EUROPEAN UNION AGENCY
FOR CYBERSECURITY

METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS

EU Cybersecurity Certification Framework

SEPTEMBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use SCSA_Methodology@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Elzbieta Andrukiewicz, Eve Atallah, Cord Bartels, Christian Dörr, Louis Marinos, Alexandra Michota, Jordi Mongay Batalla, Kim Nguyen, Patrice Payen, Nineta Polemi, Bart Preneel, Jean-Pierre Quemard, Ingrid Schaumüller-Bichl, Georg Stütz, Jeremy Ward

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue Number: TP-01-21-174-EN-N – ISBN: 978-92-9204-535-7 - DOI: 10.2824/490490

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cybersecurity certification under the European Union Cybersecurity Act (CSA) is intended to increase trust and security for European consumers and businesses and help to achieve a genuine digital single market[1].

This requires that all relevant levels of the ICT market, from sectoral ICT services and systems via ICT infrastructures to ICT products and ICT processes, will be addressed and that the related cybersecurity certification schemes are well accepted by the market. The CSA stipulates specific requirements, which target efficiency and coherence between schemes of the CSA's cybersecurity certification framework. These requirements include:

- The security and assurance requirements for ICT services, ICT processes or ICT products should be defined based on the risk associated with their intended use.
- Assurance levels should be implemented consistently across schemes.
- Support for security-by-design.

The methodology for sectoral cybersecurity assessments described in this document (hereinafter called SCSA Methodology) addresses these objectives in the context of drafting sectoral cybersecurity certification schemes, which address ICT services in individual market sectors. It is designed to be used as a preparatory step for the definition of a candidate scheme involving sectoral stakeholders.

A basic principle of the proposed methodology is to establish a sound understanding of the sectoral ICT services and system as a foundation for all other functions:

- A cybersecurity assessment at the sectoral level will provide information about the objectives of the sectoral stakeholders and will identify the primary assets and related risks. As an enhancement of the typical risk assessment procedure, a 'deep dive' to gain detailed information about the intended use of relevant subsystems, products or services will be conducted. In addition, cyberthreat intelligence (CTI) will be employed to provide information on potential attackers, their motivation and capabilities. This adds an important parameter to the risk analysis and contributes to the information needed to assign security and assurance requirements to ICT subsystems, ICT products or ICT services based on risk.
- The SCSA Methodology provides the option to integrate sectoral, product, process and potentially also ISMS-based cybersecurity certification schemes. It offers a concept of internal risk, security and assurance reference levels. If these are commonly used, they will support consistency in the definition of risk, security and assurance across schemes. The SCSA Methodology is designed to address a wide range of certification schemes, beyond Common Criteria or other ISO/IEC 15408-based schemes. Optionally other types of certification schemes can be integrated in order to establish consistency across the various types of schemes that support the proposed methodology.

[1] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

- A link between the ISO/IEC 270xx series of standards and ISO/IEC 15408 is needed to allow information to be exchanged between the outcome of risk assessment and the specification of security and assurance of products. The expert team has developed a mapping approach that addresses existing divergences of terminology between these standards and allows the transfer of the information that is required.

- The introduction of a common, scalable approach to risk-based security and assurance supports the definition of scaled controls. These controls are associated with clear security levels which are defined in accordance with their ability to treat risk and protect against known attack potentials. The expert team has drafted a sample list of scaled controls and has described how these controls can be used in a coordinated way.

Based on these properties and functions, the SCSA Methodology has the potential to fully support the aforementioned requirements stipulated by the CSA and to promote the market acceptance of cybersecurity certification in the following ways:

- The SCSA 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 architecture. In applying the methodology, relevant stakeholders will be responsible for the identification of risks and they will be involved in the definition of security and assurance requirements. This will allow them to 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 of schemes under the CSA.

- As required by the CSA, 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 may emerge as a result of specific requirements from different markets.

- Introducing a common concept for security levels facilitates the definition of controls which can be commonly used across participating schemes. This provides a sound basis for the introduction of libraries of such controls. The availability of those could significantly promote the introduction of security-by-design, as well as the implementation of defined security levels in ICT products, ICT processes and also in ICT systems.

Applying the SCSA Methodology will generate sound information about the sectoral system and defined relationships between the stakeholders involved, which may enable additional tangible benefits, including:

- Product and service providers will benefit from reliable information about the intended use of their products and services, as well as sectoral security and assurance requirements. This will allow them to optimize their products and their market reach.

- The defined relationships between risk, security and assurance proposed by this methodology support the definition of horizontal products and services, which can serve various sectors.

- A sound understanding of the ICT system, the defined roles of the relevant parts and stakeholders, and the availability of controls with defined properties concerning risk and

attack potential open new options, especially for sectors that have, for example, to deal with cost pressures and attackers with an elevated potential at the same time. Based on this methodology, the deployment of controls may be coordinated and firmly agreed between stakeholders. For example a basic-level control in an IoT device and a medium-level control in the sectoral back-office may be concatenated and coordinated in such a way that they jointly reach a security level that also protects against elevated attack potentials.

The version of the methodology described in this document is sufficiently mature to allow a first practical use in drafting sectoral cybersecurity certification schemes. Experience gained from this first deployment should be used to improve and consolidate the methodology.

In summary, the proposed methodology not only supports the workflow of drafting the CSA cybersecurity scheme but also offers a potential for a broader use by sectors and providers of infrastructure.

1. INTRODUCTION TO THE SCSA METHODOLOGY

1.1 BACKGROUND AND REQUIREMENTS

The European Cybersecurity Act (CSA) stipulates fundamental requirements for the definition, implementation and maintenance of EU cybersecurity certification schemes. The use of these schemes is voluntary. Therefore their market take-up, as a prerequisite, requires acceptance by the ICT industry and the consumers.

The market success of the EU cybersecurity certification framework requires, amongst other things, a balance to be struck between potentially contradictory requirements, as follows:

1. **Flexibility vs consistency**
   The individual market needs of sectors or product and system vendors may require the flexibility to establish specific schemes at sectoral level or for certain categories of ICT services, products and processes. The CSA supports this flexibility.

   However, it is also of fundamental importance for market acceptance that certificates issued by one scheme can be re-used and recognized by other schemes under the CSA. This requires a well-balanced compromise between flexibility and consistency of scheme definition and a clear definition of the relationship between schemes under the CSA. The CSA stipulates that assurance levels should be implemented consistently across sectoral schemes, which would then support the recognition of certified products, processes and services by those sectoral schemes.

2. **Cost vs benefit of security and assurance**
   The optimization of investments in security and assurance is a fundamental criterion for market acceptance by ICT system owners. The CSA supports this requirement by stipulating that the security and assurance requirements of ICT services, products and processes should be defined based on the risk associated with their intended use. This allows an informed decision to be made based on an appropriate balance between the level of risk that would be acceptable to the risk owners and the cost of security and assurance.

   The implementation of this principle requires that the risk associated with the intended use of an ICT product or process at sectoral level is understood and that this information can be used to optimize the security and assurance of the product or process accordingly.

3. **High attack potential vs limitations of controls**
   Some market sectors, for instance those which make use of ‘Internet of Things’ (IoT) elements, must take account of the pressure to limit costs associated with the mass-market or the limitations inherent in consumer devices. This may prohibit the deployment of high-level controls and assurance, despite the fact that highly skilled attackers may be motivated to conduct attacks against such devices.

   There should therefore be a method that helps to identify and document such cases and which supports the development of appropriate remedies.

The implementation of practical and sound solutions to these questions requires a transparent methodology. This methodology is introduced in Section 1.2 of this document. Section 1.3 describes how it can be applied in the process of developing a cybersecurity scheme.

A detailed interpretation of the requirements given by the CSA is provided with the documentation of the methodology in sections 4.1 and 5.1.

1.2 INTRODUCTION TO THE SCSA METHODOLOGY

This document describes a methodology designed to be used in the process of drafting cybersecurity certification schemes for sectoral ICT services and systems in order to address the issues mentioned in Section 1.1. It was developed by a cross-functional team of experienced European ICT experts led by ENISA. The following paragraphs describe the steps that had to be taken to establish the methodology.

1. **Understanding sectoral services and schemes - introduction of a structured approach to cybersecurity certification schemes**
   The first step in the development of the methodology was to clarify the types of cybersecurity certification schemes to be supported and to define the relationships between these with the goal of enabling the re-use of certificates. For this purpose, the methodology introduces a layered architecture model that distinguishes between the layer of sectoral ICT systems, which support sectoral ICT services, the layer of ICT infrastructures and the layer of generic ICT products and processes. It categorizes the related types of cybersecurity certification schemes into sectoral, infrastructural, ISMS and product schemes, and defines the relations between these for the propagation of risk information, security and assurance requirements and the recognition of certificates.

   A typical sectoral ICT system employs:

   - numerous types of ICT systems which are part of an internal ISMS,
   - generic ICT products provided by external vendors, and also, very likely
   - ICT services provided by ICT infrastructures such as mobile networks, payment or ID services.

   It would not be practical to request that a sectoral cybersecurity certification scheme evaluates and certifies all of these elements. Instead, such a scheme should, for each individual element, reference, as far as possible, those certificates that have been issued by any schemes which address those elements. Chapter 4 documents these considerations.

2. **Enabling information exchange between the relevant standards**
   Sectors typically use a combination of ISMS certification and certified ICT products and processes for the certification of the required levels of security and assurance for the sectoral ICT system that enables their ICT services. The risk assessment of information security and ISMS certification is standardized by ISO/IEC 270xx, while the leading series of standards for ICT product security evaluation is ISO/IEC 15408. These standards have different approaches and use different terminology, which makes the transfer of information and requirements between them difficult.

   The CSA stipulates that the definition of security and assurance requirements for ICT products, ICT processes and ICT services should reflect the risk associated with their intended use. The identification of this risk is typically conducted at sectoral system level using an ISO/IEC 270xx-conformant risk assessment. However, the specification of the security and assurance requirements of an ICT product is typically carried out using ISO/IEC 15408. Before the development of this methodology there was no link between

the two standards, which could be used to transfer the information in a defined way. The specification of ICT products by protection profiles or security targets has to date typically been based on assumptions by the product vendor or by limited stakeholder groups, not on input from the sectoral system owner.

As one of the foundations of the methodology, the working-group experts have developed an approach to analyse and compare the viewpoints and the meanings of terms in ISO/IEC 270xx and in ISO/IEC 15408. This is documented in Annex A. A comparison of different meanings in the two groups of standards is given in Section 2.3. On the basis of this analysis and comparison, it was possible to develop the method mentioned in the previous paragraph. This method allows the exchange of the required information between the sectoral level, which uses ISO/IEC 270xx, and product level specifications based on ISO/IEC 15408.

Using this innovative approach it will be possible to optimize the development of ICT products, ICT processes and ICT services by providing information about the precise security context and needs of the sectors in which the ICT products, ICT processes and ICT services will be deployed. Sectors can also be sure that they are in a position to communicate their requirements to the developers and vendors of ICT products, ICT processes and ICT services, and will be able to check if certified ICT products, ICT processes and ICT services suit their purposes.

3. **Using existing risk assessment methods and cyberthreat intelligence**
Balancing the potentially contradictory objectives described in Section 1.1 requires a sound understanding of the objectives of the sectoral stakeholders, the sectoral system and the intended use of supporting ICT services, ICT products and ICT processes which are employed by the sector.

The basis for the required knowledge is established by conducting a risk assessment at sectoral level. Established ISO-conformant methods such as Ebios RM[2] may be used to identify and document risks from the perspective of the sectoral stakeholders. The proposed methodology is designed to re-use these existing risk assessment methods, not to replace or modify them.

However, the targeted purposes require the classical risk assessment methods to be supplemented by additional elements. The working-group's proposals for doing this are described in this methodology. First, there is a need to document the intended use of supporting ICT products, ICT processes and ICT services. Second, cyberthreat intelligence (CTI) should be 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. Section 5.3 contains detailed descriptions of how these additional elements should be used. Chapter 9 provides an introduction to CTI and to the methods for estimating the potential of attackers.

4. **Supporting a flexible definition of risk and consistent implementation of assurance and security**
Chapter 5 describes not just how to apply risk assessment and CTI tools but it also describes a core part of the methodology, the concept of how to balance consistency in the implementation of assurance levels and the flexibility to adapt to the individual requirements of particular markets. The principles behind this concept are documented in Section 5.1.

[2] For an inventory of Risk Assessment and Management Methodologies see:
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

The CSA defines three assurance levels and stipulates that each assurance level should be consistent between the sectoral domains. This is essential to avoid fragmentation between schemes and is a precondition for a broad recognition of certificates issued under the CSA.

As a first step in identifying a consistent implementation, the expert team defined an approach, the 'common assurance reference' (CAR) concept, which aims at comparability between implementations instead of full consistency and, by this, allows deviations between scheme-specific implementations of assurance levels. This supports the flexibility to follow market requirements and maximizes the options to integrate certificates from CSA-internal, incumbent Common Criteria and also industry schemes while maintaining a sufficient level of comparability.

The common assurance reference concept is derived from the AVA_VAN assurance family, which is the basis for the vulnerability analysis in ISO/IEC 15408-3. The use of AVA_VAN as a key parameter allows flexibility in comparing implementations of assurance levels. Moreover, deviations from the standard are allowed as documented in Subsection 5.6.6. This concept would support the integration of certificates which are issued by schemes that employ the evaluation methodologies defined in ISO/IEC 15408 and ISO/IEC 18045. This includes EUCC, SOGIS and other CC schemes, and also, potentially, a variety of industry schemes which re-use parts of ISO/IEC 18045 because of its maturity and reputation in the market.

Other evaluation methodologies and related certification schemes, including those which are not related to ISO/IEC 15408, could potentially also be linked to the proposed common assurance reference concept. This could allow the integration of cybersecurity certification schemes with different approaches into the cybersecurity certification framework under the CSA.

The CAR concept supports five levels. These levels can be mapped to the CSA assurance levels as it is known from the EUCC candidate scheme. The considerations concerning the common assurance reference concept are documented in Section 5.6. The CAR-concept can be viewed as the cornerstone of the SCSA Methodology. It is intended to introduce consistency across sectors and schemes.

The CSA suggests that the definition of security and assurance requirements is based on risk. This leads to the two other critical features of the methodology, the 'meta-risk classes' (MRC) to allow a common approach to risk assessment, and 'common security levels' (CSL) to allow a consistent approach to security controls. In the proposed methodology, each level of common assurance reference (CAR) and common security level (CSL) corresponds to a particular meta-risk class (MRC). The concept of meta-risk classes and how they are defined based on risk and CTI information is documented in Section 5.3. The common security levels and the selection of levels based on the meta-risk class and attack potential are described in Section 5.5.

This relationship between meta-risk classes and common assurance references and common security levels satisfies the CSA's requirement for risk-based assurance and security and also the requirement for a consistent definition of assurance levels. If applied in all sectoral scheme drafting projects, it will help suppliers to define generic ICT products, ICT processes and ICT services, whose certificates can be recognized in all these sectors. In particular, from a security certification perspective, the common methodology to define assurance levels allows the comparability of certificates issued by different certification schemes.

The SCSA Methodology also defines how the assurance level to be claimed for the certification of an ICT product or ICT product type is determined, and which information, from any sectoral risk assessment, would be a valuable input for vulnerability analysis.

Then, certificates issued by any certification scheme can be compared based on their claimed assurance level and be recognized between different sectors in which the certified ICT product is intended to be used.

However, the requirement for consistency and coherence of schemes under the CSA has to be balanced with the need for the flexibility that will allow particular schemes and their evaluation methodologies to be adapted to the requirements of certain markets. The SCSA Methodology introduces this required flexibility in two ways:

1. The identification of risks and the assignment of these risks to meta-risk classes is the responsibility of the sectoral stakeholders. Based on their 'risk-appetite', stakeholders from different sectors may select different meta-risk classes for comparable risks.

2. Sectoral stakeholders may deviate from the defaults for the selection of assurance and security levels based on meta-risk classes if these deviations are explained and documented.

It can be concluded that, using the methodology as documented in Chapter 5, it should be possible to balance consistency and flexibility as required in Section 1.1.

5. **Enabling a coordinated application of security controls**

According to the CSA, it is the purpose of controls to decrease risk and to prevent cybersecurity incidents. Therefore *control strength*, which is defined by this methodology in relation to common security levels, takes into account not only the risk but also the potential of motivated attackers to cause an impact. Section 5.5 documents this part of the methodology.

Based on the common security level concept it should also be possible to develop libraries of controls scaled according to their common security levels. These libraries could help product vendors as well as owners of ISMS to implement a well-defined level of security. They would also provide a practical approach to security-by-design. This would be of particular help to developers, who are not cybersecurity experts, in the correct implementation of IT security. An example of such a library, which includes single examples of controls assigned to common security levels, is given in Annex F.

The use of the methodology set out in this document should generate a sound and comprehensive understanding of sectoral ICT systems with respect to all aspects related to cybersecurity risks, controls and assurance. Such systems include all the ICT products, ICT processes and ICT services deployed, as well as the cybersecurity functionality contributed by the ISMS implemented by sectoral stakeholders.

In the absence of this methodology ICT product developers and vendors, as well as those responsible for sectoral ISMS, will be restricted to an understanding only of those cybersecurity risks and controls implemented in the domains for which they are responsible. With the support of this methodology, however, they will be able to plan the provision of cybersecurity controls to a level that is appropriate to the demands of overall sectoral cybersecurity risk management. As described in the previous section such planning is vital if, for example, an ICT product imposes limits on the degree to which its

level of security can be raised, while at the same time an elevated attack potential has to be assumed.

Based on knowledge of the system as a whole, which can be generated by this methodology, it should be possible to apply cybersecurity controls in a coordinated and holistic way. For example, the cybersecurity controls inherent in an ICT product and the cybersecurity controls implemented within a sectoral ISMS can support each other to gain the level of security required to manage the overall risk. This concept is termed 'concatenation of controls' and is described in Subsection 5.5.3. An example is given in Chapter 8. This approach should help to deliver a viable balance between risk and attack potential and the limitations imposed by ICT products – such as those associated with the application of IoT devices.

1.3 APPLYING THE SCSA METHODOLOGY

The SCSA Methodology described in this document should address the objectives given in 1.1 in the context of the workflow for drafting sectoral cybersecurity certification schemes. It is designed to be used in a preparatory step for the definition of a candidate scheme and should be conducted in cooperation with stakeholders and experts invited by ENISA to an ad hoc working group. It is important that the required expertise (in risk assessment, CTI, definition of controls etc.) should be considered when selecting participants. Chapter 6 describes the setup and the workflow to be followed.

1.4 STATE OF THE WORK

The version of the proposed methodology described in this document contains all the features and functions which are necessary for an application in the context of drafting a sectoral cybersecurity certification scheme. The methodology relies as far as possible on standards and proven concepts. However, some parts were developed specifically for this methodology and can be seen as innovations.

The practicality of the SCSA Methodology and its applicability in the area of 5G was evaluated in a dedicated pilot project. Respective improvements and enhancements have been added to this version.

1.4.1 Potential future steps

The sample list of security controls could be enhanced to cover more control objectives and more technical or organizational controls. In addition, the practicality of the methodology could be significantly increased by the development of methods to assign controls to a specific common security level (CSL, cf. Section 5.5) and to estimate the overall CSL resulting from a concatenation of controls.

The new methods for identifying the potential of attackers specified in Chapter 9 should be consolidated after their first practical implementation.

2. DEFINITIONS AND ABBREVIATIONS

2.1 DEFINITION OF TERMS

Generally, the definitions of terms as given in the regulatory documents and references listed in Chapter 3 apply in this report. However, terms given in the CSA have the highest priority. This section provides definitions for terms which are not included in those normative references or which are of special relevance for the methodology described in this report.

Asset: Anything related to information security that has value to the sectoral ecosystem.

Note 1 to entry: Two kinds of information security related assets can be distinguished:

- the primary assets:
  - business processes & activities
  - functional assets
  - information assets.
- the supporting assets (on which the primary assets rely) of all types:
  - ICT system
  - hardware component
  - software component
  - network infrastructure
  - personnel
  - site
  - organization's structure.

Note 2: Primary assets are critical to the achievement of business objectives.

Assurance level: Basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but, as such, does not measure the security of the ICT product, ICT service or ICT process concerned (cf. CSA, article 2.22).

Attack scenario: Description of an attack, including attacker types, considerations of attacker objectives, attack potential, motivation and the primary asset and supporting assets potentially targeted by the attack.

Horizontal: Adjective indicating that an ICT product, ICT process or ICT service targets multiple markets and that the related cybersecurity certificate may be recognized by corresponding cybersecurity certification schemes of these targeted markets.

ICT process: Set of activities performed to design, develop, deliver or maintain an ICT product or ICT service (cf. CSA).

ICT product:	Element or a group of elements of a network or information system (cf. CSA).
ICT service:	Service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems (cf. CSA).
ICT system:	Network or information system (cf. CSA); combination of ICT products and ICT processes that supports one or more ICT services.
Risk scenario:	Description of a potential event or incident that could have a negative impact on one or more stakeholder objectives. NOTE: The risk scenario defines a particular combination of parameters that define the incident. These include, primarily, a stakeholder objective related to a specific business process and a primary asset in which ICT security is essential for this stakeholder objective. In addition, the related stakeholder requirements, supporting assets as well as relevant attacker information and attack scenarios are included.

2.2 ABBREVIATIONS

AP	Attack potential
APL	Attack potential level
AVA_VAN	Assurance family defined by ISO/IEC 15408-3; addresses the vulnerability analysis
CAR	Common assurance reference
CC	Common Criteria
CSA	European Union Cybersecurity Act
CSL	Common security level
CTI	Cyberthreat intelligence
EAL	Evaluation assurance level as defined in ISO/IEC 15408
EUCC	European Union Common Criteria cybersecurity certification scheme
IC	Impact class
ICT	Information and communication technology
IoT	Internet of things
ISAC	Intelligence sharing and analysis centre

ISMS	Information security management system as defined in the ISO/IEC 270xx series of standards
MRC	Meta-risk class
OSP	Organizational security policies
PP	Protection profile
SAR	Security assurance requirements
SCSA	Sectoral cybersecurity assessment
SCSAM	Sectoral cybersecurity assessment methodology
SFR	Security functional requirements
SPD	Security problem definition
ST	Security target as defined in ISO/IEC 15408-1
TOE	Target of evaluation as defined in ISO/IEC 15408
TSF	Target of evaluation security functionality
TTP	Techniques, tactics and procedures

2.3 OVERVIEW OF DIVERGING USES OF TERMS

The normative references for the methodology described in this document use certain terms in the context of different concepts and with different meanings. The following table provides an overview of those terms, provides a short interpretation of the meaning of each term for each normative reference and explains how the term is used in the context of this document. The conceptual considerations that lead to the interpretation of meanings concerning ISO/IEC 270xx and ISO/IEC 15408 are documented in Annex A.

Cyber threat intelligence (CTI) is currently not covered by specific standards and typically uses ISO/IEC 270xx as a basis for the definition of the terms it uses. The following table shows, in some cases, a CTI-specific use of terms. However, when no statement for CTI is provided, it can be assumed that the use of a term in CTI follows ISO/IEC 270xx.

Basic term	Meaning in the CSA	Meaning in ISO/IEC 27000:2018	Meaning ISO/IEC 15408-1:2014	Meaning in Cyberthreat intelligence (CTI)
Attacker	Term not defined but used in CSA, Art. 52.7 providing a description of evaluation activities relevant to assurance level 'high'. One such activity is: (..) *an assessment of their resistance to skilled attackers, using penetration testing.*	Term not defined but used to characterize the factors of a risk: *— for deliberate threat sources: the motivation and capabilities, which change over time, and resources available to possible **attackers**, as well as the perception of attractiveness and vulnerability of assets for a possible **attacker*** [ISO/IEC 27005, Clause 8.3.3].	Term not defined but used (see 'attack potential' below). 'Threat agent' is defined as *entity that can adversely act on assets.* Both terms are used in similar context but the meaning of 'threat agent' is broader. It can be a hacker, user, computer process, and accident (see Annex A).	Attacker and adversary are used synonymously.
Remarks on the use of term 'attacker'	In this document, the term means an actor or actors who could potentially perform an attack. The terms 'attacker', 'adversary' and 'threat agent' are used synonymously. The CSA and ISO/IEC15408-1 use this term in the context of evaluation, assessing the resistance of the ICT product against skilled attacks, while ISO/IEC 27000 considers it as a source for influencing risk.			
Attack potential	Term not defined nor used.	Term not defined but indirectly used when analysing deliberate threat sources (see 'attacker') for the purposes of risk assessment.	Attack potential – term defined as *measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation*.	Attack potential is characterized by the opportunity, means and motivation of the attacker.
Remarks on the use of term 'attack potential'	CTI uses three factors to describe an attack potential: motives, means and opportunities. This document follows the use of the term introduced by CTI as necessary to conduct risk assessment in sectoral schemes. ISO/IEC 15408-1 and ISO/IEC 18045 use the term to describe the level of effort evaluators are obliged to use in performing vulnerability assessments. In this context there are five factors that characterize an attack potential: *Elapsed Time*, *Window of Opportunity, Specialist Expertise*, *Knowledge of the TOE, IT hardware/software or other equipment*. In addition, ISO/IEC 18045 provides classifications for each factor and provides a scale for the calculation of the potential value of a particular attack. (See below and Subsection 5.6.5.)			
Attack potential (means)	n/a	n/a	***IT hardware/software or other equipment*** refers to the equipment required to identify or exploit a vulnerability.	Capability and Resources: access to vulnerabilities, exploits, tooling, and financial means necessary to conduct attacks.
Attack potential (skills)	n/a	n/a	**Expertise**: refers to the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows). **Knowledge of TOE**: is a specific expertise with respect to the TOE that goes beyond generic knowledge	Skill: knowledge and expertise to conceptualize and realize a particular attack.

Basic term	Meaning in the CSA	Meaning in ISO/IEC 27000:2018	Meaning ISO/IEC 15408-1:2014	Meaning in Cyberthreat intelligence (CTI)
Attack potential (opportunity)	n/a	n/a	**Elapsed Time**: is the total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to mount the attack against the TOE. **Window of Opportunity**: related to the Elapsed Time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to a TOE that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the TOE to exploit. Access may also need to be continuous, or over a number of sessions.	Opportunity: Possibility of the adversary getting access to the system or artifact, presence of exploitable vulnerabilities.
Control	Control – term used in CSA, Art. 52.4: *The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including **technical controls**, the purpose of which is to decrease the risk of, or to prevent, cybersecurity incidents.*	Control - term defined as a *measure that is modifying risk*.	Control – term not defined but used in relation to 'security': *(…) it is recognised that significant security can often be achieved through or supported by administrative measures such as organisational, personnel, physical, and procedural controls*.	
Remarks on the use of the term 'control'	In this document the term means a measure to decrease risk or to prevent cybersecurity incidents. It should be noted that ISO/IEC 27000 uses the term 'control' in direct relation to 'objective' and to 'risk', while in ISO/IEC 15408 it is related to 'security'. CSA understands 'technical control' as a measure for decreasing the risk, which is similar to ISO/IEC 27000.			
Objective	security objective – term not defined but used with reference to requirements set up by cybersecurity certification schemes (CSA, Art. 51): *A European cybersecurity certification scheme shall be designed to achieve, as applicable,*	control objective – term defined as *statement describing what is to be achieved as a result of implementing controls.*	security objective – term defined as *statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions*.	

Basic term	Meaning in the CSA	Meaning in ISO/IEC 27000:2018	Meaning ISO/IEC 15408-1:2014	Meaning in Cyberthreat intelligence (CTI)
	at least the following security objectives (..).			
Remarks on the use of the term 'objective'	In this document, the term is generally used in its common dictionary meaning. If a specific context of risk management is concerned ISO/IEC 270xx is followed. The use in the CSA is different from the referenced standards where the meaning is related to what is to be achieved by implementing controls (ISO/IEC 270xx) or security functionality (ISO/IEC 15408). The CSA understands 'security objectives' as 'high-level security requirements'.			
Process	[ICT] process – term defined as *set of activities performed to design, develop, deliver or maintain an ICT product or ICT service*.	Process – term defined as *set of interrelated or interacting activities which transforms inputs into outputs.*	Process – term not defined and used with its common meaning.	
Remarks on the use of term 'process'	In this document, the definition provided by the CSA is used. Both CSA and ISO/IEC 270xx consider 'ICT service' as a subject of certification. It should be noted that ISO/IEC 15408 does not present a process-oriented approach.			
Product	[ICT] product – term defined as *an element or a group of elements of a network or information system.*	product – term not used	[IT] product – term not defined but used with its common meaning. In the context of evaluation, ISO/IEC 15408 establishes an important distinction between an IT product and a TOE (Target of Evaluation): *The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these*.	
Remarks on the use of term 'product'	In this document the definition provided by CSA is used. It should be noted that the CSA is very general when speaking of certification / evaluation with regards to ICT products. Existing schemes based on ISO/IEC 15408/ISO/IEC 18045 allow certification of Protection Profiles that relate to types of ICT products, not specific ones**.**			

Basic term	Meaning in the CSA	Meaning in ISO/IEC 27000:2018	Meaning ISO/IEC 15408-1:2014	Meaning in Cyberthreat intelligence (CTI)
Requirement	[security] requirement – term not defined but used in the context of conformity assessment performed against the technical specification that contains such requirements (see CSA, Art. 46.2): *(..) to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified* ***security requirements*** *for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services (..).*	requirement – term defined as *need or expectation that is stated, generally implied or obligatory.*	[security] requirement – term defined as *requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE [Target of Evaluation].*	
Remarks on the use of term 'requirement'	In this document the term follows the definition given in ISO/IEC 270xx. It should be noted that this term is used in similar ways in the referenced documents – all lead to establishing relationships between 'conformity' and 'requirement', although ISO/IEC 15408 uses this term in a narrow technical context. Further, it should be underlined that ISO/IEC 270xx defines 'conformity' as 'fulfilment of a requirement' and considers 'conformance' used in ISO/IEC 15408 as a synonym. Finally, ISO/IEC 15408 uses 'requirement' with a direct relationship to 'objectives'.			
Service	[ICT] service – term defined as *Service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.*	Service – term not defined and used with its technical meaning to describe relationships between various elements of an information system; additionally, it is used to describe business relationships in the ISMS (for example an organization's relationship with a service provider); providing services can be included in the scope of the ISMS.	Service – term not defined and used only with its technical meaning to describe relationships between elements/ components of the information system.	
Remarks on the use of term 'service'.	In this document the use of this term follows CSA. Both CSA and ISO/IEC 270xx consider 'ICT service' as a subject of certification.			

Basic term	Meaning in the CSA	Meaning in ISO/IEC 27000:2018	Meaning ISO/IEC 15408-1:2014	Meaning in Cyberthreat intelligence (CTI)
Security	[cyber] security - term defined as: *activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyberthreats*.	[information] security – term defined as *preservation of confidentiality, integrity and availability of information.*	security – term not defined but considered as a fundamental concept with many characteristics, for example: security attribute, security problem, security requirement, security functionality.	
Remarks on the use of term 'security'	'Security' in the CSA means 'activities', while in referenced standards 'security' is considered as a state for the object described (a security attribute that can be lost – loss of confidentiality, integrity of availability). It is to be noted that ISO/IEC 15408 defines 'secure state' as *state in which the TSF [Target of Evaluation Security Functionality] data are consistent and the TSF continues correct enforcement of the SFRs [Security Functional Requirements].* In this document the term is used in both meanings, i. e. describing the state or the activities, depending on the context.			

3. REGULATORY DOCUMENTS AND REFERENCES

The following regulatory documents are binding for the methodology described in this document:

Regulatory documents	Short name	Source
Cybersecurity Act REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)	CSA	European Union

The following standards serve as references for the described methodology:

References	Short name	Source
ISO/IEC 15408 series of standards (including ISO/IEC 18045)	ISO/IEC 15408	ISO/IEC
ISO/IEC 27000 series of standards (in particular ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005)	ISO/IEC 270xx	ISO/IEC

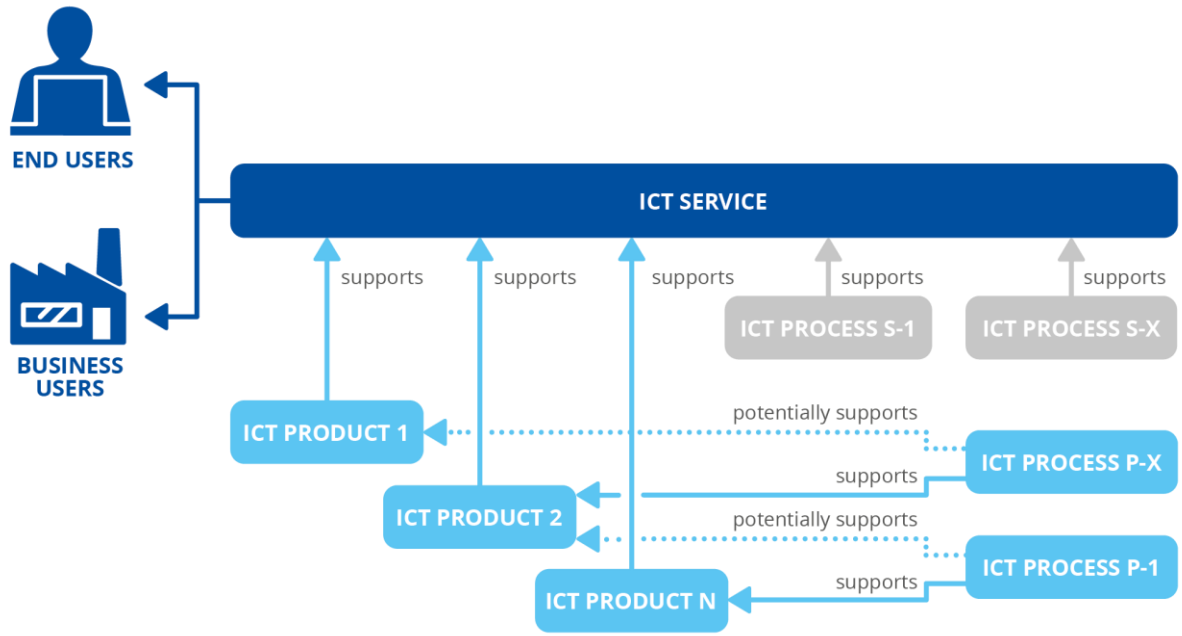
Since the meaning of terms may diverge between aforementioned regulatory documents and references, there is a comparison of such terms in Section 2.3. The definition of terms given in the regulatory documents is binding for this methodology.

4. INTRODUCTION TO SECTORAL SYSTEMS AND CYBERSECURITY CERTIFICATION SCHEMES

4.1 SECTORAL SYSTEMS IN THE CONTEXT OF THE CSA

The CSA defines and distinguishes between ICT products, ICT processes and ICT services. The relationships between these elements can be visualized as follows:

Figure 1: CSA-defined elements and their relations



The CSA stipulates that an ICT service is supported by ICT products and ICT processes. This combination of ICT products and ICT processes that support an ICT service is called an ICT service system or, in brief, an 'ICT system'.

In addition, there are ICT processes that support ICT products, for example product development processes. These are usually different from those that support ICT services.

Typically, there is a coordinated use of several ICT products to support all product-based functions needed for the implementation and operation of the ICT service. The specification of this coordinated use of several ICT products is called the *system architecture*.

It should be noted that ICT processes are also able to use ICT products.

With a view to conducting risk assessment, evaluation and certification, it is necessary to distinguish between the following layers of an ICT system:

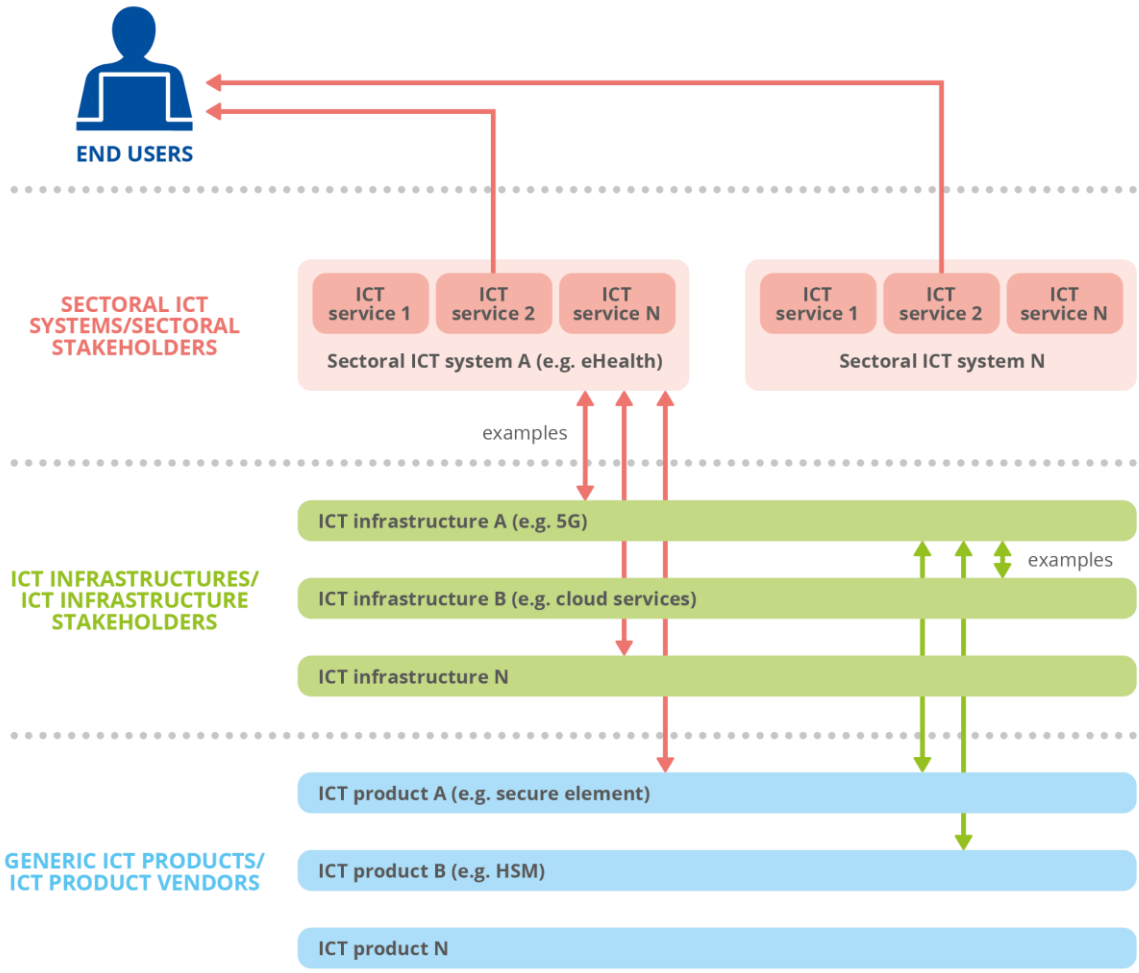
1. **ICT Infrastructures**
   ICT infrastructures serve several markets, applications and end-user services. Examples are mobile networks, cloud services and payment or ID services if these can be integrated into sectoral ICT systems. ICT infrastructures could also be regarded as providing ICT services to the owners of the sectoral ICT systems they support. From a business perspective, this could be seen as a relationship between unrelated organizations in the roles of an ICT infrastructure service provider and a business user.

2. **Sectoral ICT Systems**
   Sectoral systems include all functions that are specific to the provision of services to a particular market sector targeted at end-users. Sectoral ICT systems usually rely on ICT infrastructure services for specific functions. Whenever security-relevant functions of a sectoral ICT system depend on external ICT services, these are regarded as ICT infrastructure services.

Combinations of ICT infrastructures and sectoral ICT systems are common. For example in 5G, payment and ID services are typically both integrated by sectoral systems and offer ICT services to end-users. Both infrastructures and sectoral ICT systems combine ICT products and ICT processes as defined in the CSA. The following picture shows the characteristic relationships between:

- sectoral ICT systems, which support one or more sectoral ICT services,
- ICT infrastructures, which potentially provide ICT infrastructure services to support sectoral ICT systems, and
- ICT products, which may be used in both, sectoral ICT systems and ICT infrastructures.

Figure 2: Relations between system architecture levels



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 ICT system but also the allocation of responsibilities within them, since the owners of each of the building blocks must carry out risk assessments, implement appropriate controls, and support evaluation and certification at their level.

This consideration leads to an important difference between ICT infrastructures and ICT products: the definition, implementation and operation of ICT infrastructures is the responsibility of the stakeholders in an ICT infrastructure. In contrast, responsibility for the integration and operation of an ICT product in accordance with its intended use is with the entities that purchase the ICT product, i.e. the stakeholders of ICT infrastructures or sectoral ICT systems. The vendor is responsible for evaluation and certification of ICT products.

4.2 RISK-BASED DEFINITION OF SECURITY AND ASSURANCE ACROSS ARCHITECTURE LEVELS

The structure and relationships between the building blocks of an ICT service system, as defined in the previous section, provide the basis for risk-based identification of security and assurance requirements at all levels.

The basic relationships are as follows:

1. The sectoral stakeholders should identify the security and assurance requirements to the sectoral ICT system and the supporting ICT infrastructures and ICT products based on a risk assessment from the perspective of the targeted sectoral ICT services.

2. ICT infrastructure stakeholders should consider these sectoral requirements when defining the security and assurance of their ICT infrastructure and confirming the compliance of their ICT services to the owners of sectoral ICT systems in service level agreements.

3. Security and assurance requirements from all supported sectors must therefore be considered when ICT infrastructures and their ICT services, ICT products and ICT processes are being implemented.

4. ICT products and processes, which are employed by sectoral ICT systems or ICT infrastructures, must comply with the stipulated requirements covering their intended use in all environments where they are targeted for deployment.

5. All stipulated requirements made by the targeted sectoral ICT systems or ICT infrastructures should be consolidated and included in the definition of the security problem, the security functional requirements and security assurance requirements of the ICT product.

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

Risk assessments must also be carried out for ICT infrastructure services and systems.

Section 4.4 will provide more detail on how cybersecurity certification schemes for sectoral ICT systems and ICT infrastructures should be prepared and implemented.

4.3 INTRODUCTION TO SECTORAL ICT SYSTEMS

4.3.1 Properties of sectoral ICT systems

Subsection 4.1 introduced definitions for the terms ICT system, sectoral ICT system and ICT infrastructure and described the relationships between these building blocks of an ICT service system, both amongst each other and in relation to the terms defined by the CSA.

The following properties characterize a sectoral ICT system:

- Sectoral systems support one or more ICT services, which are offered by the sectoral ICT service provider(s) to end-users.

- A potentially large number of stakeholders, in several well-defined roles with dedicated responsibilities and functions, cooperate in the implementation and operation of these sectoral ICT services. Typically, it is the responsibility of these stakeholders to operate their own ICT processes and ICT products, which could be seen as ICT subsystems of the sectoral ICT system.

- Frequently several sectoral stakeholders participate in the same role (e.g. mobile network operators or health insurance companies). These stakeholders may be in competition.

4.3.2 Typical system architecture of sectoral ICT systems

As described in Subsection 4.1, sectoral ICT systems typically use ICT infrastructures and generic ICT products for defined functions that are required for the implementation and operation of sectoral ICT services. **Figure 2** shows the relation between the sectoral ICT system and these underlying layers of the overall system architecture.

Usually, the system architecture of a sectoral ICT system consists of numerous ICT subsystems, which are owned, operated and maintained by individual sectoral stakeholder organizations. These ICT subsystems are interconnected as specified by the architecture of the sectoral ICT system and act as required in support of the sectoral portfolio of ICT services.

4.3.3 Coordination of sectoral activities

The implementation and operation of sectoral ICT systems needs a common understanding between all stakeholders concerning the supported portfolio of ICT services. This understanding must comprise a common set of objectives and rules, common specifications and processes that govern the interactions between the various stakeholders and their ICT systems, as well as a common view on risks and the appropriate levels of security and assurance. This requires a dedicated organization or structure that provides such guidance to and the coordination of all parties involved in the sectoral ICT system.

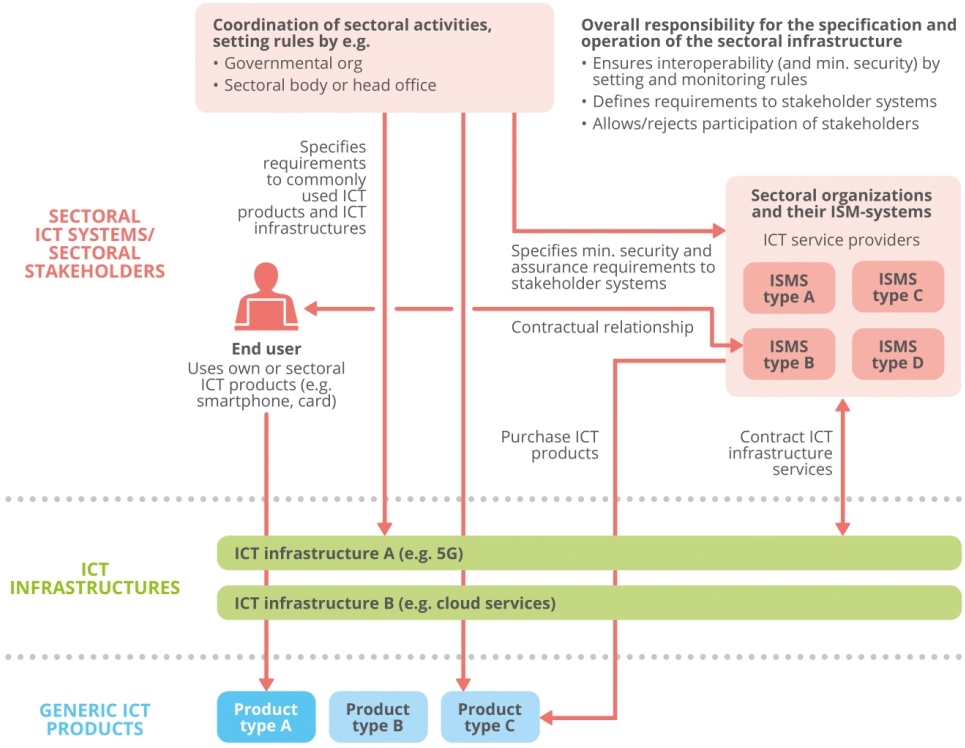
A typical objective of sectoral ICT systems is to support ICT services on a national scale or even throughout the EU internal market. This would probably require cooperation between numerous sectoral stakeholders from the targeted areas and demand coordination of their technical and operational activities. However, such coordination is also likely to support societal goals such as non-discriminatory access for all interested stakeholder organizations, vendors and users, fostering competing offers and avoiding misuse of market power, as well as meeting the needs for privacy and data protection.

In practice, such coordination functions could be established by a combination of governmental rules, which set the boundary conditions for protecting societal goals and by implementing a sectoral organization, which conducts the day-to-day coordination work within these boundaries.

There are examples of governmental institutions or organizations that have been established by sectoral stakeholders to coordinate and guide the activities of ICT services in sectors such as health, ID and mobility. Similar coordinating entities also exist in ICT infrastructures such as mobile networks or payment schemes.

Figure 3 visualizes the relations between the coordinating entity, the sectoral stakeholder organizations, the end-users and the ICT infrastructure service and ICT product suppliers.

Figure 3: High-level roles in sectoral ICT systems



Typical responsibilities and activities of the individual roles in a sectoral ICT system are given below:

1. The coordinating entity defines rules for the participation of stakeholder organizations in the sectoral ICT system. Such rules may require, for example, functional and security certification of the ICT subsystems or ICT products as a precondition for participating in or operating the ICT system.

2. The coordinating entity specifies the sectoral ICT services to be provided and which ICT infrastructure services, ICT products and ICT processes are to be commonly used, as well as specifying details of their functions, security and assurance levels. The sectoral stakeholders must comply with these specifications for their own ICT operations and will reference these sectoral specifications when ordering ICT infrastructure services or when purchasing ICT products.

3. Typically, sectoral systems are organized in such a way that end-users of sectoral ICT services have a contractual relationship (service level agreement) with the 'ICT service provider' or the 'ICT service retailer'. These end-users may be equipped with ICT products such as smartcards by their sectoral contract partner or they may be entitled to use a

sectoral application on their smartphone. Such '3rd party ICT product'-scenarios must also be addressed by the functional and security specifications of the sector.

Interestingly, it is quite common for ICT infrastructures to both support sectoral organizations as business users and to offer ICT services to end-users. A typical case would be a mobile network, which could be seen as providing both ICT infrastructure services and end-user services.

4.4 CYBERSECURITY CERTIFICATION OF SECTORAL ICT SYSTEMS

4.4.1 Considerations from the architectural point of view

From the perspective of cybersecurity evaluation and certification it is important to note that the sectoral ICT system as well as the stakeholder's ICT subsystems can be quite complex. In addition, the implementation of the required functions can vary significantly from stakeholder organization to stakeholder organization. This applies in particular if sectoral ICT systems arise from a newly established cooperation between stakeholder organizations, with the resulting integration of the stakeholder organization's incumbent ICT subsystems. Such complexity and diversity usually prohibit the definition of a clear-cut protection profile as used for ICT products and required for product certification.

Instead, the implementation and certification of ICT security at both the sectoral layer and the stakeholder organization's ICT subsystems is usually based on the standards of information security management systems such as ISO/IEC 27001 and related certifications. These provide a proven and practical approach to system security and are well established in many sectors. However, they do not support the concept of defined assurance levels as provided by ISO/IEC 15408 for ICT products. A consistent implementation of security and assurance requirements across all ICT subsystems of sectoral stakeholder organization's which use an ISMS would be hard to support, based on the current status of the standard. This limitation must be considered when defining the security architecture and the certification concept of a sectoral ICT system.

In a typical sectoral ICT system, the ISMS-based approach to ICT security and certification covers processes at the level of the sectoral ICT subsystems, which use the bulk of ICT products and ICT processes within a sectoral ICT system. ICT product certification is mainly used for ICT products, which support critical functions of the sectoral ICT system and require a defined level of security and assurance.

Consequently, cybersecurity evaluation and certification in sectoral ICT systems and their supported ICT services is typically a combination of ICT product, ICT process and ISMS certification.

4.4.2 Enabling the recognition and reuse of certificates

The recognition and reuse of certificates that have been granted by horizontal cybersecurity certification schemes to ICT infrastructure services, ICT products or ICT processes is a prerequisite for the practicability and economic viability of sectoral cyber security certification schemes and should be a central goal in their definition. This should include certificates from cybersecurity certification schemes under the EU cybersecurity framework and potentially also from other schemes that are relevant in the particular market sector.

The following prerequisites must be in in place to enable the necessary synergies with horizontal cybersecurity certification schemes:

1. **Compliance with sectoral requirements**
   The certified ICT infrastructure service, ICT product or ICT process must conform to the functional, security and assurance requirements as stipulated by the sectoral ICT system. Section 4.2 documents how these requirements should be defined based on a risk assessment that takes the perspective of the targeted sectoral ICT services as its starting point.

   The sectoral cybersecurity certification scheme should support processes that communicate these requirements, including all relevant information on the 'intended use', to the relevant suppliers and their certification schemes. There should also be a means to allow the identification of suitable certified ICT infrastructure services, ICT products or ICT processes, which are already available in the market. Also required is a process that evaluates other certification schemes for their compliance with the sectoral requirements for cybersecurity certification.

2. **Consistent definition of risk, security and assurance**
   The reuse of certified ICT infrastructure services, ICT products or ICT processes requires that the definitions of security requirements and security levels as well as the definitions for assurance requirements and assurance levels are consistent and comparable across all relevant cybersecurity certification schemes, and that the methods used for evaluation are accepted by the sectoral scheme as appropriate for the defined levels. In addition, there needs to be a common understanding of the underlying risk. The definitions of generic risk classes should support a consistent and comparable approach to risk levels and risk acceptance criteria.

3. **Common terminology**
   The recognition and reuse of certificates requires that the sectoral ICT cybersecurity certification scheme and the schemes that are referenced use the same terminology and definitions, or that a commonly accepted means is available to translate those terms or definitions that are different.

4.4.3 Setup of sectoral cybersecurity certification schemes

The partitioning of a sectoral ICT system with regard to cybersecurity certification is to a large extent defined by internal roles and responsibilities within the sectoral ICT system. The stakeholder organizations are responsible for conducting cybersecurity certification for their own ICT subsystems. They have to ensure that ICT infrastructure services, ICT products and ICT processes they purchase from their suppliers comply with sectoral certification requirements. By this means, the totality of certificates provided by sectoral stakeholder organizations will address cybersecurity certification for the largest part, by far, of a sectoral ICT system.

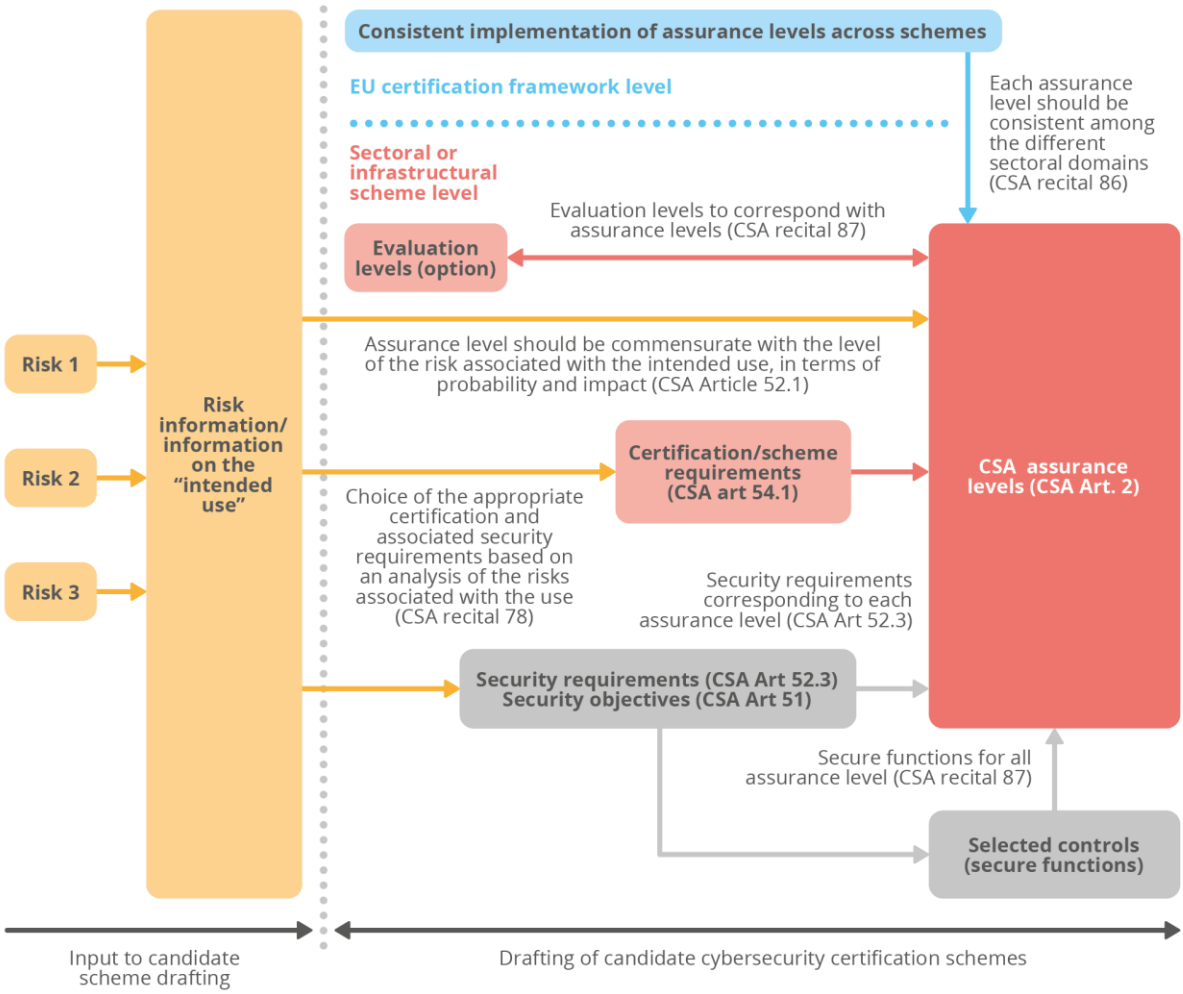
The definition of a sectoral cybersecurity certification scheme should try, as far as possible, to optimize practicality and economic efficiency by supporting the re-use of the ISMS-certifications that are the responsibility of the different sectoral stakeholder organizations, as well as the horizontal certifications for ICT infrastructure services, ICT processes and ICT products. By this means, the certification of a sectoral system would, to a large extent, build on all the certificates of underlying ICT subsystems, ICT services, ICT products and ICT processes. In an ideal case, only the evaluation and certification of those ICT processes and ICT products which are the responsibility of the sector's coordinating entity would need to be evaluated by the sectoral ICT scheme.

5. CONSISTENT DEFINITION OF RISK, SECURITY AND ASSURANCE

5.1 REQUIREMENTS AND OBJECTIVES

The CSA stipulates objectives, requirements and definitions as the basis of the definitions of risk, security and assurance and the relations between these. **Figure 4** illustrates the relationships between these elements, as documented in the CSA:

Figure 4: CSA-defined elements and their relations



The key requirements for cybersecurity certification schemes, drafted under the CSA, can be summarized as follows:

1. As known from ISO/IEC 15408, security and assurance are seen as distinct, independent objectives. However, the CSA introduces an association between assurance levels and security requirements as well as selected security functions.
2. Assurance levels should be implemented consistently across schemes.
3. The definitions of security and assurance requirements as well as assurance levels should be based on the risk associated with the intended use, in terms of probability and impact, of the respective ICT product, ICT process or ICT service.
4. The definition of methods and specifications shall as far as possible follow European and international standards.

Furthermore, the following conclusions can be deduced:

1. The definition of requirements for the security and assurance of ICT products, ICT processes or ICT services, based on risk, requires a preparatory step that documents the intended use of the ICT product, ICT process or ICT service and identifies the risk related to that use.
2. Risks related to the intended use of ICT products, ICT processes and infrastructural ICT services can only be determined in the context of the sector in which they are to be used. Consequently, relevant results of the risk assessment must be made available to suppliers and schemes that are responsible for the development and certification of these ICT products, ICT processes and infrastructural ICT services.

5.2 CONCEPTUAL APPROACH FOR THE CONSISTENT DEFINITION OF RISK, SECURITY AND ASSURANCE

5.2.1 Introduction and principles

The SCSA Methodology, which is documented in the following sections, is in compliance with the requirements mentioned in the previous sections and supports a practical and sound approach for the identification of risk and the definition of security and assurance to be used in the drafting of sectoral or infrastructural candidate cybersecurity certification schemes.

A. **Integration into the workflow for drafting sectoral schemes**
   This sectoral assessment methodology should be integrated into the workflow for sectoral schemes as a preparatory activity in drafting the candidate scheme. This puts in place the following boundary conditions and requirements for a consistent methodology for risk, security and assurance:

   1. The methodology must be applied in the preparatory phases of drafting sectoral candidate schemes for the EU cybersecurity certification framework.

   2. The methodology should be able to take advantage of risk assessment methods already in use by sectors or infrastructures. Consequently, the methodology does not define a specific risk assessment approach; assuming that existing risk assessment methods will conform to the ISO/IEC 270xx series of ISMS-standards. Definitions used by the targeted methodology regards the series of ISO/IEC 270xx standards as normative references and focuses on enhancements whenever necessary. Deviations from these standards are not permitted.

3. Cyberthreat Intelligence (CTI) shall contribute to the identification of risk and to the estimation of the capabilities of potential types of adversaries. Existing methods for CTI and available information sources such as ENISA's threat landscape shall be re-used.

B. **Balancing flexibility and consistency**

The CSA acknowledges that the design of cybersecurity certification schemes needs flexibility to adapt to the requirements of a specific sector or class of ICT products, ICT processes or ICT services. However, the need for flexibility potentially conflicts with the objective of implementing assurance levels consistently across schemes, which is a prerequisite for the recognition and re-use of certificates within cybersecurity certification schemes under the CSA.

Taking into account the CSA's requirements concerning relationships between risk, security and assurance, it can be concluded that the following concept can be adduced in support of an appropriate balance between flexibility and consistency:

1. Assurance levels, risk and security, and the relations between these, should be firmly defined. These definitions should be applied to any sectoral or infrastructural cybersecurity certification schemes under the CSA. This will provide the consistency required for the definition of ICT products, ICT products and infrastructural ICT services, which are designed for use in several sectors. It will also allow the re-use and recognition of certificates.

2. Differing sectoral views concerning risk tolerance or appetite can be accommodated during risk assessment. The result of allowing this flexibility would mean that sectors could rate a comparable risk differently, thus leading to different sectoral assurance and security requirements without affecting the goal of consistency. In addition, there should be the option to deviate from the relationships described in the previous paragraph, if the deviation is fully justified and well-documented.

Figure 5 illustrates this concept. It distinguishes between the sectoral risk assessment methodology used, which allows sectors their own specific view on risk, and the mapping of this assessed risk to so-called 'CSA meta-risk classes' (MRC). These MRCs provide a normalized definition of risk which should be used in all sectoral or infrastructural schemes. MRCs are the starting point for a firm definition of relations with assurance levels, security objectives and the level of controls related to these security objectives.

Figure 5: Conceptual approach for flexibility and consistency

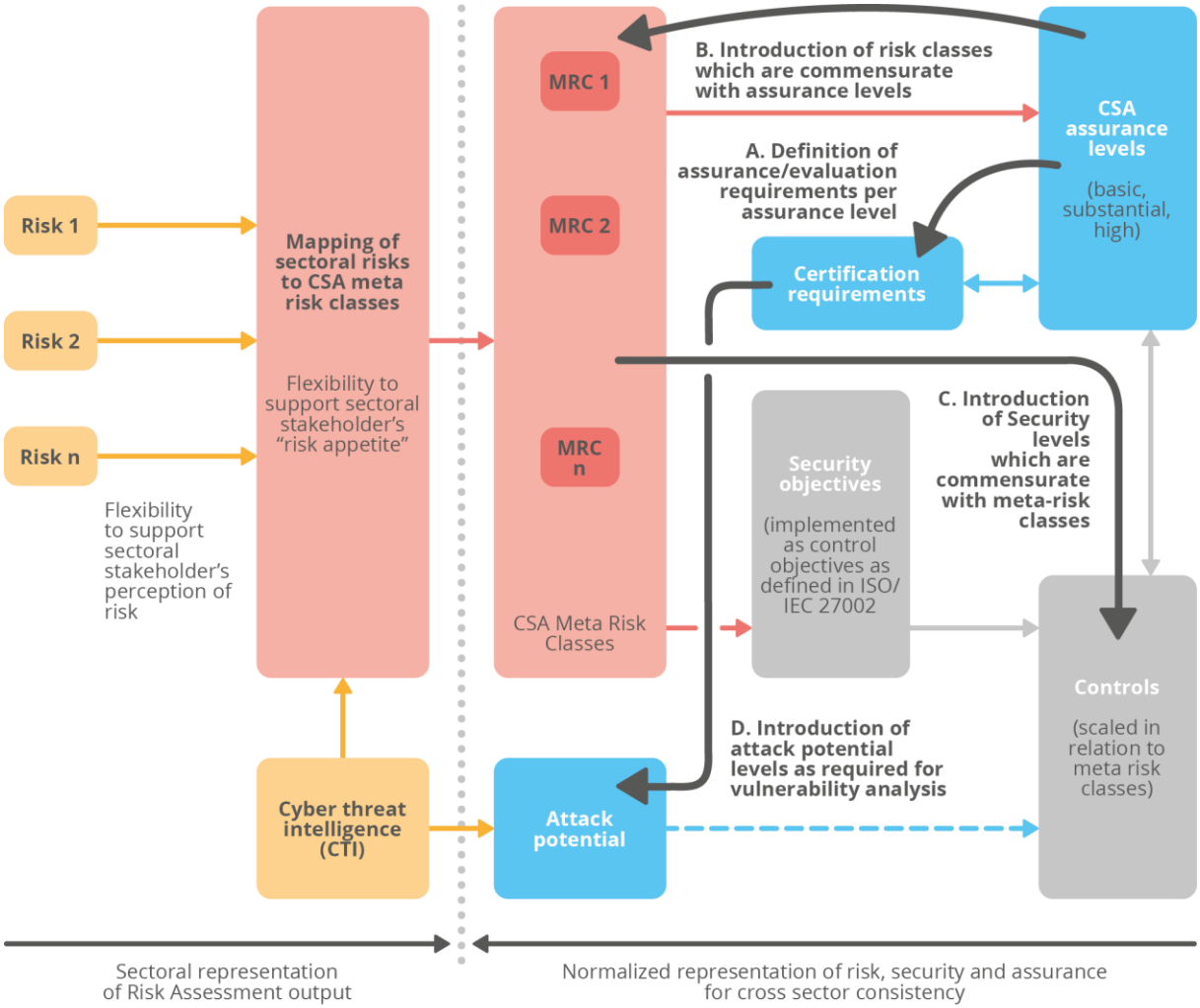


Figure 5 also shows the principles of how the CSA's requirements for consistency can be implemented by the methodology defined in this document. The individual steps are marked by the letters A to D.

A. A detailed definition of the assurance levels related to assurance requirements and evaluation specifications is a starting point for considerations under this methodology.

B. This step introduces a level structure for MRCs that corresponds with the defined assurance levels. This means that there is a defined relationship between a level of assurance and an MRC.

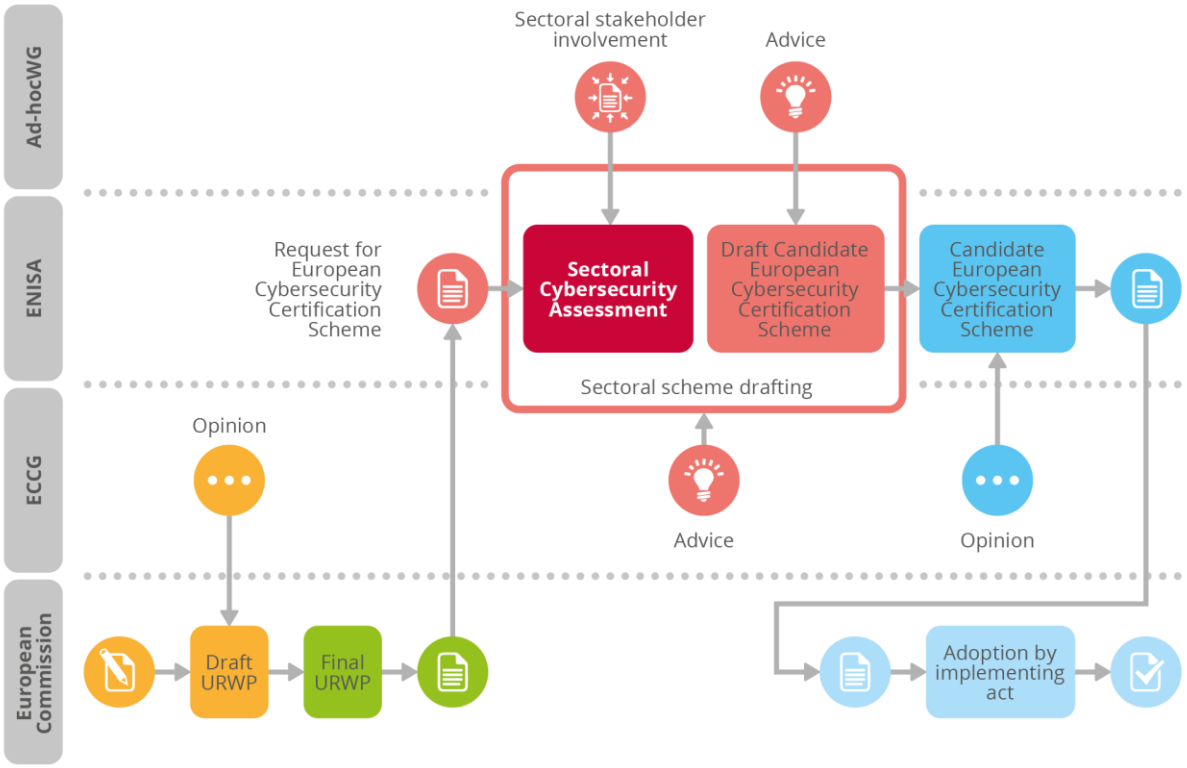
C. The CSA requests that specific controls should be related to particular assurance levels. Since MRCs are matched with assurance levels, this can be supported in a generic way by introducing a level structure for controls that matches the level structure for MRC.

D. The level structure for attack potential, which is used by the evaluator as part of his vulnerability analysis, should also be implemented in the CTI-based determination of attack potential.

5.2.2 Integration with the preparation of a cybersecurity certification scheme

The SCSA methodology can be integrated as a preparatory step into the workflow for drafting a cybersecurity certification scheme governed by the CSA as shown in Figure 6.

Figure 6: Application of the methodology in the context of drafting a sectoral cybersecurity scheme



The application of the methodology for the sectoral cybersecurity assessment should be conducted in workshops with the ad hoc working group.

All relevant sectoral stakeholder roles should be represented in the ad hoc working group.

In order to ensure transparency and continuity, all information and results generated by the sectoral assessment should be documented. Accurate documentation is particularly important where stakeholders decide to deviate from the default relationships defined by the concept for consistent implementation of security and assurance.

Special attention should be paid to the documentation of information from the sectoral level. This is needed by sectoral ISMS-owners and external suppliers of ICT products, ICT processes and ICT services in order to adapt these to the requirements of the sector.

5.2.3 Establishing the context for the sectoral cybersecurity assessment

As known from information security risk management according to ISO/IEC 27005, the application of the SCSA Methodology requires documentation of the context in which the sectoral cybersecurity assessment should be carried out. This includes all information that is of relevance for the assessment of risks and the definition of security and assurance requirements:

1. Description of the scope of the sectoral cybersecurity assessment,
2. Documentation of the sectoral stakeholder's roles and responsibilities and the business processes relevant for the defined scope,
3. Documentation of the sectoral stakeholder's objectives and requirements with regard to the documented business processes,
4. Description of the architecture of sectoral ICT subsystems or operational processes supporting the documented business processes,
5. Identification and documentation of primary information or functional assets supporting the business processes,
6. Identification of ICT subsystems, products, processes and services (supporting assets) supporting the primary information or functional assets,
7. Documentation of threat landscape and CTI information for the selected scope, in particular relevant attacker types, their potential objectives, motivation and attack potential level.

The detailed workflow for conducting context establishment is documented in Section 6.2.

5.2.4 Incorporating Cyberthreat Intelligence Information

As discussed in detail in Chapter 9, cyberthreat intelligence (CTI) provides further insights into the threat landscape, as well as a characterization of potential attackers that constitutes a crucial component of the SCSA Methodology.

Attackers can be characterized by the means, motives and the opportunities they have for launching an attack – as described in Chapter 9 and illustrated in figure 7. The portfolio of potential attackers, as well as their characteristics, have a major influence on the level of risk and the required levels of security and assurance of any ICT system as the following two examples may illustrate:

1. Even if the level of security of a control is high, it will be ineffective if it is lower than the level of attack capability that an adversary can bring to bear. This means that cyber risk and the choice of security controls directly depend on the potential that an attacker has to impact the ICT system while it is in use.
2. A sophisticated adversary with ambition to target a critical infrastructure sector, such as energy, will have not only the means to execute such an attack - for example being funded and staffed by a nation state – but is also likely to be able to develop sufficient opportunities to execute an attack with significant success.

Therefore, the assessment of risks, the security of a sectoral ICT system and its ICT products, ICT processes and ICT services and the need for assurance should be evaluated in the context of any adversary seeking to attack it.

In the methodology described in this document, different components of attack potential are considered and used as input at different stages of the assessment:

1. The motive of potential attackers and an estimate of their attack potential level form part of the determination of sectoral risks.
2. Attack potential and the means of the attackers as well as their opportunity to conduct attacks are used as input to determine the appropriate security and assurance levels for sectoral ICT systems, ICT processes and ICT products.
3. The potential of an attacker's means and opportunities guide the selection of suitable controls able to withstand an attack.

4. Attack potential[3] as defined by CTI should be seen in relation to its use as defined by ISO/IEC 18045 for ICT product evaluation. This would allow a confirmation of the targeted level of resistance against the CTI-defined attack potential by an evaluation.

These components and the relationship between attack potential and risk, security and assurance level are described in further detail in sections 5.3 through 5.6. Subsection 9.6 describes two new methods which support the estimation of the attack potential level.

5.2.5 Method for linking cybersecurity risks with security and assurance requirements

A major objective of the SCSA Methodology is to link the risk associated with the intended use of ICT systems, products, processes and services with the requirements for the certification, the security and the assurance of these components. This requires a dedicated method which is described in this subsection.

The assessment of cybersecurity risks is based on the relevant business processes and the sectoral stakeholders' related objectives that could be impacted by ICT security incidents. These considerations focus on business, governmental or societal views on the sectoral system and should reflect the sectoral role model and work split between stakeholders as described in Chapter 4.

In contrast, the definition of requirements for certification, security and assurance requires a technical and system architecture perspective. These requirements target sectoral ICT subsystems, products, processes and services that support the implementation of the relevant business processes at the sectoral system level, called 'supporting assets'.

The SCSA Methodology connects these two perspectives by introducing 'primary information assets' and 'primary functional assets' in the following way:

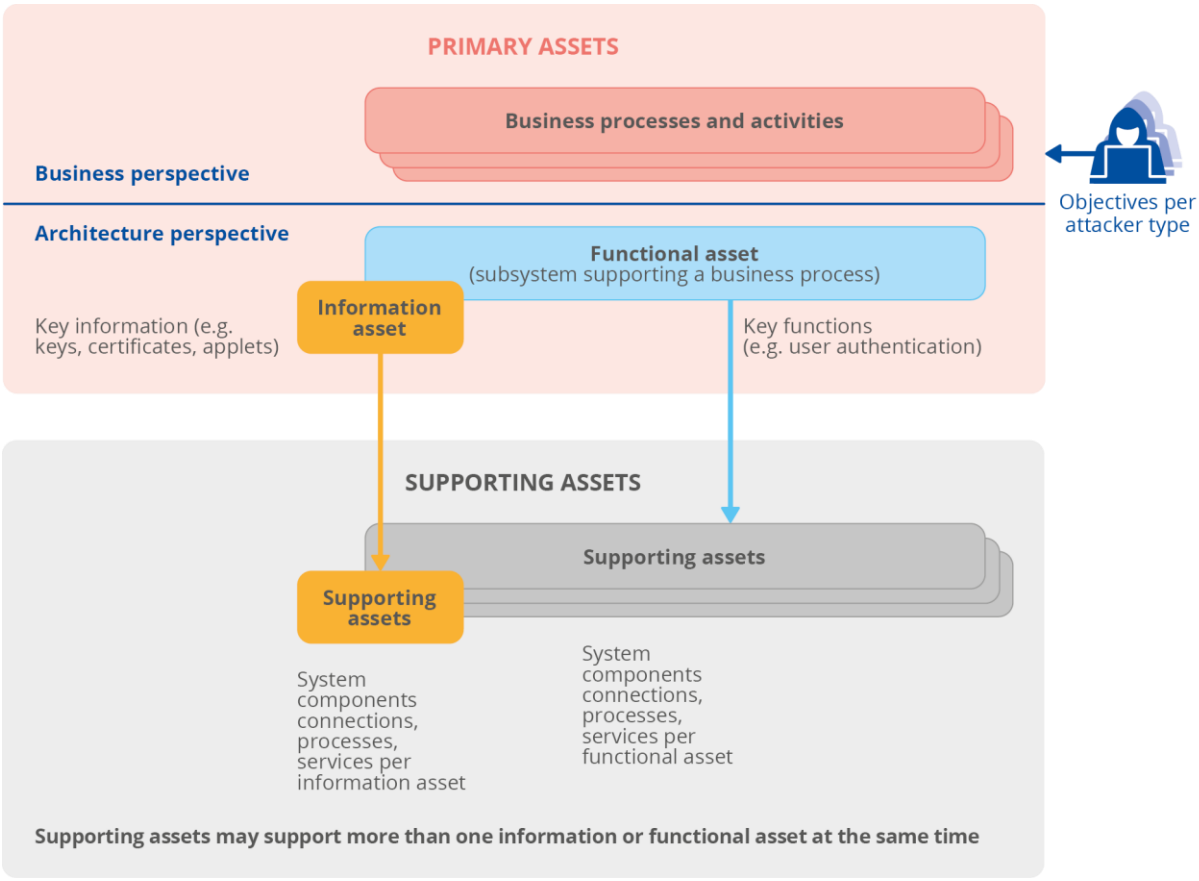
In line with the definition given in ISO/IEC 27005, these types of primary assets stand for information or functions which are of special relevance for the sectoral stakeholder's objectives. For both types of primary assets it is possible to document, on the one hand, the potential impact of a successful attack on the sectoral stakeholders' objectives and, on the other hand, to determine which 'supporting assets' of the sectoral architecture support and protect the particular information or function.

Information assets are essentially data (such as cryptographic keys, certificates, applets, personal data of customers or product configuration parameters) whereas functional assets are those that are directly deployed in the system as hardware or software in support of a primary activity (for example 'user authentication' or 'secure boot function').

Supporting assets are those that are deployed, as the name implies, to support the primary assets. They constitute the critical elements of the systems which enable the primary assets to support the business process efficiently and effectively. It is important to note that there is not necessarily a one-to-one relationship between supporting assets and primary assets; one supporting asset may be important to more than one primary asset. The relations between assets used by this method are presented in Figure 7.

[3] The meanings of the term in both areas are explained in section 2.3.

Figure 7: Relationships of assets and information security attributes



5.2.6 Introduction of risk scenarios

Subsection 5.2.5 describes the method for linking the business-related assessment of risks with the technical considerations on security and assurance requirements to single supporting assets. Subsection 5.2.4 documents that information on attackers, their motives and capacity has a major influence on the assessment of risks and the definition of the security and assurance requirements to ICT components or processes that serve as supporting assets.

In order to ensure consistency of considerations of risk, attack potential, security and assurance and to support reversibility when changing between the different perspectives described in Subsection 5.2.5, the parameters that are relevant for these considerations and their relationship have to be well defined.

Attackers follow their own objectives concerning the sectoral system which determine their attacks and their motivation for conducting attacks. Since these objectives could diverge significantly from the objectives of the sectoral stakeholders, it is not practical to deduce the impact on stakeholders' objectives or the probability that this impact will occur from the attacker's motivation and potential with regard to his own objectives. A solution has to be found for linking attacker information to considerations of the stakeholders' risks.

Assuming that it is very likely that an attack implementing the attacker's objectives would affect primary functional or primary information assets defined from the stakeholder's perspective, the SCSA Methodology selects also, in this case, the two types of primary assets described in Subsection 5.2.5 as linking elements. Based on an assumed attack scenario that involves a

primary asset, the impact on a stakeholder's objectives and the probability of such an incident occurring could be estimated.

The introduction of risk scenarios by the SCSA methodology implements this approach.

A risk scenario describes a potential event or incident that could have a negative impact on one or more business objectives. This description includes the documentation of the relevant parameters from the following domains:

Business perspective:	Targeted business process, involved stakeholders and their objectives and requirements concerning the targeted business process.
Architecture perspective:	Primary asset (information and functional) in relation to the targeted business process, supporting assets for the primary asset.
Attacker perspective:	Attacker types that may be capable and motivated to conduct attacks on the primary asset. All relevant information is summarized in attack scenarios which should be associated with the primary asset.

The identification of risk scenarios should be conducted in relation to a business process and a primary asset that is of relevance for the objectives of this business process. After this, an attack scenario which could potentially lead to an incident via an attack on the primary asset would be added.

Risk scenarios are assigned with a meta-risk class (MRC) based on impact and probability. A detailed description is given in Section 5.3.

5.2.7 Layered approach to sectoral cybersecurity assessment

Subsection 5.2.5 and Subsection 5.2.6 describe the method applied for linking the business, the architectural and the attacker perspectives on the sectoral system to enable a risk-based, consistent definition of security and assurance requirements. For this purpose, primary assets and risk scenarios have been introduced in Subsections 5.2.5 and 5.2.6 respectively.

Based on these considerations, the SCSA Methodology proposes to conduct the assessment of the following three layers in sequential steps:

1. **Assessment of business layer**
   Following the pattern set by the normative standard ISO/IEC 27005, the sectoral assessment will start at the business process layer. The relevant business processes and the business, governmental or societal objectives of the sectoral stakeholders with regard to these business processes should be documented. The identification of objectives should be discussed with the sectoral stakeholders and should be consolidated with regard to the risk areas given in Annex B.

   On this basis, the primary information and primary functional assets as well as the supporting assets can be identified. This step is considered part of the 'sectoral context establishment' described in Subsection 5.2.5.

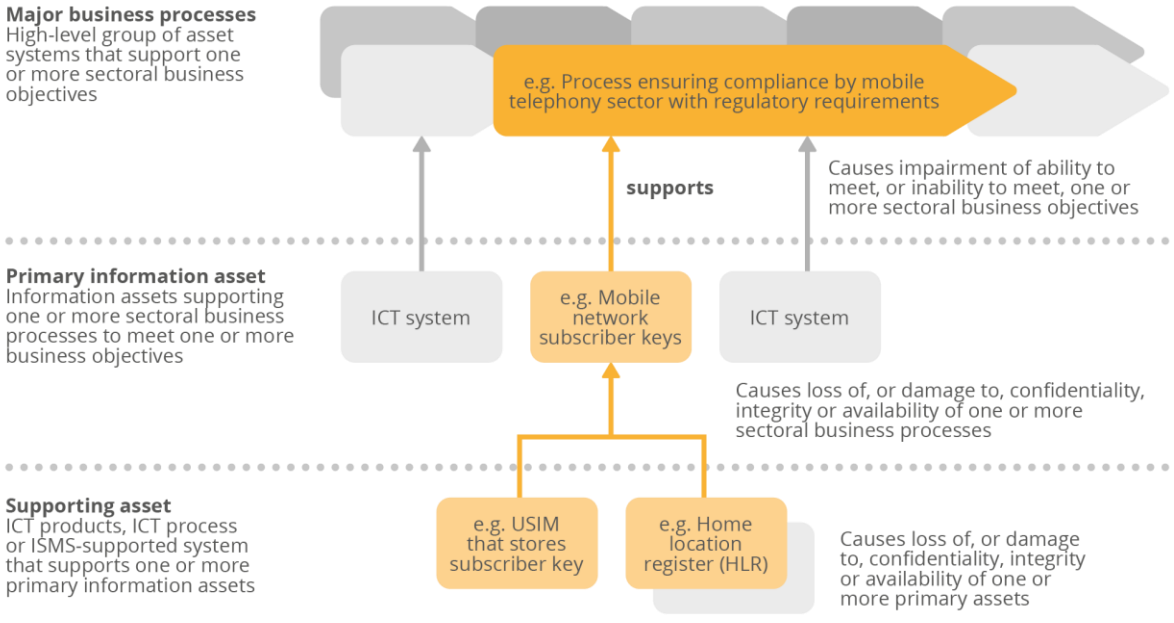
2. **Assessment of primary asset layer**
   In the second step, the potential impact on the stakeholder's objectives of successful attacks on primary assets and the probability that this impact may occur are estimated and

documented. Information from CTI on threats and attack potential is used to consolidate the stakeholders' estimate of an impact and the probability of a particular incident as described in Section 5.3. In addition, risk information provided by sectoral stakeholders or generated by any ISO/IEC 27005-conformant risk management tool can be included. All this is packaged by risk scenarios as described in Subsection 5.2.6. On this basis Meta-risk classes (MRC) can be assigned to the identified risk scenarios as described in Section 5.3. This MRC is inherited by all supporting assets associated with the risk scenario.

3. **Assessment of supporting assets**
   The third layer of the assessment targets the definition of the security and assurance requirements to ICT subsystems, products, services and processes that serve primary information and functional assets as supporting assets. The risk information, in particular the MRC, which applies to a particular supporting asset is inherited from the assessment of the primary information or functional asset which is supported by the supporting asset to be assessed. For the definition of the security and assurance requirements for the supporting asset, the MRC and the capacity of the relevant attacker types to conduct attacks, the attack potential level (APL) and also the intended use and the operational environment will be taken into account. The definition of APL and the method for determining the APL are described in Section 5.4. The methods for defining the required security and assurance levels in a risk-related and consistent way are described in Section 5.5 and Section 5.6.

Figure 8 visualizes the relationship between the business layer, the primary asset and the supporting assets for a mobile network as an example.

Figure 8: Example of the relationship between business, primary asset and supporting asset layer



The detailed workflows for conducting the context establishment and the assessment using the layered approach are documented in Chapter 6.

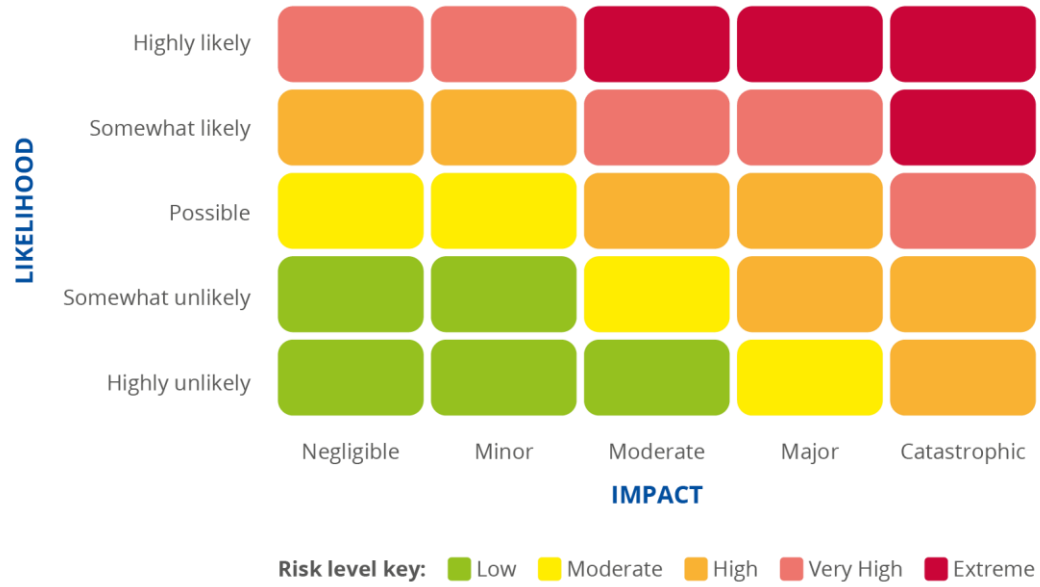
5.3 CSA META-RISK CLASSES – A COMMON APPROACH TO THE SCALING OF RISK

5.3.1 Introduction to sectoral risk assessment

Risk assessment is a prerequisite for the establishment of security and trust in ICT systems. Risk assessment enables risks to be understood and therefore correctly mitigated through the use of risk controls. Most modern information security and risk management standards therefore call for a risk-based approach to the selection of appropriate security controls.

The typical approach followed in an organizational information security management system (ISMS) is that the level of risk is assessed as a function of the impact (or consequences) of an event and the likelihood (probability) of it occurring. Although this approach enables the loss or damage as a result of an incident or event to be estimated, it is increasingly inaccurate where events have either (or both) a very low probability and the potential to cause a very high degree of impact.

Figure 9: Example of qualitative risk mapping in an ISMS based on ISO/IEC 31010



An example of using a qualitative method for risk assessment is illustrated in **Figure 9**. The criteria chosen by the organization are applied to all qualitative levels of likelihood and impact and the formula for risk estimation is given to achieve qualitative levels of risk expressed by appropriate names and colours.

To provide a consistent approach to certification and to ensure that certificates are comparable and consistent throughout a whole sector, it is necessary to base the considerations on comparable risk levels appropriate for that sector.

Sectoral risk assessments must be carried out at a high level for instance by the coordinating entity for the sector or by the developer of a sectoral cybersecurity certification scheme. Both would need to involve the relevant stakeholder roles from within the sector and its constituent organizations:

- The stakeholders and coordinating entity that are engaged in providing the sectoral services (‘business risk owners’).

- Consumers of sectoral services.
- Society generally, both at the European and international levels.
- Governmental risk owners.

According to the approach defined in Subsection 5.2.7, the sectoral risk assessment is carried out in the primary asset layer assessment. As described in the following subsections, CTI and attacker information will be used to improve the reliability of the estimations of impacts and their probability[4] compared to the classical approach described above.

Further, the SCSA Methodology implements the risk scenario approach (see Subsection 5.2.6) to support consistency and the reversibility of considerations on risk, attack potential, security and assurance that bridge all three levels of the sectoral assessment.

5.3.2 Attacker information as criteria for risk assessment

Section 5.2 describes the use of CTI and attacker information for sectoral assessment at a high level. This subsection explains how to apply attacker information to assess the risks and how to assign meta-risk classes when assessing the primary asset layer.

For the assessment of risks and the estimation of the MRC, the portfolio of possible adversaries and their attack potential should be considered, concentrating on their motives. If a sophisticated adversary, such as a nation-state actor, cyber terrorist or foreign military force has its own objectives and, based on these, a strong motivation to target a particular sectoral system, we have to assume that the adversary will be likely to develop the means to execute and succeed in such an attack. Such a scenario must be discussed with the sectoral stakeholders so that it can be reflected in the description of the risk and the assignment of the MRC. A similar reasoning follows if the ICT system is subject to highly skilled adversaries, such as cybercriminal groups, who may not have direct governmental support or military capabilities, but still have sufficient funding and skills to develop significant offensive capabilities.

Consequently, an assessment of potential attacker types must be conducted as part of the context establishment. The result should be a list of potential types of adversaries[5], their potential objectives and resulting motivation and a high-level estimate of their means. Based on these objectives, attack scenarios that could affect the primary information and functional assets should be analysed and rated with regard to the motivation and means of the respective attacker types. This information should be considered by the sectoral stakeholders as input to the identification and assessment of the risk and the related MRC classification.

During the context establishment and the primary asset layer assessment, only general considerations of a potential attacker's means and opportunity can be taken into account as the supporting assets, which would be the targets of attacks, and their environment are not yet fully identified. Any estimation of the attack potential level is preliminary and must be renewed during the assessment of supporting assets in the context of the specific supporting asset.

However, for the assessment of risks in the primary asset layer, these limitations of the estimated attack potential are acceptable since the focus is on the estimation of the probability of an incident that may affect the stakeholders' objective. This largely depends on the objectives and motivations of the attacker types which can be estimated for each risk scenario based on its associated attack scenario. With regards to attacker potential, it suffices to have a high-level indication as to whether the attacker types referenced in the attack scenario would be capable of implementing the attack.

[4] For consistency with the CSA, the term Probability is used by this methodology as equivalent to the term Likelihood.
[5] A generic list of attacker types is given in Chapter 9.

Details about the different focus of the use of CTI information for the assessment of risks in the primary asset layer and for the identification of security and assurance requirements for supporting assets at the assessment layer for these assets are described in Section 9.5 and in Section 9.6.

The workflows for establishing the context with regard to CTI and attacker types, the estimation of impact and probability, and the definition of meta-risk classes are documented in Chapter 6.

5.3.3 Sectoral risk assessment – guidance for impact estimation

A principle of our methodology is that sectoral stakeholders will identify risk scenarios that can cause damage to the objectives of one or more stakeholders. The identification of these scenarios will be based on the means and motivation of attackers as well as on the opportunities they have to have an impact on the functional (primary or supporting) assets. From the identification of the risk scenarios, it should be possible for the stakeholders to estimate their impact on the business and the probability that the scenario will occur. Both impact and probability strongly depend on the characteristics of the sectoral business, concretely, the level of the impact depends on the business objectives affected and the perspective of the particular stakeholder.

It is worth remarking that a risk scenario may concern several stakeholder's objectives and, at the same time, different stakeholders in the sector may take a different view of the related impact. Therefore, in this methodology we introduce two concepts for harmonizing the decisions concerning the impact that could be caused by the implementation of a given risk scenario.

On the one side, in order to ensure comparability of impact estimation across sectors, generic levels of impact are defined for use in sectoral risk assessments. These levels, called impact classes (IC), qualitatively measure the damage a risk scenario can cause to the business of the stakeholders. The impact classes defined are shown in **Table 1** below.

Table 1: Definition of 5 impact classes of incidents (IC1-IC5)

IC1	IC2	IC3	IC4	IC5
Negligible impact	Minor impact	Moderate impact	Major impact	Catastrophic impact

Obviously, the stakeholder may map qualitative dimension into quantitative. For example, a major impact could mean the loss of 10% of revenues due to breach of contract or a drop of 15% in clients due to loss of confidence. Even in this example, we may observe that the impact may be considered in many areas of the stakeholder's business. Since stakeholders, depending on their objectives, could have different perceptions of the impact that could potentially be caused by a risk scenario and might select a different IC, a moderation with the goal of defining a common IC should be conducted. This discussion should also consider relevant attackers and their potential that may influence the classification of impact as described in Subsection 5.3.2. The stakeholder's initial selections of IC should be documented.

Applying the concept of risk areas is the second concept that we define in the SCSA Methodology for harmonizing impact analysis. As described in Subsection 5.2.7, a generic description of risk areas given in Annex B should support the stakeholders in taking into consideration all relevant areas when defining their objectives and requirements in relation to a particular business process. To support consistency for the definition of IC, this description of generic risk areas in Annex B includes a definition of a minimum IC. The selection of the IC for a risk scenario which is associated with objectives that have been selected in the context of a risk

area must not fall below the minimum IC given for this risk area. A risk scenario may potentially impact different risk areas, with a different level of impact. In our methodology, each scenario will be attached to the highest impact class (IC) that the scenario may cause.

5.3.4 Sectoral risk assessment – probability estimation

In addition to the definition of impact classes, the sectoral stakeholders involved in a risk scenario must estimate the probability that an incident as described in an identified risk scenario will occur. The estimation of the probability may come from different sources:

- The experience of the stakeholders and/or the organization that provides coordination of all parties involved in the sectoral ICT system.
- The analysis of the potential attackers, their motivations, means and opportunities. Such information should be provided by CTI as described in Subsection 5.3.2 and is referenced by the risk scenario.
- If the risk scenario is not specific to the sector, then the probability may be estimated based on information of similar attacks in other ICT systems, in particular those with a similar supply chain.

The abovementioned information is measured or estimated in a different way. In general the experience of the stakeholders with previous risk events may provide a measurable probability (e.g. the number of a certain type of attack suffered during a year), especially in the case of ICT systems already running for a long time. Other information is more qualitative as, for example, the information provided about the motivation and capabilities of an organization to attack the sector ICT system. The disparity of information brings the necessity of introducing qualitative levels for measuring the probability that a risk event will occur. A classification into five levels, as presented in **Table 2**, is considered in the SCSA methodology.

Table 2: Definition of 5 levels of probability of incidents (P1-P5)

P1	P2	P3	P4	P5
Incidents are highly unlikely to occur	Incidents are unlikely to occur	Incidents are somewhat likely to occur	Incidents are highly likely to occur	Incidents are almost certain to occur

Each sector shall determine its own definitions of probability assigned to risk scenarios for each of the five levels, bearing in mind the following factors:

- Risk assessments are prone to errors in estimation where probability is at a low level. This introduces the potential for misclassification of risks, which may result in an inappropriate risk treatment. Given the importance of sectoral systems, it is important to ensure, as far as possible, that errors of this kind are minimized.
- Sectoral risks, given their scope, are such that even low impact events will tend to cause significant disturbances to the stakeholders within a sector, the sector's customers and governmental risk owners or even to society as a whole. Furthermore, even if a single event causes insignificant damage, it will not be acceptable if such events happen frequently. These factors must be taken into account in both sectoral risk assessment and treatment, ensuring that such risks are assessed at an appropriately high level and are not left untreated.

5.3.5 Assessing sectoral meta-risk classes

The level of meta-risk class for a sectoral ICT product, ICT service or ICT process is assessed as a function of the estimated consequences (harmful impact) and the perceived likelihood of those consequences happening (probability). In practice, the two parameters we must consider when making this assessment are those outlined in the three previous sections (5.3.2, 5.3.3 and 5.3.4):

- Estimated consequences – or Impact Class (see IC1-IC5 in **Table 1**)
- Probability of the incidents occurring (see P1-P5 in Table 2).

The two parameters in **Table 1** and **Table 2** are combined to enable the meta-risk class to be deduced. By consulting the matrix, estimates of probability and impact class can be used by a sector to deduce a meta-risk class from 1 to 5 (as shown in the cells in **Table 3**). In assessing a meta-risk class the highest assessed impact class (IC) is the one that must be used.

For the definition of such material a number of general design considerations must be taken into account as described above:

- Incidents of a catastrophic nature shall be assigned a high MRC (5) even where these have a very low level of probability (P1).
- Incidents at IC1 level can have serious consequences if they occur at a high frequency and must therefore be assigned a MRC5.

These factors must be taken into account in assigning the MRC in order to ensure that such risks are assessed at an appropriately high level and are not left untreated. In **Table 3**, therefore, it will be noted that there are 9 instances of MRC5, 8 of MRC4, 5 of MRC3, 2 of MRC2 and only 1 instance of MRC1. A description of the risk assessment process used by a sector to assess MRC is outlined in Chapter 6.

Table 3: Matrix showing meta-risk classes 1-5 for given estimates of probability and impact class

	Probability Levels				
Impact Class	**P1**	**P2**	**P3**	**P4**	**P5**
IC5	MRC5	MRC5	MRC5	MRC5	MRC5
IC4	MRC4	MRC4	MRC4	MRC4	MRC5
IC3	MRC3	MRC3	MRC4	MRC4	MRC5
IC2	MRC2	MRC3	MRC3	MRC4	MRC5
IC1	MRC1	MRC2	MRC3	MRC4	MRC5

5.4 USING ATTACK POTENTIAL FOR THE SELECTION OF SECURITY AND ASSURANCE LEVEL

Typically, the opportunity and means of an attacker type are to a certain degree dependent on the type and intended use of the ICT product, ICT process or ICT service that serves as a supporting asset. Therefore, it is important to review the attack potential that was estimated in the first step of the assessment when conducting the second step at the level of supporting assets, i.e. ICT products, ICT processes, ICT services and supporting ISMS of sectoral

stakeholders. Depending on the type of the supporting asset, this could result in different attack potentials for the same adversary. In addition, the detailed estimation of the parameters, opportunity and means requires an assessment for each supporting asset and its intended use. Chapter 6 describes how this is implemented in the workflow for the assessment of supporting assets.

As discussed in Chapter 9 and shown in **Figure 10**, 'attack potential (AP)' consists of motive, means and opportunity. A high-level estimation of attack potential and motivation is considered by sectoral stakeholders to identify risk and define the related MRC. The two remaining components of 'attack potential (AP)', namely opportunity and means, will be used for the definition of the implementation of security and assurance as described in Sections 5.5 and 5.6.

Attack potential not only influences the level of risk, but also the required level of security and assurance needed by the ICT system. If the sectoral system is likely to be subject to a sophisticated adversary, such as a nation-state actor with significant capabilities such as the ability to understand the weaknesses and vulnerabilities of the ICT system, this must be reflected in the way security controls and evaluation are designed and selected.

CTI must therefore provide information that supports the selection and adjustment of security controls, based on the sector's control objectives. Using CTI information, sectoral risk owners will have the information to deploy only those controls with security levels, as described in Section 5.5 that can withstand the attack potential. For instance, if the attacker is assumed to be capable of extracting credentials stored on smartcards by deploying attacks at the hardware level, the ICT products used by the sector must be hardened and certified to withstand such attacks.

It is therefore proposed that, in estimating meta-risk levels for a sector, attack potential should be taken into account using the five levels (AP1-AP5) defined in the examples shown in **Table 4** below. Please note that, in this table, 'motivation' is assumed at all levels of attack potential.

Table 4: Example definitions for the five levels of attack potential (AP1-AP5)

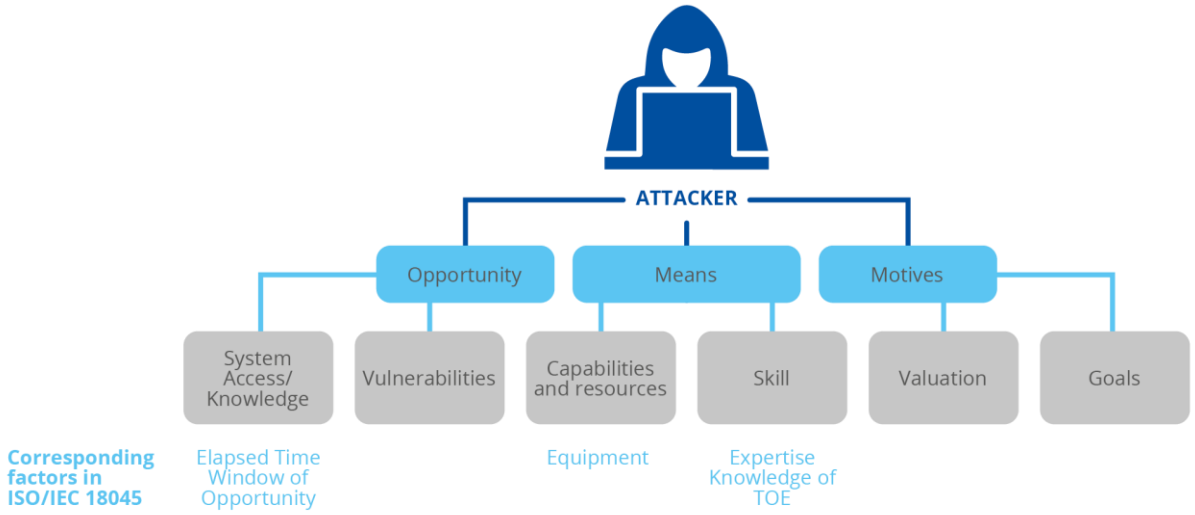
	AP 1	AP2	AP3	AP4	AP5
Adversary Characteristics	Unskilled adversary	Skilled adversary with limited resources and opportunity	Skilled adversary with significant resources and opportunity	Highly skilled adversary with significant resources and opportunity	Highly sophisticated adversary with significant resources and opportunity
Equivalent ISO/IEC 18045 attack potential	Basic	Enhanced-Basic	Moderate	High	Beyond High
Related AVA_VAN assurance component	AVA_VAN.1/2	AVA_VAN.3	AVA_VAN.4	AVA_VAN.5	None available

The table furthermore lists, from a CTI perspective, for each attack potential the equivalent attack potentials in ISO/IEC 18045 and the related AVA_VAN assurance component. If a sectorial ICT system is, for example, subject to an adversary with attack potential AP3, evaluation at level AVA_VAN.4 would be necessary as a sufficient deterrent against this threat. As the table indicates, the highest attack potential of 'beyond high' has at the moment no corresponding product evaluation level.

'Beyond high' in ISO/IEC 18045 is typically applicable if the adversary has expert-level expertise, bespoke equipment, significant knowledge of the Target of Evaluation (TOE) and significant time available. All of these are features of a sophisticated adversary such as a nation-state actor or a sophisticated cybercriminal group. These actors may be considered as possible adversaries of a sectoral ICT system, meaning that controls evaluated above AVA_VAN.5 would be required. The current lack of a product evaluation level to fill this need for the protection of critical sectorial ICT systems should be noted.

Given the lack of such a certification level and the absence of appropriate products, it should be noted that a system may also be secured through architectural means, such as the combined deployment of multiple controls rated at AVA_VAN.5. This approach is, in communication systems for example, referred to as 'defence in depth'. However, even the combination of multiple controls at a lower level may not be sufficient to prevent an adversary from succeeding in a compromise. It may merely result in the attack being slowed down sufficiently to enable detection and response.

Figure 10: Characteristics of attackers in CTI and ISO/IEC 18045



As shown in **Figure 10**, the information provided by CTI on opportunity and means has a direct analogy to the parameter of attack potential as specified in ISO/IEC 18045 for product evaluation. After a product is evaluated, aspects of the evaluation such as the window of opportunity, the elapsed time the evaluator had to spend with the product, or the knowledge and equipment necessary to compromise the product is considered to determine the attack potential rating from 'Basic' to 'Beyond High' (see ISO/IEC 18045, p. 288). Manufacturers would thus have their products evaluated and certified with respect to a particular attack potential.

It should be noted in the assessment of supporting assets that the same type of information is used but from a different viewpoint. In this case stakeholders will have obtained, from their portfolio of potential adversaries, an estimate of attackers' capability and skills (means), as well as their opportunity to, for example, potentially gain access to the product or system. In the selection of suitable controls for the sectoral system, stakeholders must therefore choose those controls appropriate to the level of attack potential derived from this information.

5.5 RISK-BASED DEFINITION OF COMMON SECURITY LEVELS AND SELECTION OF CONTROLS

5.5.1 Basic requirements, conceptual approach

Section 5.1 provides an overview on the CSA's requirements concerning the security of ICT services, ICT products and ICT processes and its relationships with risk and assurance.

The CSA stipulates that security requirements for ICT services, ICT products and ICT processes should be determined based on the risk associated with their intended use. It introduces a structured approach to security, as known from ISO/IEC 27002, by distinguishing between security requirements / security objectives and secure functions / controls for the implementation of these requirements / objectives.

The CSA also describes the relationship between the concepts of security and assurance. According to CSA, Article 2.1, the assurance level shall establish confidence that the security requirements of a particular scheme for ICT services, ICT products and ICT processes are met, but it does not measure the security of the ICT service, ICT product or ICT process. In addition, EU cybersecurity certification schemes are asked to document security objectives for each assurance level and to provide examples of controls that address these security objectives.

One can conclude that the CSA establishes a direct relationship between the level of risk, which was identified in relation to the intended use of ICT services, ICT products and ICT processes, and the level of security required to mitigate this risk. The relationship between security and assurance is described as more indirect.

Overall, the level of risk can be seen as the leading parameter when determining the level of security required. In addition, security requirements and controls shall be documented for each assurance level. This combination of requirements makes security and the introduction of security levels a subject to be considered for consistency across schemes.

The considerations mentioned above lead to the following conclusions for the design of the targeted methodology:

1. A structure of Common Security Levels (CSL) that is commensurate with the meta-risk classes defined in section 5.3 should be established.

2. To avoid inconsistencies and fragmentation between schemes caused by deviations in the assignment of security controls of particular strength to assurance levels, the CSL should be commensurate with the definition of common assurance reference (CAR) levels defined in section 5.6. This can be achieved indirectly since both, CSL and CAR levels, can be directly linked with respective MRC levels.

The availability of CTI provides the opportunity to consider information on attackers. The methodology will employ information on the relevant attack potential as input to the estimation of the required security level.

As the methodology for sectoral risk assessment shall comply with the ISO/IEC 270xx series of standards, definitions and terminology used in the following subsections on security and CSL, it will also follow this series of standards, in particular ISO/IEC 27002. If possible, there should be a common set of control objectives and controls that can be used across sectors and schemes.

The concept for the introduction of CSL and the application of controls by means of CSL is explained in the following sections.

5.5.2 Definition of Common Security Levels

Subsection 5.5.1 explains that coherence between schemes under the CSA requires a common approach to security levels and that security levels need to be commensurate with the level of concepts for risk and, although indirectly, assurance.

Consequently, the concept of Common Security Levels (CSL) is defined with five levels. Starting from CSL1, each common security level is more stringent than the previous one.

Table 5 provides an overview on the defined structure of CSL and the default relationships between CSL, meta-risk classes (MRC) and attack potential levels (AP).

The information on risks and the associated MRC supports the definition of control objectives and the required CSL of the related controls so that these are able to mitigate the risk efficiently and effectively.

The association with the parameter AP level, which is determined by CTI, allows checking as to whether the selected CSL has the strength to withstand the assumed attack potential.

In both cases there is a default one-to-one relationship between the same levels of the parameters MRC and CSL, as well as between AP and CSL. However, sectoral stakeholders may decide to deviate from this default relationship during the sectoral assessment.

Table 5: Definition of Common Security Levels (CSL) and their default relationships

Common Security Level	Description	Default relationships between CSL and MRC, AP	
		CSL mitigates risk of level	CSL protects against attack potential
CSL1	CSL 1 provides a basic level of security against unskilled adversaries.	MRC1	AP1
CSL2	CSL 2 adds requirements to CSL1, providing security against skilled adversaries with limited resources and opportunity to attack a system.	MRC2	AP2 or lower
CSL3	CSL 3 extends the coverage of the security against skilled adversaries with significant resources and/or significant opportunity to attack a system.	MRC3	AP3 or lower
CSL4	CSL 4 provides security against a highly skilled adversary with significant resources and opportunity.	MRC4	AP4 or lower
CSL5	CSL 5 provides the highest level of security, capable of protecting against highly sophisticated adversaries with significant resources at their disposal and/or opportunity for an attack.	MRC5	AP5 or lower

The estimation of the attack potential of a particular type of attacker, which also provides the criteria and examples for the classification of AP used above, is explained in Chapter 9.

The allocation of controls and the strength of their mechanisms to CSL should be discussed and agreed with the relevant stakeholders in dedicated workshops as part of the development of a horizontal scheme and maintenance activities under the CSA.

The implementation of an authentication mechanism for use with mobile ICT services could serve as an example:

CSL1: Implementation of an authentication protocol on a common OS-platform.

CSL3: Implementation of an authentication protocol in a protected execution environment of the mobile OS.

CSL5: Implementation on a platform, which is equipped with controls against logical and physical attacks on hardware and the OS.

5.5.3 Application of controls by using the CSL-concept

As stipulated by the CSA and as defined in ISO/IEC 27002, there is a two-step-approach to implementing controls. In the first step, control objectives targeting the mitigation of the identified sectoral risks will be defined. For each risk, there can be more than one control objective.

A control objective is met by implementing a set of controls. For each control objective, more than one control can be applied.

The common security level (CSL) specifies the strength of a control. Since the objective of a control is independent of its strength, only controls are categorized according to the CSL structure.

1. **Employing Meta-risk Classes (MRC) and Common Security Levels (CSL) for sectoral risk treatment**
   During sectoral risk assessment, any identified risk will be associated with a meta-risk class. In a second step, the sectoral ad hoc working group will define control objectives to mitigate the risk. These control objectives inherit the assigned MRC as a parameter.

   In order to ensure that MRC and CSL are commensurate, there shall be by default a one-to-one relationship between MRC and CSL of the same level. During sectoral assessment, the sectoral stakeholders may deviate from this default relationship in specific cases. Such deviations should be justified and documented during sectoral assessment.

   The controls that support the control objective will be selected in accordance with the MRC that is associated with the control objective. Consequently, controls with an adequate CSL will be selected for risk treatment.

   In some cases, there may be no control that supports the required CSL. If so, a control or combination of controls that supports the next higher CSL should be selected. Controls can be of a technical, operational or organizational nature.

2. **Attack Potential (AP) as criterion for selecting the CSL of controls**
   It is a fundamental principle that controls should withstand the assumed types of attackers and their capabilities. As described in Section 5.4, the potential of relevant attackers will be estimated during sectoral assessment. The motivation of potential attackers contributes to the classification of risk as described in section 5.3. However, it could occur that despite a high attack potential, risk assessment could result in the assignment of a lower MRC. This would lead to a CSL that could not protect against the assumed attack potential. In such case, the following rule shall apply:

If the MRC is at a lower level than the estimated AP, the AP level should determine the CSL, which is used for selecting the strength of the controls employed for the treatment of risk. The CSL should be selected to provide protection against the assumed AP.

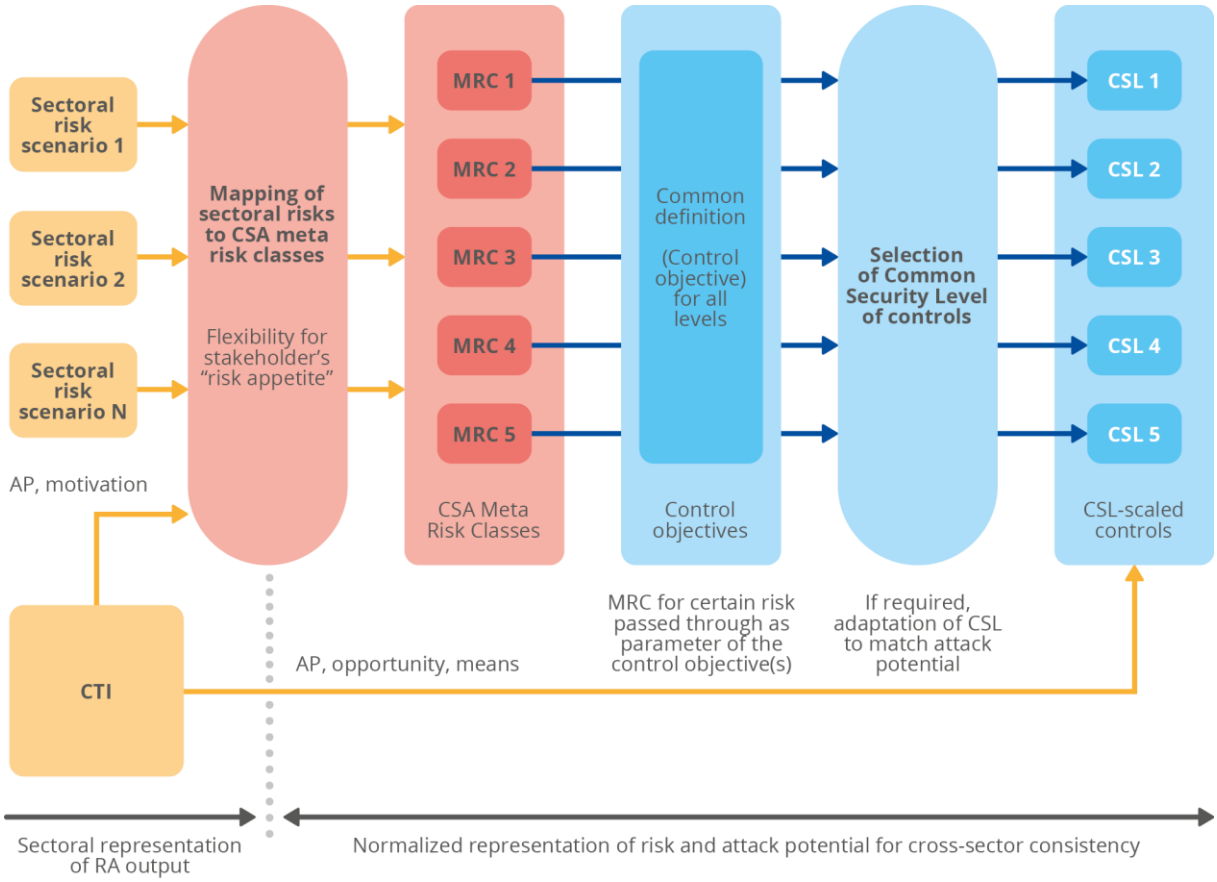
It should also be noted that a meaningful selection of controls could reduce the window of opportunity that an adversary may use and in this way help to reach the required CSL.

During sectoral assessment, the sectoral stakeholders may deviate from this default relationship in specific cases. Such deviations should be justified and documented.

3. **Concatenating controls to meet the required CSL**
Practical risk treatment may require that a certain CSL is reached by a well-defined combination of controls with lower CSL. For example, low cost, high volume ICT products such as IoT devices may not allow costly controls. In such cases, ICT product-based controls with lower CSL could be combined with controls in the system's back office or network to jointly match the required CSL level. Additional information on this concept is provided in Chapter 8.

Figure 11 visualizes the flow of activities for sectoral risk assessment and risk treatment and the relationships between CSL, MRC and AP.

Figure 11: Relationship between MRC, CSL and AP levels



The following table shows the possible combinations of MRC, AP and the resulting CSL for the default scenarios.

Table 6: Common Security Levels (CSL) scorecard

		AP levels				
		AP1	AP2	AP3	AP4	AP5
MRC	MRC1	CSL1	CSL2	CSL3	CSL4	CSL5
	MRC2	CSL2	CSL2	CSL3	CSL4	CSL5
	MRC3	CSL3	CSL3	CSL3	CSL4	CSL5
	MRC4	CSL4	CSL4	CSL4	CSL4	CSL5
	MRC5	CSL5	CSL5	CSL5	CSL5	CSL5

Deviations from this default are allowed under conditions as described above.

5.5.4 The CSL-concept as a basis for security-by-design and control libraries

A defined structure of security levels which is commensurate with related level structures for risk and assurance not only supports consistency and coherence between schemes and the re-use of certified ICT products etc, but it can also be used to develop libraries of CSL-conformant controls. These libraries could help product vendors and owners of ISMS-supported IT systems to implement a well-defined level of security and assurance. They would also allow a practical approach to security-by-design for developers who are not experts in implementing IT security and assurance.

5.6 THE COMMON ASSURANCE REFERENCE CONCEPT – CONSISTENT IMPLEMENTATION OF ASSURANCE

5.6.1 Objectives

The Cybersecurity Act (CSA) stipulates the definition and implementation of a scalable concept for assurance requirements that shall support the basic, substantial and high levels and stipulates a consistent implementation of these assurance levels across the schemes of the EU cybersecurity certification framework.

This requires consistency for the specifications of security and assurance requirements as well as evaluation and certification.

5.6.2 Introduction to a common assurance concept

The objective of a consistent implementation of assurance levels should be seen in the context of the following targets:

1. The CSA established the EU cybersecurity certification framework to overcome the fragmentation between cybersecurity certification schemes in the internal market. A consistent implementation of key parameters such as risk, security and assurance level across schemes will avoid fragmentation between schemes and enable the re-use and referencing of certificates.

2. The CSA anticipates that the requirements for the certification of ICT products, ICT processes and ICT services may vary depending on technologies, targeted markets, responsible stakeholders etc. Specific cybersecurity certification schemes both under public or industry responsibility may have to be established to support these needs. Consequently, there may be numerous schemes under the EU cybersecurity certification framework. All these schemes will try to optimize their operations, which is likely to lead to deviations. Without appropriate measures, these deviations could lead to a fragmentation between the schemes under the EU cybersecurity certification framework and prohibit the recognition of certificates.

It will be apparent that there is a potential conflict between the two targets. Therefore, a balance between the targets of recognition and re-use of certificates and the required flexibility for the implementation of schemes has to be established.

It is proposed that the common assurance reference concept, which is described in the following sections, would support the implementation of such a balance. It should be applied to all cybersecurity certification schemes covered by the EU cybersecurity certification framework.

The idea is to establish a common set of parameters across all schemes, which will allow the implementation of assurance between schemes to be compared as a prerequisite for the recognition and re-use of certificates.

However, the need for flexibility mentioned above does not lend itself to a single, firm definition of assurance for all schemes of the EU cybersecurity certification framework. Therefore, a common assurance reference concept requires a pragmatic approach.

The idea is to adhere as far as possible to proven, trusted standards and methods but to allow their use in a very flexible way. This is likely to lead to uncertainties and a need for interpretation and alignment. In order to address this, the EU cybersecurity certification framework could establish structures such as, for example, a team of experts from the schemes involved, to

promote alignment with regard to the comparability of definitions of scheme-specific assurance levels within the schemes involved.

5.6.3 Selection of the basis for the common assurance reference concept

Several criteria should be taken into consideration to help define a meaningful selection of the principles for the concept of common assurance levels for the EU cybersecurity certification framework:

1. **European or international standards**
   The CSA stipulates that European cybersecurity certification schemes should be based on European or international standards. This also applies to crucial parts of the schemes and is an important prerequisite both for acceptance in the European market and to enhance the marketability of European suppliers in international markets. The assurance level concept to be selected for the EU cybersecurity framework should therefore be based on specifications in either European or international standards.

2. **Availability and maturity of evaluation methods**
   The credibility of assurance levels is largely dependent on the trust of the market in the evaluation methods that are associated with these levels. Such trust cannot be gained overnight. The development of new evaluation methods for elevated security and assurance levels, the deployment of evaluation facilities, the training of developers and evaluators and, in particular, gaining the trust of the market in these new methods would probably take years. As a consequence, existing evaluation methods should be used if available and applicable.

3. **Available base of certified ICT products**
   Especially for the ramp-up phase of the EU cybersecurity certification framework, there will be a need to integrate certified ICT products which are already available in the market. The proposed assurance reference concept should allow these certified ICT products to be re-used. This applies for certified ICT products which are already in use in a sectoral or infrastructural ICT system and also to those which are to be introduced.

   The following considerations should be taken into account:

   - It is advisable to rely on established European or international standards for scaled assurance and to re-use the associated proven evaluation methodologies as far as possible.

   - The EU cybersecurity certification framework is intended to serve a wide variety of market sectors and related schemes. Therefore, sector-specific standards are unsuitable as a basis for a consistent implementation of assurance levels across all schemes. This narrows the options down to two sector-independent families of international standards, the ISO/IEC 270xx and the ISO/IEC 15408 series of standards.

   - The ISO/IEC 270xx series of standards is widely used for the implementation of Information Security Management Systems (ISMS) in ICT systems and for the certification of these implementations. It provides potentially the broadest coverage globally for ICT systems owned by organizations. Information security risk assessment methods are used for the identification of risk related to the intended use of ICT products, ICT processes and ICT systems, taking into account the perspective of organizations that provide ICT services. However, the ISO/IEC 270xx series of standards does not define the term assurance, it does not use the concept of assurance levels and does not support well-specified common evaluation methods.

- In contrast, the ISO/IEC 15408 series of standards supports scalable assurance and complies with the above criteria. However, specific considerations are required if ISO/IEC 15408-concepts, which are mainly known from Common Criteria certification schemes, are to be used in a broad range of schemes for different ICT products, ICT infrastructures and sectoral ICT systems under the EU cybersecurity certification framework. This will be discussed in the following sections.

5.6.4 Potential for use of ISMS as a basis for the common assurance reference concept

The proposed common assurance reference concept shall support ICT systems which employ certified ICT services, ICT products and ICT processes and which, for the security of stakeholder ICT systems, rely on ISMS certification. Consequently, the common assurance reference concept should be defined in such a way that the integration of product certification schemes and ISMS certification is possible.

ISMS certification takes its perspective from the system level, making sure that ICT products and processes are integrated, operated and maintained as required to meet the information security objectives of the organization.

Typically, ISMS certifications do not audit vulnerabilities on the ICT products, which are part of the system. As described in Section 5.6.3, ISMSs do not work with defined security and assurance levels since the targets for these vary, depending on the individual information security objectives of the organization. Currently, there is no open evaluation methodology in place, which could be commonly used across organizations and their ISMSs and referenced by a cybersecurity certification scheme. The applicability of the proposed common assurance reference concept to current ISMS-based certification concepts is therefore limited.

Product certification schemes, on the other hand, are not suitable for evaluations at system levels. Their domain is the in-depth evaluation of ICT products up to a high level of assurance and resistance against high attack potential.

Because of these fundamental differences in applicability, ISMS and product certification schemes can be seen as complementary or even synergistic. Especially so, if ICT systems within an ISMS are aiming to reach elevated assurance levels. Substantial or high assurance can be associated with an ISMS if it employs ICT products certified at an appropriate assurance level. As a result, the security architecture of sectoral or infrastructural ICT systems should be defined in such a way that the required level of assurance is introduced through well-defined, certified ICT products, ICT processes and supporting ICT services.

Based on these considerations, the definition of the common assurance reference concept should focus on ICT product cybersecurity certification schemes as a foundation. An extension to support ISMS-based approaches should be implemented as soon as the prerequisites are in place, and in particular when one or more ISMS-based multi-level schemes for ICT systems or ICT services will be publicly available. This will largely depend on the availability of an open, common evaluation methodology for ICT systems that are used within an ISMS.

5.6.5 Definition of a common assurance reference concept based on ISO/IEC 15408

ISO/IEC 15408 specifies seven Evaluation Assurance Levels (EAL) together with related definitions of assurance components to be addressed at each level. The analysis of vulnerabilities can be seen as the central part of the evaluation activities described in the EAL assurance packages and thus qualifies as the key parameter for a comparison of assurance.

ISO/IEC 15408-3 specifies the vulnerability analysis by defining AVA_VAN assurance components. These have five levels of increasing rigor and depth. The evaluation methodologies for the AVA_VAN assurance components are well-defined, trusted by the European and international markets and are implemented in numerous evaluation facilities globally.

It may be worthwhile noting that AVA_VAN-based concepts are also used by some industry-owned cybersecurity certification schemes. Although these may not always fully conform to ISO/IEC 15408, they employ the AVA_VAN concept to take advantage of its proven evaluation methodologies. This feature could provide a starting point to investigate the comparability of assurance by using the structures mentioned in Section 5.6.2.

Following these considerations, the EU cybersecurity certification framework should establish the common assurance reference concept based on ISO/IEC 15408's AVA_VAN approach to assurance levels and re-use the associated evaluation methodologies.

In order to allow deviations from the strict definitions of AVA_VAN assurance components in ISO/IEC 15408, it is proposed that the term 'Common Assurance Reference' (CAR) should be introduced.

The definition of Common Assurance References, based on ISO/IEC 15408's definition of AVA_VAN assurance components, is shown in the following table:

Table 7: Overview of Common Assurance Reference (CAR) levels

Common Assurance Reference (CAR)	ISO/IEC 15408 baseline specification			Associated baseline contents for the AVA_VAN assurance components
	Selected lead parameter	Associated EAL package	Related attack potential	
1	AVA_VAN.1 Vulnerability survey	EAL1	Basic	See Annex D.2
2	AVA_VAN.2 Vulnerability analysis	EAL2	Basic	See Annex D.3
3	AVA_VAN.3 Focused vulnerability analysis	EAL4	Enhanced-basic	See Annex D.4
4	AVA_VAN.4 Methodical vulnerability analysis	EAL5	Moderate	See Annex D.5
5	AVA_VAN.5 Advanced methodical vulnerability analysis	EAL6	High	See Annex D.6

AVA_VAN assurance components define so-called 'dependencies', which provide a minimum configuration of other assurance components that have to be addressed with vulnerability analysis. In order to achieve full conformance with ISO/IEC 15408 the entire set of assurance components from the lowest-level EAL package that includes the particular AVA_VAN-component have to be carried out. This concept is also used in the EUCC scheme.

While this methodology does not imply full ISO/IEC 15408 conformance, it however requires that the ATE_IND component of the lowest-level EAL package, which includes the selected AVA_VAN-component is also included as part of the assurance activities of the associated CAR.

5.6.6 Implementation of the common assurance reference concept

The application of the common assurance reference concept, as defined in Section 5.6.5, could be described for three implementation scenarios. These are described in the following subsections.

5.6.6.1 EUCC and other ISO/IEC15408-conformant cybersecurity certification schemes

The EUCC and potentially other public or industry schemes will implement assurance concepts as described by the EUCC scheme based on the AVA_VAN assurance components.

Since full conformance with ISO/IEC15408 can be assumed, no further information exchange or alignment between schemes in the EU cybersecurity certification framework is deemed necessary in this scenario.

5.6.6.2 Cybersecurity certification schemes for cost-sensitive and evaluation time critical conditions

European cybersecurity certification schemes, which address cost-sensitive ICT products with basic or substantial assurance requirements, or which have to ensure short, predictable evaluation times, may have to deviate from the methods implemented by classical CC schemes such as the EUCC. Nevertheless, such schemes may wish to make sure that their certificates are recognized by other cybersecurity schemes of the EU cybersecurity certification framework.

The common assurance reference concept could help these schemes adapt to economic or market requirements while keeping comparability of assurance in the following ways:

1. The schemes could accept alternative approaches to provide evidence concerning certain assurance components. Documentation could, for instance, be replaced by information provided in audits or workshops.
2. If duly justified, certain assurance components could be skipped.

In the first case, conformance with ISO/IEC 15408 could still be possible.

In both cases, deviations from the standards and the classical approach must be justified and documented in detail.

Deviations will probably lead to a need for discussion and alignment with the schemes that are interested in recognizing the certificates. As proposed in Section 5.6.2, the EU cybersecurity certification framework could establish structures (e.g. an expert group) that involve representatives of the certifying scheme and those schemes that are interested in re-using these certificates. This expert group could support the scheme by selecting an approach that is commonly accepted for the targeted level of assurance.

Examples for alternative approaches to provide evidence are given in Annex E.

5.6.6.3 Evaluating assurance of external schemes

As stated before, there are market-relevant industry schemes, which re-use parts of ISO/IEC 15408 such as the AVA_VAN assurance component definitions, as well as evaluation methodologies from the ‘smartcard’ technical domain. Other known examples, such as the eIDAS implementing regulation (Regulation (EU) 2015/1502)[6], refer to or employ

[6] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

ISO/IEC 15408's terminology on 'attack potential' to define their security and assurance requirements.

The implementation of the proposed common assurance reference concept by the EU cybersecurity certification framework would provide the option to use these similarities as a starting point for a rough comparison of assurance with the respective specifications of such cybersecurity certification schemes.

As described in Section 5.6.6.2, the EU cybersecurity certification framework could establish structures that conduct an assessment if the assurance level provided by an external scheme complies with the requirements of the EU cybersecurity certification framework. Of course, this would require transparency concerning the methodologies applied by the external scheme.

5.6.7 Relevance of evaluation methodologies, support for new technical domains

Evaluation methodologies, which are trusted by the market to prove the promised level of assurance, are important assets of any cybersecurity certification scheme. This applies in particular to elevated assurance levels.

Common Criteria schemes, like the EUCC, support the evaluation and certification of any kind of ICT product up to AVA_VAN.3. Evaluation and certification for higher levels is restricted to certain categories of products, termed 'technical domains'. These provide domain-specific information, for example on vulnerabilities, as well as dedicated methodologies, for instance those used for evaluation and estimation of attack potential. This information and these methodologies should not be re-used for other product domains without careful consideration, and they will probably require adaptation before use.

EUCC currently supports two technology domains: 'Hardware devices with security boxes' and 'smartcards and similar devices'.

New technology or architectural trends may lead to a need for new technical domains. It can be assumed that the evaluation of software (for example operating systems and web applications) or cloud service systems for levels higher than CAR3/AVA_VAN.3 cannot be implemented based on information and methodologies designed, for example, for the 'smartcard' technical domain.

The implementation of all necessary guidance and the methodology for a new technical domain takes a considerable amount of time and must be conducted using transparent, inclusive processes.

It should be noted that the distinction between security functional requirements and security assurance requirements, as stipulated in ISO/IEC 15408, could help to support a stepwise approach in the event that the methods and guidance information of a technical domain are not yet completely available. It would be possible to define a high level of security for the first step of implementation but limit the level to CAR3/AVA_VAN.3. The upgrade to assurance at CAR4/AVA_VAN.4 or CAR5/AVA_VAN.5 level could follow as a second step once the evaluation methodologies for the technical domain are completely implemented.

5.6.8 Mapping to CSA assurance levels

The previous chapter documents the reasoning why the common assurance level concept, which is based on ISO/IEC 15408's AVA_VAN assurance components and the related EAL packages, should be the basis for a consistent definition of common assurance references throughout the schemes of the EU cybersecurity certification framework. The five CAR-levels,

which are defined by the common assurance reference concept, have to be assigned to the three levels of assurance, which are stipulated by the CSA.

The following should also be considered:

- In addition, for economic reasons, it is advisable that the evaluation should be carried out in relation to the 5 common assurance reference levels or the equivalent AVA_VAN-based definitions given in the EUCC. A structure that supports only 3 levels would probably not support the degree of granularity needed to balance assurance requirements against the effort of evaluation.
- Both the CSA assurance level and the CAR-level should be documented in the certificate.

Theoretically, the assignment of common assurance references to CSA assurance levels could be handled individually for each scheme. Moreover, in such cases, the proposed common assurance level concept could serve as a reference for the consistent implementation of assurance levels across all schemes of the EU cybersecurity certification framework.

5.6.9 Relationship between risk and assurance level concepts

According to the conceptual approach for consistency between risk and assurance, which is described in Section 5.1, there should be, by default, a one-to-one relation between the same levels of MRC and CAR.

However, it is a fundamental principle that the evaluation should reflect the assumed types of attackers and their capabilities. As described in Section 5.4, the attack potential, which includes the opportunity, means and motives of assumed attackers, will be estimated during the sectoral assessment, which will be carried out in the preparatory phase of sectoral candidate scheme drafting. The relationship between the levels of attack potential identified by CTI and the respective levels specified in ISO/IEC 18045 is given in **Table 4**.

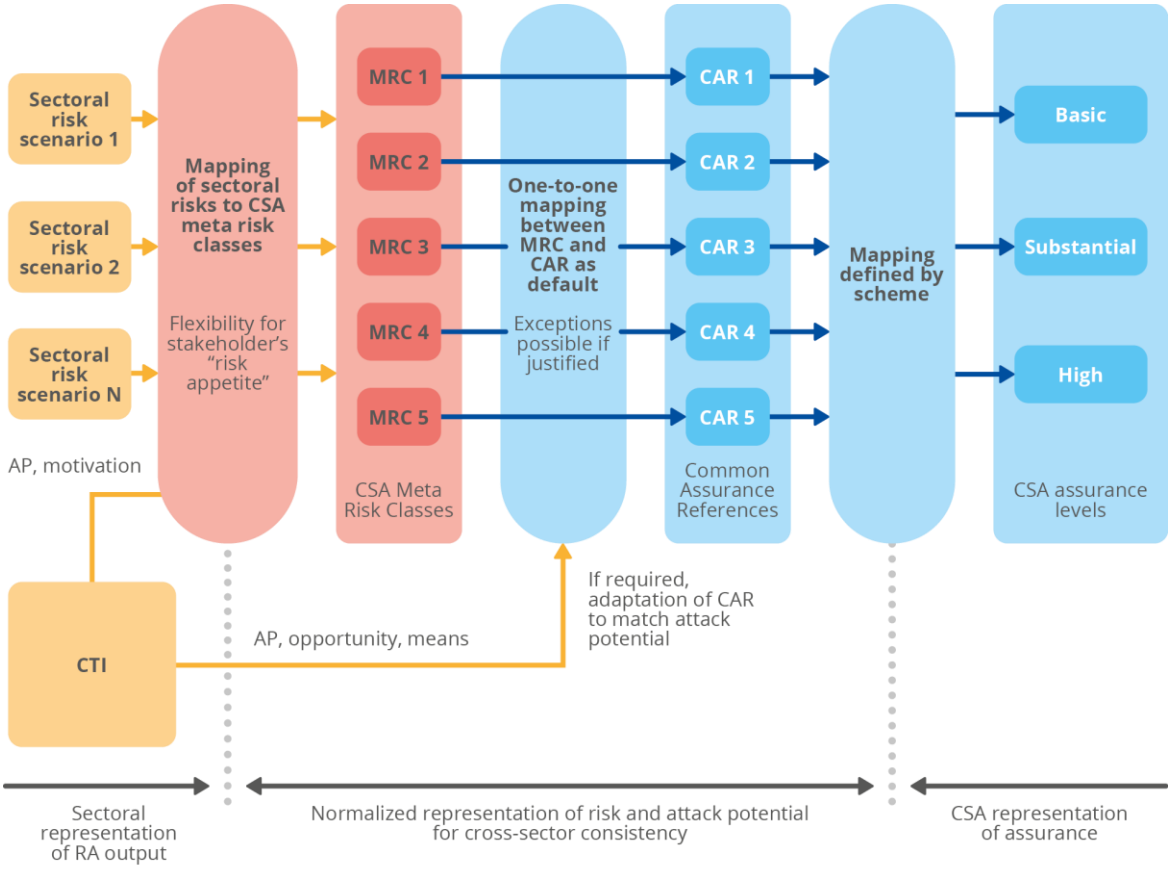
The motivation of potential attackers contributes to the classification of risk as described in Section 5.3. However, it could occur that the risk assessment assigns a lower level to the MRC than was detected by CTI for the AP. This could lead to a CAR below the related level of attack potential AP. In such a case, the following rule shall apply:

If the MRC is at a lower level than the AP level, the AP level should determine the level of the CAR by using the relationship defined in **Table 4**. For instance, as shown in Table 8, for the combination MRC1 and AP3, the CAR should be determined based on AP3. By this, it can be ensured that the evaluation matches the opportunity and means of the potential adversaries.

During the sectoral assessment, the sectoral stakeholders may deviate from this default relationship in some cases. Such deviations should be justified and documented during the sectoral assessment.

A special case occurs if AP5, which matches a ‘beyond high’ attack potential according to ISO/IEC 18045, was identified for the adversary. Evaluation methodologies for this level are currently not available. Section 5.4 describes this case. The following figure illustrates the principle:

Figure 12: Relationship between MRC, CAR and CSA assurance levels



The following table shows the possible combinations of MRC, AP and the resulting CAR for the default scenarios.

Table 8: Common Assurance Reference (CAR) scorecard

		AP levels				
		AP1	**AP2**	**AP3**	**AP4**	**AP5**
MRC	**MRC1**	CAR1/2	CAR3	CAR4	CAR5	Not supported
	MRC2	CAR2	CAR3	CAR4	CAR5	Not supported
	MRC3	CAR3	CAR3	CAR4	CAR5	Not supported
	MRC4	CAR4	CAR4	CAR4	CAR5	Not supported
	MRC5	CAR5	CAR5	CAR5	CAR5	Not supported

It should be noted that, as shown in **Table 4**, the parameter AP is related to the levels of attack potential given in ISO/IEC 18045. The 'Basic' level relates to AVA_VAN.1/CAR1 and also AVA_VAN.2/CAR2.

Exceptions from the default relationship between MRC, AP and CAR are allowed provided the deviation is justified and documented. Extreme combinations such as MRC 1 in combination with AP3 or AP4 may suggest careful considerations.

5.7 TRIGGERS FOR REACTIONS TO UNEXPECTED EVENTS

There may be unexpected events (e.g. geopolitical crisis like the Covid-19 pandemic or massive changes in the cyberthreat landscape) that could cause significant changes to the risk exposure of the sectoral system and its ICT services (e.g. new vulnerabilities, new attack methods, change of attacker motivation).

The sectoral stakeholders should implement a method that can re-start the methodology described in this document in response to a defined trigger and specify the criteria for releasing such a trigger.

6. IMPLEMENTATION OF THE SECTORAL CYBERSECURITY ASSESSMENT

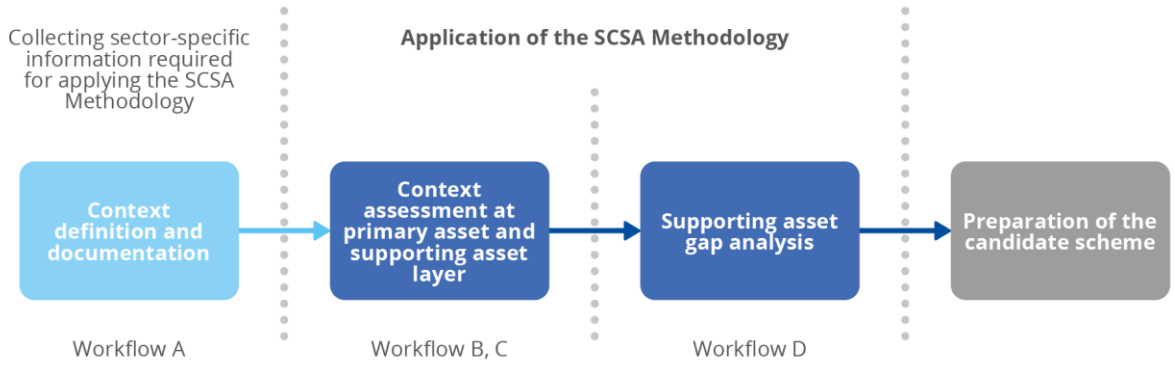
The objectives, principles and the approach for the sectoral cybersecurity assessment are described in Chapter 5. The following sections document the workflows proposed for the preparation and implementation of sectoral cybersecurity certification schemes.

6.1 OVERVIEW OF THE IMPLEMENTATION STEPS

The integration of the SCSA Methodology into the CSA's workflow for the preparation of cybersecurity certification candidate schemes is described in Subsection 5.2.2 and shown in **Figure 6**.

Figure 13 shows the sequential steps that should be carried out and names the workflows that are proposed for each step.

Figure 13: Sequential steps for the implementation of the SCSA Methodology



The workflows are described in the following sections.

6.2 WORKFLOW A 'CONTEXT ESTABLISHMENT AND BUSINESS LAYER ASSESSMENT'

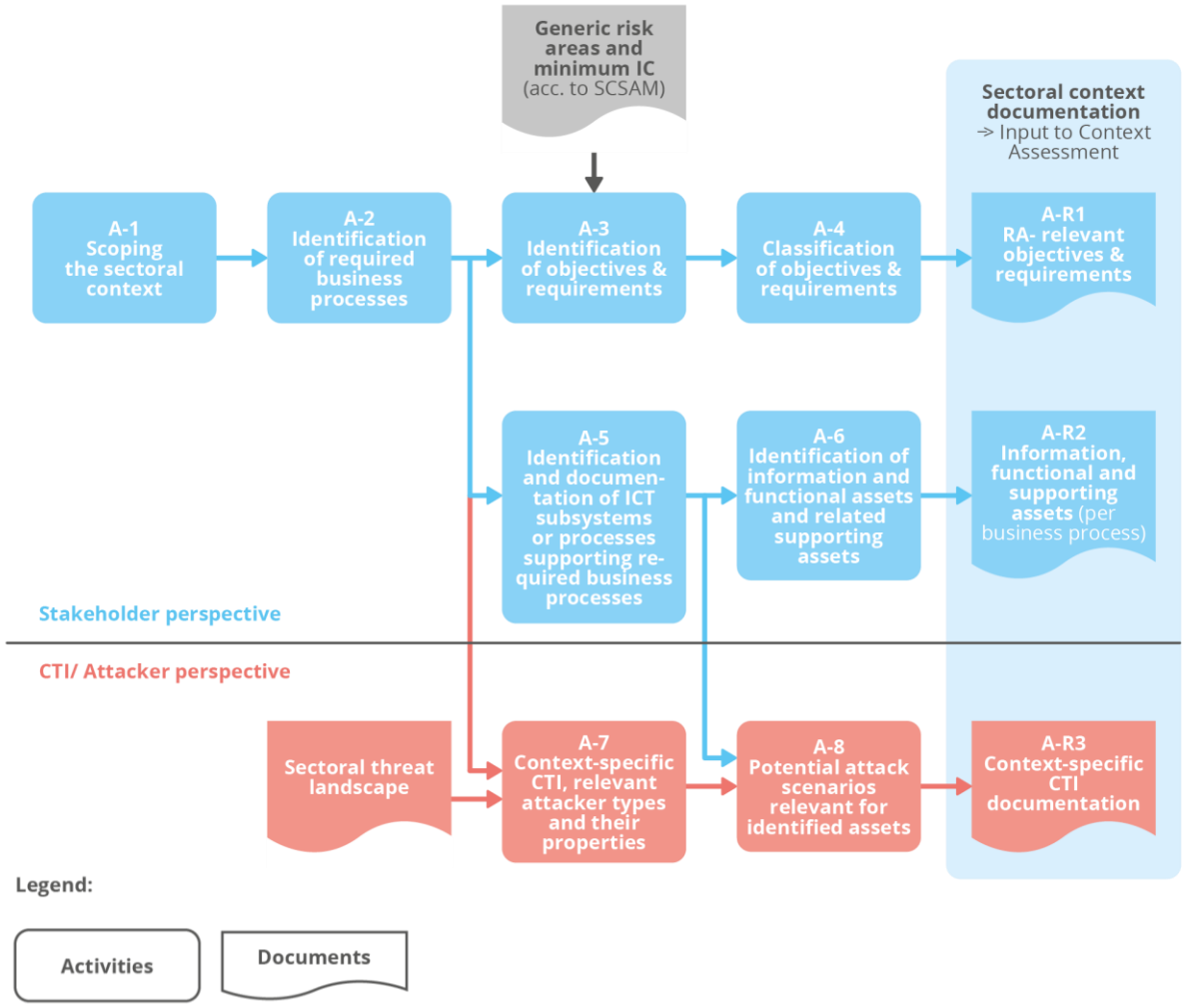
The documentation of the sectoral context can be seen as an equivalent to the 'context establishment' known from ISO/IEC 27005 for ISMS risk management[7]. All information relevant for the assessment of sectoral risks and the definition of certification, security and assurance requirements is collected and documented.

According to the SCSA Methodology, and as an extension to the approach given in ISO/IEC 27005, not only is information relevant for consideration from the perspective of the sectoral stakeholders (i.e. risk owners in terms of ISO/IEC 27005) documented but CTI and attacker information are also documented.

[7] ISO/IEC 27005 builds on the method defined in ISO/IEC 31000 for information security

Figure 14 depicts the proposed workflow for the documentation of the sectoral context which was chosen as the basis for the sectoral assessment and for assessing the relevant business layer information.

Figure 14: Workflow A 'Context establishment and business layer assessment'



The activities to be conducted in the individual steps are described in the following list:

A-1 Scoping the sectoral context

This activity defines the sectoral context which defines the basis for the sectoral assessment. The scope should be defined based on the customers that the sector wants to address and the services and use cases that should be provided to these customers. At this stage the sectoral stakeholders and their roles and responsibilities should also be documented. The identification of stakeholders should include those sectoral roles that contribute to the delivery of the targeted services, the coordinating entity, consumers or their organizations, and governmental authorities that supervise or regulate the sector.

A-2 Identification of required business processes

Based on the results from A-1 the business processes which are required to support the targeted services and use cases should be documented. In addition, the sectoral

stakeholders contributing to or depending on the particular business processes should be identified.

The following steps establish the context from the perspective of business processes and related objectives:

A-3 Identification of stakeholder objectives and requirements for each business process

The objectives and requirements of the involved stakeholders should be documented for each business process. The goal should be to collect, depending on the roles of the stakeholders involved, the relevant range of objectives from the business, customer, societal or governmental perspective for each business process. Practical experience shows that general objectives cannot always be linked to ICT incidents as would be required for the assessment of risks. Therefore it is advisable to add more specific ICT-related requirements to those objectives.

In addition, steps should be taken to ensure that generic risk areas are taken into account for the definition of objectives and requirements for each business case. Annex B contains a list of these risk areas.

A-4 Classification of objectives and requirements

The stakeholder's objectives and requirements related to the particular business processes may be relevant in the assessment of risks but there could also be requirements that concern the characteristics of the cybersecurity scheme or others that indicate stakeholders' needs for assurance. The objectives and requirements should be categorized and documented accordingly.

For the further steps of the workflow, the relationship between objectives and their requirements, stakeholders and business processes must be kept.

The following steps establish the context from the architectural perspective:

A-5 Identification and documentation of ICT subsystems or processes supporting business processes

Based on the documentation of the business processes, the ICT subsystem or process supporting a particular business process should be documented. This should include the architecture and all involved ICT products, services and processes, as well as external ones that contribute to the ICT subsystem. In case of processes, for instance the supply chain, the process flow and the supporting architecture and components should be documented.

A-6 Identification of information and functional assets and related supporting assets

As described in Subsection 5.2.5 and based on the result of A-5, the primary information and functional assets and their supporting assets should be identified and documented for each ICT subsystem or process identified in A-5. In addition, an initial ranking of the relevance of primary information and functional assets with regard to stakeholders' objectives identified in A-3 should be aligned with the sectoral stakeholders involved in the related business process.

Information from A-8 on potential attack scenarios and attackers that could be motivated and, in principle, be capable of conducting such attacks on information or functional assets should be taken into account for this priority ranking. Those information or functional assets prioritized by the ranking discussion should be seen as

primary assets and would become the basis for the definition of risk scenarios in context assessment.

The following steps establish the context from the perspective of CTI and adversaries:

A-7 Documentation of context-specific CTI and relevant attacker types and their properties

The first step of the context establishment regarding threats and adversaries should generate an assessment of threats, CTI information and relevant attacker types for the scope and business processes defined in A-1 and A-2. Existing sector-specific information such as threat landscapes should be used as input. The identification of relevant attacker types should use the list of attacker types given in Chapter 9 as its basis. The estimation of the attack potential level and the motivation of attackers should also apply the characteristics and methods defined in Chapter 9.

A-8 Documentation of relevant attack scenarios

Based on the results of A-7 and information on the relevant subsystems of the sectoral architecture (A-5), relevant attack scenarios that could affect the primary assets (A-6) should be identified and documented. The relevant attacker types and probability of the implementation of the attack should also be estimated for each attack scenario.

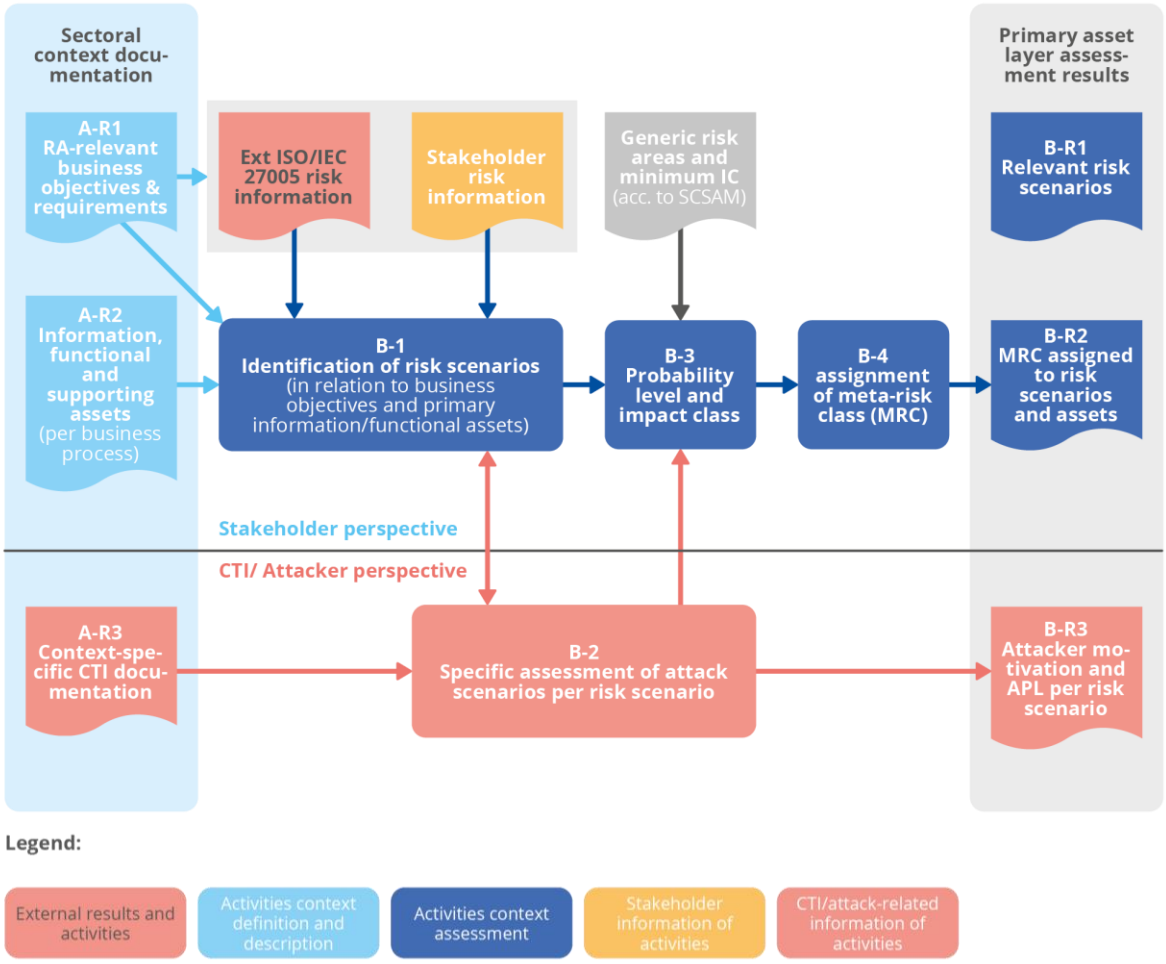
The outcome may lead to a re-prioritization of the information and functional assets identified in A-6. If any of these assets cannot be associated with an attack scenario that is likely to occur it should be disregarded.

6.3 WORKFLOW B 'PRIMARY ASSET LAYER ASSESSMENT'

As described in Subsection 5.2.7, the primary asset layer assessment builds on the results of Workflow A, 'Context establishment and business layer assessment'.

The main targets of this workflow are the identification of relevant risk scenarios and the assignment of meta-risk classes for each risk scenario. **Figure 15**depicts the proposed workflow.

Figure 15: Workflow B 'Primary asset layer assessment'



The activities to be conducted in the individual steps are described in the following list:

B-1 Identification of risk scenarios

In this step of the workflow, risk scenarios as described in Subsection 5.2.6 will be defined based on the following information:

- Stakeholder objectives or requirements related to a specific business process as documented in A-R1.
- Specific primary information or functional asset relevant to the selected stakeholder objective or requirement as documented in A-R2.
- Attack scenario targeting the specific primary information or functional asset as documented in A-R3. Before applying this attack scenario it will be reviewed and potentially specified in more detail by activity B-2.

- Information from an ISO/IEC 27005-conformant sectoral risk assessment may be associated to the risk scenario.
- Stakeholder information.
- CTI information.

A specific stakeholder objective or requirement and a thereto related specific primary information or functional asset which, if successfully attacked, could lead to cybersecurity risks for the selected stakeholder objective are used as a starting point for consideration. In the next step an attack scenario that targets the primary information or functional asset and other information listed above will be added to the risk scenario.

If no scenario of an attack on the primary information or functional asset can be identified and if there is no information from CTI or stakeholders that indicates the practical relevance of the risk scenario, the risk scenario can be disregarded.

B-2 Specific assessment of attack scenarios for each risk scenario

As a supporting activity in parallel to B-1, the attack scenarios documented in A-R3 will be reviewed for their relevance for a specific risk scenario which is defined in B-1. In this process additional information from CTI or stakeholders may be added to enhance and consolidate the description of the attack scenario.

B-3 Assignment of probability level and impact class for each risk scenario

For each risk scenario defined in B-1, the potential impact and the probability of its occurrence is estimated. The methods for assigning the impact class and the probability level are described in Subsection 5.3.3 and in Subsection 5.3.4. This activity should be conducted in direct discussions with the stakeholders whose objectives could be impacted by an incident as described by the risk scenario.

Every stakeholder type should describe his perception of the severity of the impact an incident would have on his objectives or requirements and select an impact class. Should the perceptions and choices of stakeholders diverge, a discussion that leads to a jointly accepted impact class for the risk scenario should be facilitated. All stakeholder positions and selections should be documented.

As a final step of the impact class identification, it must be verified that the selected impact class complies with the minimum IC value given for the defined risk areas in Annex B. The relation to a risk area is given if the stakeholder objective was defined in relation to one of these risk areas as described in A-3.

The selection of the probability level depends mainly on the probability that the attack scenario associated with the risk scenario will be implemented by the attacker. This probability should be estimated based on the detailed attack scenario description generated by B-2 and information that may be provided by stakeholders.

B-4 Assignment of the meta-risk class for each risk scenario

For each risk scenario that went through the assignment of an impact class and a probability level in step B-3, a meta-risk class is assigned. The method for assessing meta-risk classes is described in Subsection 5.3.5.

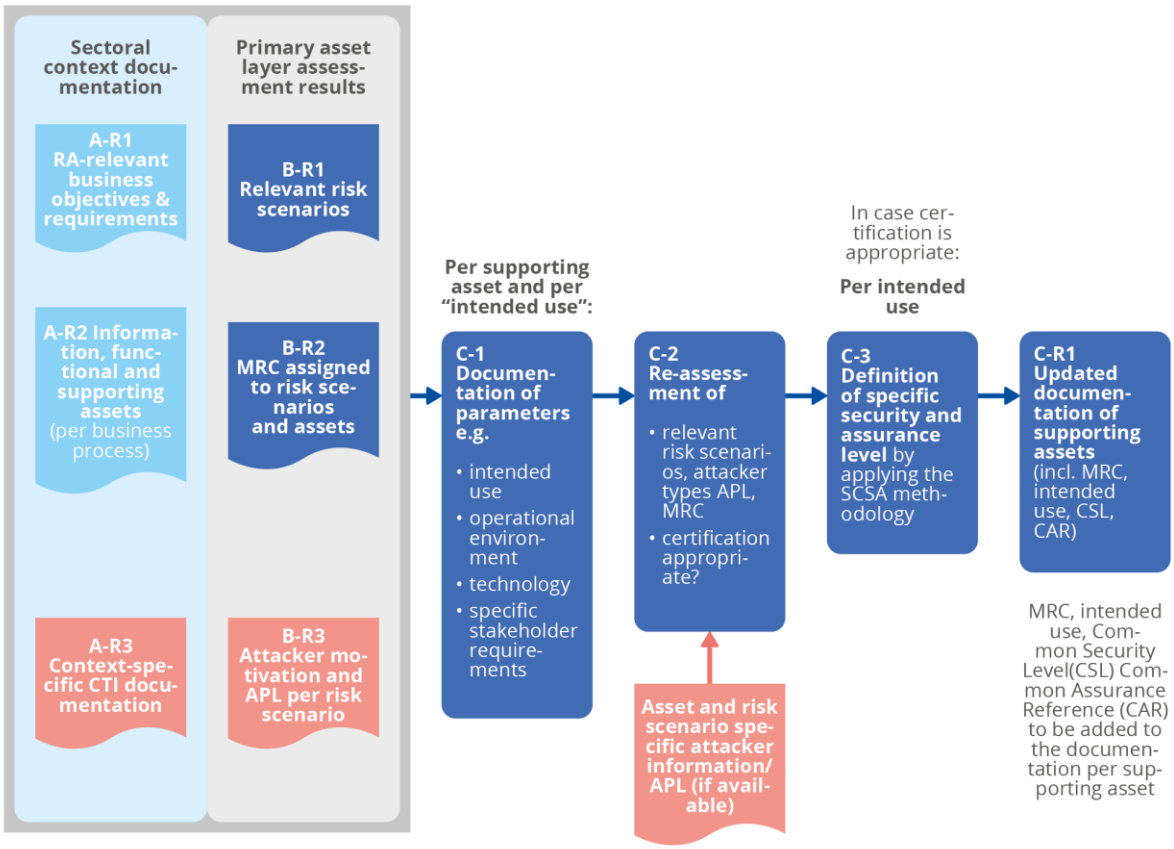
Risk scenarios should be documented including the impact class, the probability level and the meta-risk class. The meta-risk class may be used for prioritising risk scenarios for the assessment of supporting assets. The meta-risk class assigned to a risk scenario is inherited by the primary asset and all its supporting assets.

6.4 WORKFLOW C 'ASSESSMENT OF SUPPORTING ASSETS'

As described in Subsection 5.2.7, the assessment of supporting assets builds on the results of workflows A and B, the context establishment, business layer assessment and the primary asset layer assessment.

The main targets of this workflow are the identification of the certification, security and assurance requirements for supporting assets. The supporting assets to be assessed are defined by the risk scenarios selected for the assessment. **Figure 16** depicts the proposed workflow.

Figure 16: Workflow C 'Assessment of supporting assets'



The activities to be conducted in the individual steps are described in the following list:

C-1 Documentation of relevant parameters for each supporting asset and its intended use

As a first step in the assessment of a specific supporting asset, parameters relevant to that assessment are documented. This has to be conducted for the particular 'intended use'. The intended use of the supporting asset is defined, for instance, by the business process to be supported, by its place and role in the ICT architecture and by the primary assets that it supports.

The following parameters are deemed relevant for the subsequent steps of the workflow and should be documented:

1. 'Intended use' of the supporting asset with reference to the supported business process and its supporting primary information or functional assets.

2. Meta-risk class for the intended use. The supporting asset inherits the MRC from the risk scenario of which it is a part.
3. Operational environment for the specific intended use.
4. Typical high-level architecture and implementation technology.
5. Specifications and standards.
6. Specific stakeholder requirements.
7. Other sectors where the supporting asset may be in use.

Any business-layer requirements that, independently of risk- or attacker-based considerations, could have an impact on the security, assurance or certification requirements of the supporting asset should also be documented. This could apply, for instance, where relevant regulations by national authorities exist.

It is not untypical that ICT products, processes or services serve a sectoral system in various 'intended uses' or appear as supporting assets in several risk scenarios. If so, the assessment has to be carried out for each relevant case. The MRC and the certification, security and assurance requirements could diverge. Faced with such results, the supplier would have the choice to either develop portfolios of ICT products, processes or services optimized for the particular intended use or to have just one offer which conforms to the most demanding case of 'intended use' but can be used for those with lower requirements as well.

C-2 Re-assessment of estimated parameters

In the primary asset layer assessment, the MRC was assigned to a risk scenario based on considerations of the consequences of a potential incident on the objectives of stakeholders. Assuming that the incident could, in principle, be caused by attacks on any supporting asset, the risk scenario's MRC is inherited by those supporting assets. However, this is not always the case. It could very well be that certain supporting assets supporting a primary asset are not as prone to attacks as others and would hence not contribute to the probability of the risk occurring as assumed at the primary asset layer. If a supporting asset is also used by other sectors, this should be taken into account as this could increase the motivation of attackers and the probability of an attack.

Another parameter to be re-assessed is the APL of the attacker types listed in the risk scenario's attack scenario. In context establishment and in primary asset layer assessment, due to the lack of detailed information on the targeted supporting assets, only a general estimate of the APL is possible. C-1 generates information about the operational environment, the technology etc. which could significantly change the estimate of the opportunity and means of the relevant attacker types concerning the particular supporting asset.

The re-assessment of the parameters estimated in Workflow A and Workflow B could be conducted in the following steps:

1. The list of relevant attacker types and their APL associated with the relevant risk scenarios should be reviewed with regard to the specific technology and operational environment of the supporting asset. If available, CTI information concerning the type of supporting asset should be taken into account. Any changes to the most relevant attacker types and their APL and motivation should be documented.

2. If changes to the probability level for the relevant risk scenarios have been encountered in the previous step, the MRC should be recalculated. The revised

value should be assigned to the supporting asset and used for the definition of its security and assurance levels. Furthermore, it should be checked whether new or changed views on relevant attacker types, their capacities and motivation stemming from the detailed assessment at supporting asset level, might suggest an adapted assignment of the MRC that was associated with the risk scenario at primary asset level in Workflow B. The revised value should be used for the definition of the security and assurance level of the supporting asset.

Typically, sectoral stakeholders prefer to apply cybersecurity certification only to those system components for which this is clearly warranted by an elevated level of risk or by a dedicated need for assurance.

3. Therefore, in a further step in C-3, it could be decided that the re-assessed MRC and attacker information suggests certification of the supporting asset is required. Stakeholder objectives and requirements collected in A-3 and categorized in A-4 that indicate a need for assurance with regard to this supporting asset should support such decision. In addition, whether sectoral measures already deployed for the supporting asset would make a certification redundant needs to be checked.

C-3 Definition of specific security and assurance levels

Based on the consolidation of the APL, the probability level and MRC for the specific supporting asset, and by considering potential risk-independent obligations in C-2, the CAR and CSL levels should be defined. If the sector plans to deploy different variants of the supporting asset depending on its intended use and operational environment, the assignment of security and assurance levels should be carried out for each variant.

The use of attack potential for the selection of security levels and assurance levels is described in Section 5.4.

The risk-based definition of common security levels and the assignment of the CSL based on the MRC and the APL are described in Section 5.5.

The risk-based definition of common assurance levels and the assignment of the CAR based on the MRC and the APL are described in Section 5.6.

Certain results of this workflow should be made available to suppliers or owners of supporting assets so that they can optimize their ICT systems, products, processes or services with regard to the requirements identified. This includes, for instance:

- Information about the ‘intended use’ and the operational environment of the supporting ICT product, ICT process or infrastructural ICT service,
- Minimum security and assurance requirements to be implemented by the sectoral stakeholders in their ISMS-supported ICT systems,
- Information as required by ICT product developers for the ICT product’s security problem definition, security functional requirements (SFR) and security assurance requirements (SAR).

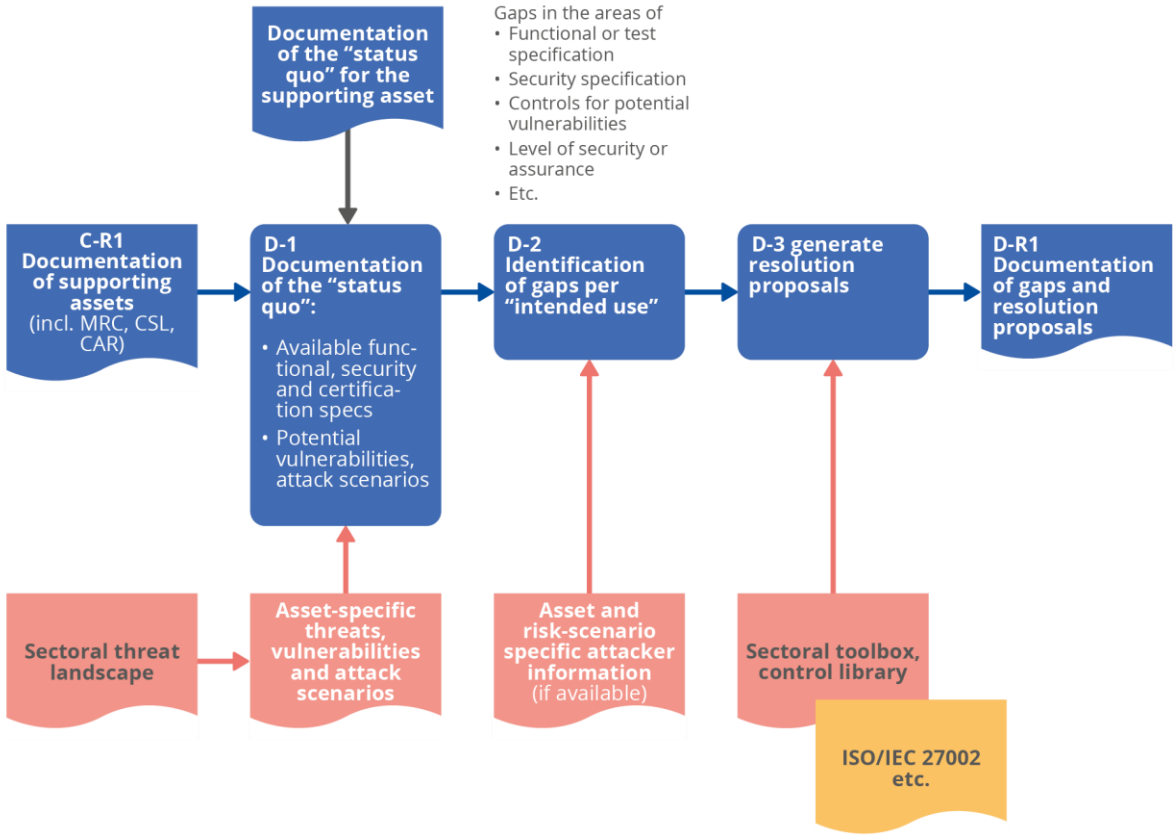
The SCSA Methodology provides in Chapter 7 and in Annex D guidance for the transfer of this information and for its translation into the terminology typically used by ICT product definition and evaluation.

6.5 WORKFLOW D 'SUPPORTING ASSET GAP ANALYSIS'

The assessment of supporting assets described in Section 6.4 documents the 'intended use' of supporting assets and identifies the requirements for certification, security and assurance. The goal of workflow D is to ensure that these requirements can be implemented and verified. Existing specifications and certification means should be re-used as far as possible.

This workflow starts with an analysis of the extent to which these requirements are already covered by the supporting asset and the extent to which existing means could be used for evaluation and certification. Gaps should be identified and resolutions to these gaps proposed. **Figure 17** depicts the proposed workflow.

Figure 17: Workflow D 'Supporting asset gap analysis'



The activities to be conducted in the individual steps are described in the following list:

D-1 Documentation of the 'status quo'

As a first step of this workflow, the status quo of the supporting asset and the certification scheme that is potentially already applicable should be identified. The following information should be collected and documented for the supporting asset type:

- System specifications describing the role of the supporting assets in the system,
- Open specifications and standards describing the functions and architecture of the supporting asset,
- Security specifications,
- Specifications for security evaluation and certification that already exist.

D-2 Identification of gaps

D-1 documented the status quo regarding the relevant specification of the supporting asset. In this step the extent to which these available specifications and tools cover the specific intended use and the identified requirements for certification, security and assurance should be assessed:

- An analysis should be carried out to ensure that all functions of the supporting asset, which are required for its intended use, are sufficiently specified. The relevant standards should be referenced and gaps should be documented.

- An analysis should be carried out to clarify if all required functions and security features of the supporting asset are supported by the existing specifications at the CSL and CAR levels required. Any gaps should be documented.

The results of the gap analysis should be summarized in a way that it can be used as input to the definition of a security problem and the definition of security objectives for ISO/IEC 15408-conformant product certification, and also for comparison with existing protection profile (PP) or security targets, or as external requirements to define an ISMS and its risk management process, whichever is appropriate for the particular supporting asset.

D-3 Generate resolution proposals

To support the appropriate implementation of the supporting asset's defined features, security and assurance level, resolutions for the gaps identified in D-2 should be developed and communicated.

7. RE-USE OF SECTORAL ASSESSMENT RESULTS FOR ICT PRODUCT DEFINITION

7.1 OBJECTIVES AND BACKGROUND

The CSA stipulates that the security and certification requirements for ICT services, ICT products and ICT processes and the related assurance levels should be identified based on the risk associated with their intended use. This requires an assessment of the sectoral or infrastructural environment that employs these ICT services, ICT products and ICT processes.

The previous chapter proposes a consistent approach to risk, security and assurance. It documents how a sectoral risk assessment in combination with CTI can provide required information about the MRC, the use and the operational environment of the ICT services, ICT products or ICT processes, which are a supporting asset for the sector or infrastructure. This information also includes, for instance, the identification of potential adversaries, their motivation and capacity to launch an attack.

The proposed methodology for identifying security and assurance requirements at sectoral or infrastructural level uses the ISO/IEC 270xx series of standards as normative references. Terms that describe risk etc. are in accordance with ISO/IEC 270xx. The employed risk assessment methods, which may be specific to sectors, and their results are conformant with ISO/IEC 27005.

However, the security and assurance requirements for ICT products and potentially ICT processes are often documented using the ISO/IEC 15408 series of standards. The difficulty is that the two series of standards are not harmonized. Terms and methods may diverge.

The objective of the conceptual work described in this section is to allow an exchange of relevant information between the methodology applied at sectoral and infrastructural level, which follows ISO/IEC 270xx, and an ISO/IEC 15408-based approach to security and assurance of ICT products.

The following use cases should be supported:

1. Submission of security and assurance requirements associated with sectoral use as input to the definition of an ICT product.

2. Assessment of ICT products already certified to check their suitability for sectoral use, based on their existing certification.

3. Submission of information on attacker capabilities (attack potential) for the purpose of an evaluation.

All three cases require the provisioning of relevant information from the sectoral assessment methodology and its mapping into an ISO/IEC 15408-compliant format.

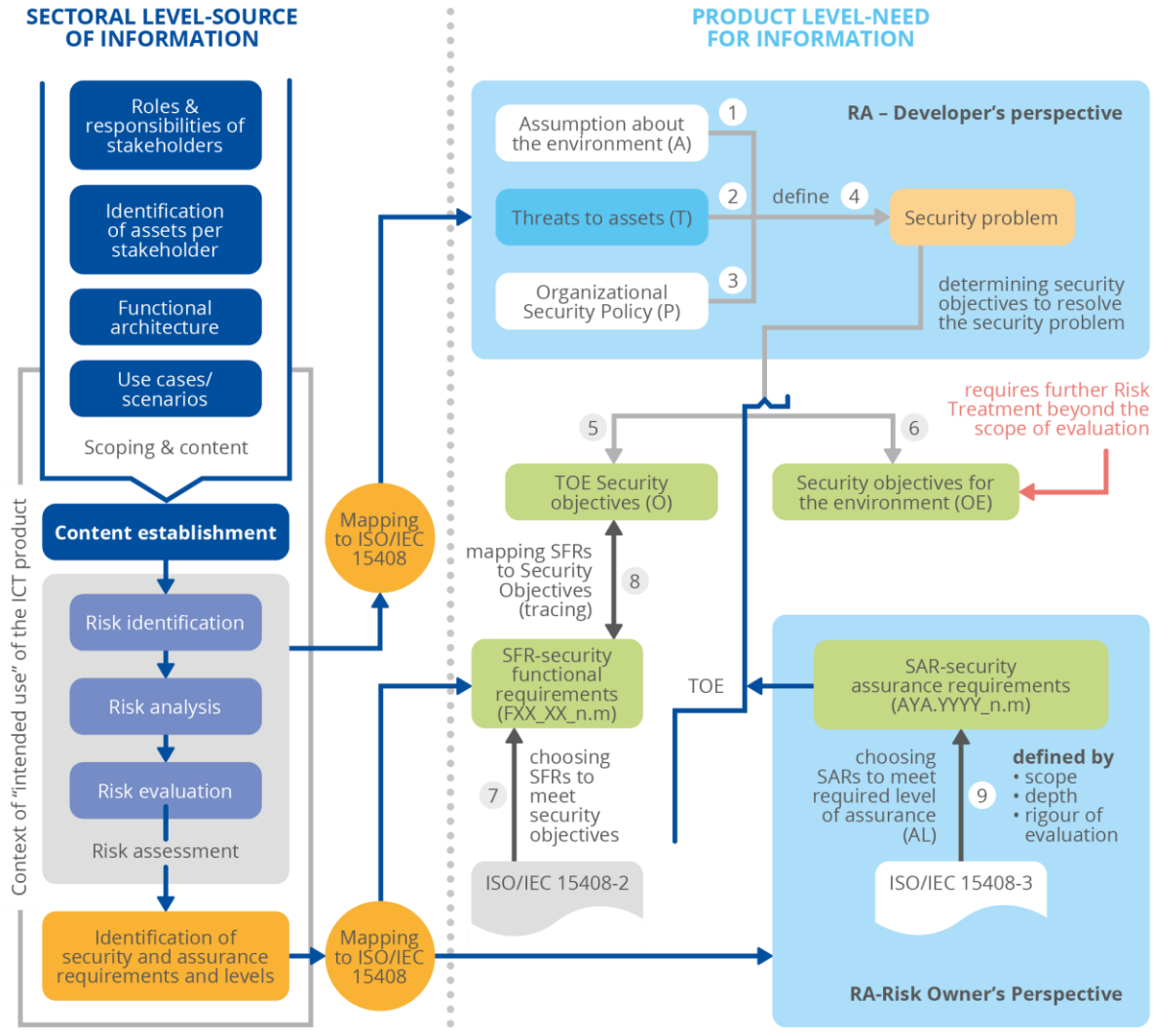
7.2 CONCEPTUAL APPROACH

The targeted re-use of information from sectoral assessments for the purposes of the developer of an ICT product or ICT process has the following prerequisites:

1. **Clarification of terms and definitions**
   The terms defined in the ISO/IEC 270xx and ISO/IEC 15408 series of standards may diverge. For a transfer of information generated by methods governed by one standard to the other it is necessary to identify potential divergences and to consider the particular context in which they will be used. Section 7.3 contains a comparison of divergent terms and describes the boundary conditions which should be taken into account when transferring related information.

2. **Mapping table**
   A dedicated table should support the mapping of the information generated by a sectoral assessment with the information needed for the definition of security and assurance requirements for ICT products by an ISO/IEC 15408-based methodology. **Figure 18** illustrates the principle.

Figure 18: Mapping between ISO/IEC 270xx and ISO/IEC 15408 methodologies



The following sections describe the mapping. A mapping table is given in Annex C.

7.3 GUIDANCE FOR DIVERGENT DEFINITIONS OF TERMS

Some definitions of terms given in the series of ISO/IEC 270xx and the series of ISO/IEC 15408 standards, which are the normative references for this project, diverge from each other. A transfer of information from the sectoral assessment to the specification of security and certification of ICT products requires a sound understanding of the meaning of the relevant terms on both sides.

A simple mapping of terms could lead to misinterpretations because the ISO/IEC 270xx series and the ISO/IEC 15408 series of standards follow very different philosophies and purposes. The concept, which was developed for this project, considers these specific boundary conditions and explains terms in both groups of standards based on their overall objectives and the relationships between terms in each standard (see Section 2.3). These considerations and a mapping between terms in ISO/IEC 270xx and ISO/IEC 15408 are given in Annex A.

7.4 MAPPING TO SECURITY PROBLEM DEFINITION

The outputs of the sectoral risk assessment generated by an ISO/IEC 27005-conformant method, and used for the definition of the meta-risk class (see Section 5.3) can be re-used as inputs to the definition of the security problem in the context of the ISO/IEC 15408 security assessment of an ICT product.

A security problem definition typically consists of the determination of the threats the ICT product must be able to counter, the assumptions about the environment the product potentially relies on to ensure its security, and the organizational policies to be put in place by the ICT product itself or by its environment to fulfil various type of requirements as standards, regulations or interoperability requirements.

7.4.1 Threats

Threats against an ICT product can be seen as an action against an asset associated with the ICT product, performed by an attacker with particular expertise and means, and which results in an unwanted event from the perspective of the ICT product with a negative impact, more or less directly, on the overall ICT system.

Each item of a threat is detailed in the subsequent sub-sections and a synthesis is shown in Annex C.

7.4.1.1 Assets

The list of assets associated with an ICT product constitutes the target of attacks. At the product level, such assets can be of different types, as data (e.g. keys, passwords, user personal data) or services (e.g. access to encryption, signature verification).

Some assets can be related to the assets of an ICT service or ICT infrastructure making use of the ICT product, such as, for example, a cryptographic key associated with an ICT service. A description of these assets from the point-of-view of the ICT service/infrastructure, also called primary assets, must be provided as part of the output of the sectoral assessment.

Other assets are specific to the ICT product implementation. These are to be determined by the related standards and/or the ICT product developer.

7.4.1.2 Unwanted events (incidents) with negative effects

In defining the security problem, a list of assets is not sufficient to determine how attacks can be exploited to cause damage. For instance, considering a cryptographic certificate, for extracting it is unlikely to have a negative effect (assuming it is public information), while replacing it could result in an impersonation attack with negative consequences.

Therefore, in order to determine the risk, it is also necessary to identify the unwanted events (incidents) that could happen to the ICT product and that would have subsequent negative effects on the ICT system.

Negative effects on the ICT system are mostly identified by the sector and/or organization through risk assessment. For instance, without understanding the context within which a signature service is used, it would not be possible to determine if the inability to access that service would have negative consequences on the overall ICT system, the result being that such negative consequences cannot be defined at the ICT product development level.

Thus, from knowledge of both negative effects and of how the ICT product functions, the consequences of unwanted events at the ICT product level can be determined. For instance, if the inability to access a signature service is indeed considered a negative effect, an associated unwanted event at the ICT level could be the erasing of the signature key.

As another example, if the disclosure of some user data is considered a negative effect, an associated unwanted event at the ICT level could be a bypassing of the mechanism for controlling access to the confidential information.

The list of unwanted events is determined in part (at a sectoral level) based on the estimation of an impact class as described in subsection 5.3.3.

7.4.1.3 Attack surface, inherent and potential vulnerabilities

The hardware and software components and interfaces of an ICT product determine its attack surface. Knowledge of this attack surface is needed to allow the definition of what means of attack and techniques can be used to target an ICT product. For instance, the use of a well-known hardware or software technology could directly discount some attacks and attack techniques and thus the threat from those attacks.

Knowledge of the attack surface also enables the existence of inherent or potential vulnerabilities to be determined. For example, the use of a certain CPU implies that Spectre[8]-like attacks are automatically applicable, or the use of some specific DDRAM implies that Rowhammer[9]-like attack techniques can be used to inject faults. As a result, threats based on this type of fault injection must be taken into consideration.

The dimension of the attack surface is also an essential indicator of the effort that might be expended on vulnerability analysis, as well as of the probability of the presence of security issues.

Information to establish this attack surface mainly comes from the ICT product developer. However, as part of its risk assessment the sector may also monitor vulnerabilities related to the hardware and/or software technologies within the ICT products used in the ICT system.

Furthermore, some sectors and organizations have compiled checklists with common potential vulnerabilities that can be followed. One resource that can be used in the context of such an assessment is the Common Weakness Enumeration (CWE)[10], which lists, describes and structures typical software and hardware vulnerabilities in ICT systems. Note that, at the level of threat definition, the attack surface does not need a lot of technical detail.

[8] https://spectreattack.com
[9] https://en.wikipedia.org/wiki/Row_hammer
[10] https://cwe.mitre.org/

7.4.1.4 Threat agents

Threat agents are potential attackers of the ICT product. 'Attackers' can be of different types (e.g. human or accidental) and have different motivations (e.g. financial for crime organizations, reputation for independent hackers). See Subsection 9.3 for more details on threat agents.

Depending on the context in which an ICT product will be used, not all threat agents are relevant and related threats can therefore be excluded. For instance, for an ICT product used in a not-for-profit, non-political organization, threats agents are unlikely to be criminal organizations with sophisticated means of attack (see next section).

The threat agents applicable to an ICT product therefore depend on the operational environment and the final use to which the product is put. Such information can only be provided by the organization or the sector using the ICT product, and is typically an output of the sectoral and organizational risk assessment.

Member state agencies tasked with cyber defence frequently provide briefings and threat landscape overviews on currently occurring threats to selected sectors, for example, those with organizations that are part of a critical infrastructure. Other means of obtaining this information are through the membership in ISACs (Intelligence Sharing and Analysis Centres)[11] as well as community-driven and commercial providers of threat intelligence.

Note that the exclusion of threat agents is usually one of the assumptions made concerning the operational environment (see Subsection 7.4.2).

7.4.1.5 Attack means

Means of attack include all the hardware and software tools and techniques that a threat agent could use to attack an ICT product, such as, for example, lasers, electromagnetic probes or binary editors.

As is the case for threat agents, not all attack means are relevant and related threats can be excluded depending on the context in which the ICT product is used. For instance, for an ICT product not physically accessible by any attacker, all threats based on attack techniques requiring physical access to the ICT product do not apply.

Note that attack means are closely related to the expertise, the financial resources and the privileges of the threat agent.

As for threats agents, the means of attack applicable to an ICT product depend on the operational environment and the final use of the product, which can only be provided by the organization or the sector deploying the ICT product. Such information is typically an output of the sectoral and organizational risk assessment, as well as forensic investigations of previous incidents which are shared among stakeholders, for example in the context of an ISAC.

Note that exclusion of attack means is usually part of the assumptions made concerning the operational environment (see Subsection 7.4.2).

7.4.2 Assumptions

The context in which of an ICT product is used can allow the mitigation of some threats when counter measures cannot be implemented in the ICT product itself, for various reasons (e.g. technical, financial, human). For instance, the administrator of an ICT product must be trusted as no counter measures can fully prevent malicious actions by a user with high-level privileges.

[11] https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center

The definition of assumption is mainly based on the outputs of risk assessments. This includes, in particular, the list of security measures implemented by the operational environment and that are essential to the security of the product.

Note that the list of such security measures may originate from security requirements stipulated by the ICT product developer.

7.4.3 Organizational Security Policies

Organization security policies are implementation requirements for an ICT product or for its operational environment. These policies specify some aspects of the implementation of the ICT product or its operational environment. For instance, a policy could specify which algorithm is to be implemented to allow the interoperability requirement from a sector or to fulfil a national regulation.

Typical organizational security policies express requirements from national or sectoral regulations, standards to be followed, accreditation and certification to be obtained, etc.

The definition of security policies can originate from different needs such as national regulations, sector requirements for interoperability, etc. All these are usually identified by risk assessment.

7.5 MAPPING TO ASSURANCE LEVELS

For the assessment of ICT products based on ISO 15408, Evaluation Assurance Levels (EALs) need to be defined. No formal methodology to determine this assurance level has been defined. However, in practice outputs from risk assessments used to determine such assurance levels include the list of unwanted events (see 7.4.1.2), an estimation of the impact each event may have and the likelihood of each event occurring. Annex C provides examples of the information to be provided to assess the risk and determine the level of assurance.

These inputs are part of those required for the establishment of the CSA meta-risk class defined in Section 5.3. Details about the relations between the risk assessment items used to establish the assurance level and CSA Meta-Risk classes are shown in Subsection 5.6.9.

A mapping between the Common Assurance Reference (CAR) and the EALs defined in ISO/IEC 15408 is provided in Chapter 5.6.5.

7.6 MAPPING TO SECURITY LEVELS

For ICT product assessment based on ISO 15408, a security level concept is not defined.

However, the choice of security features (similar to security controls) during the security definition of the ICT product is commonly based on the outputs of risk assessment , such as unwanted events, the evaluation of the impact of each event and the likelihood of an event occurring, as well as the ICT product architecture and related potential of known vulnerabilities. As shown in Subsection 5.5.3, this methodology also includes the attack potential as a parameter.

Annex C. provides examples of the information to be provided by risk assessment for determining the security level.

Those inputs are part of those required for the establishment of the CSA meta-risk class defined in Section 5.3. Details about the relations between the risk assessment items used to establish the security level and CSA meta-risk classes are shown in Subsections 5.5.3 and 5.6.9.

8. DEFINITION AND APPLICATION OF COMMON CONTROLS

8.1 OBJECTIVES AND BACKGROUND

In general, the CSA promotes a proactive approach to implementing security. Security-by-design is proposed as a way to put this in place.

In the context of cybersecurity certification, the CSA stipulates that the security and certification requirements for ICT services, ICT products and ICT processes and the related assurance levels should be identified based on the risk associated with their intended use. In addition, the CSA requires that certificates should reference technical controls [CSA, Art. 52.4] and that these should be documented for each assurance level [CSA, recital 86].

8.2 COMMONLY USED CONTROLS

The consistent definition of risk, security and assurance is a key part of the SCSA Methodology. Chapter 5 documents how a default relationship between the common assurance reference level and common security levels can be established by using the meta-risk classes and attack potential as joint reference points. This addresses the CSA's requirements described in Section 8.1. Section 5.5 describes how the concept of common security levels can be used to define controls in accordance with their capabilities to mitigate certain levels of risk and attack potential. On this basis, there is now the option to define and deploy controls, which are scaled according to the CSL concept, in a way that is common across sectorial domains and the supporting ICT systems, ICT products and ICT processes.

This option for a common, cross-sector use of controls suggests that a set of controls for common use should be defined. Such a set of controls:

- could serve as reference for the introduction of security-by-design,
- could reduce the time-demand and cost of development, implementation and testing of ICT systems, ICT products and ICT processes,
- could significantly reduce the evaluation effort for the supported ICT systems, ICT products and ICT processes, as a set of controls could be integrated in the form of a certified product.

In the long run, developing and deploying certified libraries of controls for common use could improve security and assurance across sectors and at the same time reduce the cost and risk of development and implementation.

Further benefits could arise when combining common controls with the scalability provided by the common security levels described in Section 5.5. Two examples are described in the following two paragraphs.

8.2.1 Introducing common security levels to ISMS

When deployed in the ISMS of sectoral stakeholders, scaled CSL-enabled controls which are defined as a result of the assessment of sectoral risk and attack potential could introduce a

defined and appropriate level of security to certain functions of the ICT system, a feature which is currently not supported by the ISMS-standard series ISO/IEC 270xx.

8.2.2 Concatenating controls

As described in Subsection 5.5.3, it may be necessary to protect against a certain attack potential or risk by developing the common security level required to mitigate the certain level of this attack or risk using a well-defined combination of concatenated controls. Such cases are quite common where parts of the ICT system provide limited options to deploy controls with elevated CSL. An example could be a low-cost IoT device where elevated CSL and CAR would be unaffordable but where, at the same time, an elevated risk or attack potential applies. Another common case could arise from third-party devices, which are intended to be integrated into the sectoral system, but where there is an option for adapting the CSL or CAR to the necessary levels.

Such concatenation of controls should be discussed and documented during the sectoral risk assessment and treatment conducted by the ad hoc working group that supports the preparatory phase for drafting a sectoral candidate scheme. If a set of concatenated controls is to be implemented across various ICT products, ICT processes and ICT services, it is essential that all involved stakeholders are well informed. Examples for concatenated controls are given in Section 8.4.

8.3 SAMPLE LIST OF COMMON CONTROLS

Generating an exhaustive library of common controls would have exceeded the scope of the project for developing this methodology. Instead, there is now an indicative list of samples that can be used to demonstrate the principle for scaling controls according to the CSL structure and their application in sectoral ICT systems, ICT subsystems within ISMS, in ICT products and in ICT processes. This list of indicative examples is given in Annex F.

8.3.1 Terminology

According to the methodology, the selection of controls would be based on information generated by an ISO/IEC 270xx-based sectoral risk assessment. Therefore, the terminology used for the definition of controls follows ISO/IEC 270xx.

8.3.2 Definition of controls and assigning the common security level (CSL)

As described in Section 5.5, the definition of controls will follow the principle described in ISO/IEC 27002. One or more control objectives will be defined to address a certain risk. In a next step, controls that support these control objectives are defined. There may be several controls for each control objective and these may vary depending on the targeted component (ICT product, ICT process or ICT system), on the market, technology etc.

To establish a common set of controls it would probably make sense to reuse control objectives from ISO/IEC 27002 or define new control objectives which could be employed across sectors.

The association of a control with a particular CSL should be based on an estimation of the attack potential (AP) that the control could resist. The characteristics defined for the description of attackers and the estimation of attack potential given in Chapter 9.4 provide guidance on performing this categorization.

8.4 EXAMPLES OF THE COORDINATED APPLICATION OF CONTROLS

A coordinated application of controls enables a common security level to be increased by introducing several controls at a lower level. The idea is that a combination of two or more controls at CSL x can lead to an overall CSL greater than x for the system. In the following example scenarios, the CSLs listed in the tables are sometimes lower than the overall targeted

CSL for the system. The idea is to show two scenarios, one with a hardened secure processing environment in the mobile phone at the targeted system CSL and one for a mobile phone with lesser capabilities but 'compensating' backend support.

8.4.1 Example use case 'Mobile device based authentication system'

Mobile phones are a constant companion in everyday life and are increasingly used in solutions where more traditional methods might have been deployed, in, for example, controlling access to buildings.

1. **Area of usage**
   – Corporate building or site access control,
   – Managed shared building or site access control,
   – Public transport.

2. **Adversary**
   Depending on the site, building, or company's assessment of risk, the required CSL can take any level from 1 to 5.

3. **Control objectives and examples for concatenating controls**
   The use case described does not address all security aspects and functions. Instead, this example centres on controls used to store and process access credentials in a mobile phone. The minimum security functionalities in the mobile phone features include trusted product identity, secure communication support, secure storage and secure processing of cryptographic functions. For simplicity, these are summarized under the control objective *mobile phone access control support features*.

The access control system itself includes at least a backend system to manage different accounts and access profiles.

Scenario CSL2

Control Objective	Control	CSL	Implementation notes	Notes
Secure and trustworthy access credential processing environment	Mobile phone access control support features	2	The mobile phone implements all access control support features within at least a trusted execution environment, maybe facilitating white-box cryptography to mitigate adversary access to cryptographic assets.	Long term credentials may be stored in the mobile phone.
Secure access credential management	Backend system	2	The backend system deploys, on registration or change of access profiles, the new or updated credentials to the registered mobile phones. At least a logging of access events is enabled in the backend system.	

Scenarios CSL3

Control Objective	Control	CSL	Implementation notes	Notes
Secure and trustworthy access credential processing environment	Mobile phone access control support features	3	The mobile phone implements all access control support features within a dedicated processing environment which is separated from the host processor. The dedicated processing environment must protect its assets against moderate attacker potential.	Long term credentials may be stored in the mobile phone.
Secure access credential management	Backend system	3	The backend system deploys, on registration or change of access profiles, the new or updated credentials to the registered mobile phones using secured communication links. The logging is used to create user profiles on top of which a misbehaviour detection is installed.	
Secure and trustworthy access credential processing environment	mobile phone access control support features	2	The mobile phone implements all access control support features within at least a trusted execution environment, maybe facilitating white-box cryptography to harden adversary access to cryptographic assets.	Medium term credentials may be stored in the mobile phone.
Secure access credential management	Backend system	3	The backend system deploys on a regular basis new access tokens with a limited lifetime or limited use to the registered mobile phones. The logging is used to create user profiles on top of which a misbehaviour detection is installed.	

Scenarios CSL4

Control Objective	Control	CSL	Implementation notes	Notes
Secure and trustworthy access credential processing environment	Mobile phone access control support features	4	The mobile phone implements all access control support features within a secure element. The secure element must protect its assets against HIGH attack potential.	Long term credentials may be stored in the mobile phone.
Trustworthy mobile phones	Mobile phone OS security attestation	3	The backend of the phone OS provides a security indicator to the backend system of the access control system.	
Secure access credential management	Backend system	4	The backend system deploys, on registration or change of access profiles, the new or updated credentials to the registered mobile phones. The logging is used to create user profiles on top of which a misbehaviour detection is installed. Furthermore, the security indicator provided by the phone OS backend is used to detect misbehaviour.	It is assumed that other security controls are on a commensurate security level
Secure and trustworthy access credential processing environment	mobile phone access control support features	3	The mobile phone implements all access control support features within a dedicated processing environment which is separated from the host processor. The dedicated processing environment must protect its assets against moderate attacker potential.	Short to Medium term credentials may be stored in the mobile phone.
Trustworthy mobile phones	Mobile phone OS security attestation	3	The backend of the phone OS provides a security indicator to the backend system of the access control system.	
Secure access credential management	Backend system	4	The backend system deploys, on registration or change of access profiles, the new or updated credentials to the registered mobile phones. The logging is used to create user profiles on top of which a misbehaviour detection is installed. Furthermore, the security indicator provided by the phone OS backend is used to detect misbehaviour.	It is assumed that other security controls are on a commensurate security level

9. CYBERTHREAT INTELLIGENCE

Cyberthreat intelligence - the study of adversaries and their techniques, tactics and procedures - can provide an important contribution to a risk assessment process. Being a relatively new field, this chapter provides a brief introduction into threat intelligence, as well as some discussion how information of threats can be used for risk assessment and treatment.

9.1 WHAT IS THREAT INTELLIGENCE?

In order to effectively defend yourself, you have to understand what threats you might be potentially facing and how they operate. Consider the example of a shop keeper who would like to protect the business against a burglary. In order to confidently invest into security, the shop keeper needs to know how burglaries would typically take place, such as would robbers pick the lock or smash the window, and then use this knowledge to, for example, invest in a better door lock in lieu of bars in front of the shop window. Although this seems an obvious and natural strategy in the case of physical security, the same holds true for cyberthreats. Sound investments into security can only be made given sufficient information about threats.

While characterizing and assessing cyberthreats we know about is already somewhat challenging, we also need to consider the known unknowns and even the unknown unknowns. In other words, there are threats we are aware of but have no readily available data at hand to quantify, and there are threats that we do not even know exist and hence are not part of the current risk management methodology. The goal of cyberthreat intelligence is to identify and characterize potential threat actors, exchange information about their tactics, techniques and procedures (TTPs) and observables, and build a comprehensive view about the cyberthreat landscape an organization, sector or society is facing.

As such, cyberthreat intelligence (CTI) is a natural complement to an ISO 31000 risk management process and augments it as shown in **Figure 19** in various stages.

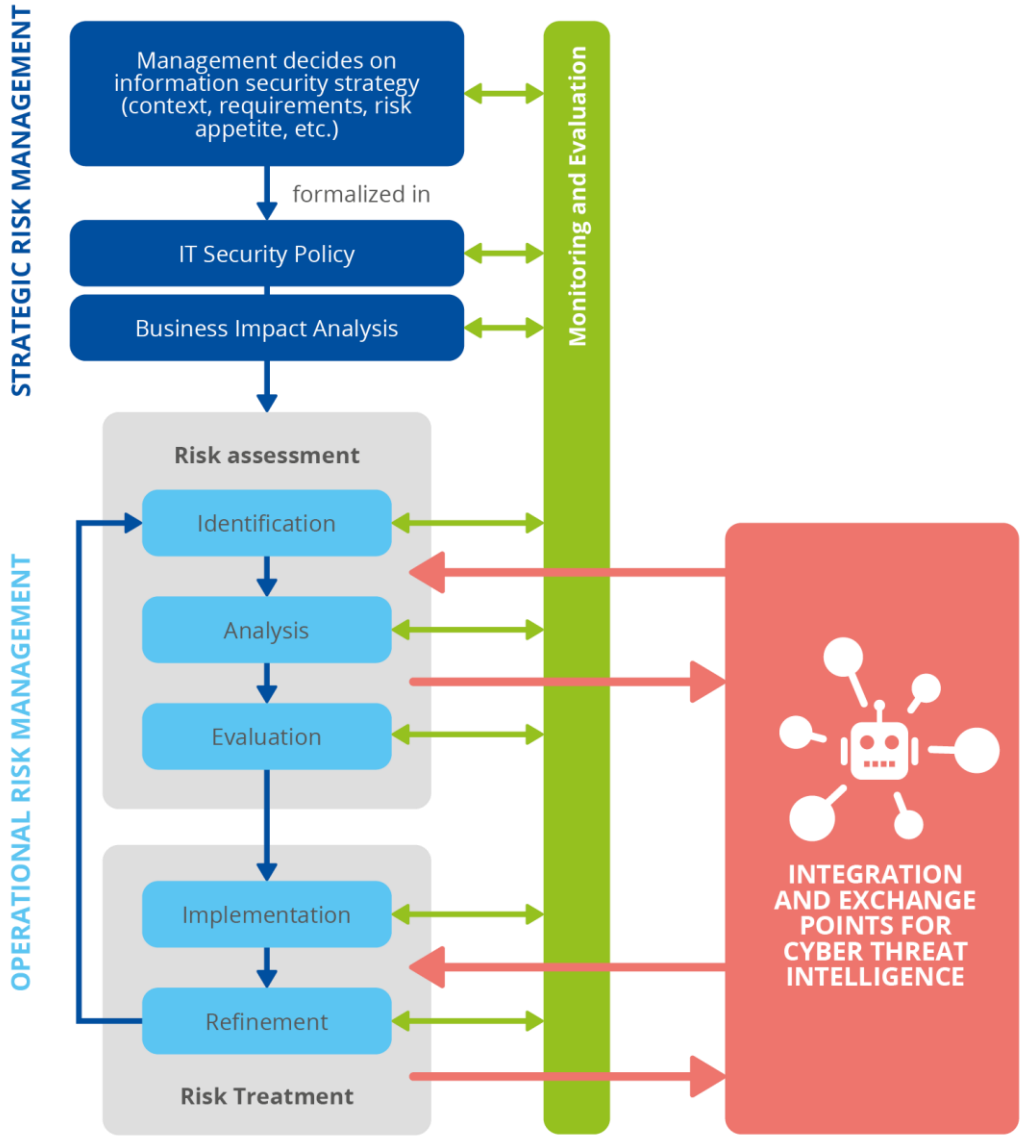
First, the operational risk management cycle requires a comprehensive identification of all potential risk sources. Here, cyberthreat intelligence can supplement insights into threats that occurred elsewhere but were previously not considered by the organization.

Second, for the analysis and evaluation of cyber risks, CTI can provide information about whether a particular threat is targeting a particular geographical region or industry and how it operates, and thus help quantify the likelihood and potential impact of a particular risk.

Third, controls need to be selected to adequately treat a risk. With respect to cyberthreats and their dynamic behaviour this means that the organization needs to select those controls that exceed the currently level of capability, otherwise a particular countermeasure is easily bypassed by an adversary. Here, cyberthreat intelligence can provide insights on current techniques in use by threat actors and their capability levels.

Finally, by sharing information about the threats faced and past incidents with others in their sector, organizations can further adapt their control portfolio, deploy new or tune existing controls, and improve detection by monitoring for specific artefacts known to belong to particular threat actors.

Figure 19: Interconnection of cyberthreat intelligence with organizational risk management

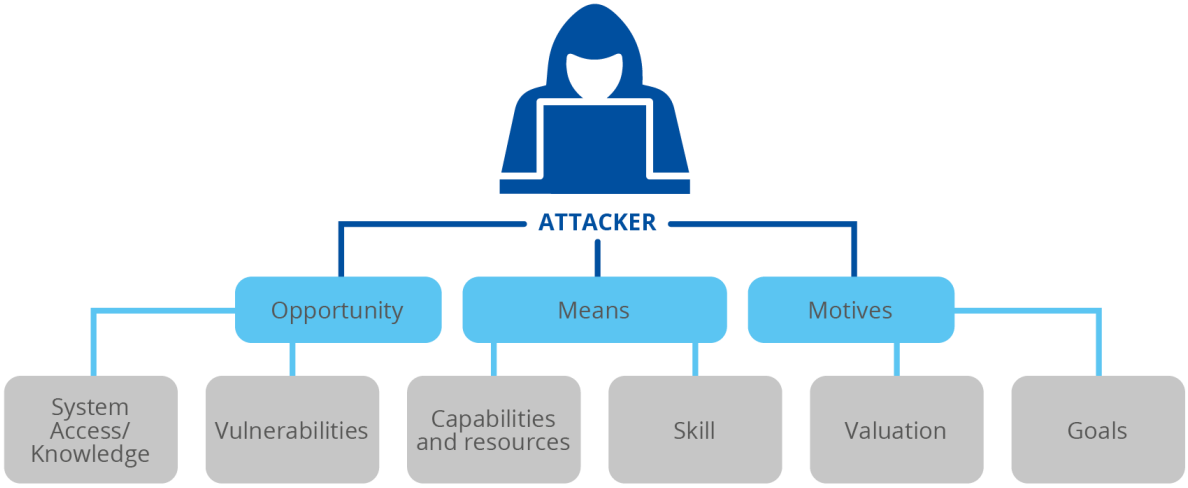


9.2 WHAT IS A THREAT?

In risk management, the level of risk is typically measured as a function of likelihood and impact, i.e. risk = likelihood x impact or, more generically, risk = f(likelihood, impact). While this method works well for non-cyberthreats where a good quantification of frequency and consequences is available, this is more challenging in case of cyberthreats and especially adversaries that act intentionally. Here, threats do not remain static but will on the one hand change over time and on the other hand also change in response to the organization and the measures it takes.

This makes it frequently challenging to determine reliable estimates for these values. We also have to realize these values are a direct outcome of the interplay between adversary and victim. Consider again the example of the physical shop: if a burglar intends to break in and existing controls such as the door lock, security door or safety glass exceed the criminal's level of capability, the probability that this threat actor at this particular moment will successfully break in is zero. If the controls, however, are insufficient and below the adversary's attack capabilities, a successful break-in would likely be certain.

Figure 20: Adversaries can be characterized in terms of their means, motives and opportunities to establish whether they pose a threat to an organization.



Whether or not a particular actor is actually a threat to an ICT system or to an organization thus depends on the characteristics of the adversary, namely his/her means, motive and opportunity as shown in Figure 20. An adversary only presents a potential cyberthreat, if the attacker has the means to execute an attack, the opportunity to do so and exploit a vulnerability, and a motive to target the victim in question. Threat actors pose no risk if any of the three components is not present. Examples would be an adversary who would be interested in performing the attack but does not have the capability to surpass existing controls, or an attacker who has the capability but does not go after a particular type of victim.

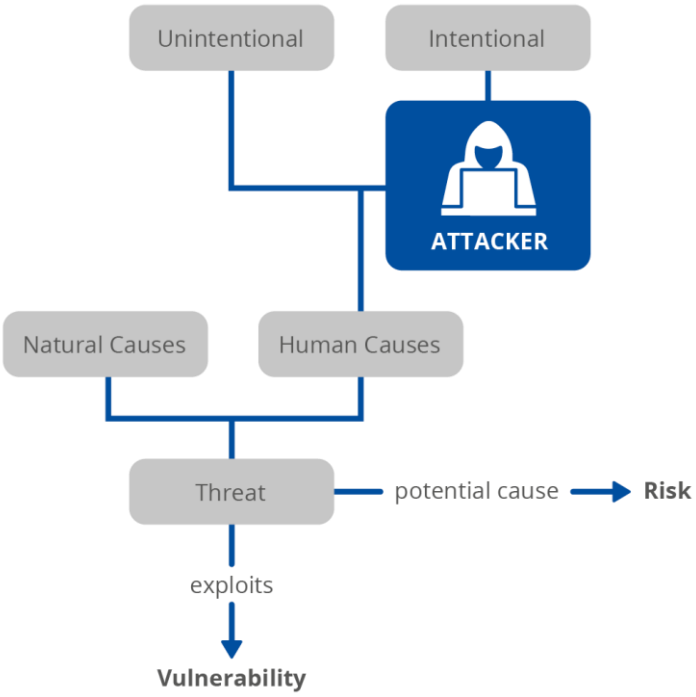
Interestingly, money can substitute for any components under opportunity and motive. For example, an adversary lacking the necessary capabilities could buy an exploit for a vulnerability or outsource an attack to more capable cyber mercenaries. Thus, within the context of intentional cyberthreats, risk thus becomes a function of likelihood, impact and the threat actor.

Cyberthreat intelligence provide insights into the means, motives and opportunities of adversaries. This includes information about the threat actors, their intentions and past targets and accomplishments, but also insights into techniques a particular actor has used before and the tools to which the adversary has been observed to have access. Based on information from past compromises (or attempts at doing so), CTI also collects information about vulnerabilities particular actors have exploited in the past and the various modus operandi they have used previously.

9.3 TYPES OF ATTACKERS

A high-level view of the potential threats to an ICT system is presented in Figure 21. In a first stage we differentiate between a threat that is the result of a natural cause, such as flood, tectonic activity or wind, and one that is the result of a person triggering the vulnerability. Even further, when it comes to human actors, we need to differentiate, for the sake of cyber defence, between an actor who is unintentionally creating damage and an actor who has a deliberate intention to cause harm. In the latter case, we typically refer to the threat actor as an attacker or adversary.

Figure 21: High level decomposition of threats into natural and human causes, as well as unintentionally and intentionally-acting adversaries.



In the literature of cyberthreat intelligence, lists and taxonomies of cyberthreat actors are still being developed. Overall most proposal lists identify the following threat actors with specific motivations and abstract levels of capability:

INTENTIONAL ACTORS

Disgruntled Employees or Insider Attackers are a class of threats with detailed knowledge of an organization and its systems. Examples of this adversary class are staff, contractors, vendors, customers, or former employees. While this type of adversary has only medium-level capability (while of course there could also be insiders with intricate system knowledge and skills), a complicating factor in this group is that attackers have access to valid credentials, know about processes and security systems and how to circumvent them. Common motivations for these attackers are dissatisfaction about the working environment, the organization's or industry's activities, corruption, or revenge.

Cyber Terrorists perform violent activities and sabotage in an attempt to influence public opinion and decision-making. Although the primary objective of cyber terrorist activities is the sabotage and destruction of property, these actors are also indifferent or even in support of creating harm to people and society in general. Cyber terrorists may command significant resources. The asymmetry between the costs to defenders and offenders in an attack means that even moderately funded groups can have a significant impact on assets and systems.

Hacktivists / Civil Activists most commonly extract and expose data or disrupt business operations for ideological reasons or to draw attention to a political, social or moral agenda. While highly motivated, actors in this group are typically non-violent and may draw on external support in terms of capabilities and resources.

(Organized) Cyber Crime. The shared motivation of the broad spectrum of actors in this class is the goal of obtaining a financial profit from online criminal activities. Cyber-criminal activities

span the entire spectrum from coercion and ransom, abuse of e-finance or e-payment services, malware authoring and distributing, cryptomining, the collection, sale and abuse of personal data, to the sale of counterfeit goods. By now, a very diverse ecosystem of specialization exists in the cybercrime underground economy, which means that specialist knowledge, expert tools or even (parts of) the criminal activity can be outsourced or externally acquired. This effectively lowers the bar to entry, as attackers with insufficient capabilities and resources can augment their deficiencies using money, potentially in the form of a cut from the criminal proceeds, culminating in the emergence of 'cybercrime as a service'.

Script Kiddies are typically incapable from the perspective of technology, and make use of externally provided tooling and instructions to perform their activities. Common motivation for this type of adversary is the interruption of service, often executed through distributed denial-of-service attacks, with the underlying goal of public recognition or exploration. The frequent lack of inherent capabilities is often compensated for by outsourcing as, for example, tooling or even attacks themselves can be acquired via the criminal underground at a trivial cost.

State-Sponsored Attackers / Government Spies operate to obtain access to privileged information, such as intellectual property, business plans, roadmaps, personnel or customer data, etc. as well as insight into business operations and upcoming decision-making or to establish a foothold in systems in order to achieve future objectives. This information is used to gain an edge in negotiations, predict future activities or ascertain likely responses. Frequently, these actors are in direct contact with commercial entities in their respective countries to deliver information that could be used for a commercial advantage. Their activity is driven by ideology and personal gain, and they are a potent attacker as they can command government resources and have an advanced set of skills and capabilities.

Competitors / Commercial Industrial Espionage Agents try to gain a commercial advantage through the theft of intellectual property, documentation on business operations and decisions or customer data. They may also damage the targeted organization by modifying or destroying business information. If not executing these activities themselves, they often outsource them to cyber mercenaries, highly trained specialists with sophisticated tooling who pursue offensive cyber activities for profit.

Cyberwarriors / Individual Cyber Fighters are patriotically motivated types of actors, who are not on a government payroll but operate independently. They may be directly controlled or influenced by a nation or are individuals or groups of people driven by their political, social, ethical, or religious values. They may be officially sanctioned or supported by a nation state, and could be equipped with resources or training by the nation state, which significantly raises their level of opportunity and means.

Cyber Vandals / Cyber Punks' main motivation is the destruction of property, driven by the quest for personal satisfaction and dominance. This group of actors is usually not driven by ideology, and has a narrow spectrum of capabilities around attacks on availability.

Blackhat Hackers / Crackers try to gain access to systems out of curiosity and personal gain, which may range from financial rewards from exploiting data, products and systems they obtain, or in terms of reputation and recognition among their peers. While a highly diverse group of actors, their capabilities may be highly sophisticated and they may command significant resources.

UNINTENTIONAL ACTORS

Untrained Employees and Reckless Employees are two types of unintentionally acting adversaries, who still have the potential to cause harm to the organization. They do not act on a specifically malicious motivation, but may cause incidents as a result of insufficient knowledge or negligence of security precautions or procedures in order to attain a (non-malicious) goal. As these threat actors have valid access credentials, their activities can inadvertently lead to significant damage.

To date, there is however no universally accepted standard for a threat taxonomy, and new definitions and proposals for taxonomies are still emerging. Even within the different member states and EU bodies, there exists a wide variety of how actors are classified. In the threat landscape reporting of the Netherlands, actors are classified as government, critical, private citizen with the goal of either espionage, disruption, sabotage, data theft, leak and system manipulation. In the UK, the classification differentiates criminals, nation-state actors, patriotic hackers, terrorist groups, and hacktivists.

In addition, across EU agencies, different classification schemes are in use. In 2013, ENISA defined a taxonomy of 15 actor types characterized in terms of the sector they are active in, their capabilities and their underlying motives. This model is developed further by this methodology.

With the major development of the cyberthreat landscape over the past decade, this report consolidated, refined and enhanced previous taxonomies into the above set of 11 attacker types, which both reflect the current threat landscape and can be mapped to other taxonomies in use at member states and EU bodies.

9.4 CHARACTERIZATION OF ATTACKERS

The goal of CTI in sectoral assessment is to provide information about potential adversaries, their characteristics and resulting attack potential, the assessment of risk, the definition of controls and the evaluation process. In this section, a generic, abstract method aimed at achieving these objectives is described, which needs to be customized after further research into specific scenarios.

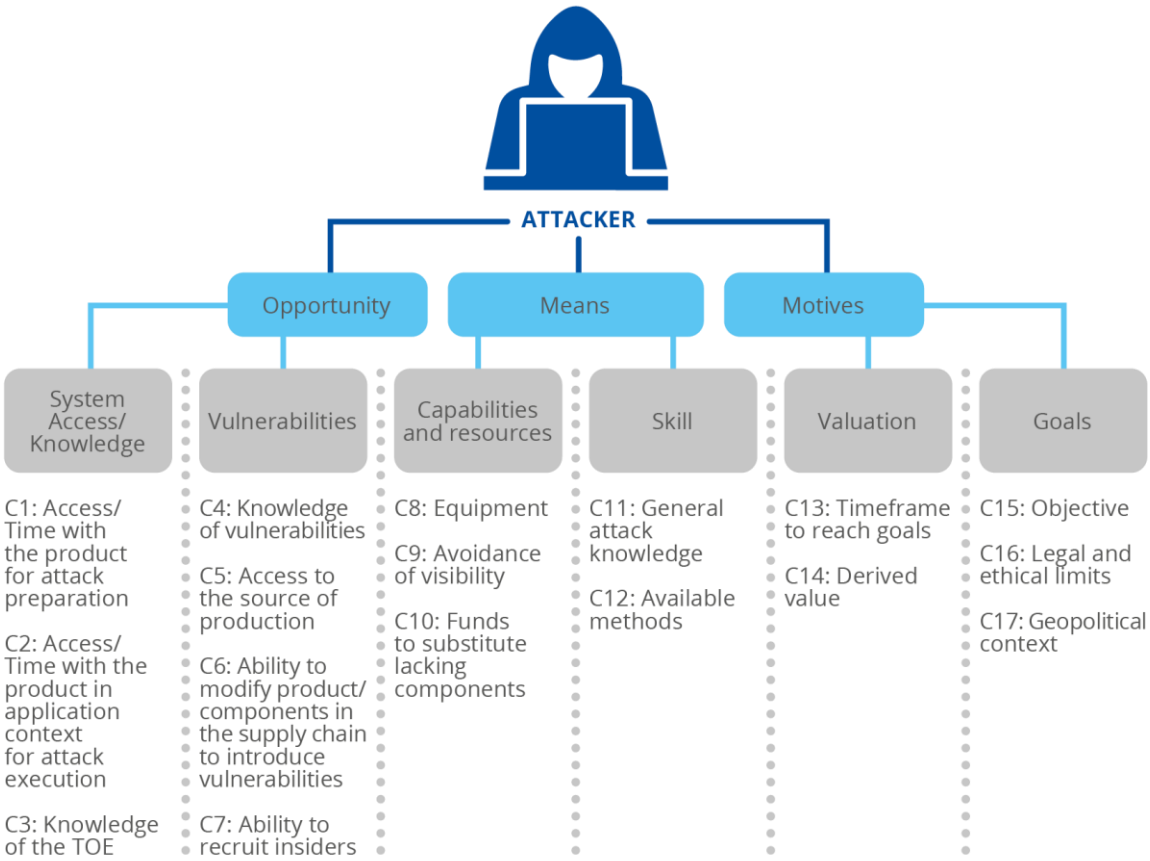
In the scheme presented in this document, the information provided by cyberthreat intelligence serves three purposes:

Firstly, CTI is used to identify the set of actors that are relevant and likely attackers of an ICT product or system;

Secondly, given their capabilities, means and motives, it defines the security criteria that would enable a particular product to withstand an adversary; and

Thirdly, it provides input for the evaluation of the product to confirm that these security criteria are fulfilled and the product can thus be expected to successfully thwart an attack.

Figure 22: 17 characteristics of adversarial motives, means and opportunity



The motives, means and opportunity of an attacker can be characterized in a plethora of ways, each one capturing a different facet of the abstract, complex concept of a persona and its interaction with an ICT system or product and the context in which it is used. Figure 22 shows a selection of 17 dimensions towards such characterization:

9.4.1 Area System Access / Knowledge

In order to be presented with an opportunity for an attack, the adversary must gain access to the ICT system/product/service and have sufficient knowledge to interact with it.

C1	**Access/time with the product for attack preparation** Certain types of attacks require extensive preparation with the actual TOE, such as for obtaining measurements or training models. It has to be assessed whether the adversary can obtain an equivalent product, that is to be attacked later, for internal evaluation, and whether there is sufficient time between the acquisition of the specimen and the time the attack must take place.
C2	**Access/time with the product in application context for attack execution** Evaluation as to whether the adversary will be able to gain direct access to the component to launch the attack, and the maximum timespan of such a potential interaction with the TOE. C1 and C2 have an analogous match in window of opportunity and elapsed time in ISO/IEC 18045.

C3	**Knowledge of the TOE** The adversary's specific expertise with regard to the TOE, such as whether the adversary can only draw from public knowledge or has access to sensitive information about the artefact. This component of CTI has a direct equivalent in ISO/IEC 18045.

9.4.2 Area Vulnerabilities

An attack may only happen, if there is a vulnerability in the component that can be exploited.

C4	**Knowledge of vulnerabilities** Evaluation as to whether the adversary is expected to have knowledge over vulnerabilities in the system, either obtained through independent investigation or acquired from a third party

Even if no vulnerability exists or none is known to the attacker, such an opportunity may be created by an adversary through one of the following ways:

C5	**Access to the source or production** Characterization of access to the development and production information about the TOE and/or the ability to modify it. For example, access to the source code would make the search for a vulnerability significantly easier. If the adversary could introduce changes (open source code, support of insiders, compromised tooling etc.) a suitable vulnerability might be planted.
C6	**Ability to access/modify product/components in the supply chain to introduce vulnerabilities** The identification or introduction of vulnerabilities can also target the supply chain, either by an attack on raw or intermediate components that will be included in the product or the ability to intercept and modify products between the warehouse and the deployment location.
C7	**Ability to recruit insiders** Insiders may be corrupted or coerced to cooperate with the attacker, to disable controls or provide access to the TOE, or development or production components.

9.4.3 Area Capability and Resources

Certain types of attacks require specific assets to be successful. CTI can provide an estimation of available support in terms of physical assets or monetary funds.

C8	**Equipment** Characterization of the type of equipment to which the adversary has access and could enable him/her to identify and exploit a vulnerability, and an estimation of the volume of such materials if the duration of an attack can be shortened by parallelization. This aspect has an equivalent component in ISO/IEC 18045.

C9	**Avoidance of visibility** Evaluation as to whether the attacker needs to conduct the operation in a stealthy manner so that it remains undetected even after completion, and whether he is concerned that the activities could potentially be attributed to him.
C10	**Funds to substitute for lack of components** Short-comings in system access, knowledge, vulnerabilities, capabilities or resources can be overcome by outsourcing to third parties. Characterization of the funding situation of the attacker and his willingness to contract out attack components.

9.4.4 Area Skill

To identify vulnerabilities and execute an attack, specialist expertise is needed. CTI can provide an estimation of the skill level of potential adversaries:

C11	**General attack knowledge** Overall expertise and generic knowledge of the adversary in product design, engineering principles, and attack vectors.
C12	**Available methods** Diversity of the portfolio of attack methods available in order to pivot if necessary and surpass the deployment of stacked controls. This component may be used for the planning of suitable, complimentary controls in a defence-in-depth approach. C10 and C11 have a corresponding counterpart in specialist expertise in ISO/IEC 18045.

9.4.5 Area Valuation

An attack is only likely if the attacker can draw a value out of the activity, for example a monetary or ideological gain. The characterization of the adversary by CTI provides insight into the value perceived by adversaries:

C13	**Time window to reach goals** Characterization of the time by which the attack has to be finished if it is to deliver value to the adversary. For example, this could be based on overall duration or external trigger events.
C14	**Derived value** Characterization of the value the adversary is pursuing (if applicable), an estimation of the monetary gain the adversary might derive from the activity.

9.4.6 Area Goals

The ultimate goal of the adversary determines to a large degree the attack vector used. Cyberthreat intelligence provides information about intentions, and information about past behaviour and modus operandi.

C15	**Objective** Information about the end goal of the adversary's modus operandi, such as the disruption of a service for public consumption or the theft of customer data, is used towards the planning and correct localization of the controls in the organization.
C16	**Legal and ethical limits** Boundaries that constrain the adversaries in their activities, such as a code of conduct or the limits of law.
C17	**Geopolitical context** Geopolitical developments are main triggers of tensions between various types of stakeholders and are considered to be a strong motive in pursuing mutual attacks among parties.

9.5 ESTIMATING THE POTENTIAL OF ATTACKERS BASED ON CTI

As discussed above, the purpose of CTI in the SCSA Methodology is to provide information about potential adversaries and to estimate their attack potential. Section 9.4 proposed parameters that characterize the opportunities, means and motives of attackers. By rating the capacities of adversaries based on these parameters, the assignment of an attack potential to a particular type of attacker will be possible.

The motivation and capabilities of an attacker may vary depending on, for instance, the market sector and the technology that supports controls. Therefore, the potential of a particular type of attacker must be identified for each market sector and each supporting asset that could be the target of an attack. Note that the attacker profile will change over time, necessitating a regular update of the assessments.

Information on attacker types and attack potential are important contributions at two points in the methodology proposed in this document:

1. The identification and assessment of risks in the primary asset layer assessment described in subsection 5.2.7 requires information on the relevant types of attackers. The focus here is on identifying the potential attackers and on understanding the motives they may have with regard to the specific sector. All information and characteristics that CTI can offer to understand the motives (see section 9.4) should be used. In this case, a generic estimation of the capabilities of the type of attacker may be sufficient.

2. If a sectoral risk is identified, which implies that there are potential attackers with a significant motivation, there will be a deeper look at the adversaries and the system components that might be subject to an attack at the layer of assessing supporting assets. At this stage, a full investigation of relevant attackers and their attack potential will be conducted. With motives already established in the previous phase, the focus of this activity mainly lies on the means and opportunities of motivated attackers. The identified attack potential may serve as input to the definition of security and assurance requirements of the supporting ICT products, ICT processes and ICT services, and is applicable both for the evaluation of primary assets as well as supporting assets.

It can very well be that the potential of an attacker varies as a function of the type of ICT product, ICT processes, ICT service and their intended use.

Chapter 6 describes the steps of the sectoral assessment, which are related to the identification and application of the attack potential in detail.

To allow ICT product vendors to benefit from the results of the assessment of supporting assets, it is important to ensure comparability of the relevant parameters with ISO/IEC 15408 and ISO/IEC 18045 is achieved. These standards are typically used for the definition of products with regard to security, assurance and evaluation. Chapter 7 and Annex C provide details how this mapping can be implemented.

The parameter 'attack potential' is also used in ISO/IEC 18045 for the purposes of product evaluation for a specific attack rating. The required characteristics are a subset of those given in Section 9.4 as C1 to C17. With the full adversarial assessment of means, motive and opportunity in hand through the method presented, we not only support the sectoral risk assessment but can also reuse the outcomes to compute the attack potential level as described in ISO/IEC 18045. This selection is described in further detail in Subsection 9.6.2, and it ensures that the level of attack potential identified for each supporting ICT product, ICT process and ICT service is thus comparable to the level used by an evaluator in the vulnerability analysis of the same components.

9.6 STEPS FOR THE IMPLEMENTATION OF CTI-BASED ASSESSMENTS OF ATTACK POTENTIAL

This section describes methods for the qualitative assessment of attacker potential based on the characteristics given in Section 9.4 for both scenarios described in the previous section.

Subsection 9.6.1 describes the process for generating attack potential scores for each of the three adversarial characteristics, means, motive and opportunity. These scores can be aggregated to create an overall attack potential score for each general type of attacker. It can be applied to establish the context and to assess the primary asset layer. In addition, with more detailed information about the supporting asset and its intended use, it can be applied at the layer for assessing a supporting asset.

Subsection 9.6.2 contains a description for the mapping of cyberthreat intelligence information to attack potential as defined by ISO/IEC 18045. This will ensure for the assessment of supporting assets comparability with the concept typically used in product security evaluation.

Until experience has shown that both methods provide consistent results, it is advisable to use the method described in Subsection 9.6.2 for ICT products which are expected to be evaluated and certified in an ISO/IEC 15408-conformant scheme.

9.6.1 CTI-based qualitative assessment of attack potential for risk assessment

Cyberthreat intelligence provides information about attacker capabilities, their modus operandi, targeted victims, and attack campaigns based on collected observations and interpretation. This information is usually assembled with respect to specific actors, in other words CTI tracks the activities and developments of specific adversaries which, when taken together, provide an insight into the threat landscape a particular organization faces. For the purposes of sectoral risk assessment, this level of detail is not necessary, and would only add significant complexity and workload while providing relatively little benefit.

If we consider a particular system to be a likely target of a particular type of attacker, any existing perpetrator within this class of attacker could be the source of an attack. For instance, if a sectorial system is a likely target for cyber terrorists, there is little utility in enumerating the different cyber terrorist groups and their specific capabilities in defence planning. It would be better to design protections against the capabilities that can be expected within this particular class of adversaries. This not only simplifies the analysis and avoids issues of data scarcity, but it is a more realistic assessment of the threat landscape as adversaries are known to exchange knowledge and tools and to hire expertise from others when needs arise.

The analysis of attackers and their potential thus begins by collecting evidence on any actual actors within a specific attacker type, and then aggregating every piece of information within each category to arrive at an evaluation for the components C1 through C17 for this particular class.

In summary, the methodology follows the following steps:

1. For the complete list of attacker types, cyberthreat intelligence on the motivations of attackers is collected. Information about valuation, goals and past targets is used to derive an attack potential score for each particular type of adversary. The sectoral stakeholders decide, based on this information, whether an attacker type is deemed a relevant threat actor for the sectoral system. This information is used in workflow A. For the selected attacker types, the methodology is then continued.

2. Given the list of relevant attacker types, a body of threat intelligence is assembled, detailing past attacks and campaigns, the attack vector and approach used, and the means used to create an compromise by a perpetrator belonging to this attacker type. An analysis of each group of specific threat actors within an attacker type is not necessary, as it can be assumed that the capabilities and opportunities available to one type would also be attainable by another group of actors of the same type. The data collected should span a multi-year timeframe to avoid individual campaigns skewing the data and biased reporting and to allow sectoral stakeholders to not only evaluate current capabilities and opportunities but also to attempt an extrapolation into the near future. The extrapolation should assess the expected progression in attack potential until the next application of the methodology and the completion of a re-assessment and an update.

3. All reporting related to threat actors of a particular attacker type is analysed and the characteristics of this general attacker type are scored with respect to the criteria named below. This delivers an estimation of the characteristics C1 through C17 for each selected attacker type. Each characteristic contains the levels low, medium and high, which are characterized by specific features. The scoring for each characteristic C1 through C17 should be assigned the highest level value occurring when assessing the applicable criteria, i.e. if 2 out of 2 criteria for level low are met, 1 out of 2 for level medium, and 0 out of 2 for level high, the overall value for this criteria shall be medium. When different attacks, known from CTI, exhibit different levels, for example, three attacks used a medium level while the same actor employed different techniques in a fourth campaign that would be associated with the high level, the actor type is ranked as high as this level has already been attained.

4. The outcome provides aggregate attack potential scores for the three aspects, means, motive and opportunity, as discussed in Subsection 9.6.1.1, which can be further aggregated using the techniques in Subsection 9.6.1.2 to a general attack potential level for this particular attack type. Subsections 9.6.1.1 and 9.6.1.2 also provide justification and motivation for the aggregation method and fusion of the individual scores.

AREA OPPORTUNITY

An attack may only happen if there is a vulnerability in the supporting asset that can be exploited. To quantify knowledge of the exposure of the system, as well as the potential for exploitable vulnerabilities, seven characteristics are used to assess adversarial opportunity.

C1: Access/time with the supporting asset for attack preparation

Certain types of attacks require extensive preparation with the actual supporting asset, such as for obtaining measurements or training models. It has to be assessed whether the adversary can obtain a product that is equivalent to the product that will be attacked later for internal evaluation, and whether there is sufficient time for that evaluation between the acquisition of the specimen and the time the attack must take place. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Supporting asset is publicly available for purchase and/or provided to users as part of service. • It is estimated that the attacker takes less than 2 weeks to identify an attack vector / exploit, and develop it.
Medium	• Supporting asset is only sold after the vetting of customers and their use case. Delivered products are not expected to be tracked over their lifetime. • It is estimated that the attacker takes more than 2 weeks but less than 4 months to identify an attack vector and exploit, and to develop it.
High	• Supporting asset is available only to selected customers, substantial efforts are needed to obtain a sample. • It is estimated that the attacker takes more than 4 months to identify an attack vector / exploit, and to develop it.

C2: Access/time with the supporting asset in application context for attack execution

Evaluation as to whether the adversary will be able to gain direct access to the supporting asset to launch the attack, and the maximum timespan for such a potential interaction with the supporting asset.

C1 and C2 have an analogous match in the window of opportunity and elapsed time in ISO/IEC 18045. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Attacks are targeted at Internet-connected assets without (by default or by access) industry-standard authentication, providing for an unlimited window of opportunity. • Operational tempo is regularly high as attacks are quick to execute.
Medium	• Attacks are targeted at assets not connected to the Internet, but the exploit can be delivered by pivoting through assets that are connected to the Internet (lateral movement).
High	• The campaign is targeted at assets which are not internet-connected directly and are not pivoted via Internet-connected assets (air-gapped). • Exploitation requires physical access, using either accomplices or unknowingly infected insiders for installation and/or execution. • Operational tempo can vary from low to high but time horizon, including attack preparation, is long due to complexity of the attack.

C3: Knowledge of the supporting asset

The extent of the adversary's specific expertise with regard to the supporting asset, such as whether the adversary can only draw on public knowledge or has access to sensitive information about the artifact. This component of CTI has a direct equivalent in ISO/IEC 18045. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Knowledge required for the execution of attack(s) is sourced from generally available sources on the Internet or other open sources. • When knowledge is sourced from documents leaked from restricted, sensitive and critical sources, it should also be considered public.
Medium	• Knowledge required for the execution of attack(s) is sourced from restricted sources (e.g. code repositories of closed development communities).
High	• Knowledge required for the execution of attack(s) is sourced from sources only available to the developer/manufacturer of the supporting asset. According to CTI, the attacker is likely to have had access to inside sources to obtain this supporting asset. • Knowledge required for the execution of this campaign is sourced from highly restricted sources, only available to staff from the developer of the supporting asset, on a need-to-know basis. • According to CTI, the attacker likely had access to inside sources to obtain knowledge of the supporting asset. As opposed to sensitive, the knowledge obtained of the supporting asset is information about the security and actual vulnerabilities of and threats to critical parts of the supporting asset.

C4: Knowledge of vulnerabilities

Evaluation as to whether the adversary is expected to have knowledge of vulnerabilities in the system, either obtained through independent investigation or acquired from a third party. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• The adversary has been observed to exclusively use publicly disclosure vulnerabilities in their activities.
Medium	• The adversary has been shown to and can be expected to adopt new vulnerabilities after public disclosure, and active deployment will be faster than the median turnaround time in the defender's vulnerability management process.
High	• The adversary is able to create vulnerabilities and introduce them into the product or service. • The adversary has been shown to have knowledge of zero-day vulnerabilities, targeted specifically towards organizational assets.

C5: Access to the source or production

Characterization of access to development and production information about the supporting asset and/or the ability to modify it. For example, access to the source code would make the search for a vulnerability significantly easier. If the adversary could introduce changes (open source code, support of insiders, compromised tooling etc.), a suitable vulnerability could be planted. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Product uses open source code, which the adversary may inspect for vulnerabilities and/or introduction of vulnerabilities. • Hardware design may be obtained from inspection of the supporting asset, software can be extracted at C8 Medium level from the product.
Medium	• Product uses open source code for security- or mission-critical functionality, which the adversary may inspect for vulnerabilities and/or introduce vulnerabilities.
High	• Adversary has access to the production facility and can introduce changes to the supporting asset. • Adversary has single or sustained access to the source code and/or hardware design of the supporting asset. • Adversary has the capability to take over maintenance of an open source code repository.

C6: Ability to access/modify supporting asset in the supply chain to introduce vulnerabilities

The identification or introduction of vulnerabilities can also target the supply chain, either by an attack on raw or intermediate components that will be included in the supporting asset, or the ability to intercept and modify products between the warehouse and the deployment location. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	*No capability to interfere with the supply chain*
Medium	• Adversary can exchange and modify product during transport and storage before it is delivered to the customer, prior to an inspection before deployment.
High	• Adversary can maliciously influence the design process, the use of protocols, algorithms, cryptographic primitives and/or configurations. • Adversary can modify the tooling used during design, development, production, implementation or testing, to introduce changes or hide past modifications to the supporting asset.

C7: Ability to recruit insiders

Insiders may be corrupted or coerced to cooperate with the attacker, disabling controls or providing access to supporting assets, or development or production components. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Adversary would recruit the services of an insider if offered the opportunity, but not actively seek out insiders.
Medium	• Adversary can be expected to try to proactively recruit insiders within the victim organization or business partners as support, using financial compensation and/or release of personal information to entice insiders
High	• Adversary can be expected to try to proactively recruit insiders within the victim organization or business partners as support, using any kind of means such as financial compensation, coercion, physical force etc.

AREA MEANS

Certain types of attacks require specific assets to be successful. CTI can provide an estimation of the support available in terms of physical assets or monetary funds.

C8: Equipment

Characterization of the type of equipment to which the adversary has access to and may use this to identify and exploit a vulnerability, and an estimation of the quantity of such materials if the attack duration can be shortened by parallelization. This aspect has a comparable component in ISO/IEC 18045. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Capabilities are sourced from publicly available websites and source code repositories and do not require tailoring towards the TOE. • Capabilities are sourced from non-free but otherwise commercially available sources (e.g. commercial/professional-grade penetration test suites).
Medium	• Capabilities are custom-developed involving experts from multiple domains (assembly developers, reverse engineers, payload delivery developers). • The capabilities observed are not generally available and only available to restricted communities (law enforcement, intelligence) or through illegitimate means (dark web). • In the observed attack(s), the attacker exploited a non-targeted zero-day (potentially affecting multiple unrelated organizations).
High	• Capabilities are custom-developed involving experts from multiple domains (assembly developers, reverse engineers, payload delivery developers). • In previously observed attack(s), the attacker exploited a zero-day vulnerability specifically targeting this organization's assets. • Capabilities deployed in this campaign were kinetic, aiming to physically destroy target assets. • Development of the capabilities required testing on and actual possession of the affected assets.

C9: Avoidance of visibility

Evaluation as to whether the attacker needs to conduct the operation in a stealthy manner so that he/her remains undetected even after completion, and whether he/her is concerned that the activities could potentially be attributed to him/her. Adversaries will be more sophisticated the greater the concern they have for avoiding visibility, as well as if they have the means to conduct attacks generating minimal visibility. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Adversary has little concern to be publicly attributed with the attack. Past activities by this actor might be well known publicly and documented. • Adversary relies on commonly known tools, techniques and tactics for a compromise, that are well documented and observable using state-of-the-art defences • Adversary has little concern to be publicly attributed with the attack, nor to obfuscate his activities.
Medium	• Adversary uses various means to hide origin of and responsibility for the attack using, for example, technical means such as proxies, onion routing, compromised intermediaries to launch and conduct activities, as well as means for hiding the flow of funds with respect to the financing of the attack and its proceeds. • Adversary outsources the attack to a third party or proxy as a means of hiding his own involvement.

Level	Criteria
High	• Adversary makes significant efforts to avoid detection by, for example spreading out the attack in time and space using multiple vantage points for the attack and reducing the momentary intensity. • Adversary has the ability to develop and/or uses custom tooling that is not widely known and available to defenders. Tools may be adapted between attempts and victims to avoid detection. • Adversary has to expect consequences such as public shaming, retaliation, sanctions and intensive law enforcement actions if his involvement is detected.

C10: Funds to substitute for a lack of components

Short-comings in system access, knowledge, vulnerabilities, capabilities or resources can be resolved by outsourcing to third parties. Characterization of the funding situation of the attacker and his willingness to contract out attack components. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• The adversary has insufficient funds to outsource attacks to specialized third parties, and has previously not been observed to buy system access, knowledge, vulnerabilities or other resources used in an attack.
Medium	• Expenditures required to overcome short-comings are significant with respect to the total turnover of the adversary or the expected proceeds from an attack.
High	• The adversary has sufficient funds to outsource and buy in capabilities from third parties, either based on expected/past proceeds of the attack or internal or external funding. • Cost of acquiring support is minor given the overall budget and financial capability of the actor. • The adversary has a strong non-monetary motivation so that a negative return on investment for this attack or for entire campaigns is acceptable.

C11: General attack knowledge

Overall expertise and generic knowledge of the adversary in product design, engineering principles, attack methods. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• The adversary relies exclusively on publicly known and well understood attack vectors, for which existing tools may already be available.
Medium	• The adversary has the ability to adopt and modify attacks, which requires moderate domain knowledge or system expertise. • The adversary has command over a portfolio of potential attack vectors, and is able to deploy several of these to accomplish the desired objective. Using these the adversary is able to circumvent or react to basic information security controls.
High	• The adversary is expected to derive new attack vectors, which were either not observed before and are potentially unknown to the targeted organization, vendors or other stakeholders. • The adversary can draw on advanced knowledge in multiple domains, such as software engineering, networking, system architecture, hardware, or the target's subject domain. • The adversary has command over a portfolio of potential attack vectors, and has the ability to adapt and/or innovate them to accomplish the desired objective. The adversary is able to circumvent or react to medium level information security controls.

C12: Available methods

Diversity in the portfolio of available attack methods available in order to pivot if necessary, and surpass the deployment of stacked controls. This characteristic may be used for the planning of suitable, complimentary controls in a defence-in-depth approach. C11 and C12 have a corresponding counterpart in specialist expertise in ISO/IEC 18045. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Tactics and procedures observed in this attack(s) do not require specific expertise, experience or specialization towards the supporting asset.
Medium	• Tactics and procedures deployed are common and/or regularly observed in industry reporting. • Targeting of widely/commonly used software, exploitation of known vulnerabilities using known, detectable malware code.
High	• Tactics and procedures require several years of industry experience and expertise, or highly specialized training (stealth exfiltration of sensitive data, spear phishing critical employees). • Custom development of tools instead of simple copying. • Exploitation of industry- or organization specific or tailored software, tactics and procedures involving the targeting of personal or home devices of critical employees. Delivery of implants via tampered devices • Tactics and procedures deployed require the sustained involvement of multiple experts due to the deep familiarity required for the exploitation of target systems (e.g. combining novel delivery vector with novel deception TTPs to remain undetected). • Tactics and procedures deployed include specialized malware. • Tactics and procedures deployed include supply chain attack vectors (tampering firmware to include a backdoor, or inserting counterfeited hardware into the supply chain).

AREA VALUATION

An attack is only likely if the attacker can obtain value from the activity, for example a monetary or ideological gain. CTI's characterization of adversaries provides insight into how adversaries perceive value.

C13: Time window to reach goals

Characterization of the time window during which the attack must be finished to deliver value to the adversary, based on overall duration, for example, or external trigger events. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• The attack has to be planned, executed and the results used in a very short amount of time. • Assets that might be stolen have only a utility window of a few days before expiry or public release of the information devaluates it.
Medium	• Attack might require significant preparation and time for execution, but obtainable assets can be monetized within a short time frame, and/or hold their value for weeks or longer
High	• Obtainable assets have a validity exceeding months or may hold value permanently. • The adversary can modify technology or organizational processes to maintain a long-term foothold in the organization. This would shorten the time needed to access perishable assets.

C14: Derived value

Characterization of the value the adversary is pursuing and/or, if applicable, an estimation of the monetary gain the adversary might obtain from the activity. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Obtainable assets in a compromise will be of minor economic value for each compromise and will not exceed the adversary's cost and effort in realising the attack. A positive return on investment is realised by replicating the attack across many victims.
Medium	• Assets obtainable from even a single attack will clearly exceed the cost and effort needed to implement the attack. A positive return on investment is very likely.
High	• Assets obtained from the compromise will provide a significant technological advance or competitive business advantage to the opponent and/or the economy of the adversary. • The attack will significantly weaken the ability of the victim to maintain its operation and conduct business or significantly reduce its ability in the future. • The adversary is not required to derive economic value from its activities. The adversary might not be funded by the proceeds from the attack and/or its value is related to other aspects such as geopolitical factors, social issues, moral agendas, or personal motives.

AREA GOALS

The ultimate goal of the adversary determines to a large degree the attack vector used. Cyberthreat intelligence provides information about intentions as well as information about past behaviour and modus operandi.

C15: Objective

Information about the end goal of the adversary's modus operandi, such as the disruption of a service for public consumption or the theft of customer data, is used in the planning and correct localization of controls in the organization. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Unguided destruction of property, driven by a quest for personal satisfaction and dominance • Compromise is creating major public exposure on the victim organization, and/or gain in reputation for the perpetrator
Medium	• Attack is used as a platform for the communication of a political/social/moral agenda • Theft or modification of general information assets that provide a significant economic advantage to the adversary
High	• Theft or modification of intellectual property and information assets critical to the organization and/or of high value to the adversary and the adversary's economy • Damage and destruction of the victim's infrastructure and the services it provides

C16: Legal and ethical limits

Boundaries that constrain the adversaries in their activities, such as a code of conduct or the limits of law to which the attacker adheres. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	• Victim organization is universally recognized as protected by international law or agreements such as the Hague Conventions, for example medical services and infrastructure. The attacker type wants to avoid the risk of being associated with the consequences of his actions.

Level	Criteria
Medium	• Adversaries hired as executing proxies by the perpetrator, which may operate without or ignore legal and ethical limits • Vector, modus operandi and targeted victim will make it unlikely that the attack can be traced back to the perpetrator, which is otherwise bound by limits and fear of public exposure
High	• Actor groups operating without restraint and consideration of international treaties, such as cyber terrorists, cyber anarchists, individual cyber fighters, organized cyber criminals

C17: Geopolitical context

Geopolitical developments are main triggers of tensions between various types of stakeholders and are considered to be strong motives in provoking mutual attacks among rival parties. The level for this characteristic should be assigned the value of the highest applicable criteria:

Level	Criteria
Low	*no (geo)political motivation observed*
Medium	*no (geo)political motivation observed*
High	• Attack on the victim occurs within the context of or as a proxy for aconflict between states. • Targeted organization provides adversary with the ability to completely or largely disable infrastructure and systems regarded as critical infrastructure

9.6.1.1 Calculation of Attack Potential Level for each category

a) Opportunity

The characterization of Opportunity refers to the use of the component 'system access / knowledge', i.e. whether the information asset is sufficiently exposed to the adversary for a compromise to take place. It also refers to using a component 'vulnerability', i.e. whether there exist weaknesses that the adversary might take advantage of in the attack. Vulnerabilities can be inherent to the design and only known to the adversary or be explicitly planted by the adversary to realize an attack.

To compute the APL of Opportunity, the following principle applies:

- The level of vulnerability is equal to the maximum level of C4, C5, C6 and C7 as any vulnerability will be exploitable, regardless of how it was made available.
- Attack preparation can either be online or offline, depending on system access and deployment. The level of system access will therefore be the maximum of C1 and C2.
- Knowledge of the system is a critical component in realising the attack. The combined score of system access/knowledge is thus the minimum of system access and C3, as system access without knowledge will be just as ineffective as a high degree of knowledge without system access.

Based on this reasoning, a combined Attack Potential Level for Opportunity is calculated as follows:

APL_O = MIN [MIN(MAX(C1, C2), C3)], [MAX(C4, C5, C6, C7)]

b) Means

The characterization of Means assesses whether the adversary has the technical capabilities and equipment to accomplish a particular goal, as well as the required knowledge to use it towards a compromise. With the wide-spread availability of 'cybercrime-as-a-service, even specialist knowledge and equipment can be bought or hired, hence an unequipped attacker, if provided with sufficient funding (C10)' would still pose a relevant threat.

To compute the APL component of Means, the following principle applies:

- The level of technical means and skills is equal to the minimum level of C8, C11, C12, as all three components determine the severity of a potential approach.
- As a lack of technical means and skills can be overcome through outsourcing or the hiring of external talent, the overall level of means is increased to the level of expected external support C10 if it exceeds its own technical competences.
- If the adversary has advanced capabilities and is sufficiently patient so that the attack can be spread out over time and space, detection and response is further complicated for the defender. In case component C9 is larger than the result of the above two items, the overall attacker potential level for Means should be increased to the next level.

Based on this reasoning, a combined Attack Potential Level for Means is calculated as follows:

APL_Me = MAX [C10, MIN(C8, C11, C12)]

Given the third principle, an additional adjustment applies. If the score assigned to C9 is larger than the current value of APL_Me, the Attack Potential Level for the means shall be rounded up to the next integer.

c) Motive

To compute the APL component of Motive, the following principle applies:

- Timeframe and derived value are counteracting forces. If the value is high but the time window in which the information asset can be exploited is very short, this limits the overall value that can be derived. The combined level for value will be the higher of the two scores C13 and C14, but this may be discounted by one level if either C13 or C14 is determined to be low.
- The main driving force for goals is adversarial objective, with C16 and C17 only acting as secondary criteria that only become relevant for select and advanced attacker types. The level of goals is equal to C15, and needs to be increased to the maximum of C16 and C17 if these are higher.

Based on this reasoning, a combined Attack Potential Level for Motive is calculated as follows:

APL_Mo = MAX [MAX(C13, C14) - MIN(|C14-C13|, 1)], MAX[C15, MAX(C16, C17)]

9.6.1.2 Calculation of attack potential level (APL)

From the above calculations, we obtain rankings of low, medium and high for each APL component for each attacker type. The overall attacker potential level is the arithmetic average of the sub scores for motive, means and opportunity. For this, we assign an integer value of 1 to level low, and integer value of 3 to a level medium, and a value of 5 to the level high. The resulting average is then rounded up to the next integer.

9.6.2 CTI-based qualitative assessment of attack potential at supporting asset layer

The use of attack potential in a risk assessment involves evaluating potential attackers that may wish to target the primary functions which are the subject of a sectoral risk assessment. However, in reality the primary functions themselves are not suitable as targets of attack, as they are composed of a broad ecosystem of many interlinked and interdependent ICT products, ICT processes and ICT services. Attackers will instead look to target those individual ICT products, ICT processes or ICT services which they perceive as being either most critical to the broader ecosystem or the easiest to attack.

As described in Chapter 6 the sectoral risk assessment is a process which moves from sectoral business objectives, through the primary business functions which help to achieve these, and on to the individual assets (ICT products, ICT processes and ICT services) which support the primary business functions. However, the process is also iterative – so that risks to primary business functions must be re-assessed in the light of assessed risk to the supporting assets once these have been identified and evaluated. It is proposed that attack potential is taken into account at the stage of the iterative re-assessment.

The method provides a CTI-based definition of the attack potential at supporting component level, focusing on the means and opportunity of the attacker in order to support the definition of security and assurance requirements. This approach is close to the one defined in ISO/IEC 18045. This ensures consistency with the definitions of attack potential used in evaluation and assurance and supports comparability.

For this bridging, the subset of criteria that have a direct equivalence in ISO/IEC 18045 are selected for the estimation of the attack potential for the vulnerability assessment from the previously prepared cyberthreat intelligence results. Table 9 lists the matches between attacker characteristics and the corresponding element in ISO/IEC 18045. Table 10 proposes how the corresponding evaluation criteria based on CTI input is to be set.

Table 9: Summary of CTI criteria for use by the method for the assessment of AP at the product level

CTI Criteria	Type of criteria	ISO/IEC 18045 rating criteria correspondence
C1 - Access/time with the product for attack preparation	Opportunity	Part of window of opportunity and elapsed time
C2 - Access/time with the product in application context for attack execution	Opportunity	Part of window of opportunity and elapsed time
C3 – Knowledge of the TOE	Opportunity	Knowledge of the TOE
C4 - Knowledge of vulnerabilities	Opportunity	No direct equivalence but could be part of knowledge of the TOE
C5 - Access to the source or production	Opportunity	Access to source: part of knowledge of the TOE Access to production: no equivalence but could be rated under Window of opportunity and/or *Means (to be studied further)*
C6 - Ability to access/modify product/components in the supply chain to introduce vulnerabilities	Opportunity	No direct equivalence but could be in Window of opportunity *and/or Means (to be studied further)*
C7 - Ability to recruit insiders	Opportunity	No direct equivalence but could be in Window of opportunity *and/or Means (to be studied further)*
C8 – Equipment	Means	Equipment

CTI Criteria	Type of criteria	ISO/IEC 18045 rating criteria correspondence
C9 - Avoidance of visibility	Means / Motive	No equivalence
C10 - Funds to substitute for lack of components	Means	No direct equivalence but could be part of Equipment (as the price is considered)
C11 - General attack knowledge	Means	Expertise
C12 - Available methods	Means	Expertise (related to the use of equipment and methods)
C13 – Time window to reach goals	Motive	No equivalence
C14 - Derived value	Motive	No equivalence
C15 - Objective	Motive	No equivalence
C16 - Legal and ethical limits	Motive	No equivalence
C17 - Geopolitical context	Motive	No equivalence

The table below lists a method to determine an attack potential level based on those CTI inputs that have an impact on the vulnerability analysis of an ICT product or system and that are to be considered in the determination of CAR (see Chapter 5.6) and CSL (see Chapter 5.5).

Four groups of attacker characteristics based on these CTI inputs have been determined: the expertise, the knowledge, the resources, and the opportunity of an attacker to perform an attack.

Each of these groups is associated with four levels of attacker expertise: Layman, Proficient, Expert and Multi-Expert. Level definitions are for the current version of this document taken directly from ISO/IEC 18045.

Table 10: Method for estimating AP by applying CTI characteristics relevant to the vulnerability analysis

CTI characteristics	ISO 18045 equivalence	AP1 Unskilled	AP2 Skilled, limited resources and opportunity	AP3 Skilled, significant resources and opportunity	AP4 Highly skilled, significant resources and opportunity	AP5 Highly sophisticated, significant resources and opportunity
Expertise *C11, C12*	Expertise	Layman	Proficient	Proficient	Expert	Multi-Expert
Knowledge *C3, C4, C5*	Knowledge of the TOE	Public	Public	Restricted	Sensitive	Critical
Resources *C5, C6, C7, C8, C10*	Equipment	Standard	Standard	Specialized	Specialized	Bespoke
Opportunity *C1, C2, C5, C6*	Windows of opportunity Elapsed Time	Unlimited / Easy	Easy	Moderate	Difficult	Difficult

The method should be applied for those types of attackers that have been identified as relevant by the assessment of sectoral risk in relation to the particular supporting ICT product, ICT process or ICT service.

The overall attack potential level assigned to a supporting ICT product, ICT process or ICT service for a particular attacker type is defined by the highest one selected for a group of characteristics.

Where there are several motivated attackers, the overall attack potential level assigned to a supporting ICT product, ICT process or ICT service is defined by the highest level reached by a relevant type of attacker.

A ANNEX: CONCEPTUAL APPROACH FOR CONSISTENCY OF TERMINOLOGY

A.1 BACKGROUND

According to the ISO/IEC JTC1 Directives, Part 2, Clause 16.4, 'Terms and definitions should preferably be listed according to the hierarchy of the concepts (i.e. systematic order). Alphabetical order is the least preferred order.'

Concept approach is described in several international standards related to terminology developed by the ISO Technical Committee TC37 Language and Terminology.

A fundamental principle for this approach is that one term corresponds to one concept, and only one concept corresponds to one term in a given domain or subject in a given language.

For this document, relevant terms are defined as follows:

- concept means a unit of knowledge created by a unique combination of characteristics;
- term means a verbal designation of a general concept in a specific domain or subject;
- definition means a representation of a concept by a descriptive statement which serves to differentiate it from related concepts.

The concept can have its definition but this is not always the case.

Systematic order requires identification of unique concepts and further determining terms which relate to the concept and provide the necessary characteristics. Characteristics can bind terms in subsequent levels of dependency, thus creating a hierarchy of terms. Systematic order is achieved by the proper numbering in the hierarchy of terms to reflect levels of dependency on the concept (see Figure 23). In standards one can find different styles of numbering that express the hierarchy of terms (see Figure 24). The only condition is to use the style consistently.

The style of numbering shown in Figure 23 is used in this document.

Figure 23: Numbering of terms showing dependency on the concept (1. example)

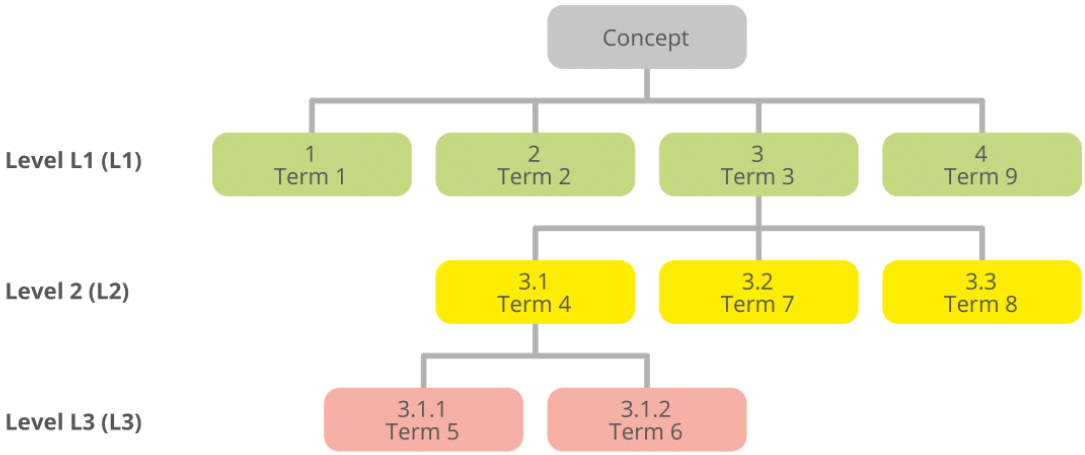
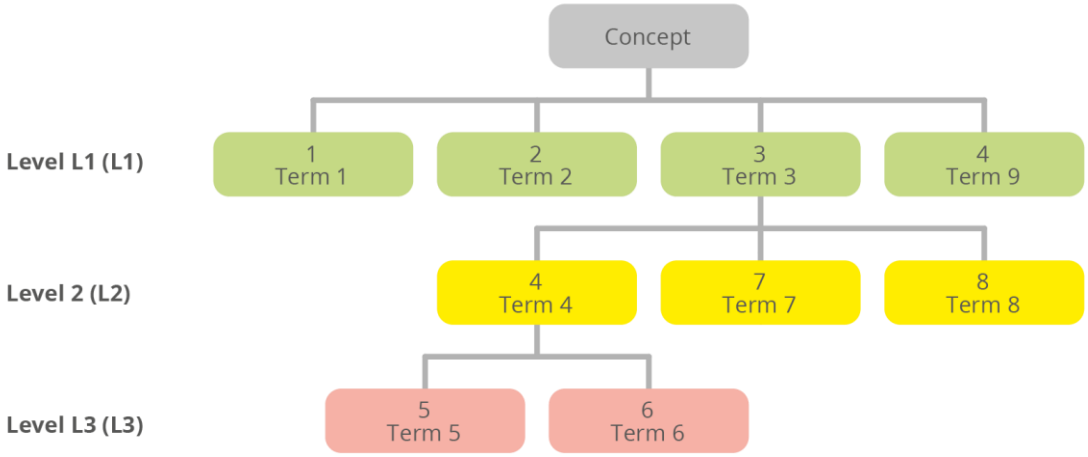


Figure 24: Numbering of terms showing dependency on the concept (2. example)



Minimising the number of concepts is recommended in order to produce a clear picture of the relationships inside a single concept map and limit cross-relations between concepts.

An excellent introduction to the concept approach is given in JTC1 Standing Document N20 Best practices for IT Vocabulary.

Although the systematic approach has been used in ISO standards for the presentation of terminology for many years (see, for example, ISO/IEC 9000) it has not been widely applied in the IT security domain due to its complexity and heritage of old security references. However, the concept approach can help in understanding the terminology and facilitate interconnection between different realms of knowledge.

Often terminology is presented in the form of concept mapping, which allows all relationships to be shown and emphasizes the significant characteristics of the concept. Such will be the form in this document.

A.2 THE CONCEPTUAL APPROACH APPLIED TO THE 15408-BASED MODEL OF IT SECURITY EVALUATION

A.2.1 The 'TOE' concept preliminary considerations

ISO/IEC 15408-1 presents two high-level models upon which IT security evaluation is based, i.e. the security model and the evaluation model.

If one concept is to be chosen to describe what IT security evaluation really means then that would be **Target of Evaluation (TOE).**

The definition for TOE included in ISO/IEC 15408-1 includes 'set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation'.

If we were to analyse the whole set of almost two hundred terms in ISO/IEC 15408 and ISO/IEC 18045 five essential characteristics of the TOE could be found, i.e. (1) Asset, (2) Operational environment, (3) Security Problem Definition, (4) TOE Security Functionality, (5) Vulnerability.

These five principal characteristics form the highest level of systematic order for the TOE. These characteristics are further explained with the second and third level of terms, if applicable (see Table 11). Terms relate to each other and, if significant relationships are found, such a map would be a simple representation of the IT product security evaluation, which is depicted in **Figure 25**.

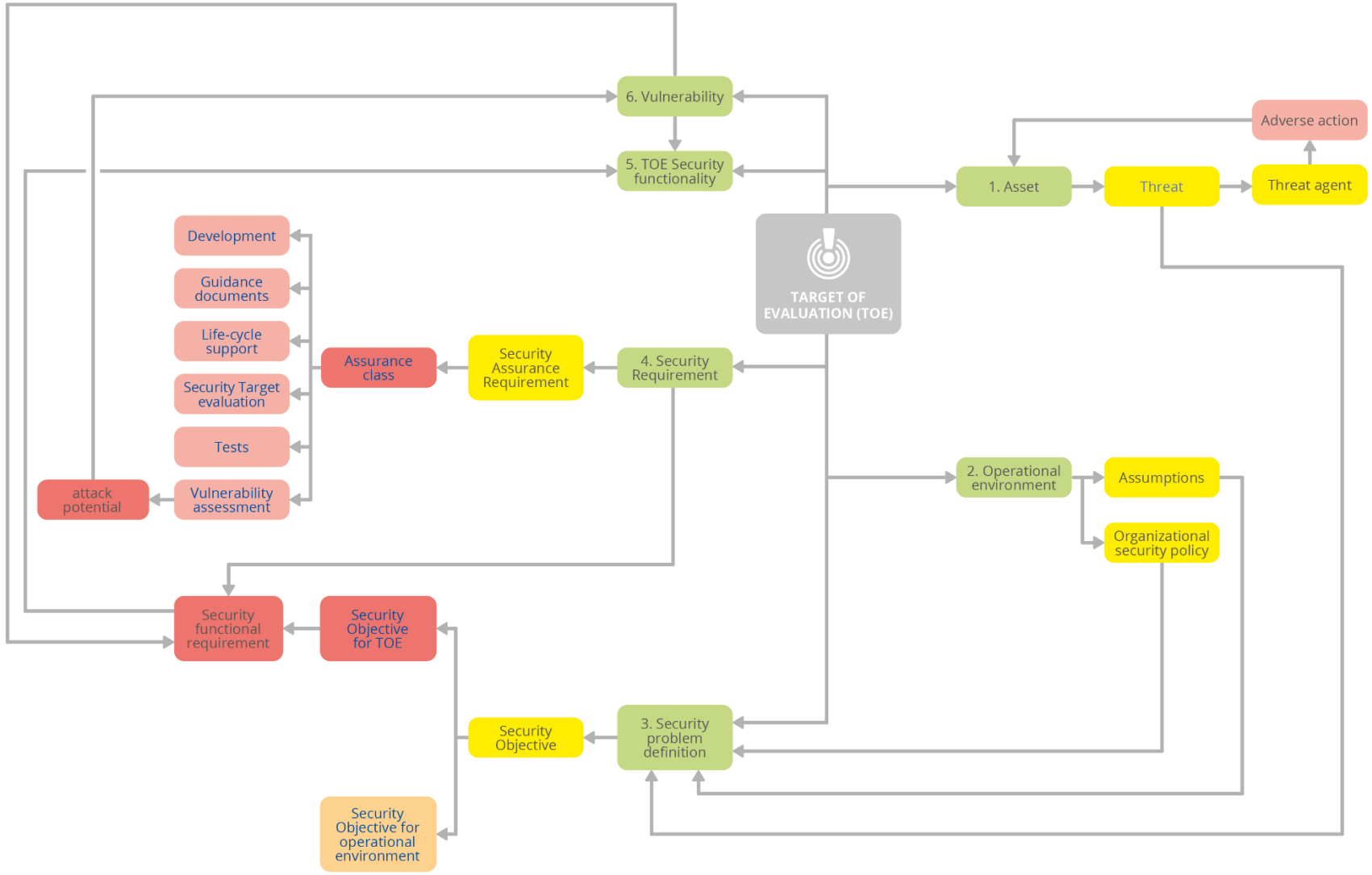
A chosen subset of terminology from ISO/IEC 15408 and ISO/IEC 18045 is sufficient for the methodology.

NOTE 1: Colours of the nodes presented in the map indicate subsequent levels (L1-L3) of terms given in systematic order. The same colours are reflected in the table containing terms and their definitions.

NOTE 2: Terms in blue font contained in the concept map do not have separate definitions in ISO/IEC 15408-1 or ISO/IEC 18045 for three reasons: a) they have their common dictionary meaning (e.g. threat), or b) they can be derived from a defined term (e. g. security objective for an operational environment), or c) two defined terms combined create a new term (e.g. assurance class). There are no separate levels for such terms,

NOTE 3: Assurance classes indicated in the picture are shown for completeness of the assurance description. For the simplicity of the concept map, only the vulnerability assessment class is further analysed.

Figure 25: Concept map for TOE



A.2.2 Terms in systematic order

Table 11 presents all relevant terms in systematic order. Terms in green represent major characteristics for the TOE (in red font, the concept).

Table 11: Systematic order for the TOE concept

L1	L2	L3	L4	L5	L6	Term	Current definition
1						asset	entity that the owner of the TOE presumably places value upon
1	1					threat agent	entity that can exercise adverse actions on assets protected by the TOE
1	1	1				adverse action	action performed by a threat agent on an asset
2						operational environment	environment in which the TOE is operated
2	1					organizational security policy OSP	set of security rules, procedures, or guidelines for an organization Note 1 to entry: A policy may pertain to a specific operational environment.
3						security problem security problem definition SPD	statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address Note 1 to entry: This statement consists of a combination of: threats to be countered by the TOE and its operational environment, the OSPs enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.
3	1					security objective	statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions
3	1	1				security functional requirement, SFR	security requirement, which contributes to fulfil the TOE's Security Problem Definition (SPD) as defined in a specific ST or in a PP
4						security requirement*	requirement, stated in 15408 standardized language, which is part of a TOE security specification as defined in a specific ST or in a PP
4	1					security assurance requirement*, SAR	security requirement, which refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user
4	1	1				attack potential	measure of the effort needed to exploit a vulnerability in a TOE Note 1 to entry: The effort is expressed as a function of properties related to the attacker (for example, expertise, resources, and motivation) and properties related to the vulnerability itself (for example, window of opportunity, time to exposure).
5						TOE security functionality TSF	combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs
6						vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment
						*definitions taken from ISO/IEC DIS 15408-1 (Draft International Standard) currently being under revision	

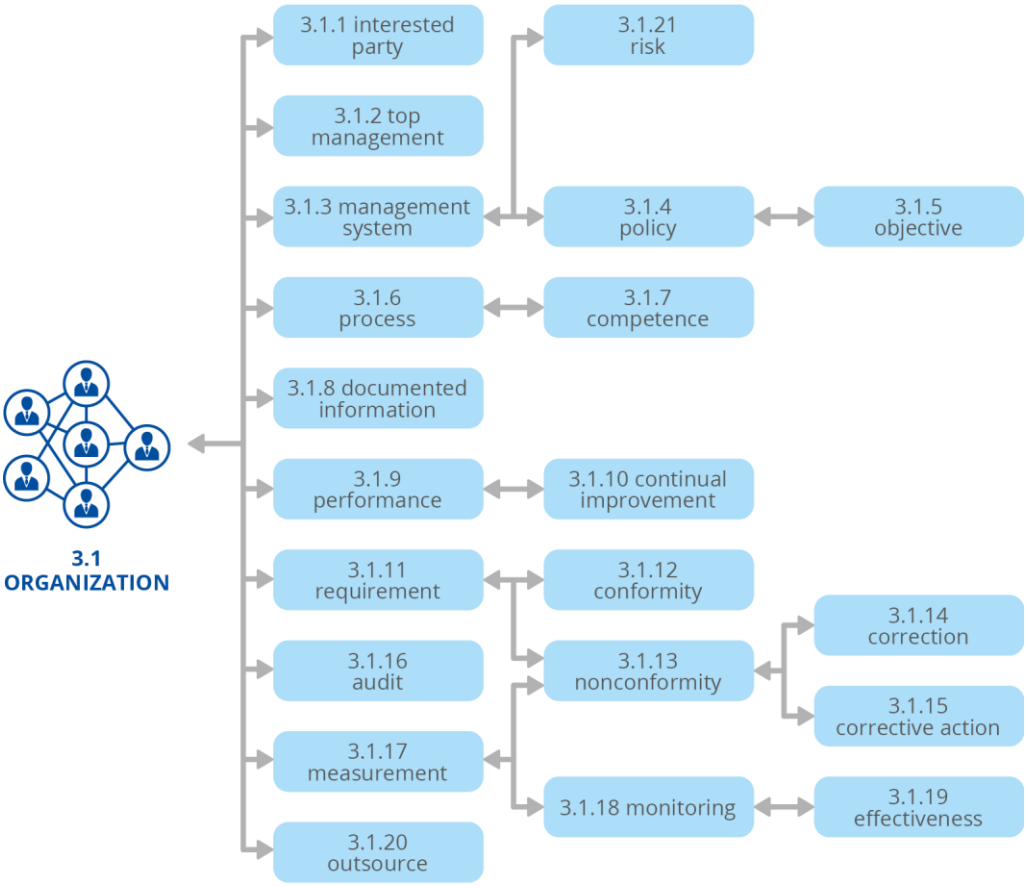
A.3 THE CONCEPTUAL APPROACH APPLIED TO ISO/IEC 27001- BASED ISMS

A.3.1 The 'organization' concept - preliminary considerations

The concept mapping related to terms used in management standards has been developed by a special ISO Task Force called the Joint Technical Coordination Group (JTCG) on MSS [Management System Standards]. This group has developed a conceptual diagram of common terms and core definitions related to management systems[12] (see **Figure 26**). The map created by JTCG is built around the concept of an **'organization.'**

[12] ISO/IEC JTC1/SC27 internal document

Figure 26: Concept diagram for common terms and core definitions – JTCG View



Assuming that part of the terminology defined by the JTCG is identical for all MSSs in the ISO world (including ISO/IEC 27001), terms in the family of ISMS standards have several relationships through the management system objectives specific to ISO/IEC 27001, i.e. related to 'security'. A more detailed concept map relevant to information security risk is presented in Figure 27.

The concept 'organization' has its own definition:

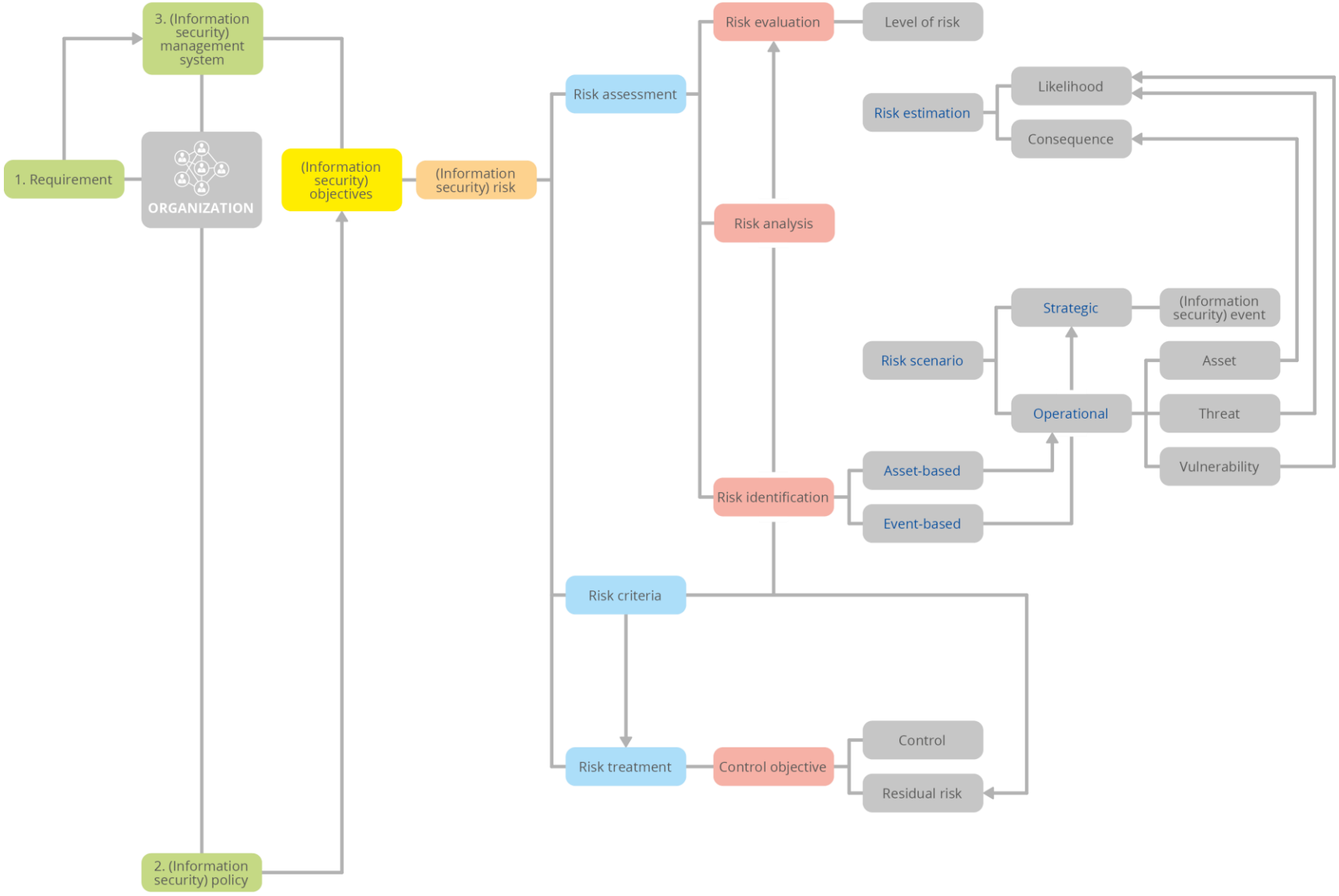
A person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

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.

The same approach as for the ISO/IEC 15408 and ISO/IEC 18045 'TOE' concept applies (see NOTE 1, NOTE 2 and NOTE 3 in Subsection A.2.1).

A chosen subset of terminology from ISO/IEC 27000 is sufficient for the purpose.

Figure 27: Concept map for 'organization.



A.4 THE CONCEPTUAL APPROACH APPLIED TO ISO/IEC 27001- BASED ISMS

The relationships between the two concepts discussed earlier (TOE and organization) are built around risk. It should be noted that the concept of organization leads to the organization's information security management system, which in turn, is based on [information security] objectives. Risk management is dealing with uncertainty on [information security] objectives. Some of the objectives can be assigned to particular assets (we avoid here a discussion on assets, their characteristics, relation to business processes), and typically they are defined with respect to loss of confidentiality, integrity or availability.

If one identifies a risk related to loss of confidentiality or integrity of an asset, and then finds the level of risk unacceptable compared to risk criteria, one possible option to protect the assets is to choose controls to mitigate the risk. If a control appears to be an ICT product, it could be chosen and then implemented based on two criteria set up by the risk owner:

1. specification of [information security] requirements which allow assessed risk related to the asset(s) to be mitigated,

2. expression of needs related to the confidence that implementation of security functionality in the product is done correctly and functionality is sufficient.

The developer responds to the first criterion by designing the security functionalities properly. In that case, the developer performs its own assessment of risk and its treatment leading to the required security functionality.

The vendor of the product (it could be the developer) responds to the need related to confidence by setting up security assurance requirements with clearly defined assurance levels expressing the scope, rigour and depth of the evaluation.

The ICT product, while implemented in its operational environment, mitigates the risk by protecting the asset(s) as expected. In terms of [information security] objectives, the uncertainty is controlled by the control (ICT product).

The relationships between the concepts are shown in **Figure 28**.

Following the guidance given by the developer/vendor, the risk owner may decide to implement relevant controls to address the risks related to the operational environment of the product. In that way the risks identified by the risk owner are addressed completely.

The relationships between the concepts that complement the product itself are shown in **Figure 29**.

Figure 28: Relationships between two concepts based on the risk – assurance view

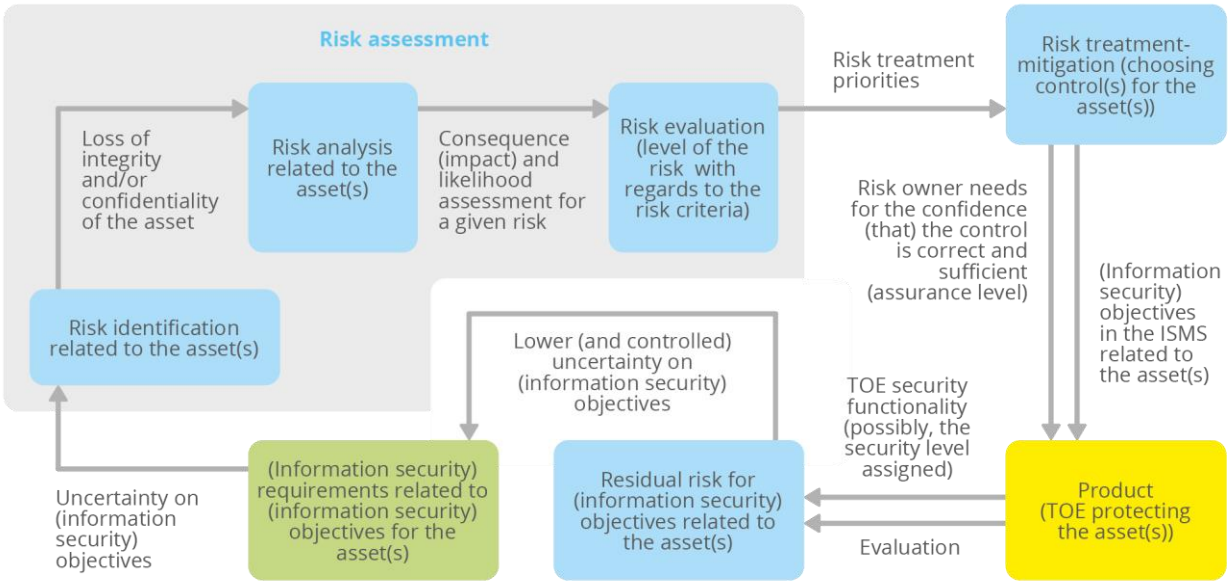
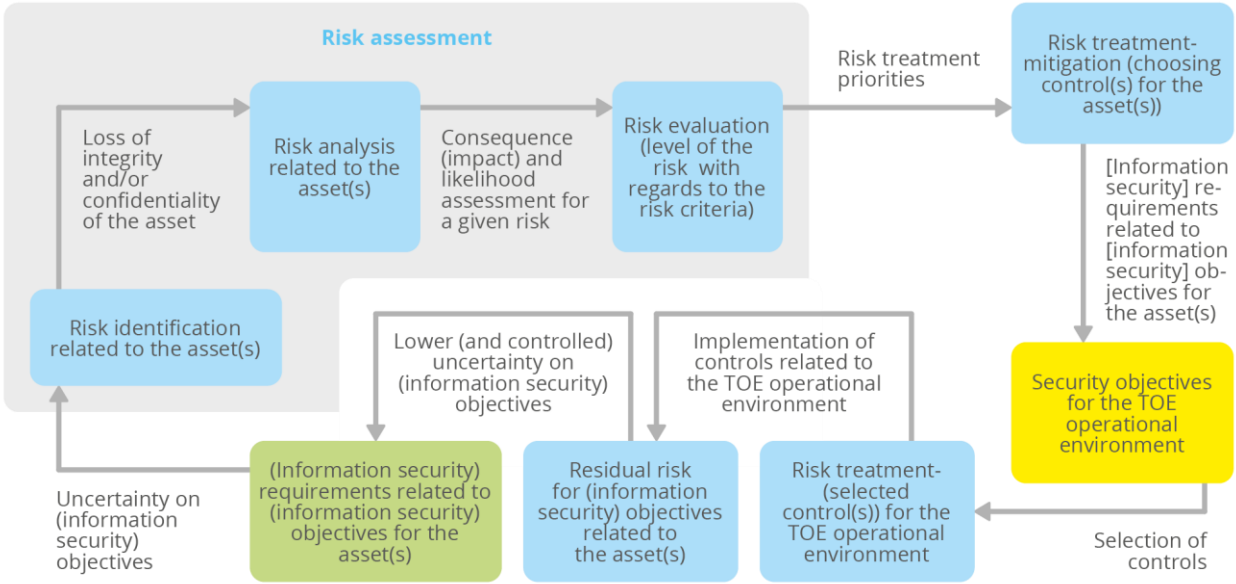


Figure 29: Relationships between two concepts based on risk for the TOE operational environment



The following table provides the definition of terms as given in ISO/IEC 270xx and explains how these should be understood and used in the context of specification of security and assurance in accordance with ISO/IEC 15408.

Table 12: Mapping between terms in ISO/IEC 270xx and ISO/IEC 15408

Term	Current definition in the context of ISMS acc. to the ISO/IEC 270xx series of standards	Application in ISO/IEC 15408-environments
Requirement	Need or expectation that is stated, generally implied or obligatory	This term has a very broad use in ISMSs, and it is related to the organization, while in ISO/IEC 15408 the term [security] requirement is related to the TOE.
[Information security] policy	Intentions and direction of an organization as formally expressed by its top management	[Information security] policy is related to [information security] objectives; meaning of Organizational Security Policy used in ISO/IEC 15408 is different i.e. 'set of security rules, procedures, or guidelines for an organization'.
[Information security] management system	Set of interrelated or interacting elements of an organization to establish policies and **objectives** and processes to achieve those **objectives**	No direct relevance / not applicable for IT products
[Information security] objective	Result to be achieved [by an organization]	[Information security] objective can relate to the security objectives set up to the TOE for protection of specific information asset(s); that could create a base for the organization in choosing the ICT product that meets its needs and expectations
[Information security] risk	Effect of uncertainty on **objectives**	Term not defined in ISO/IEC 15408 although used in the security model to show that the risk owner needs to reduce the risks of the intended use of the product. The information on risk can be used as an input to SPD and SAR.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation [SOURCE: ISO Guide 73:2009]	Term not defined in ISO/IEC 15408. Relevance exists if the organization or the sector assesses the risk related to the intended use of TOE, or broader, the ICT product.
Risk identification	Process of finding, recognizing and describing risks [SOURCE: ISO Guide 73:2009]. Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences.	See risk assessment
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk	See risk assessment
Asset	Anything that has a value for an organization Note 1 to entry: definition re-introduced from version of ISO/IEC 27000:2014	Equivalent to the definition provided by ISO/IEC 15408. Information asset(s) are typically protected by the Security Functionality defined in the TOE or broader ICT product.
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization	The term 'threat' is not defined but used in ISO/IEC 15408 to indicate an adverse action performed by a threat agent on an asset.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats	The term 'vulnerability' is functioning in a different context in ISO/IEC 15408 as it reflects the perspective of the TOE; 'attack potential' is used to prove or deny that the TOE security functionality remains in a secure state regardless of whether the vulnerability is identified or discovered.

Term	Current definition in the context of ISMS acc. to the ISO/IEC 270xx series of standards	Application in ISO/IEC 15408-environments
Likelihood	Chance of something happening	Term not defined in ISO/IEC 15408. Indirect relevance which can be used as an input to SPD and SAR; see risk assessment.
Consequence	Outcome of an event affecting **objectives**	Term not defined in ISO/IEC 15408. Indirect relevance which can be used as an input to SPD and SAR; see risk assessment
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable	Term not defined in ISO/IEC 15408. See risk assessment.
Risk treatment	Process to modify risk Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as 'risk mitigation', 'risk elimination', 'risk prevention' and 'risk reduction'.	Term not defined in ISO/IEC 15408. The TOE - or broader - ICT Product, meets the organization's security requirements aimed at the protection of specific asset(s) and, if evaluated, provides the ground for confidence that the product fits its intended use.
Control	Measure that is modifying risk	Term not defined in ISO/IEC 15408. This term can be seen as equivalent to the Security Functional Requirements (SFRs) defined in ISO15408.
Residual risk	Risk remaining after risk treatment	This term is not used in ISO/IEC 15408, although it directly relates to the risk of the intended use of the ICT product.

B ANNEX: GUIDANCE FOR THE RISK-BASED SELECTION OF IMPACT CLASSES

Six risk areas are proposed as generally applicable to all sectors. These include impact on business operations and functionality; citizens; the type of data processed; reputation and trust; compliance with contractual requirements; and health and life.

Table 13 shows 5 proposed sectoral impact classes (IC1 to IC5) within the 6 risk areas outlined above. The number of impact classes has been selected to correspond to the 5 levels of the Common Security Level (CSL) and the Common Assurance Reference (CAR) that are presented in Subsection 5.5.2 and in Subsection 5.6.5. The risk areas given in Table 13 are not exhaustive but may be added, or adapted, to meet the requirements of different sectors.

The impact defined for each class with the risk areas must be regarded as the minimum level that shall be applied by a sector. However, sectors are permitted to increase the impact class level definition where they feel this is justified. For example, any impact on personal data, in the risk area concerning type of data processed, shall be assessed at least at IC2. However, the sectoral stakeholders may consider that this particular factor is of more concern to their sector, and the impact on personal data should have an impact level of IC3 or higher.

In addition, sectors could decide to create more specific definitions. For example, a sector may consider that the definition of IC2 in that risk area should instead be: ‘personal data of fewer than 10 individuals’. Whilst the definition of IC3 in that risk area should be: ‘special categories of personal data OR personal data of more than 10 individuals’. Sectoral stakeholders are also free to add additional risk areas to their assessment.

As **Table 13** represents minimum requirements, a reduction in impact class is not foreseen. For example, the stakeholders may not reduce the IC level if loss of life (IC5) has to be assumed as an impact. Thus, in other words, cell contents may be shifted to the right, but not to the left.

Table 13: Definitions for 5 levels of sectoral impact classes (IC1-IC5) in 6 risk areas.

Risk Area	IC1	IC2	IC3	IC4	IC5
1. Business operations and functionality	Limited impact on a single organization	Significant impact on a single organization	Limited impact on multiple entities in a sector or Significant impact on a few entities in a sector	Significant impact on multiple entities within a few sectors or Significant impact on a few entities within multiple sectors	Disruption of an entire sector and/or significant impact on the business, economy and society as a whole
2. Impact on citizens (e.g. failure to meet expected availability of services)	Minor impact on daily activities of citizens		Major impact on daily activities of citizens		Severe impact on daily activities of citizens
3. Type of data processed	Sectoral Intellectual Property	Personal data	Special categories of personal data	Data essential for critical infra-structures	Data affecting national security
4. Reputation and trust	Minor damage to reputation of a few organizations	Minor damage to reputation of many organizations and/or a sector	Major damage to reputation of many organizations and/or a sector	Major damage to reputation of whole sector and/or damage to trust in specific technology or service(s)	Major damage to reputation of more than one sector and/or loss of trust in specific technology or service(s)
5. Contractual requirements	Minor non-compliance with contractual requirements		Major non-compliance with contractual requirements		
6. Health and life			Negative effects on health for people and/or environment that may not be recoverable	Life-changing health effects and/or environmental damage	Potential loss of life and/or environmental damage

C ANNEX: MAPPING BETWEEN ISO/IEC 270XX-BASED RISK ASSESSMENT INFORMATION AND ISO/IEC 15408-BASED PRODUCT SPECIFICATION

The following table provides an overview of information generated by the sectoral cybersecurity assessment that could be of use for the definition of ISO/IEC 15408 items. Italic print indicates the step of the workflows described in Chapter 6 where this information is generated.

ISO/IEC 15408 items to be defined for product definition	Sectoral risk analysis information needed for the definition of ISO/IEC 15408 items *(relation with workflows described in Chapter 6)*	Examples
Threats	List of primary information or functional assets *(supported by A-6)*	Sensitive data (e.g. user data, cryptographic data, logs) - confidentiality, integrity, access Sensitive code - confidentiality, integrity, access Sensitive documents/information - confidentiality, integrity, access Restricted services - access Restricted services/areas - access Material (e.g. goods)
	List of unwanted incidents described by risk scenarios *(supported by B-1, C-2)*	Confidential data disclosure Confidential code disclosure Confidential information disclosure Data modification Code modification Information modification Code execution disturbance Illegal access to / use of restricted data/feature Illegal access to / use of restricted information/area Stealing of material
	Identification of attack surface / interfaces *(supported by C-1)*	Product hardware interfaces (e.g. CPU, memories, buses, debug port) Product software interfaces (APIs, binary, debug software features) Site areas entry points (e.g. doors, fire doors, windows, perimeter entries)

ISO/IEC 15408 items to be defined for product definition	Sectoral risk analysis information needed for the definition of ISO/IEC 15408 items *(relation with workflows described in Chapter 6)*	Examples
	List of known inherent vulnerabilities *(supported by C-2)*	Use of CPU sensitive to micro-architectural attacks Use of DDRAM sensitive to Rowhammer attacks
	Identification of potential attacker types *(supported by C-2)*	Independent hackers Organizations, states Users (e.g. product owners, employees, customers) Software processes Accidents
	Identification of attack means *(supported by C-2)*	Hardware tools (e.g. lasers, EM probes, bus probes, FIB) Software vectors Badges Employee compromising Social engineering
Assumptions	List security measures (controls) *(supported by C-1)*	Trust in administrators Trust in (privileged) employees Protection by physical access restriction
OSPs	List of regulations to be implemented *(supported by C-1)*	Directives, laws
	List of organization policies, requirements and objectives to be implemented by the product or the environment *(supported by C-1)*	
	List of standards and processes to be implemented (e.g. for interoperability) *(supported by C-1)*	Specifications, algorithms
	List of required certificates (security certificates, interoperability certificates) *(supported by C-1)*	ISO/IEC 27001, if applicable combined with sector/application specific standard (ISO/IEC 27010, 27011, 27017, 27018, 27019)
		Product certificates (e.g. ISO/IEC 15408 certificates for supporting products or product components)
		Interoperability certificates
Evaluation Assurance Level	List of reasons why an unwanted incident would occur including risks sources *(supported by B-1, B-3)*	Existence of valuable assets (CIA) and unwanted events (risks) Existence of theoretical vulnerabilities

ISO/IEC 15408 items to be defined for product definition	Sectoral risk analysis information needed for the definition of ISO/IEC 15408 items *(relation with workflows described in Chapter 6)*	Examples
	Evaluation of type of impacts of each incidents *(supported by B-3)*	Business impact Reputation and trust impact Citizens impact Privacy impact Health and life impact Compliance impact
	Identification of mitigation of listed incidents *(supported by B-2, C-1, C-2)*	Scalability: only specific target, any target Likelihood: system/product specific environment, attacker motivations and profile
Security Level	Identification of attack surface	Product hardware interfaces (e.g. CPU, memories, buses, debug port) Product software interfaces (APIs, binary, debug software features) Site areas entry points (e.g. doors, fire doors, windows, perimeter entries)
	Identification of attack means *(supported by A-7, C-2)*	Hardware tools (e.g. lasers, EM probes, bus probes, FIB) Software vectors Badges Employee compromising Social engineering
	List of known inherent vulnerabilities *(supported by C-2, if available)*	Use of CPU sensitive to microarchitectural attacks Use of RAM sensitive to Rowhammer attacks
	Evaluation of type of impacts of each unwanted incident *(supported by B-3)*	Business impact Reputation and trust impact Citizens impact Privacy impact Health and life impact Compliance impact
	Identification of mitigation of listed unwanted incidents *(supported by B-2, C-1, C-2)*	Scalability: only specific target, any target Likelihood: system/product specific environment, attacker motivations and profile

D ANNEX: GUIDANCE FOR THE RISK-BASED SELECTION OF IMPACT CLASSES

This annex was generated to support the internal considerations on the common assurance reference concept, which are documented in Section 5.6. It summarizes relevant parts of the ISO/IEC 15408 series of standards for a better overview and could therefore be useful for readers of this document.

This annex is of an informative nature. In case of deviations from the standard, the standard applies.

D.1 OVERVIEW

Every assurance component of the AVA_VAN family is characterized by three elements: scope, depth and rigour of vulnerability assessment. Based on the characteristics of these elements, five levels are defined and briefly described

Level ID	Scope (input documentation for devising pen tests)	Depth of scrutiny	Depth of pen tests measured by attack potential	Rigour - pen test method applied
AVA_VAN.1 Vulnerability survey	TOE, ISO/IEC 15408 Security Target, documentation ensuring correct configuration of the TOE in a secure manner, as intended by the developer, basic security functional specification	Tests devised based on basic security functional specification	Basic	Survey on publicly known vulnerabilities
AVA_VAN.2 Vulnerability analysis	Same as previous level + security architecture, basic decomposition to subsystems, functional specification of TOE interfaces enforcing security functional specification	Tests devised based on detailed documentation of data flow on TOE interfaces and between subsystems	Basic	Same as previous level + potential vulnerabilities identified based on documentation analysis
AVA_VAN.3 Focused vulnerability analysis	Same as previous level + complete decomposition to subsystems and modules, functional specification of all TOE interfaces, implementation representation (e.g. source code), basic test documentation (showing internal interfaces in modules)	Tests devised based on detailed documentation of data flow on TOE interfaces between modules and internal module interfaces, source code analysis	Enhanced Basic	Same as previous levels + focused analysis based on the flow hypothesis approach

AVA_VAN.4 Methodical vulnerability analysis	no differences compared to previous level	no differences compared to previous level	Moderate	Same as previous levels + structural (predetermined) analysis based on the flow hypothesis approach
AVA_VAN.5 Advanced methodical vulnerability analysis	requirements defined by the scheme		High	requirements defined by the scheme

The following subsections of this annex contain detailed analyses of each AVA_VAN component in terms of:

- description of documentation required by evaluator to perform intended actions.
- what is required to prepare TOE for penetration tests (preparatory actions).
- description of penetration testing.

Descriptions of subsequent sub-activities are based on the content of ISO/IEC 15408-3.

Numbering of subsequent actions are taken from appropriate section of ISO/IEC 18045 relevant to particular AVA_VAN components.

D.2 BASELINE AVA_VAN.1

Dependencies	Assurance component description	Additional remarks
ADV_FSP.1	Basic functional specification	Basic requirements of the functional specification that describes the TSF interfaces (TSFIs) i.e. a characterisation of all TSFIs and a high level description of SFR-enforcing and SFR-supporting TSFIs
AGD_OPE.1	Operational user guidance	Necessary for corect configuration of the TOE
AGD_PRE.1	Preparative procedures	Necessary to ensure that the TOE has been received and installed in a secure manner as intended by the developer
Developer action		
AVA_VAN.1.1D	The developer shall provide the TOE for testing.	
Content and Presentation		
AVA_VAN.1.1C	The TOE shall be suitable for testing.	
Actions/Work units		
AVA_VAN.1.1E	The information provided meets all requirements for content and presentation of evidence to be confirmed	
1.	Test configuration is consistent with the configuration under evaluation as specified in the ST	
2.	TOE has been installed properly and is in a known state	

AVA_VAN.1.2E	Search of public domain sources
3.	Sources of information publicly available to identify potential vulnerabilities in the TOE to be examined While examining the evidence provided, the evaluator will use the information in the public domain to further search for potential vulnerabilities. Where the evaluators have identified areas of concern, the evaluator should consider information publicly available that relates to those areas of concern.
4.	Identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment to be recorded in the ETR
AVA_VAN.1.3E	Penetration testing
5.	Penetration tests to be devised
6.	Penetration test documentation to be produced
7.	Penetration tests to be conducted
8.	Actual results of the penetration tests to be recorded
9.	Penetration testing effort, outlining the testing approach, configuration, depth and results to be recorded
10.	The results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a **basic** attack potential, are to be examined.
11.	All exploitable vulnerabilities and residual vulnerabilities to be reported in the ETR
Evaluation evidence:	
Input:	
a) ST; b) Guidance documentation; c) TOE suitable for testing; d) Information publicly available to support the identification of potential vulnerabilities.	
Other input:	
a) Current information regarding potential vulnerabilities (e.g. from an evaluation authority.	

D.3 BASELINE AVA_VAN.2

Dependencies	Assurance component description	Additional remarks
ADV_ARC.1	Security architecture description	Necessary requirements and analysis of the TOE based on properties of domain separation, self-protection, and non-bypass ability. Note: The properties of self-protection, domain separation, and non-bypass ability are distinct from security functionality expressed by Part 2 SFRs because self-protection and non-bypass ability largely have no directly observable interface at the TSF.
ADV_FSP.2	Security-enforcing functional specification	The developer is required to provide the purpose, method of use, parameters, and parameter descriptions for all TSFIs. Additionally, for the SFR-enforcing TSFIs the developer has to describe the SFR-enforcing actions and direct error messages.
ADV_TDS.1	Basic design	The design shall describe the structure of the TOE in terms of subsystems. The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
AGD_OPE.1	Operational user guidance	Necessary for correct configuration for the TOE
AGD_PRE.1	Preparatory procedures	Necessary to ensure the TOE has been received and installed in a secure manner as intended by developer
Developer action		
AVA_VAN.2.1D	The developer shall provide the TOE for testing.	
Content and Presentation		
AVA_VAN.2.1C	The TOE shall be suitable for testing.	
Actions/Work units		
AVA_VAN.2.1E	That the information provided meets all requirements for content and presentation of evidence is to be confirmed	
1.	Test configuration is consistent with the configuration under evaluation as specified in the ST	
2.	TOE has been installed properly and is in a known state	
AVA_VAN.2.2E	Search of public domain sources	
3.	Sources of information publicly available to identify potential vulnerabilities in the TOE to be examined. While examining the evidence provided, the evaluators will use the information in the public domain to further search for potential vulnerabilities. Where the evaluators have identified areas of concern, the evaluators should consider information publicly available that relate to those areas of concern.	
AVA_VAN.2.3E	**Independent** vulnerability analysis of the TOE, using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE, to be performed The unstructured analysis permits the evaluators to consider the generic vulnerabilities. The evaluators will also apply their experience and knowledge of flaws in similar technology types.	
4.	Subject to the SFRs the TOE is to meet in the operational environment, the evaluators' independent vulnerability analysis should consider generic potential vulnerabilities under each of the following headings: a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may be supplied by the evaluation authority; b) bypassing; c) tampering; d) direct attacks; e) monitoring; f) misuse.	

5.	Identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment to be recorded in the ETR
AVA_VAN.2.4E	Penetration testing
6.	Penetration tests to be devised
7.	Penetration test documentation to be produced
8.	Penetration tests to be conducted
9.	Actual results of the penetration tests to be recorded
10.	Penetration testing effort, outlining the testing approach, configuration, depth and results to be recorded
11.	The results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a **basic** attack potential, are to be examined.
12.	All exploitable vulnerabilities and residual vulnerabilities, to be reported in the ETR
Evaluation evidence:	
Input:	
a) ST; b) Functional specification; c) The TOE design; d) The security architecture description; e) The guidance documentation; f) The TOE suitable for testing; g) Information publicly available to support the identification of possible potential vulnerabilities.	
Other input:	
a) Current information regarding public domain potential vulnerabilities and attacks (e.g. from an evaluation authority).	

D.4 BASELINE AVA_VAN.3

Dependencies	Assurance component description	Additional remarks
ADV_ARC.1	Security architecture description	Necessary requirements and analysis of the TOE based on properties of domain separation, self-protection, and non-bypass ability. Note: The properties of self-protection, domain separation, and non-bypass ability are distinct from security functionality expressed in Part 2 SFRs because self-protection and non-bypass ability largely have no directly observable interface at the TSF.
ADV_FSP.4	Complete functional specification	The developer is required to provide information of all TSFIs - whether SFR-enforcing, SFR-supporting, SFR-non-interfering - and each must be described to the same degree, including all of the direct error messages.
ADV_TDS.3	Basic modular design	A mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design is to be provided by the developer.
ADV_IMP.1	Implementation representation of the TSF	The implementation representation is made available to allow analysis of other TOE design decompositions (e.g. functional specification, TOE design), and to gain confidence that the security functionality described at a higher level in the design actually appears to be implemented in the TOE. The implementation representation is expected to be in a form that captures the detailed internal workings of the TSF. This may be software source code, firmware source code, hardware diagrams and/or IC hardware design language code or layout data.
AGD_OPE.1	Operational user guidance	Necessary for the correct configuration of the TOE
AGD_PRE.1	Preparative procedures	Necessary to ensure that the TOE has been received and installed in a secure manner as intended by developer
ATE_DPT.1	Testing: basic design	Evidence of testing of this TOE design must show that the internal interfaces have been exercised and seen to behave as described. Testing at the level of the TOE subsystems provides assurance that the TSF subsystems behave and interact as described in the TOE design and the description of the security architecture.
Developer action		
AVA_VAN.3.1D	The developer shall provide the TOE for testing.	
Content and Presentation		
AVA_VAN.3.1C	The TOE shall be suitable for testing.	
Actions/Work units		
AVA_VAN.3.1E	That the information provided meets all the requirements for content and presentation of evidence is to be confirmed	
1.	Test configuration is consistent with the configuration under evaluation as specified in the ST	
2.	TOE has been installed properly and is in a known state	
AVA_VAN.3.2E	Search of public domain sources	

3.	Sources of information publicly available to identify potential vulnerabilities in the TOE are to be examined While examining the evidence provided, the evaluators will use the information in the public domain to further search for potential vulnerabilities. Where the evaluators have identified areas of concern, they should consider information publicly available that relates to those areas of concern.
AVA_VAN.3.3E	**Independent, focused** vulnerability analysis of the TOE, using the guidance documentation, functional specification, TOE design, security architecture description and **implementation representation** to identify potential vulnerabilities in the TOE, is to be performed. A focused approach to the identification of vulnerabilities is an analysis of the evidence with the aim of identifying any potential vulnerabilities evident in the available information. It is an unstructured analysis, as the approach is not predetermined. During the conduct of evaluation activities the evaluator may also identify areas of concern. These are specific portions of the TOE evidence that the evaluator has some reservation about, although the evidence meets the requirements for the activity with which the evidence is associated.
4.	The evaluator uses knowledge of the TOE design and operation gained from the TOE deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE and potential errors in the method specified for the operation of the TOE. The following are some examples of the approach a hypothesis may take: a) consideration of malformed input for interfaces available to an attacker at the external interfaces; b) examination of a key security mechanism cited in the description of the security architecture, such as process separation, hypothesizing internal buffer overflows that may lead to degradation of separation; c) search to identify any objects created in the TOE implementation representation that are then not fully controlled by the TSF and could be used by an attacker to undermine SFRs. The identification process is iterative, i.e. where the identification of one potential vulnerability may lead to the identification of another area of concern that requires further investigation. Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent vulnerability analysis should consider generic potential vulnerabilities under each of the following headings: a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may be supplied by the evaluation authority; b) bypassing; c) tampering; d) direct attacks; e) monitoring; f) misuse.
5.	Identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment are to be recorded in the ETR
AVA_VAN.3.4E	Penetration testing
6.	Penetration tests to be devised
7.	Penetration test documentation to be produced
8.	Penetration tests to be conducted
9.	Actual results of the penetration tests to be recorded
10.	Penetration testing effort, outlining the testing approach, configuration, depth and results to be recorded
11.	The results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing an **enhanced-basic** attack potential, to be examined
12.	All exploitable vulnerabilities and residual vulnerabilities, to be reported in the ETR

Evaluation evidence:
Input:
a) ST; b) Functional specification; c) The TOE design; d) The security architecture description; e) The implementation representation; f) The guidance documentation; g) The TOE suitable for testing; h) Information publicly available to support the identification of possible potential vulnerabilities; i) The results of testing the basic design.
Other input:
a) Current information regarding public domain potential vulnerabilities and attacks (e.g. from an evaluation authority).

D.5 BASELINE AVA_VAN.4

Dependencies	Assurance component description	Additional remarks
ADV_ARC.1	Security architecture description	Necessary requirements and analysis of the TOE based on the properties of domain separation, self-protection, and non-bypass ability. Note: The properties of self-protection, domain separation, and non-bypass ability are distinct from security functionality expressed by Part 2 SFRs because self-protection and non-bypass ability largely have no directly observable interface at the TSF.
ADV_FSP.4	Complete functional specification	The developer is required to provide information of all TSFIs - whether SFR-enforcing, SFR-supporting, SFR-non-interfering - and each must be described to the same degree, including all of the direct error messages.
ADV_TDS.3	Basic modular design	A mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design is to be provided by the developer.
ADV_IMP.1	Implementation representation of the TSF	The implementation representation is made available to allow analysis of other TOE design decompositions (e.g. functional specification, TOE design), and to gain confidence that the security functionality described at a higher level in the design actually appears to be implemented in the TOE. The implementation representation is expected to be in a form that captures the detailed internal workings of the TSF. This may be software source code, firmware source code, hardware diagrams and/or IC hardware design language code or layout data.
AGD_OPE.1	Operational user guidance	Necessary for the correct configuration of the TOE
AGD_PRE.1	Preparatory procedures	Necessary to ensure the TOE has been received and installed in a secure manner as intended by developer
ATE_DPT.1	Testing: basic design	Evidence of testing of this TOE design must show that the internal interfaces have been exercised and have been seen to behave as described. Testing at the level of the TOE subsystems provides assurance that the TSF subsystems behave and interact as described in the TOE design and the description of the security architecture.
Developer action		
AVA_VAN.4.1D	The developer shall provide the TOE for testing.	
Content and Presentation		
AVA_VAN.4.1C	The TOE shall be suitable for testing.	
Actions/Work units		
AVA_VAN.4.1E	That the information provided meets all the requirements for content and presentation of evidence is to be confirmed	
1.	Test configuration is consistent with the configuration under evaluation as specified in the ST	
2.	TOE has been installed properly and is in a known state	
AVA_VAN.4.2E	Search of public domain sources	
3.	Sources of information publicly available to identify potential vulnerabilities in the TOE are to be examined While examining the evidence provided, the evaluators will use the information in the public domain to further search for potential vulnerabilities. Where the evaluators have identified areas of concern, they should consider information publicly available that relates to those areas of concern.	

AVA_VAN.4.3E	**Independent , methodical** vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and **implementation representation** to identify potential vulnerabilities in the TOE is to be performed The methodical analysis approach takes the form of a structured examination of the evidence. This method requires the evaluator to specify the structure and form the analysis will take (i.e. the manner in which the analysis is performed is predetermined, unlike the focused identification method).
4.	The evaluator uses the knowledge of the TOE design and operation gained from the TOE deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE and potential errors in the method specified for the operation of the TOE. The following are some examples of the approach a hypothesis may take: a) consideration of malformed input for interfaces available to an attacker at the external interfaces; b) examination of a key security mechanism cited in the description of the security architecture such as process separation, hypothesizing internal buffer overflows that may lead to degradation of separation; c) search to identify any objects created in the TOE implementation representation that are then not fully controlled by the TSF and could be used by an attacker to undermine SFRs. The identification process is iterative, i.e. where the identification of one potential vulnerability may lead to the identification of another area of concern that requires further investigation. Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent vulnerability analysis should consider generic potential vulnerabilities under each of the following headings: a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may be supplied by the evaluation authority; b) bypassing; c) tampering; d) direct attacks; e) monitoring; f) misuse.
5.	Identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment are to be recorded in the ETR
AVA_VAN.4.4E	Penetration testing
6.	Penetration tests to be devised
7.	Penetration test documentation to be produced
8.	Penetration tests to be conducted
9.	Actual results of the penetration tests to be recorded
10.	Penetration testing effort, outlining the testing approach, configuration, depth and results to be recorded
11.	The results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a **moderate** attack potential, to be examined.
12.	All exploitable vulnerabilities and residual vulnerabilities, to be reported in the ETR
Evaluation evidence:	
Input:	
a) ST; b) Functional specification; c) The TOE design; d) The security architecture description; e) The implementation representation; f) The guidance documentation; g) The TOE suitable for testing; h) Information publicly available to support the identification of possible potential vulnerabilities; i) The results of testing the basic design.	
Other input:	
a) Current information regarding potential vulnerabilities and attacks in the public domain (e.g. from an evaluation authority).	

D.6 BASELINE AVA_VAN.5

Dependencies	Assurance component description	Additional remarks
ADV_ARC.1	Security architecture description	Necessary requirements and analysis of the TOE based on the properties of domain separation, self-protection, and non-bypass ability. Note: The properties of self-protection, domain separation, and non-bypass ability are distinct from security functionality expressed by Part 2 SFRs because self-protection and non-bypass ability largely have no directly observable interface at the TSF.
ADV_FSP.4	Complete functional specification	The developer is required to provide information of all TSFIs - whether SFR-enforcing, SFR-supporting, SFR-non-interfering - and each must be described to the same degree, including all of the direct error messages.
ADV_TDS.3	Basic modular design	A mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design is to be provided by the developer.
ADV_IMP.1	Implementation representation of the TSF	The implementation representation is made available to allow analysis of other TOE design decompositions (e.g. functional specification, TOE design), and to gain confidence that the security functionality described at a higher level in the design actually appears to be implemented in the TOE. The implementation representation is expected to be in a form that captures the detailed internal workings of the TSF. This may be software source code, firmware source code, hardware diagrams and/or IC hardware design language code or layout data.
AGD_OPE.1	Operational user guidance	Necessary for correct configuration of the TOE
AGD_PRE.1	Preparatory procedures	Necessary to ensure the TOE has been received and installed in a secure manner as intended by the developer
ATE_DPT.1	Testing: basic design	Evidence of testing of this TOE design must show that the internal interfaces have been exercised and have been seen to behave as described. Testing at the level of the TOE subsystems provides assurance that the TSF subsystems behave and interact as described in the TOE design and the security architecture description.
General remarks: There is no general guidance for this level in the standards. This could be subject to the common definition of technical domains as described in Subsection 5.6.7.		
Developer action		
AVA_VAN.5.1D	The developer shall provide the TOE for testing.	
Content and Presentation		
AVA_VAN.5.1C	The TOE shall be suitable for testing.	
Actions/Work units		
AVA_VAN.5.1E	The information provided meets all requirements for content and presentation of evidence to be confirmed	
1.	Test configuration is consistent with the configuration under evaluation as specified in the ST	
2.	TOE has been installed properly and is in a known state	
AVA_VAN.5.2E	Search of public domain sources	
3.	Sources of information publicly available to identify potential vulnerabilities in the TOE are to be examined. While examining the evidence provided the evaluators will use the information in the public domain to further search for potential vulnerabilities. Where the evaluators have identified areas of concern, they should consider information publicly available that relates to those areas of concern.	

AVA_VAN.5.3E	**Independent , methodical** vulnerability analysis of the TOE, using the guidance documentation, functional specification, TOE design, security architecture description and **implementation representation** to identify potential vulnerabilities in the TOE is to be performed The methodical analysis approach takes the form of a structured examination of the evidence. This method requires the evaluator to specify the structure and form the analysis will take (i.e. the manner in which the analysis is performed is predetermined, unlike the focused identification method).
4.	The evaluator uses knowledge of the TOE design and operation gained from the TOE deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE and potential errors in the method specified for the operation of the TOE. The following are some examples of the approach a hypothesis may take: a) consideration of malformed input for interfaces available to an attacker at the external interfaces; b) examination of a key security mechanism cited in the description of the security architecture, such as process separation, hypothesizing internal buffer overflows that may lead to degradation of separation; c) search to identify any objects created in the TOE implementation representation that are then not fully controlled by the TSF and could be used by an attacker to undermine SFRs. The identification process is iterative, i.e. where the identification of one potential vulnerability may lead to identification of another area of concern that requires further investigation. Subject to the SFRs the TOE is to meet in the operational environment, the evaluator's independent vulnerability analysis should consider generic potential vulnerabilities under each of the following headings: a) generic potential vulnerabilities relevant for the type of TOE being evaluated, as may be supplied by the evaluation authority; b) bypassing; c) tampering; d) direct attacks; e) monitoring; f) misuse.
5.	Identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment are to be recorded in the ETR
AVA_VAN.5.4E	Penetration testing
6.	Penetration tests to be devised
7.	Penetration test documentation to be produced
8.	Penetration tests to be conducted
9.	Actual results of the penetration tests to be recorded
10.	Penetration testing effort, outlining the testing approach, configuration, depth and results to be recorded
11.	The results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a high attack potential, to be examined.
12.	All exploitable vulnerabilities and residual vulnerabilities, to be reported in the ETR
Evaluation evidence:	
Input:	
a) ST; b) Functional specification; c) The TOE design; d) The security architecture description; e) The implementation representation; f) The guidance documentation; g) The TOE suitable for testing; h) Information publicly available to support the identification of possible potential vulnerabilities; i) The results of testing the basic design.	
Other input:	
a) Current information regarding potential vulnerabilities and attacks in the public domain (e.g. from an evaluation authority).	

E ANNEX: EXAMPLES OF ALTERNATIVE APPROACHES TO PROVIDING EVALUATION EVIDENCE

This section contains the examples mentioned in Subsection 5.6.6.2 for providing alternative evidence that may be a substitute for evidence required for the evaluation according to ISO/IEC 15408 classical CC schemes.

EXAMPLE 1: SKIPPING OR DOWNSCALING THE ASSURANCE COMPONENT ATE

ISO/IEC 15408 is very broad in its requirements to allow evaluations of a broad range of ICT products from operating systems to smart cards while giving full guidance to the evaluator. For specific technologies however, it is possible to condense the evaluation tasks specific to such technologies. An example is the silicon industry which by default applies strong testing and validation to their products due to their physical properties and potential defects. Hence, assurance efforts on functional testing in such schemes can be reduced as the manufacturer will ensure that his products are functional before delivery.

EXAMPLE 2: DEVIATIONS IN TERMINOLOGY

Another example could be that a scheme, although using the ISO/IEC15408 evaluation concept, decides to define its own easily understandable security functional requirements catalogue for the scheme. This catalogue could, for example, be in plain English language and replace the catalogue of ISO/IEC 15408 Part 2. Although such a scheme would not be compliant with ISO/IEC 15408, it may deliver the same assurance results as a compliant scheme while making understandable security claims available to its stakeholders.

F ANNEX: INDICATIVE EXAMPLES OF COMMON CONTROLS

The following table provides examples of common controls. An introduction to this subject and examples for the application of these controls are given in Chapter 8.

Table 14: Indicative examples for common controls

Control objective	Controls	Area of application	Association to AP (preliminary)	Common Security Level (CSL)	Implementation guidance (acc. to ISO/IEC 27002), comments
Prove authenticity of device or person that requests access	FIDO protocol	Mobile online services	Level 1-2	CSL 1	see specification FIDO level 1-2
			Level 2 - 3:	CSL 2	see specification FIDO level 3
			Level 4 - 5:	CSL 3 (TPM) CSL 4 (secure element)	see specification FIDO level 3+
Protect against infiltration of malware via removable media and external hardware	Restrict use of removable and external hardware via authenticity checking	ICS/Scada/OT	Level 2		8.3.1 / 8.3.3 procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
Control components connected to the Internet	Restrict use of removable and external hardware via authenticity checking	ICS/Scada/OT	Level 3		8.3.1 / 8.3.3 Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
	Only accept virus free elements	ICS/Scada/OT	Level 4		12.2.1 Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

Control objective	Controls	Area of application	Association to AP (preliminary)	Common Security Level (CSL)	Implementation guidance (acc. to ISO/IEC 27002), comments
	Remove control component connection to internet when not needed	ICS/Scada/OT	Level 2		9.1.2 Users should only be provided with access to the network and network services that they have been specifically authorized to use.
	Remove control component connection to internet when not needed	ICS/Scada/OT	Level 3		9.1.2 Users should only be provided with access to the network and network services that they have been specifically authorized to use.
	Remove control component connection to internet when not needed	ICS/Scada/OT	Level 4		9.1.2 Users should only be provided with access to the network and network services that they have been specifically authorized to use.
Protect communication against eavesdropping and modifications	Secure communication	product	basic	CSL 1	The TSF provides trusted channel functionality using secure cryptographic mechanisms for communications between the TSF and external entities. The TOE provides authentication of all communication end points, and ensures the confidentiality and integrity of the communication data that are exchanged through the trusted channel by use of the PACE or TCAP protocol.
		product	high	CSL 4	The TSF provides trusted channel functionality using secure cryptographic mechanisms for communications between the TSF and external entities. The TOE provides authentication of all communication end points, and ensures the confidentiality and integrity of the communication data that are exchanged through the trusted channel by use of the PACE or TCAP protocol.
Protect against unauthorized software updates	Secure import of update code packages	product	basic	CSL 1	The TSF verifies the authenticity of a received encrypted update code package, decrypts the update code package after it is verified to be authentic, and installs it after verifying that it is suitable for the TOE and does not downgrade the TOE's firmware to a previous version.
		product	high	CSL 4	The TSF verifies the authenticity of a received encrypted Update Code Package, decrypts the Update Code Package after it is verified to be authentic, and installs it after verifying that it is suitable for the TOE and does not downgrade the TOE's firmware to a previous version.

Control objective	Controls	Area of application	Association to AP (preliminary)	Common Security Level (CSL)	Implementation guidance (acc. to ISO/IEC 27002), comments
Protect against cloned devices and cheating vendors	Verification of product instance identity	product	basic	CSL 1	The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.
	Signature over product instance identity	product	enhanced basic	CSL 2	The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions. This information is cryptographically signed by a previously enrolled private key.
	Trusted signature over product instance identity	product	high	CSL 4	The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions. This information is cryptographically signed by a previously enrolled private key. The private key material and signature are performed in a highly secured execution environment.
Protect assets in use and at rest	Integrity and confidentiality protected storage	product	basic	CSL 1	Integrity and confidentiality protected storage secured by means of software obfuscation
	Integrity and confidentiality protected storage	product	enhanced basic	CSL 2	Integrity and confidentiality protected storage secured by hardware supported separation mechanisms
	Integrity and confidentiality protected storage	product	moderate	CSL 3	Integrity and confidentiality protected storage within a dedicated hardened execution environment
	Integrity and confidentiality protected storage	product	high	CSL 4	Integrity and confidentiality protected storage within a secure element
	Integrity and confidentiality protected processing of cryptographic assets	product	basic	CSL 1	Integrity and confidentiality protected processing of cryptographic assets by means of software obfuscation
	Integrity and confidentiality protected processing of cryptographic assets	product	enhanced basic	CSL 2	Integrity and confidentiality protected processing of cryptographic assets supported by hardened cryptographic hardware accelerators
	Integrity and confidentiality protected processing of cryptographic assets	product	moderate	CSL 3	Integrity and confidentiality protected processing of cryptographic assets within a dedicated hardened execution environment

Control objective	Controls	Area of application	Association to AP (preliminary)	Common Security Level (CSL)	Implementation guidance (acc. to ISO/IEC 27002), comments
	Integrity and confidentiality protected processing of cryptographic assets	product	high	CSL 4	Integrity and confidentiality protected processing of cryptographic assets within a secure element
Secure and trustworthy access to credential processing environment	mobile phone access control support features	product	enhanced basic	CSL 2	The mobile phone implements all access control support features within at least a trusted execution environment, maybe facilitating white-box cryptography to harden adversary access to cryptographic assets.
		product	moderate	CSL 3	The mobile phone implements all access control support features within a dedicated processing environment which is separated from the host processor. The dedicated processing environment must protect its assets against moderate attacker potential.
		product	high	CSL 4	The mobile phone implements all access control support features within a secure element. The secure element must protect its assets against HIGH attack potential.
	Mobile phone OS security attestation	system		CSL 3	The backend of the phone OS provides a security metric towards the access control backend system.

TP-01-21-174-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-535-7
DOI: 10.2824/490490