



BSI Standards Publication

Guidelines on a sectoral cybersecurity assessment

National foreword

This British Standard is the UK implementation of EN 18037:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 28521 5

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2025.

Amendments/corrigenda issued since publication

Date	Text affected

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**

Contents

Page

European foreword	4
Introduction	5
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions	7
3.1 General terms.....	7
3.2 Terms related to organization	8
3.3 Terms related to sectoral approach to cybersecurity	9
3.4 Terms related to risk.....	10
4 Abbreviations.....	12
5 Sectoral Cybersecurity Assessment	12
5.1 Application of the sectoral cybersecurity assessment methodology.....	12
5.2 Principles and new capacities.....	14
5.2.1 Relevant information, relationships between parameters.....	14
5.2.2 Supporting risk-based consistent implementation of cybersecurity and assurance	15
5.2.3 Enabling a consistent approach to assurance	15
5.2.4 Enabling information exchange between the relevant standards.....	16
5.2.5 Enabling a coordinated application of cybersecurity controls	16
6 Sectoral representation of risk.....	17
6.1 Sectoral ICT systems.....	17
6.1.1 Sectoral ICT system components and their relationships	17
6.1.2 Multi-layered architecture of sectoral ICT system	17
6.1.3 Risk –based definitions of cybersecurity and assurance requirements in sectoral systems	19
6.1.4 Sectoral ICT system architecture relevance for risk assessment.....	20
6.1.5 Cybersecurity certification of sectoral ICT systems.....	21
6.2 Consistent sectoral risk assessment.....	22
6.3 Performing sectoral risk assessment.....	23
6.3.1 General.....	23
6.3.2 Choosing an approach	24
6.3.3 Identifying business processes, objectives and requirements.....	24
6.3.4 Identifying primary and supporting assets.....	25
6.3.5 Defining risk scenarios	25
6.3.6 Assessment of consequences in risk scenarios.....	25
6.3.7 Assessment of likelihood in risk scenarios	26
6.3.8 Adding the attacker perspective: assessment of attack potential	27
6.3.9 Risk re-assessment for supporting assets	28
7 Normalized representation of risk, cybersecurity and assurance.....	29
7.1 Risk assessment results: meta-risk classes.....	29
7.2 Risk-based definition of common security levels and selection of controls	29
7.2.1 General.....	29
7.2.2 Introducing Common Security Levels (CSL).....	30
7.2.3 Applying Meta-risk Classes and Common Security Levels for sectoral risk treatment.....	30

7.2.4 Attack Potential as criterion for selecting the CSL of controls 30

Consistent implementation of assurance 31

7.2.5 General 31

7.2.6 Definition of a common assurance reference concept based on ISO/IEC 15408-3 31

7.2.7 Applying CTI concept of attack potential to CAR 32

8 Mapping cybersecurity and assurance requirements to scheme’s representation 33

Annex A (informative) Examples of normalized scales in sectoral risk assessment 34

Annex B (informative) CTI fundamentals 38

Annex C (informative) Application of Common Security Level approach - examples 60

Annex D (informative) Example of assurance level mapping 64

Bibliography 65

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.

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. [8], article 2.22).

Note 4 to entry: This document 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* (3.2.2)

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 Note 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 series 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.

3.3.4

ICT product

element or a group of elements of a network or information system

[SOURCE: [8], art. 2(12)]

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)

[SOURCE: [8], art. 2(14)]

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

[SOURCE: [8], art. 2(13)]

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 Notes 3, 5, 6 and 7]

3.4.2

asset

anything that has value to the *organization* (3.2.1)

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

- the primary assets:
 - business processes & 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 27005:2022, 3.1.9]

3.4.6**vulnerability**

weakness of an *asset* (3.4.2) or *control* (3.4.11) that can be exploited by one or more *threats* (3.4.5)

[SOURCE: ISO/IEC 27000:2018, 3.77]

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* (3.4.1)

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
CSL	Common security level
CTI	Cyberthreat intelligence
EAL	Evaluation assurance level
ICT	Information and communication technology
IoT	Internet of Things
ISMS	Information security management system, defined in [3]
MRC	Meta-risk class
SIM	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/IEC 27005-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 or confidentiality of primary assets are identified and analysed. Sectoral characteristics of threats, and in particular, description of attacks and attacker types (cyberthreat intelligence, CTI, see Annex B) that include an estimation of the attack potential level and attackers’ motivation, are used in this analysis.

Phase two consists of sequential assessments.

First, by the primary asset assessment, a rating of the risk information documented in the context is conducted by using a normalised representation (meta-risk classes, MRC, see 7.1). This assessment identifies the MRC for risks to sectoral business processes and the stakeholder organization's business objectives that may occur as result of incidents that affect the ICT security of primary assets.

On this basis the second assessment, the supporting asset assessment, can be carried out to support the treatment of the identified and rated risks. It specifies requirements to cybersecurity and assurance per supporting assets, i.e. ICT products, processes or stakeholder organization's ICT systems. This relates to the identification of common security levels (CSL, see 7.2.2) and common assurance reference (CAR, see 7.2.7).

The third phase is used to map the cybersecurity and assurance level requirements identified by the sectoral cybersecurity assessment to the representation of assurance levels, cybersecurity objectives and cybersecurity levels of the scheme that is planned for cybersecurity certification.

Figure 1 presents the outline of sectoral cybersecurity assessment.

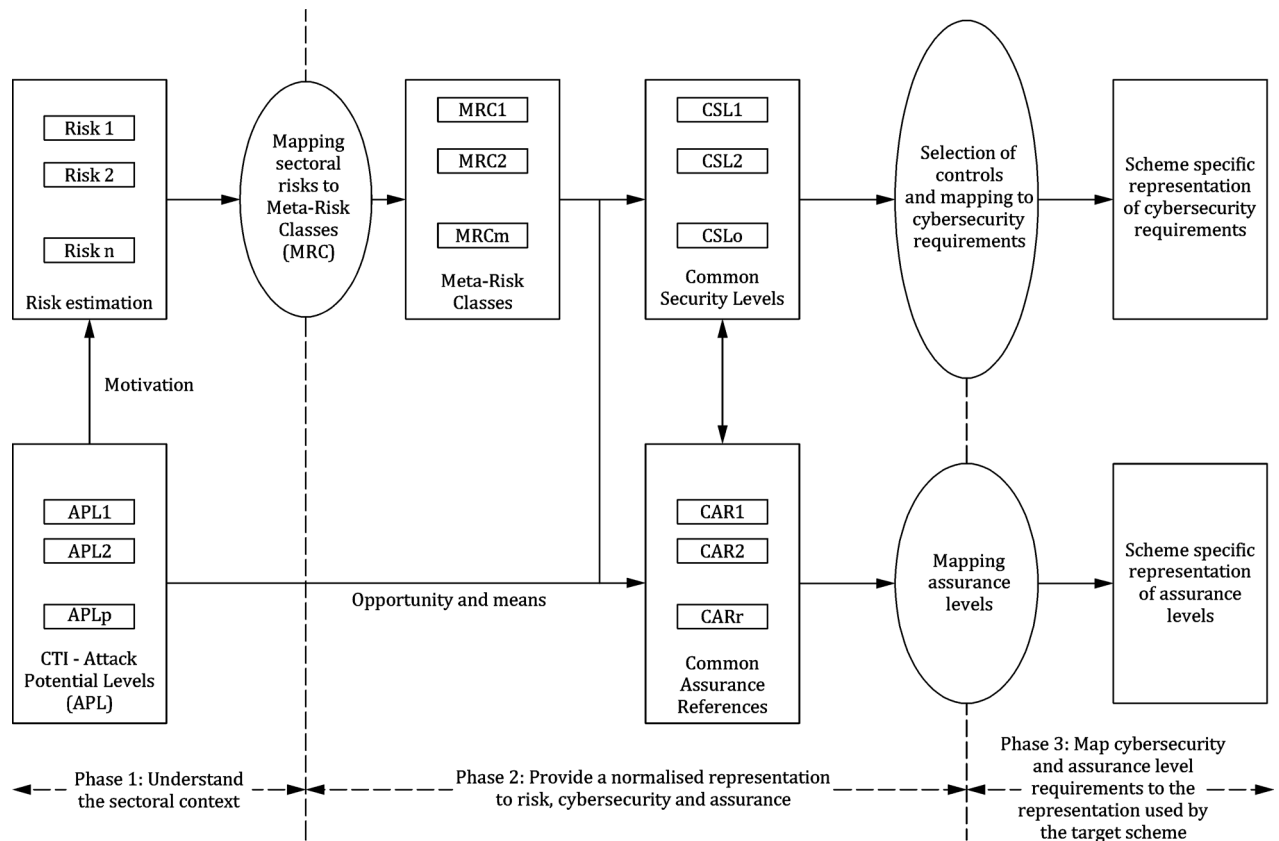


Figure 1 — Sectoral Cybersecurity Assessment

As illustrated in Figure 1 the phases of the sectoral cybersecurity assessment process are not sequential but interdependent. Some activities described in this document can contribute to more than one phase. Motives that constitute one of the attack potential characteristics should be used to estimate the likelihood of an incident based on the attacker's level of motivation in Phase 1 (see 6.3.8) while two other characteristics i.e., opportunities and means should be considered to determine the CSL (see 7.2.3) and the CAR level (see 7.2.7) in phase two.

5.2 Principles and new capacities

5.2.1 Relevant information, relationships between parameters

The sectoral cybersecurity assessment requires a sound and detailed documentation of the sectoral context. On this basis, it generates information on risks related to ICT security incidents which are then, together with other parameters like APL, used to determine appropriate cybersecurity and assurance requirements to the critical supporting assets.

A special aspect of the methodology is that the assessment is carried out in two subsequent steps.

The primary asset assessment activities follow the risk management standard ISO/IEC 27005. It determines risks to the stakeholder's business objectives arising from potential cybersecurity incidents in relation to primary information or functional assets. The second assessment step focusses on supporting assets, i.e. ICT system components that the primary assets rely on. This assessment supports the distinction between supporting asset that are critical for the ICT security of the primary assets and merit dedicated cybersecurity and assurance measures and those where this is not necessary. Critical supporting assets go through another loop of risk rating which considers the intended use, operational environment, and the relevant attack potential before assigning appropriate security and assurance requirements for risk treatment.

The supporting asset assessment step can also be used for optimizing the sectoral ICT system's security architecture, for instance as guidance if the goal is to concentrate security-relevant functions in specific components like secure elements or high security modules.

Figure 2 provides an overview on information needed, then used and information generated by the sectoral cybersecurity assessment.

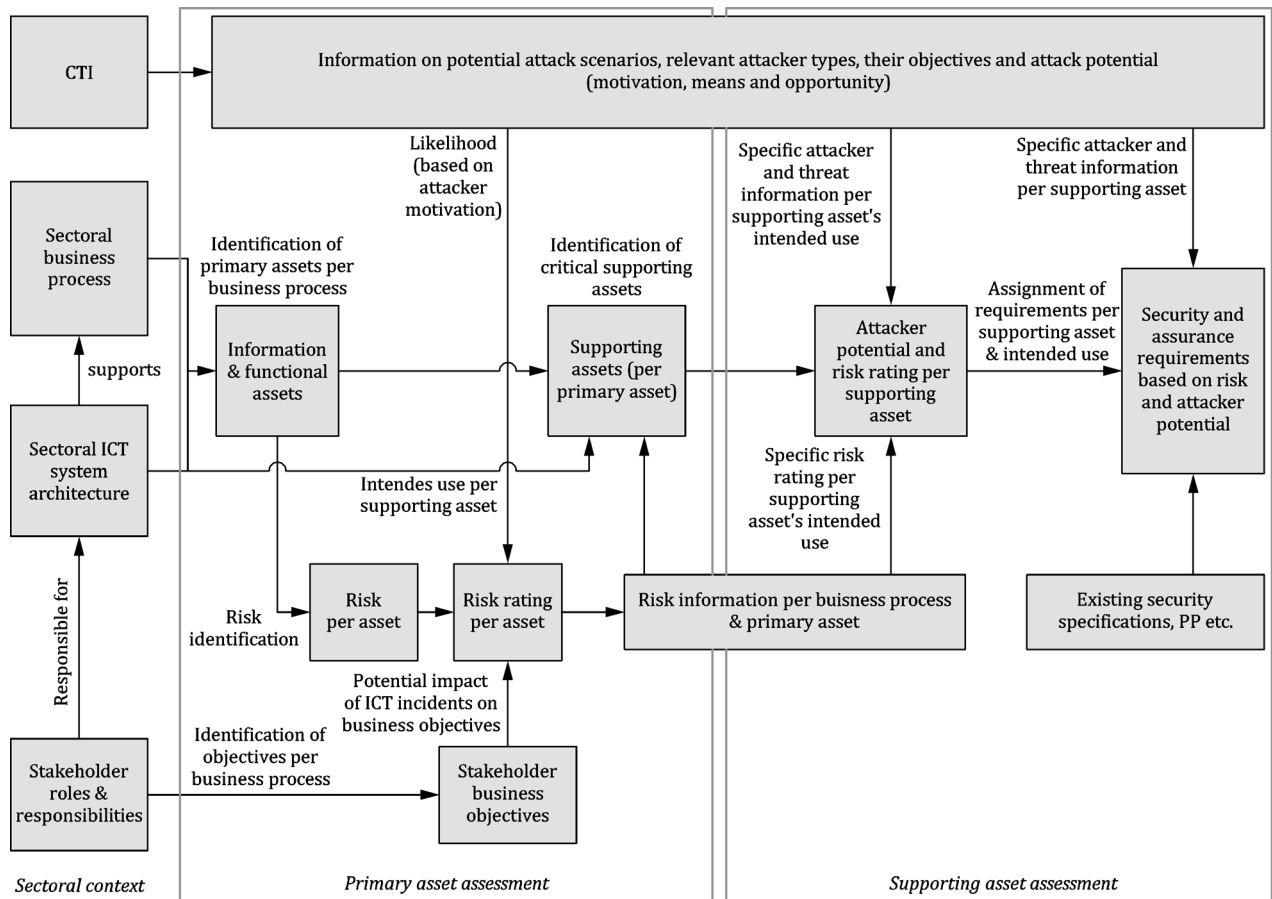


Figure 2 — Overview on information used and generated by the sectoral cybersecurity assessment

5.2.2 Supporting risk-based consistent implementation of cybersecurity and assurance

The definition of cybersecurity and assurance requirements is based on risk. Second, cyberthreat intelligence (CTI) is applied to allow the input of information about attacker types and their motivation, means and opportunities to attack targeted ICT products, ICT processes and ICT services.

This leads to the critical features of the approach i.e.:

- “attack potential levels” (APL) which rate the motivation, means and opportunities of attackers;
- “meta-risk classes” (MRC), to allow a common approach to risk assessment;
- “common security levels” (CSL), to allow a consistent approach to cybersecurity controls;
- “common assurance references” (CAR), to allow comparability between implementations of assurance in various cybersecurity certification schemes.

In the approach, each of common security level (CSL), and each of common assurance reference (CAR) correspond to a particular attack potential level (APL) and a meta-risk class (MRC).

5.2.3 Enabling a consistent approach to assurance

The common assurance reference (CAR) concept is derived from the AVA_VAN assurance family, which is the basis for the vulnerability analysis in ISO/IEC 15408-3. As known from AVA_VAN, CAR is directly

linked to the parameter attack potential level (APL) which, according to this methodology, can be identified per attacker type based on CTI information.

The capacity of an attacker type to conduct attacks, which is rated by the attacker types of APL, is essentially independent of the type of the targeted type of supporting asset component of the sectoral ICT system. Therefore, consistency of the assurance level implementation across all types of supporting assets ICT products, processes and respective cybersecurity certification schemes can be achieved by linking the CAR and the APL of the attacker types who could be motivated and capable to run attacks. In addition, the concept of using the APL as system-wide reference supports the identification of a cybersecurity certification scheme's capability to validate a specific level of assurance. For this purpose, it should be analysed up to which APL the scheme's evaluation methodology can validate resistance against the means and opportunity associated with an APL.

Using CAR instead of AVA_VAN should be considered as a key parameter for gaining flexibility in comparing different implementations of assurance levels. The CAR is designed to prioritize comparability between implementations rather than full consistency, which allows for deviations between specific schemes' assurance level implementations. It supports the flexibility to follow market requirements and maximizes the options to integrate certificates from different cybersecurity certification schemes including the Common Criteria based schemes and existing industry schemes, while maintaining a sufficient level of comparability.

NOTE This document does not refer to a specific evaluation or certification method for an implementation of certification scheme. If CTI is unavailable, this method describes in subclause 6.3.1 how to form an expert group composed of the relevant sectoral stakeholders estimating APL as a qualitative alternative.

5.2.4 Enabling information exchange between the relevant standards

The definition of cybersecurity and assurance requirements for ICT products, ICT processes and ICT services reflects the cybersecurity risk associated with their intended use. The identification of this risk is typically conducted at business system level using an ISO/IEC 27005-based information security risk assessment. However, the specification of the cybersecurity and assurance requirements to an ICT product is typically carried out using ISO/IEC 15408 series. Until now, there was no link between the two standards, which could be used to transfer the information in a specified way. The specification of cybersecurity and assurance requirements by protection profiles or security functionality specifications has been typically based on assumptions made by the product vendor or by limited stakeholder groups related to their views of "intended use", not on input from the business system owner. The approach allows the exchange of the required information between the business level, which uses ISO/IEC 27005 and related standards for defining risk-based cybersecurity requirements, and product level specifications based on ISO/IEC 15408 series used for defining security and assurance requirements. By extending the approach to the cybersecurity risks at the sectoral level the exchange of specific information and relevant requirements for sectoral cybersecurity schemes can be established.

In summary, this document provides connections between existing risk assessment methods such as these based on ISO/IEC 27005 so that it can re-use their outcomes and can focus on the existing gap between assurance levels at the component level.

5.2.5 Enabling a coordinated application of cybersecurity controls

It is the purpose of controls to decrease risk and to prevent cybersecurity incidents. Therefore, the control strength, which is specified in relation to common security levels, takes into account not only the risk but also the potential of motivated attackers to cause an impact.

Based on the common security level (CSL) concept it is also possible to use already available libraries of controls (e.g. those specified in ISO/IEC 27002) implemented and possibly scaled according to their common security levels. These libraries could help product vendors as well as owners of ISMS to implement a specified level of cybersecurity. Depending on the sector, additional libraries could be

considered, for example ISO/IEC 27011 for telecommunications industry, or ISO/IEC 27019 for process control systems used by the energy utility industry.

6 Sectoral representation of risk

6.1 Sectoral ICT systems

6.1.1 Sectoral ICT system components and their relationships

A sectoral ICT System can consist of ICT products and ICT processes that supports an ICT service.

In addition, there are ICT processes, which support ICT products, for example, product development processes. These can be different from those which support ICT services.

ICT services can be supported by both, ICT products and ICT processes, as well as the support can be provided by ICT products to individual ICT processes.

The relationship between these elements is presented in Figure 3.

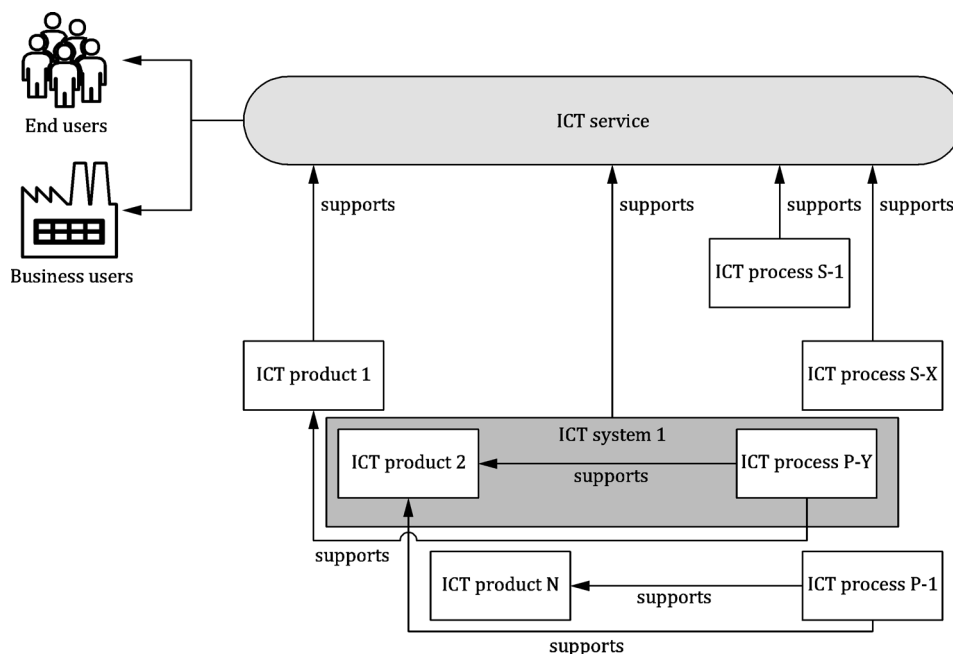


Figure 3 — Relationship between ICT services, ICT products and ICT processes

6.1.2 Multi-layered architecture of sectoral ICT system

With a view to conducting risk assessment, evaluation and certification, the sectoral ICT system architecture should be specified. A model representation of such architecture can consist of several layers, and these include:

a) Sectoral ICT systems

Sectoral ICT systems create the first, highest layer of the architecture used for providing ICT services.

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

b) ICT infrastructures

Sectoral ICT systems can rely on lower, second layer which is created by the ICT infrastructure services for functions specific to a particular market sector.

ICT infrastructures can be applied for several markets, applications, and end user services. Although they are not sector-specific, they can be integrated into sectoral ICT systems.

EXAMPLE ICT Infrastructures include mobile networks, cloud services and payment or identity management services.

ICT infrastructures could also be regarded as providing ICT services to the sectoral ICT systems they support. From the business perspective, this can be seen as a relationship between otherwise unrelated organizations in the roles of an ICT infrastructure service provider and a business user.

External ICT infrastructure services should be considered in the risk assessment as they can determine the cybersecurity and assurance levels for the sectoral ICT system.

c) Generic ICT products

ICT products can be used in both sectoral ICT systems and ICT infrastructures. From the architectural perspective, they create the next, separate layer in the model representation.

ICT products can be used in both sectoral ICT systems and ICT infrastructures. These ICT products should be considered as a separate layer in the model representation.

Generic ICT products that operate in a bigger setting, can hence be subject to certification.

The relationships between layers of a sectoral ICT system are presented in Figure 4.

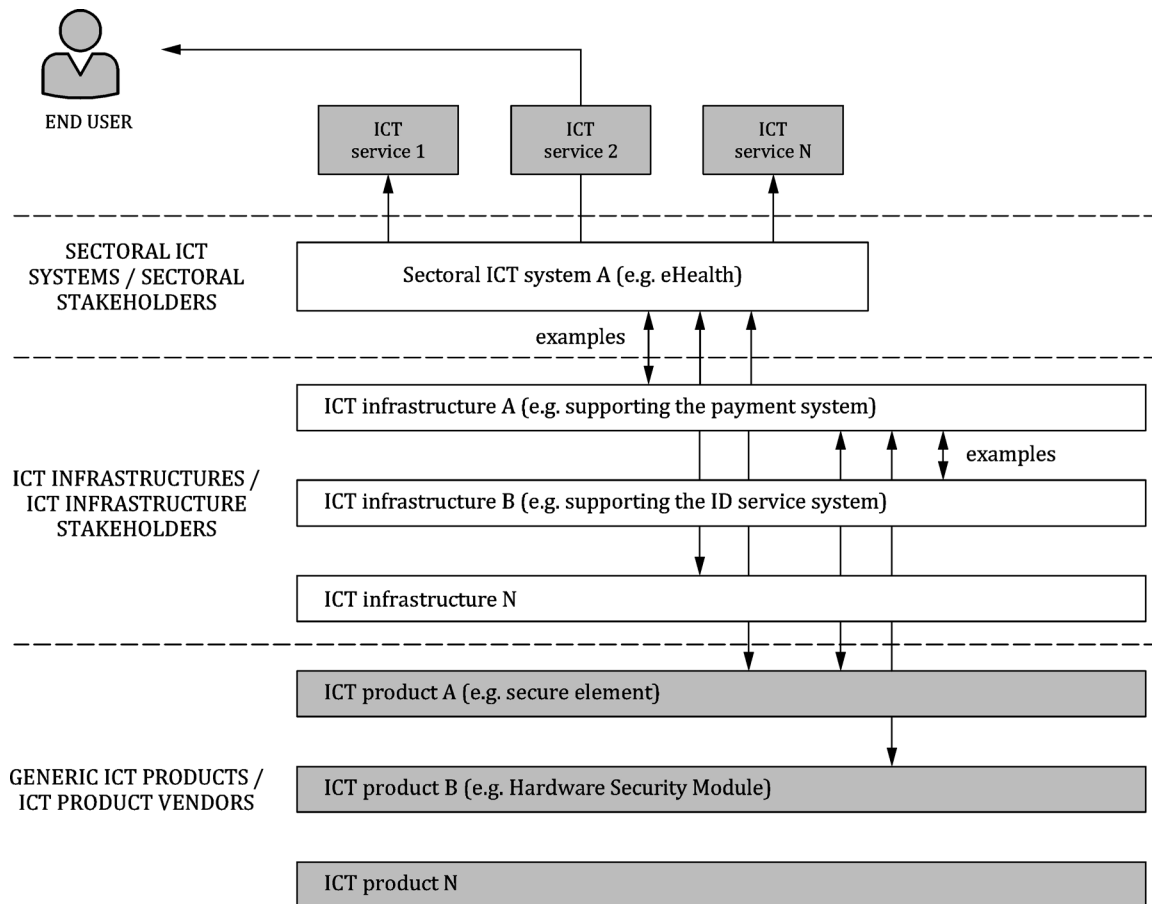


Figure 4 — Layers of sectoral ICT system

ICT infrastructures and sectoral ICT systems can be combined.

EXAMPLE 5G network, payment and identity management services are typically integrated by sectoral ICT systems and offer ICT services to users.

From the perspective of cybersecurity evaluation and certification, it is important to consider not only the technical interaction between these building blocks of the overall sectoral ICT system but also the allocation of responsibilities within them; since the owners of each of the building blocks typically carry out risk assessments, implement appropriate controls and support evaluation and certification at their level.

It is important to note a key difference between ICT infrastructures and ICT products. The owners of ICT infrastructures are responsible for defining, implementing, and operating the infrastructure. On the other hand, those who purchase ICT products are responsible for integrating and operating the product according to its intended use; this means that the vendors are responsible in case of providing evaluated and certified ICT products to the stakeholders of sectoral ICT systems or ICT infrastructures.

6.1.3 Risk –based definitions of cybersecurity and assurance requirements in sectoral systems

Sectoral risk assessments are key to the formulation of cybersecurity and assurance requirements for supporting ICT infrastructures and ICT products used by several sectors, and to those of the ICT products and ICT processes used by sectoral ICT systems internally.