European Commission

CAMSS

COMMON ASSESSMENT METHOD FOR STANDARDS AND SPECIFICATIONS

ASSESSMENT SUMMARY v1.0.0

ISO/IEC 27001 Information Security Management (ISO/IEC 27001) [1]

International Organization for Standardization (ISO)[2]

[1] ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements

[2] ISO - International Organization for Standardization

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. Introduction

The present document is a summary of the assessment of **ISO/IEC 27001 Information Security Management (ISO/IEC 27001)** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is assessing the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. Assessment Summary

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). The aim of ISO 27001 is to help organizations make the information assets they hold more secure. Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit.

ISO 27001 requires organizations to systematically examine their IT security risks, and to design and implement a coherent and comprehensive suite of information security controls and other forms of risk treatment to address those risks that are deemed unacceptable. The adoption of an overarching management process is needed to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The specification has been developed by the joint technical committee of ISO (International Standards Organization) and IEC (International Electrotechnical Commission), whose main purpose is to develop international standards that have to be approved by the national body's members.

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

The specification partially supports the principles setting context for EU actions on interoperability:

- **Subsidiarity and proportionality**
  ISO 27001 is included in at least two catalogues of recommended specifications, the Norway ICT catalogue and the Spanish ICT catalogue. These two countries are fully aligned with the European Interoperability Framework (EIF).

The specification fully supports the principles setting context for EU actions on interoperability:

- **Openness**

[3] https://ec.europa.eu/eusurvey/runner/EIFScenario_v500

[4] https://ec.europa.eu/isa2/eif_en

The ISO/IEC joint technical committee (JTC1) is the working group in charge of the maintenance of ISO 27001 Information Security Management. The access to JTC1, nonetheless is restricted to individuals and companies. To participate, a working group has to contact its national standards body and be approved to join the technical committee.

It is worth to note that the review process is restricted to members and that the standards they develop have restricted Intellectual Property rights disclosures and require payment to access their resources. Nonetheless, ISO/IEC 27001 is a widely supported standard for security and risk management in IT systems, having undergone major releases since its creation in 2003.

- **Transparency**

  As ISO/IEC 27001 explicitly address data protection and its alignment to relevant regulations, transparency goals are met by helping administrations to identify and manage possible IT risks, thus ensuring the continuous availability of administration's data and information, while rendering it secure.

- **Reusability**

  ISO/IEC 27001 Information Security Management is designed for organizations to meet all the requirements for the deploying of a healthy and strong information security management system regardless of their business domain.

- **Technological neutrality and data portability**

  It can be affirmed that ISO/IEC 27001 is technology-neutral as it is not dependant on other standards, and can be implemented without relying on specific technologies. It is also structured to be compatible with other management system standards, and is technology and vendor-neutral, meaning that it also can be considered platform-agnostic. It is worth to note that it is designed to fit the needs of any given business purpose or scale, therefore allowing for customisations and partial implementations.

  Regarding data portability, ISO/IEC 27001 is a useful auditing tool for administrations to ensure that, when needed, confidentiality of information and data being exchanged is well preserved.

***The specification does not support the principles related to generic user needs and expectations*:**

- **User-centricity**

  By securing and establishing the methods to control and reduce risks when treating sensitive information, ISO/IEC 27001 can contribute, enhance and enable the implementation of the once-only principle.

- **Inclusion and accessibility**

  The purpose of ISO/IEC 27001 is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

- **Security and privacy**

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

- **Multilingualism**
  The purpose of ISO/IEC27001 is not related to the delivery of multilingual European Public Services. Therefore, this criterion is considered not applicable to this specification.

The specification fully supports the foundation principles for cooperation among public administrations:

- **Administrative Simplification**
  ISO/IEC 27001 is an auditing tool standard that helps simplify the delivery of European public services by facilitating the creation of digitally-by-default services that reduce the administrative burden on both sides, public administrations and stakeholders.

- **Preservation of information**
  The standards that are defined by ISO/IEC 27001 explicitly tackle the long-term preservation of information and data issues providing a set of requirements necessary to store it in a secure manner, in accordance with information security management systems.

- **Assessment of effectiveness and efficiency**
  Several existing studies can be found on the web assessing the effectiveness and efficiency of ISO/IEC 27001 set of standards against information security management systems.

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes:

- Four layers of interoperability: legal, organisational, semantic and technical;
- A cross-cutting component of the four layers, ‘integrated public service governance’;
- A background layer, ‘interoperability governance’.

The Specification supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**
  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. It also can be found in the national catalogue of Norway. In terms of implementation conformity, third party resources have been found to enable automated measurement, however, the specification does not publicly provide conformance testing requirements. It is worth to note that ISO/IEC 27001 is recommended in the National IT catalogue of Norway, and it is also being implemented in a cross-border initiative by the European Space Agency.

- **Legal Interoperability**
  After checking the different standard catalogues at supra-national level, there is no mention of ISO/IEC 27001 in any official document stating its conformance in regard to Regulation 1025/2012.

- **Organisational interoperability**
  ISO/IEC 27001 provides an organizational framework from which security aspects for IT systems can be defined. ISO/IEC 27001 is a key element when it comes to designing business process and the requirements that information security management systems will have to comply with. It also helps to establish a common view and method for administrations providing public services to ensure the proper treatment of information.

- **Semantic Interoperability**
  No communities have been found created to share data and their results of the implementations of ISO 27001 neither on European nor national platforms.

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for **ISO/IEC 27001**. The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones are used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
Principle setting the context for EU actions on interoperability	100/100	100%	Seamless
Core interoperability principles	1600/2100	95,2%	Sustainable
Principles related to generic user needs and expectations	500/500	60%	Seamless
Foundation principles for cooperation among public administrations	500/500	80%	Seamless
Interoperability layers*	760/1100	100%	Sustainable
Overall Score	3460/4300	90,91%	

**The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle ''Openness''.*

With a 91% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 80,47% (3460/4300) demonstrates that the specification fully supports the European Interoperability Framework in the domains where it applies.