Guidelines on a sectoral cybersecurity assessment

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 18037:2025 sisaldab Euroopa standardi EN 18037:2025 ingliskeelset teksti.	This Estonian standard EVS-EN 18037:2025 consists of the English text of the European standard EN 18037:2025.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 26.03.2025.	Date of Availability of the European standard is 26.03.2025.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROPEAN STANDARD **EN 18037**

NORME EUROPÉENNE

EUROPÄISCHE NORM March 2025

ICS 35.030

English version

Guidelines on a sectoral cybersecurity assessment

Lignes directrices pour l'appréciation sectorielle de la cybersécurité

Leitlinien für ein sektorales Cybersecurity Assessment

This European Standard was approved by CEN on 15 December 2024.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Ref. No. EN 18037:2025 E

Contents

Page

European foreword

This document (EN 18037:2025) has been prepared by Technical Committee CEN/CLC/JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2025, and conflicting national standards shall be withdrawn at the latest by September 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

This document specifies cybersecurity assessments at the level of a market sector or an application area. It is designed to be used as a preparatory step for the drafting of cybersecurity certification schemes for ICT products, and ICT processes and ICT systems used by a market sector for providing sectoral services to the end users or business customer thus creating sectoral ICT systems.

Sectoral ICT systems can be found in application areas such as mobile networks, digital identity, e-health, public transportation, or payment.

Sectoral ICT systems can involve very large numbers of stakeholder organizations from the same market sector which cooperate in specified roles for provisioning the sectoral services. In certain roles, like Mobile Network Operators or Public Transport Service Providers, the stakeholder organizations are potentially competing.

The stakeholder organizations participating in a sectoral ICT system act according to rules which are typically specified by a "coordinating entity" or a regulator and operate the ICT systems or products under their control as functional components of the sectoral ICT system.

Cybersecurity and assurance are not only relevant from the perspective of the customers of sectoral services. In the sectoral ICT system, a clear and consistent definition of cybersecurity and assurance requirements in relation to the stakeholder role is important to establish trust among the sectoral stakeholder organizations. Since ICT security deficiencies caused by one stakeholder can lead to risks for other stakeholder's business objectives.

As with any ICT system that is intended to meet elevated cybersecurity and assurance requirements, the sectoral stakeholder organizations need to find an appropriate balance between the need for cybersecurity and assurance and the cost of its implementation. When it comes to the definition of cybersecurity and certification requirements to the sectoral ICT system, it is intended to be supported by the identification of the risks for the stakeholder's business objectives and the attack potential of the relevant attacker types associated with the intended use.

A sectoral ICT system supports numerous sectoral business processes and stakeholder business objectives which can be subject to cybersecurity risks. It can also involve a wide range of stakeholder-operated ICT systems, products and processes which usually need different evaluation and certification approaches for the validation of the implementation of security and assurance requirements. For trusted sectoral services, trust between sectoral stakeholders is essential. This applies also for re-using certificates. Certified components require a definition of assurance and security that provides consistency. For this the specification of requirements and the definition of risk levels for evaluation and certification is the basis.

The sectoral cybersecurity assessment methodology supports the aspects and requirements by the following features:

— The sectoral cybersecurity assessment will provide information about the business processes to be supported by the sectoral ICT system, the related business objectives of the sectoral stakeholders. It also identifies the primary and supporting assets which are critical for the secure implementation of the business processes (see 5. 2 and 6.3.3).

— The stakeholder-operated ICT systems, products or processes which are relevant for the security of the primary assets are identified. A 'deep dive' into the sectoral ICT system's architecture provides detailed information about their intended use (see 6.1).

— Cyberthreat intelligence (CTI) information is used to collect information on potentially relevant attacker types, their motivation, and capabilities. CTI allows to prioritize those risk scenarios, which are most relevant to be considered for further analysis. This allows the most effective use of resources during the analysis and contributes to the information needed to assign cybersecurity

and assurance requirements to ICT systems, ICT products or ICT services, based on the risk of intended use (see 6.3.8 and Annex B).

— Cybersecurity risks are identified and assessed based on consequences of cybersecurity incidents on the sectoral stakeholder's business objectives and likelihood that such incident will occur (see 6.3.6 and 6.3.7, respectively). The estimation of likelihood is derived from the potential motivation of those attacker types who are capable to conduct attacks on the identified assets.

— The methodology offers a concept of internal risk, security, assurance, and attack potential reference levels (see Clause 7). If commonly used, they will support consistency in the definition of risk, cybersecurity, and assurance. The methodology provides the option to integrate sectoral, product, process and potentially also ISMS-based cybersecurity certification schemes and it can support and integrate ICT product certification schemes, beyond Common Criteria or other ISO/IEC 15408 series based schemes.

— The risk information obtained by an ISO/IEC 27005-conformant approach at sectoral level can be transferred to ISO/IEC 15408 series based environments. By applying two different standards the risk-based definition of cybersecurity and assurance requirements can be supported (see 5.2 and Clause 8).

Based on these properties and functions, the sectoral stakeholders benefit in the following ways:

— The methodology supports the identification of risk associated with the intended use of ICT systems, ICT services and ICT processes at any level of the sectoral ICT system architecture. The sectoral stakeholder organizations can balance their view of risks against the investment needed to mitigate these risks by introducing appropriate levels of security and assurance. It can be expected that this transparent, cooperative approach will contribute significantly to the market acceptance for these requirements and the cybersecurity certification schemes developed on this basis.

— Consistency in the implementation of assurance levels can be achieved across schemes. This will allow the re-use of certificates issued by one scheme in other schemes, thus providing an important benefit both to the business interests of product and infrastructure service providers and to their customers. At the same time, the methodology's approach to consistency is also flexible enough to support the integration of new types of cybersecurity certification schemes, which can emerge because of specific requirements from different markets.

— Introducing a common concept for security levels facilitates the definition of controls which can be commonly used across cybersecurity certification schemes.

In summary, the proposed methodology does not only support the workflow of drafting market-oriented cybersecurity certification schemes but offers also a potential for a broader use by sectors and providers of infrastructure.

However legal and regulatory aspects should be considered when applying the sectoral cybersecurity assessment methodology. These include:

— if used as a preparatory step for cybersecurity certification scheme drafting, the methodology should consider the existing EU and national frameworks on the targeted market sector and on cybersecurity certification;

— compliance with applicable legal obligations such as the Cyber Resilience Act.

The specification of evaluation or certification, assurance levels and security measures as means for risk mitigation may have to follow national or sectoral provisions.

1 Scope

This document specifies an approach that supports the risk-based identification of cybersecurity, certification and assurance requirements to ICT products, processes and services for complex multi-stakeholder sectoral systems.

The sectoral cybersecurity assessment process includes all steps necessary to specify, implement and maintain such requirements.

Process performance or quality measurement are out of the scope of this document.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp/

— IEC Electropedia: available at https://www.electropedia.org/

3.1 General terms

3.1.1
information security
preservation of confidentiality, integrity and availability of information

[SOURCE: EN ISO/IEC 27000:2018, 3.28]

3.1.2
cybersecurity
activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber *threat* (3.4.5)

Note 1 to entry: ISO/IEC TS 27100:2020, 3.2 refers to 'cybersecurity' as safeguarding of people, society, organizations and nations from cyber *risks* (3.4.1)

Note 2 to entry: Safeguarding means to keep cyber *risks* (3.4.1) at a tolerable level.

[SOURCE: [8], art. 2(1)]

3.1.3
assurance level
basis for confidence that an *ICT product* (3.3.4), *ICT service* (3.3.5) or *ICT process* (3.3.6) meets the *cybersecurity* (3.1.2) *requirements* (3.2.5)

Note 1 to entry: *Cybersecurity (3.1.2) requirements* (3.2.5) can be established in a cybersecurity certification scheme.

Note 2 to entry: An assurance level indicates the level at which an *ICT product* (3.3.4), *ICT service* (3.3.5) or *ICT process* (3.3.6) has been evaluated.