SLOVENSKI STANDARD
oSIST prEN 18037:2024

01-februar-2024

Smernice za sektorsko oceno kibernetske varnosti

Guidelines on a sectoral cybersecurity assessment

Leitlinien für ein sektorales Cybersecurity Assessment

Cybersécurité et protection des données - Lignes directrices pour l'appréciation sectorielle de la cybersécurité

Ta slovenski standard je istoveten z: prEN 18037

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN 18037:2024 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 18037

November 2023

ICS

English version

Guidelines on a sectoral cybersecurity assessment

Leitlinien für ein sektorales Cybersecurity Assessment

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN and CENELEC 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Ref. No. prEN 18037:2023 E

Contents

Page

European foreword

This document (prEN 18037:2023) has been prepared by Technical Committee CEN/CLC/JTC13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

Introduction

This document describes 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 defined 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 defined 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 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-based schemes.

- The risk information obtained by an ISO/IEC 27005-conformant approach at sectoral level can be transferred to ISO/IEC 15408-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 not only supports the workflow of drafting market-oriented cybersecurity certification schemes but also offers a potential for a broader use by sectors and providers of infrastructure.

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 define, implement and maintain such requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

3 Terms and definitions

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

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

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

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
safeguarding of people, society, organizations and nations from cyber *risks* (3.4.1)

Note 1 to entry: Safeguarding means to keep cyber *risks* (3.4.1) at a tolerable level.

[SOURCE: ISO/IEC 27100, 3.2]

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 *requirements* (3.2.5)

Note 1 to entry: Cybersecurity *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.

Note 3 to entry: Assurance levels do not measure the cybersecurity of the *ICT product* (3.3.4), *ICT service* (3.3.5) or *ICT process* (3.3.6) concerned (cf. [6], article 2.22).

Note 4 to entry: This standard uses the relationship between assurance levels and the resistance of the target of evaluation against certain levels of *attack potential* (3.4.9) as defined in ISO/IEC 15408-3 as one parameter for consistent assurance level implementation across cybersecurity certification schemes, and for the identification of assurance level capacities of existing schemes.

3.2 Terms related to organization

3.2.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.3.2)

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: EN ISO/IEC 27000:2018, 3.50]

3.2.2
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

[SOURCE: EN ISO/IEC 27000:2018, 3.49, modified – Note 3 and 4 deleted]

3.2.3
policy
intentions and direction of an *organization* (3.2.1) as formally expressed by its top management

[SOURCE: EN ISO/IEC 27000:2018, 3.53]

3.2.4
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: EN ISO/IEC 27000:2018, 3.54]

3.2.5
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.2.1) and interested parties that the need or expectation under consideration is implied.

Note 2 to entry: ISO/IEC 15408 uses 'requirement' with direct relation to 'security objectives'.

[SOURCE: EN ISO/IEC 27000:2018, 3.56, modified - Note 2 to entry deleted, new Note 2 to entry added]

3.3 Terms related to sectoral approach to cybersecurity

3.3.1
sector
market sector
area in which business processes and use cases can be implemented under largely the same boundary conditions

Note 1 to entry: 'Market sector ''and 'application area' can be used synonymously.

Note 2 to entry: Boundary conditions include the types of relevant stakeholders and customers, the services to be supported, and legal and commercial aspects.

3.3.2
sectoral ICT system
system that includes *ICT products* (3.3.4) and *ICT processes* (3.3.5), as required for the provision of the services to the users of a particular market sector

Note 1 to entry: Sectoral ICT systems can rely on ICT infrastructure services for specific functions.

Note 2 to entry: Whenever cybersecurity-relevant functions of a sectoral ICT system depend on external ICT services, these are regarded as ICT infrastructure services.

Note 3 to entry: Sectoral ICT systems can be operated by different stakeholders.

3.3.3
sectoral ICT system architecture
specification of coordinated use of several *sectoral ICT systems* (3.3.2), *ICT products* (3.3.4), *ICT processes* (3.3.5) and *ICT services* (3.3.6) that enable the implementation and operation of the sector's services.

Note 1 to entry**:** Three subsequent definitions are from [**6**]

3.3.4
ICT product
element or a group of elements of a network or information system

3.3.5
ICT process
set of activities performed to design, develop, deliver or maintain an *ICT product* (3.3.4) or *ICT service* (3.3.6)

3.3.6
ICT service
service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems

3.4 Terms related to risk

3.4.1
risk
effect of uncertainty on *objectives* (3.2.2)

Note 1 to entry: An effect is a deviation from the expected— positive or negative.

Note 2 to entry: *Objectives (3.2.2)* can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event,* its consequence, or likelihood.

Note 4 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood.

Note 5 to entry: In the context of information security management systems, *information security (*3.1.1) risks can be expressed as effect of uncertainty on *information security* (3.1.1) *objectives* (3.2.2).

Note 6 to entry: *Information security* (3.1.1) risks are always associated with a negative effect of uncertainty on *information security objectives.*

Note 7 to entry: *Information security* (3.1.1) risk can be associated with the potential that *threats* (3.4.5) will exploit *vulnerabilities* (3.4.6) of an information *asset* (3.4.2) or group of information *assets* (3.4.2) and thereby cause harm to the sectoral stakeholders and the sectoral clients.

[SOURCE: ISO 31000:2018, 3.1, modified — By omitting “It can be positive, negative or both, and can address, create or result in opportunities and threats” in Note 1, and adding Note 2, 5, 6 and 7]

3.4.2
asset
anything that has value to the *organization* (3.2.2)

Note to entry 1: Two kinds of *information security* (3.1.1) related assets can be distinguished:

- the primary assets:
  - business processes and activities;
  - information;
- the supporting assets (on which the primary assets rely) of all types:
  - software;
  - network;
  - personnel;
  - site;
  - organization’s structure.

[SOURCE: ISO/IEC 27002:2022, 3.1.2]

3.4.3
information security event
occurrence indicating a possible *information security* (3.1.1) breach or failure of *controls* (3.4.11)

[SOURCE: ISO/IEC 27002:2022, 3.1.14]

3.4.4
information security incident
one or multiple related and identified *information security events* (3.4.3) that can harm an *organization's* (3.2.1) *assets* (3.4.2) or compromise its operation

[SOURCE: EN ISO/IEC 27035-1:2016, 3.4]

3.4.5
threat
potential cause of an *information security incident* (3.4.4), which may result in harm to a system or *organization* (3.2.1)

[SOURCE: ISO/IEC 27005, 3.1.9]

3.4.6
vulnerability
weakness of an *asset* (3.4.2) or *control* (3.2.1) that can be exploited by one or more *threats* (3.4.5)

[SOURCE: ISO/IEC 27000:2018, 3.79]

3.4.7
risk scenario
description of potential events or incidents that could have a negative impact on one or more business *objectives* (3.2.2)

Note 1 to entry: Risk scenarios are considered as having the potential to impact the business process and their associated business *requirements* (3.2.5) that are needed to support core business operations.

3.4.8
attacker
actor that potentially uses a weakness or otherwise exploit *threats* (3.4.5)

Note 1 to entry: Terms 'attacker', 'attacker' and 'threat agent' are used as synonyms that mean factors of *risk* (3.4.1) i.e. deliberate *threat* (3.4.5) sources.

3.4.9
attack potential
measure of the effort needed to exploit a *vulnerability* (3.4.6) in a target

[SOURCE: ISO/IEC 15408-1:2022, 3.8, modified — "TOE" has been replaced with "target"]

Note 1 to entry: According to CTI, the attack potential is characterized by means, opportunities and motives of the attacker.

3.4.10
cybersecurity objective
high-level *cybersecurity* (3.1.2) *requirement* (3.2.5)

Note 1 to entry: ISO/IEC 15408-1 defines the term in its technical meaning as "statement of an intent to counter identified *threats* (3.4.5) and/or satisfy identified organization security policies and/or assumptions".

3.4.11
control
measure that is modifying *risk*

Note 1 to entry: Controls include any *process* (3.2.4), *policy* (3.2.3), device, practice, or other actions which modify *risk* (3.4.1).

[SOURCE: EN ISO/IEC 27000:2018, 3.14, modified — Note 2 has been removed]

4 Abbreviations

APL	Attack potential level
AVA_VAN	Assurance family defined by ISO/IEC 15408-3 that addresses the vulnerability analysis
CAR	Common Assurance Reference
CC	Common Criteria
CSL	Common security level
CTI	Cyberthreat intelligence
EAL	Evaluation assurance level
eUICC	embedded Universal Integrated Circuit Card
ICT	Information and communication technology
IoT	Internet of Things
ISMS	Information security management system, defined in [3]
MRC	Meta-risk class
USIM	Universal Subscriber Identification Module

5 Sectoral Cybersecurity Assessment

5.1 Application of the sectoral cybersecurity assessment methodology

The application of the sectoral cybersecurity assessment entails the following tasks.

The first phase focuses on understanding and documenting the sectoral context as starting point for an ISO/IEC27005-conformant risks assessment and the following steps of the methodology.

It encompasses a description of the targeted sectoral services to end or business customers, the business processes required for provisioning of these services and a description of the functional architecture. On this basis primary assets, information and functional assets which are critical for the business processes, and supporting assets, ICT components which support and protect information and functional assets, can be identified.

Based on the documentation of the sectoral contexts, risks to the stakeholder organization's business objectives which may occur in case of information security incidents in relation to integrity, availability