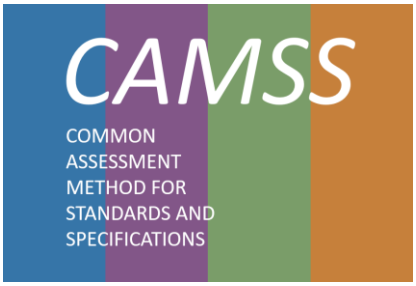

ASSESSMENT SUMMARY v1.0.0

International Standard on Assurance Engagements 3402 (ISAE 3402)[1]

Internationa Auditing and Assurance Standards Board (IAASB)[2]

[1] ISAE3402.com - A site dedicated to the ISAE 3402 Assurance Standard

[2] IAASB | IFAC

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 the International Standards on Assurance Engagement 3402 (ISAE 3402) 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

The International Standards on Assurance Engagement 3402 (ISAE 3402) , titled Assurance Reports on Controls at a Service Organization, is an international assurance standard that describes Service Organization Control (SOC) engagements, which provides assurance to an organization's customer that the service organization has adequate internal controls.

The scope of an ISAE 3402 engagement is control set of the service organization, or to be more precise the service organizations control over services, functions performed and applications that are likely to be relevant for the customer and its auditor to evaluate the internal control over financial reporting. When performing an ISAE 3402 the auditor has to take the position of the customer, selecting and testing controls that are relevant for the customer.

ISAE 3402 was developed by the International Auditing and Assurance Standards Board (IAASB) and published by the International Federation of Accountants (IFAC) in 2009. It supersedes SAS 70. and puts more emphasis on procedures for the ongoing monitoring and evaluation of controls.

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 does not support the principles setting context for EU actions on interoperability*:**

- **Subsidiarity and proportionality**
  There is no Member State that includes ISAE 3402 in their national catalogue with The National Interoperability Framework (NIF) in alignment with the three categories 1. Conceptual model for integrated public services provision, 2. interoperability layers, and 3. interoperability principles.

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

- **Openness**
  ISAE 3402 was developed to provide an international standard on assurance in the context of information security and confidentiality. The development process has been carried out by IAASB, an organization which operates as transparently as possible. Their meetings are open to the

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

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

public, and all relevant information regarding changes and requests by stakeholders is posted on their website. Moreover, IAASB is the working group that maintains the specification.

It is interesting to remark that ISAE 3402 has support from interest groups that are involved in the development of cross-border initiatives. Its change history and change management indicates that ISAE 3402 is mature for the development of digital services and also has widespread market acceptance. It is licensed under a royalty-free basis and its implementation can be certified by any public auditor.

- **Transparency**
  Transparency and comprehensibility of data and services is indirectly addressed as administrations can benefit from implementing ISAE 3402 quality controls over those processes that require payments, as it allows to clearly identify how their procedures are carried out, always taking into account the integrity of data and the confidentiality of the information being exchanged, thus ensuring the protection of personal data, which is the main purpose of ISAE 3402.

- **Reusability**
  ISAE 3402 is publicly available for its use for free at IAASB website. Additionally, ISAE 3402 financial reports compliance are designed to be used and implemented in any business domain.

- **Technological neutrality and data portability**
  In general terms, ISAE 3402 is not technology-agnostic, as it depends on other standards such as NIA 402 and ISAE 3000 to be implemented. Being part of the International Federation of Accountants (IFAC) standards providing companies in the financial sector an independent assessment tool on user entities' control over financial reporting, ISAE 3402 cannot be customised nor extended as it is only meant to be used as a whole.

***The specification supports the principles related to generic user needs and expectations*:**

- **User-centricity**
  ISAE 3402 helps to ensure that the public services requiring information from both parties (Public administrations and the service consumers) are properly managed and monitored allowing the information to be secured and exchanged between public administrations fostering the once-only principle.

- **Inclusion and accessibility**
  The purpose of ISAE 3402 is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

- **Security and privacy**
  ISAE 3402 supports trustworthy data exchange by providing a guarantee in the context of the security and confidentiality of information for users and companies. When a public administration contracts a service from a private company, it can request to assess the compliance against ISAE

3402 to ensure that their data is being managed according to adequate confidentiality and security policies and laws.

- **Multilingualism**
  The purpose of ISAE 3402 is not related to the delivery of multilingual European Public Services. Therefore, this criterion is considered not applicable to this specification.

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

- **Administrative Simplification**
  Being an international standard that encompasses the international security framework of all private and public administrations, ISAE 3402 can help create digitally-by-default services that reduce the administrative burden on both sides, public administrations, and stakeholders alike.

- **Preservation of information**
  The purpose of ISAE 3402 is not directly the long-term preservation, nonetheless, its implementation helps to control and trace the movement of the data and information as well as preserves it in order to maintain the confidentiality, integrity and availability.

- **Assessment of effectiveness and efficiency**
  There can be found different existing studies and reports pointing out the benefits of the implementation of ISAE 3402 in terms of efficiency and effectiveness.

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

- **Interoperability governance**
  ISAE 3402 is already associated with EIRA ABBs in the EIRA Library of Interoperability Specifications (ELIS). More specifically, ISAE 3402 can define the interoperability aspects of the Privacy Framework ABB of the EIRA Organisational View[5]. Despite having been included in MS's catalogues, it is not included in any catalogue at European Level. In terms of implementation conformity, ISAE 3402 is a method to audit the System and Organization Controls (SOC), and it can be used to assess and audit the performance of organizations against the requirements it

[5] https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/camss-list-standards

establishes. It is worth to note that it has been selected as the basis for the Cloud Computing Compliance Controls Catalogue (C5[6]), a cross-border project that aims to outline the prerequisites for a conformity assessment using international standards, adding cloud-specific requirements, especially for transparency.

- **Legal Interoperability**
  Although ISAE 3402 is not developed by any European organization that follow the European Standardisation Regulation, it is being recommended by the European Agency for Cybersecurity (ENISA[7]) according to the report for Security certification practice in the EU.

- **Organisational interoperability**
  Although there has not been found any information regarding the inclusion of ISAE 3402 within an agreement between organizations or countries involved in the provision of public services, ISAE 3402 audits can be helpful as it recommends best practices regarding data confidentiality and security, thus making it a standard that facilitates the modelling of business processes.

- **Semantic Interoperability**
  No communities have been found created to share data and their results of the implementations of ISAE 3402 neither on European nor national platforms.

[6] Cloud Computing Compliance Controls Catalogue (C5) (bund.de)

[7] ENISA (europa.eu)

3. ASSESSMENT RESULTS

This section presents an overview of the results of the CAMSS assessments for **ISAE 3402**. 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	20/100	100%	Ad-Hoc
Core interoperability principles	1620/2100	80,95%	Sustainable
Principles related to generic user needs and expectations	460/500	60%	Seamless
Foundation principles for cooperation among public administrations	460/500	80%	Seamless
Interoperability layers*	660/1100	90,91%	Essential
Overall Score	3220/4300	81,82%	

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

With an 81,82% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 74,88% (3220/4300) demonstrates that the specification does not support the European Interoperability Framework in the domains where it applies.