification covers the basic aspects set out in the requirement and recommendations from the European Interoperability Framework.
Sustainable	Good level of conformance with the EIF scenario - The specification covers all the requirements and recommendations set out by the European Interoperability Framework in this area.
Seamless	Leading practice of conformance level with the EIF - The specification fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.

Example – How to find the final Compliance Level

Using the score reached after the initial assessment, the interpretation can be made as follows.

1. In the summary table, observe the score for each section, e.g. EIF Core Interoperability Principles has 2200 points.

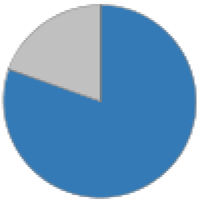
2. In the middle table – the Section Compliance Conversion Table – see that this number correlates to a column. In our example, the 2200 points of Core Interoperability Principles fall in the EIF Core Interoperability Principles row, and ‘1761 to 2200’ point range, placing it in the column 'Compliance **Seamless**'.

3. Next, in the top table – the EIF Scenario Compliance Level Conversion Table – we see Compliance Level "**Seamless**", and from its description that the specification for the EIF Core Interoperability Principles 'fully covers the requirements and recommendations set out by the European Interoperability Framework in this area.'.

For additional calculation of the assessment strength, please follow the instruction provided in the User Guide, found here.

Summary

Your Score	3460
Maximum Score	4300



Section	Score for this Section	
EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY	100 /100	
EIF CORE INTEROPERABILITY PRINCIPLES	1600 /2100	
EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS	500 /500	
EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS	500 /500	
EIF INTEROPERABILITY LAYERS	760 /1100	

Scores by Question

EIF PRINCIPLES SETTING THE CONTEXT FOR EU ACTIONS ON INTEROPERABILITY

Score for this Section: 100/100

A1 - To what extent has the specification been included in a national catalogue from a Member State whose National Interoperability Framework has a high performance on interoperability according to National Interoperability Framework Observatory factsheets?

Your answer ✓ The specification has been included within the catalogue of a Member State with a higher performance than stated in the Digital Public Administration Factsheets from the NIFO.

100 out of 100 points

EIF CORE INTEROPERABILITY PRINCIPLES

Score for this Section: 1600/2100

A2 - Does the specification facilitate the publication of open data?

Your answer ✗ NO

20 out of 100 points

A3 - To what extent do stakeholders have the opportunity to contribute to the development of the specification?

Your answer ✓ The working group is open to participation by any stakeholder but requires registration, fees, and membership approval.

40 out of 100 points

A4 - To what extent is a public review part of the release lifecycle?

Your answer ✗ Specification releases do not foresee public reviews.

20 out of 100 points

A5 - Is the specification available with any restrictions related to Fair, Reasonable, and Non-Discriminatory ((F)RAND)?

Your answer ✗ NO

20 out of 100 points

A6 - Is the specification licensed on a royalty-free basis?

Your answer ✖ NO

20 out of 100 points

A7 - To what extent is the specification sufficiently mature for its use in the development of digital solutions/services?

Your answer ✓ The specification has published major releases but without public documentation on its supporting processes (e.g. change management and release management).

80 out of 100 points

A8 - To what extent has the specification sufficient market acceptance for its use in the development of digital solutions/services?

Your answer ✓ The specification has widespread use, indicating market acceptance.

100 out of 100 points

A9 - To what extent has the specification support from at least one community?

Your answer ✓ There is a community tasked to provide public support linked to the specification and manage its maintenance.

100 out of 100 points

A10 - To what extent does the specification enable the visibility of administrative procedures, rules data, and services?

Your answer ✓ The specification actively promotes and supports visibility.

100 out of 100 points

A11 - To what extent does the specification scope comprehensibly administrative procedures, rules data, and services?

Your answer ✓ The specification actively promotes and supports comprehensibility.

100 out of 100 points

A12 - To what extent does the specification enable the exposure of interfaces to access the public administration's services?

Your answer ✓ Not Applicable

100 out of 100 points

A13 - To what extent does the specification ensure the protection of personal data managed by Public Administrations?

Your answer ✓ The specification explicitly addresses data protection and its alignment to relevant regulations.

100 out of 100 points

A14 - To what extent is the specification usable beyond the business-specific domain, allowing its usage across business domains?

Your answer ✓ The specification is domain-agnostic, designed to be used in any domain.

100 out of 100 points

A15 - To what extent is the specification usable beyond the business-specific domain, allowing its implementation across business domains?

Your answer ✓ The specification is domain-agnostic, designed to be implemented in any domain.

100 out of 100 points

A16 - Is the specification technology agnostic?

Your answer ✓ YES

100 out of 100 points

A17 - Is the specification platform agnostic?

Your answer ✓ YES

100 out of 100 points

A18 - To what extent does the specification allow for partial implementations?

Your answer ✓ The specification explicitly foresees sets of requirements that can be implemented incrementally.

80 out of 100 points

A19 - Does the specification allow customisation?

Your answer ✓ YES

100 out of 100 points

A20 - Does the specification allow extension?

Your answer ✗ NO

20 out of 100 points

A21 - To what extent does the specification enable data portability between systems/applications supporting the implementation of European public services?

Your answer ✓ The specification explicitly addresses and enables data portability.

100 out of 100 points

A22 - To what extent does the specification enable data portability between systems/applications supporting the evolution of European public services?

Your answer ✓ The specification explicitly addresses and enables data portability.

100 out of 100 points

EIF PRINCIPLES RELATED TO GENERIC USER NEEDS AND EXPECTATIONS

Score for this Section: 500/500

A23 - To what extent does the specification allow relevant information to be reused when needed?

Your answer ✓ Information is provided once-only and reused as needed.

100 out of 100 points

A24 - To what extent does the specification enable the e-accessibility?

Your answer ✓ Not Applicable

100 out of 100 points

A25 - To what extent does the specification enable the secure exchange of data?

Your answer	✓ The specification explicitly addresses and enables the secure and trustworthy exchange of data.	100 out of 100 points

A26 - To what extent does the specification enable the secure processing of data?

Your answer	✓ The specification explicitly addresses and enables the secure and trustworthy processing of data.	100 out of 100 points

A27 - To what extent could the specification be used in a multilingual context?

Your answer	✓ Not Applicable	100 out of 100 points

EIF FOUNDATION PRINCIPLES FOR COOPERATION AMONG PUBLIC ADMINISTRATIONS

Score for this Section: 500/500

A28 - Does the specification simplify the delivery of European public services?

Your answer	✓ YES	100 out of 100 points

A29 - Does the specification enable digital service delivery channels?

Your answer	✓ Not Applicable	100 out of 100 points

A30 - To what extent does the specification enable the long-term preservation of data/information /knowledge (electronic records included)?

Your answer	✓ The specification explicitly addresses and enables long-term preservation.	100 out of 100 points

A31 - To what extent are there assessments of the specification's effectiveness?

Your answer ✓ There are such assessments directly addressing the specification.

100 out of 100 points

A32 - To what extent are there assessments of the specification's efficiency?

Your answer ✓ There are such assessments directly addressing the specification.

100 out of 100 points

EIF INTEROPERABILITY LAYERS

Score for this Section: 760/1100

A33 - Is the (or could it be) specification mapped to the European Interoperability Architecture (EIRA)?

Your answer ✓ YES

100 out of 100 points

A34 - To what extent can the conformance of the specification's implementations be assessed?

Your answer ✓ The specification defines conformance as requirements with resources to enable automated measurement.

80 out of 100 points

A35 - Is the specification recommended by an European Member State?

Your answer ✓ YES

100 out of 100 points

A36 - Is the specification selected for its use in an European Cross-border project/initiative?

Your answer ✓ YES

100 out of 100 points

A37 - Is the specification included in an open repository/catalogue of standards at national level?

Your answer ✓ YES

100 out of 100 points

A38 - Is the specification included in an open repository/catalogue of standards at European level?

Your answer	✖ NO	20 out of 100 points

A39 - Is the specification a European Standard?

Your answer	✖ NO	20 out of 100 points

A40 - Does the specification facilitate the modelling of business processes?

Your answer	✓ YES	100 out of 100 points

A41 - To what extent does the specification facilitate organisational interoperability agreements?

Your answer	✓ The specification explicitly identifies all elements to be used in drafting such agreements.	100 out of 100 points

A42 - Does the specification encourage the creation of communities along with the sharing of their data and results on national platforms?

Your answer	✖ NO	20 out of 100 points

A43 - Does the specification encourage the creation of communities along with the sharing of their data and results on European platforms?

Your answer	✖ NO	20 out of 100 points

Contact	DIGIT-CAMSS@ec.europa.eu
Useful links	CAMSS Joinup Page CAMSS Library of Assessments CAMSS Assessment EIF Scenario - User Guide

Contribution ID	4321f98b-5ece-453d-8c6e-a7c3ffa6c3f5
Completed at	05/04/2022 19:16:11
Completion time	-