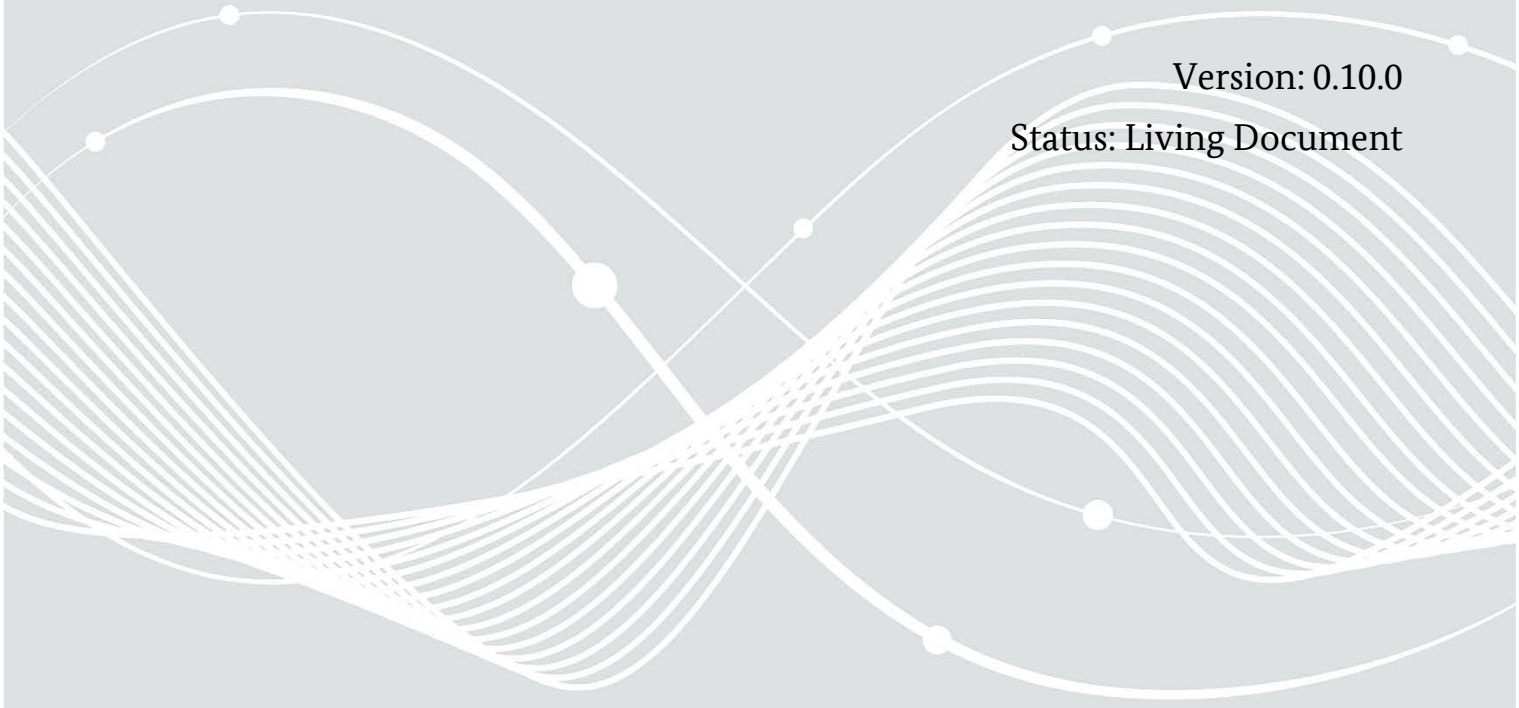
Federal Office
for Information Security

Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 1: General requirements



Version: 0.10.0

Status: Living Document

Change history

Version	*Date*	*Name*	*Description*
0.10.0	12.09.2025	Federal Office for Information Security	Version 0.10.0
0.9.0	01.10.2024	Federal Office for Information Security	Commentary Phase

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
Germany
Internet: https://www.bsi.bund.de
© Federal Office for Information Security 2024

Contents

1 Introduction

The Cyber Resilience Act (CRA) [1] is a pivotal initiative designed to enhance cybersecurity across the European Union. As digital products and services become increasingly central to everyday life and business, the CRA introduces a horizontal legal cybersecurity framework to address the cybersecurity risks resulting from the growing complexity and prevalence of products with digital elements.

By establishing essential cybersecurity requirements for products with digital elements placed on the European market, the CRA aims to reduce market fragmentation and ensure an appropriate level of cybersecurity for all users. This regulation encourages manufacturers to adopt security-by-design principles and proactive vulnerability management throughout the product lifecycle. Ultimately, the CRA supports a resilient digital environment, fosters trust in technology, and strengthens the EU's position in the global digital economy.

This Technical Guideline (TR) is intended to help manufacturers of products with digital elements in preparing for the CRA in form of requirements, recommendations, test actions and assessment criteria based on the (security) objectives stated in or derived from CRA Annex I (Essential Cyber Security Requirements), Annex II (Information and Instructions to the User) and Annex VII (Content of the technical documentation).

Feedback to this Technical Guideline can serve as input for the current and future work in the context of standardisation request in support of Union policy on cybersecurity requirements for products with digital elements. This request asks amongst others for the development of standardisation deliverables that aim to become harmonised European standards. Conformity with those harmonised European standards, will provide presumption of conformity within their scope and possible limits due to restrictions. This applies to general horizontal standards as well as product type specific vertical standards.

This Technical Guideline will be superseded in the current form as soon as its content is covered by the corresponding standardisation deliverables under the aforementioned standardisation request.

2 Important: State of this Document

As the technical and legal details of the CRA are still in development this document will be further developed in parallel with the European standardisation, legal clarification and further feedback on this guideline. For this purpose this technical guideline will be handled as a “living document” and will be updated in regular intervals.

This document can be used as

- a collection of information for manufacturers about the CRA;
- a platform for feedback for the CRA implementation and to support CRA standardisation;
- an entry into the CRA and a guideline to prepare for manufacturers without sufficiently structured security-by-design and vulnerability handling processes.

This document does NOT

- establish any obligations on manufacturers;
- grant presumption of conformity for essential cybersecurity requirements of the CRA when applied;
- always reflect the current state of standardisation contents;
- describe the only way to be address the CRA.

3 Overview Cyber Resilience

The Cyber Resilience Act (CRA) refers to the Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 and is the first horizontal European regulation to set a mandatory level of cybersecurity for products with digital elements available on the EU market. It applies to both hardware and software products that can connect directly or indirectly to a device or network, such as smartphones, laptops, smart home devices, IoT products, software applications, and even components like microprocessors and firewalls. Manufacturers need to take responsibility for cybersecurity during the entire support period of the product. On the other hand, Users will be supported in the appropriate selection of products with respect to cybersecurity properties and their secure usage. The new regulation applies in all EU member states and will be implemented gradually.

The CRA aims to:

- protect consumers and businesses from cybersecurity flaws and vulnerabilities in digital products;
- addresses cybersecurity risks across the supply chain, ensuring that products are secure by design and by default, and that users have the necessary information to use products securely;
- harmonize cybersecurity standards across the EU, replacing a fragmented regulatory landscape with a unified approach.

This chapter serves as a basic introduction to European product legislation and as an overview of the concepts and obligations set out by the CRA.

3.1 New Legislative Framework

The CRA is part of the New Legislative Framework (NLF)[4] that is a set of European Union (EU) regulations and decisions adopted in 2008, which came into full effect in 2010. It is designed to improve the functioning of the internal market for goods and to strengthen product safety and now security and regulatory coherence across the EU. It aims to facilitate the free movement of goods within the EU by harmonizing product legislation and reducing technical barriers to trade. It reinforces market surveillance rules to better protect consumers and professionals from unsafe and now unsecure products, including those imported from outside the EU. The framework sets clear rules for conformity assessments, ensuring products meet EU legislation supported by harmonised European standards before being placed on the market. The NLF provides a common legal framework for products and harmonises obligations for economic operators in the EU.

The fundamental idea of the New Legislative Framework is trust before control. The framework obliges manufacturers to ensure that their products fulfil the applicable legal requirements. By affixing the CE marking on their products, they declare that these product comply with the essential requirements of the relevant directives and regulations.

Market surveillance authorities then carry out checks, mostly through random sampling, rather than requiring pre-market approval for most products. A pre-market conformity assessment by an authorized independent third party - a notified body - is only necessary for specific product categories laid out in the corresponding regulations.

Regulations of the NLF, like the CRA, set out essential requirements related to products. Manufacturers can choose any technical solution that meets these requirements.

3.2 Scope of CRA

The CRA will apply to products with digital elements (PwDE) made available on the market, where the intended purpose or reasonably foreseeable use of which includes a direct or indirect data connection to a device or network. (Article 2(1) CRA) This includes logical connections through a software interface as well physical connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves.

A PwDE is a software or hardware product and its remote data processing solutions (RDPS), including its software or hardware components which might have been placed on the market separately. RDPS includes every data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions (Article 3(1) and (2) CRA).

Besides digital hardware, which was already mostly required to meet the requirements of the CE mark, software commercially distributed on the European Market will now be subject to the CE mark. This also includes software which is made available on the market free of charge but with commercial intent, e.g. a mobile app for an online storage service with a for-profit service model or software supported by advertisement. (Article 3(22) CRA).

3.2.1 Exclusions

The CRA excludes some product categories which are already subject to other regulations:

- medical devices that fall into the scope of Regulation (EU) 2017/745 or under the Regulation (EU) 2017/746 (Article 2(2) CRA);
- motor vehicles and their trailers that fall into the scope of Regulation (EU) 2019/2144 (Article 2(2) CRA);
- products with digital elements that are certified in accordance with the common rules in the field of civil aviation, Regulation (EU) 2018/1139 (Article 2(3) CRA);
- marine equipment that falls into the scope of Directive 2014/90/EU of the European Parliament and of the Council (Article 2(4) CRA);

The CRA does also not apply to:

- spare parts that are made available on the market to replace identical components (Article 2(6) CRA);
- products with digital elements developed or modified exclusively for national security (Article 2(7) CRA);
- products specifically designed to process classified information (Article 2(7) CRA);
- software without commercial intent, like free open-source software (FOSS) (Article 3(22) CRA);
- cloud services offers independent of infrastructure of the user, i.e. I/P/SaaS without a local client placed on the market (Article 3(1) CRA);

3.2.2 Placing on the market" and "Making available on the market"

The CRA applies to all PwDE that are “placed on the market” in the European Union. The definition originates from "The Blue Guide on implementation of EU product rules" [3] for European product legislation.

Definition: “Placing on the market” means the moment when a product is made available for the first time on the EU market. This is done by a manufacturer or an importer, and it refers to each individual product, not to a type or model. Once a product has been placed on the market, it can be resold or transferred further down the supply chain without being considered as “placed on the market” again.

Example: A manufacturer in Germany produces a batch of smart thermostats. When these thermostats are sold for the first time to a distributor in France, they are “placed on the market.”

Some requirements of the CRA also apply for products made available on the market after they have been placed on the market. This is referred to as “making available on the market.”

Definition: “Making available on the market” means any supply of a product for distribution, consumption, or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge. This refers to each individual supply of a product for distribution, consumption, or use on the EU market and covers every transfer of a product, including sales, leasing, renting, or giving away for free. It applies throughout the supply chain, after the product has been placed on the market.

Example: If a distributor in France sells the smart thermostat to a retailer, and the retailer sells it to an end user, each of these transactions is “making available on the market.”

In Summary placing on the market is the first time a product is supplied for distribution, consumption, or use on the EU market and making available on the market is any subsequent supply (sale, transfer, etc.) of the product on the EU market, after it has been placed on the market.

3.3 Manufacturer

This Technical Guideline will focus on the manufacturer’s perspective of the CRA. “Manufacturer” is defined as a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for monetisation or free of charge.

A “manufacturer” produces tangible goods, such as devices, or creates or provides intangible goods, such as software and software components. In the context of software, the "manufacturer" is synonymous with the role of software author.

This Technical Guideline will not go in detail into “distributor”, “importer” or other kind of economic operators as defined by the CRA, as the technical requirements stated in this technical guideline are not designed to fit their needs.

3.4 Timeline

The Cyber Resilience Act entered into force on 10 December 2024 but is not yet mandatory for products with digital elements placed on the European Market, as there are various transitional periods for implementing the requirements.

The reporting obligations (Article 14 CRA) for manufacturers to report actively exploited vulnerabilities and severe incidents will start on 11 September 2026.

From 11 December 2027, all CRA requirements for products with digital elements that are made available on the European market must be adhered to.

Products with digital elements that have been placed on the market before 11 December 2027 are only subject to the CRA, if those products have been subject to a substantial modification after the 11 December 2027 (Article 69(2) CRA).

There will be guidance by the European commission on how to determine what constitutes a substantial modification. Based on the NLF [4] a substantial modification is given if the type and purpose of a PwDE is changed in a way which was not foreseen in the initial risk assessment. As such typical maintenance of a PwDE with security updates and bug fixes is usually not considered a substantial modification.

Obligations laid down in Article 14 apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027 (Article 69(3) CRA).

3.5 Concepts

The CRA is based on several foundational concepts that collectively aim to strengthen cybersecurity across the European Union's digital product landscape. These concepts include:

Security by Design and by Default

The CRA mandates that manufacturers integrate cybersecurity into the planning, design, development, and maintenance of products with digital elements from the outset. This "security by design" principle ensures that security is not an afterthought but a fundamental aspect of product development. It also requires products to be secure by default, meaning users should not need to take extra steps to ensure basic security.

Risk-based approach

The essential cybersecurity requirements have to be implemented based on a cybersecurity risk assessment taking into account the intended purpose and reasonably foreseeable use of a product with digital elements. This approach ensures that all cybersecurity risks relevant to the PwDE have to be addressed ensuring an appropriate level of cybersecurity for any kind of PwDE.

Lifecycle Responsibility

Manufacturers are responsible for cybersecurity throughout the entire lifecycle of their products, not just at the point of sale. This includes providing timely security updates, handling vulnerabilities, and supporting products for a support period so that it reflects the length of time during which the product is expected to be in use, usually with a minimum of five years.

Transparency and Information for Users

The CRA emphasizes transparency, requiring manufacturers to provide clear and comprehensible information about the security features and update policies of their products. This enables consumers and businesses to make informed decisions about the products they purchase and use.

3.6 Obligations of the manufacturer

Article 13 and 14 of the CRA set out comprehensive obligations for manufacturers of products with digital elements. These obligations cover the entire product lifecycle, from design and development to post-market support. Below is a summary of the key requirements.

Pre-Market Obligations

The manufacturer has several obligations before placing a product with digital elements (PwDE) on the market:

- Ensure that products meet the essential cybersecurity requirements outlined in Annex I, which includes designing, developing, and producing products to achieve an appropriate level of cybersecurity. The level of cybersecurity is based on a cybersecurity risk assessment for each

product as well as an appropriate treatment of potentials risks to a tolerable level, considering the intended purpose, reasonably foreseeable use, operational environment, and expected period of use.

- Apply due diligence when integrating third-party components, including open source software, and address and remediate vulnerabilities in these components. The manufacturer has to report found vulnerabilities found in third-party components to the person or entity manufacturing or maintaining the component. If the manufacturer develops a software or hardware modification that addresses the found vulnerability in the component, it has to share that relevant code or documentation with the person or entity manufacturing or maintaining the component in a machine-readable format.
- Draw up the technical documentation (Article 31 CRA) containing at least the information set out in Annex VII that demonstrates compliance with the essential cybersecurity requirements. This documentation includes information about the product, its intended purpose, its design and development. It must also include a cybersecurity risk assessment that identifies potential threats and vulnerabilities, assesses their impact, and outlines the measures taken to mitigate these risks.
- Provide clear information and instructions to users set out in Annex II, such as manufacturer identification, contact details, and a single point of contact for vulnerability reporting. The PwDE has to be accompanied by the user information set out in Annex II, in paper or electronic form.
- Carry out conformity assessment procedures to demonstrate compliance with the essential cybersecurity requirements. The conformity assessment can be done through self-assessment or by a third-party notified body, depending on the type of PwDE.
- Where compliance with the essential cybersecurity requirements was demonstrated draw up an EU declaration of conformity and affix the CE marking to the product.

These obligations are designed to ensure that manufacturers take a proactive, risk-based approach to cybersecurity throughout the lifecycle of their products, thereby enhancing the overall security of digital products in the EU market.

Product Monitoring and Post-Market Obligations

After the PwDE was placed on the market the manufacturer has to systematically document and regularly review cybersecurity aspects of the product. This includes updating the risk assessment as needed new and address new risks appropriately. Additionally manufacturer ought to monitor the product for security vulnerabilities throughout its defined support period and address found vulnerabilities appropriately, including by providing security updates free of charge.

These post-market obligations have to be upheld during the support period of the product determined by the manufacturer in accordance with the expected duration of use of the PwDE. Generally, the support period is at least five years unless not appropriate for the type of product and its foreseeable duration of use.

In addition to that the manufacturer has to ensure that security updates as well as the technical documentation are available for at least 10 years after the product has been placed on the market or for the full support period, whichever is longer.

Reporting obligations

Article 14 of the CRA establishes mandatory reporting obligations for PwDE. Manufacturers have to report cybersecurity vulnerabilities of the PwDE as well as severe cybersecurity incidents negatively affecting the security of products with digital elements upon becoming aware of them. Notifications must be made simultaneously to the CSIRT (Computer Security Incident Response Team) designated as coordinator and

ENISA (European Union Agency for Cybersecurity) via the single reporting platform to be established under CRA Article 16.

The following notification timelines and content are given for vulnerabilities:

- Early Warning Notification: Must be submitted without undue delay and in any case within 24 hours of becoming aware of the vulnerability and should indicate, where applicable, the Member States where the product has been made available of which the manufacturer is aware of.
- Vulnerability Notification: If not already provided, a more detailed notification must be submitted within 72 hours of awareness. This should include general information about the product, the nature of the exploit and vulnerability, corrective or mitigating actions taken, and guidance for users. It should also indicate the sensitivity of the information, if relevant.
- Final Report: If not already provided, a final report must be submitted within 14 days after a corrective or mitigating measure for the vulnerability is available, including a description of the vulnerability, including its severity and impact, and the details about the corrective measure made available to remedy the vulnerability. If available, this report also includes information concerning any malicious actor that has exploited or that is exploiting the vulnerability

For severe incidents:

- Early Warning Notification: Must be submitted without undue delay and in any case within 24 hours of becoming aware of the vulnerability. Includes at least whether the incident is suspected of being caused by unlawful or malicious acts and should indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;
- Incident Notification: If not already provided, a more detailed notification must be submitted within 72 hours of awareness. This should include general information about the product, the nature of the exploit and vulnerability, corrective or mitigating actions taken, and guidance for users. It should also indicate the sensitivity of the information, if relevant.
- Final Report: If not already provided, a final report must be submitted within one month after incident report, including a detailed description of the incident, including its severity, impact and potential root cause, as well as the details about the mitigation measures taken.

Besides the mandatory reports manufacturers and other parties may voluntarily report any vulnerability or cyber threat that could affect the risk profile of the product as well as any incident or near-miss impacting the product's security. These voluntary notifications can be made to the CSIRT or ENISA. Voluntary reporting does not impose additional obligations on the notifier beyond what would exist without notification.

CSIRTs and ENISA must ensure confidentiality and appropriate protection of the information provided. If a party other than the manufacturer notifies a vulnerability or severe incident, the CSIRT must inform the manufacturer without undue delay. The CSIRT may prioritize mandatory notifications over voluntary ones and will process all notifications according to the procedures in Article 16 of the CRA.

3.7 Presumption of Conformity

The Cyber Resilience Act utilises the concept of "presumption of conformity" (Article 27 CRA) which means that if a product with digital elements and the manufacturer's processes comply with specific harmonised European standards, common specifications or European cybersecurity certification scheme, it's assumed to meet the essential cybersecurity requirements of the CRA.

Harmonised European standards (HES) are drawn up at the request of the European Commission by one or more European standardisation organisations. If a harmonised standard satisfies the requirements which it aims to cover the European Commission will publish a reference in the Official Journal of the European Union. HES published in this way can be used for presumption of conformity. In the context of the CRA harmonised European Standards specify the essential cybersecurity requirements set out in Annex I or part thereof.

If a requested Harmonised European standard (HES) can not be delivered or not be delivered in time, the European Commission may adopt implementing acts establishing common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements set out in Annex I.

The European Commission may also adopt specific European cybersecurity certification schemes und the Cyber Security Act (CSA) that can be used to demonstrate conformity of products with digital elements with the essential cybersecurity requirements or parts thereof as set out in Annex I.

Presumption of conformity does not free the manufacturer from fulfilling the essential cybersecurity requirements, as the harmonised European standards, common specifications as well as European cybersecurity certification schemes have to satisfy the essential cybersecurity requirements or part thereof for their given context.

Also presumption of conformity can only be used for essential cybersecurity requirements. Any obligations originating from other parts of the CRA will not be handled by harmonised European standards, common specifications or European cybersecurity certification schemes.

3.8 Product Categories

The CRA classifies products with digital elements according to their core functionality into three main product categories, each with varying levels of conformity assessment requirements. Additional guidance and clarification on core functionalities and the exact scope of the product categories will be provided by the European Commission in the form of technical descriptions [5].

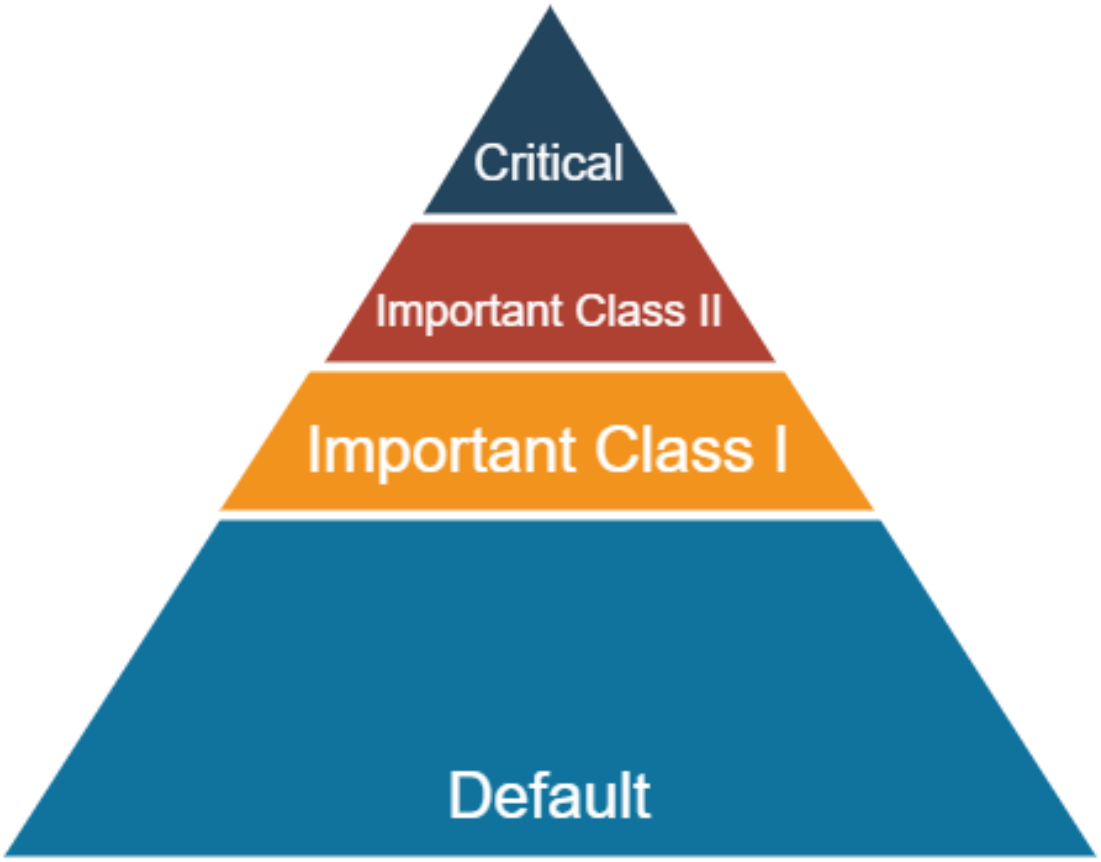


Figure 1 Product Categories

3.8.1 Default Category

Includes all products with digital elements that are not explicitly listed as important or critical. This category contains for example smart TVs, network printers, Bluetooth speakers, media player software applications. This class represents about 90% of all products with digital elements [2].

How to demonstrate conformity? Self-assessment by the manufacturer based on the essential cybersecurity requirements of Annex I CRA is sufficient for this category (Article 32 (1) CRA). This kind of conformity assessment based on internal control is under the sole responsibility of the manufacturer and does not require a third party. This is in accordance with conformity assessment procedure module "A" of the NLF. Alternatively, a third-party assessment by a notified body can be used on a voluntary basis as well as presumption of conformity via a European cybersecurity certification scheme.

3.8.2 Important Products Class I

Products with digital elements which have the core functionality of a product category set out in Annex III are considered important. Important pare split into Class I and Class II. Class I includes for example identity management systems, privileged access management software/hardware, standalone/embedded browsers, password managers, anti-malware software, VPN products, network management systems, operating systems, routers, modems, switches, microprocessors/microcontrollers with security-related

functions, smart home products with security features, internet-connected toys, personal wearable devices.

How to demonstrate conformity? Generally, a self-assessment by the manufacturer using a harmonized European standard or common specification is the primary way to demonstrate conformity to the essential cybersecurity requirements based on presumption of conformity (Article 32 (2) CRA) as described in section 3.7. Presumption of conformity is also possible using a European cybersecurity certification scheme of at least level 'substantial' which can be used to demonstrate conformity with the essential cybersecurity requirements.

If no harmonized European standards, common specification or European cybersecurity certification scheme apply, a third-party assessment by a notified body is required. This is in accordance with the conformity assessment module "B" of the NLF. The notified body will assess the product against the essential cybersecurity requirements of Annex I CRA and issue a certificate of conformity. To use the certificate for producing compliant products, the manufacturer must then ensure that the production of the PwDE ensures conformity with the approved type described in the certificate. This internal production control is based on module "C" of the NLF and can only be used in combination with other assessment modules, in this case with module "B".

Otherwise compliance can be achieved using a certified full quality assurance system, which is in accordance with the conformity assessment procedure module "H" of the NLF.

3.8.3 Important Products Class II

Important products with digital elements class II as listed in Annex III CRA include hypervisors, container runtime systems, firewalls, intrusion detection and prevention systems, tamper-resistant microprocessors and tamper-resistant microcontrollers.

How to demonstrate conformity? Class II does not allow self-assessment of the manufacturer (Article 32(3) CRA). Thus, only a third-party assessment based on module B+C or module H is possible. Presumption of conformity is only possible using a European cybersecurity certification scheme of at least level 'substantial' which can be used to demonstrate conformity with the essential cybersecurity requirements.

3.8.4 Critical Products

Products with digital elements which have the core functionality of a product category set out in Annex IV CRA are considered critical. This includes hardware security modules, smart meter gateways, smart cards, secure elements and other devices for advanced security purposes, including for secure cryptoprocessing.

How to demonstrate conformity? Critical products require a certification following an European cybersecurity certification scheme (Article 32(4) CRA). This might include European Common Criteria (EUCC)-based cybersecurity certification. The appropriate schemes will be approved for the corresponding product category via a delegated act. If no such scheme exists the conformity has to be demonstrated following the procedures for important class II.

3.9 The Essential Requirements

The central requirements of the CRA are the essential requirements set out in Annex I. For this reason this technical guideline will include them verbatim.

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

1. Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

2. On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

    a. be made available on the market without known exploitable vulnerabilities;

    b. be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

    c. ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

    d. ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

    e. protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

    f. protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

    g. process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

    h. protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

    i. minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

    j. be designed, developed and produced to limit attack surfaces, including external interfaces;

    k. be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

    l. provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

    m. provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

1. identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

2. in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

3. apply effective and regular tests and reviews of the security of the product with digital elements;

4. once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

5. put in place and enforce a policy on coordinated vulnerability disclosure;

6. take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

7. provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

8. ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

PwDEs and manufacturers have to comply and demonstrate conformity to the essential cybersecurity requirements of the CRA. As shown in Figure 2 the essential requirements are divided Part I containing requirements for the design, development and production of PwDE based on a cybersecurity risk assessment and Part II containing requirements for vulnerability handling of the manufacturer, including vulnerability identification, remediation, and disclosure.

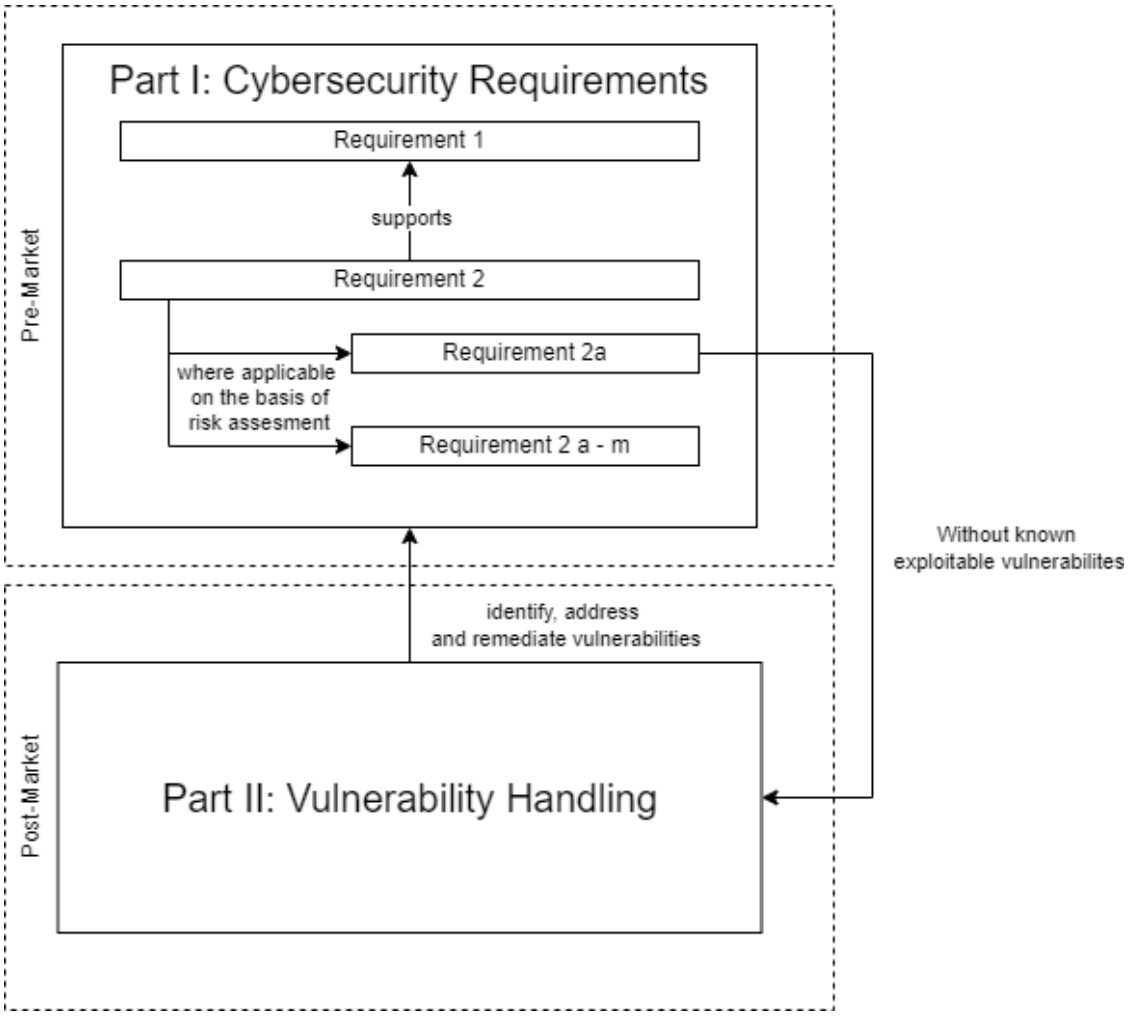


Figure 2 Structure and interplay of essential cybersecurity requirements

Only PwDE meeting requirements the requirements of Part I may be placed on the European market, this has to be demonstrated by the manufacturer beforehand. Part II requirements are to be fulfilled by the manufacturer from the moment, the PwDE is placed on the market and for the entire support period of the product. The requirements of Part I are focused on ensuring that products are secure by design and by default, while the Part II requirements focus on ongoing vulnerability handling processes.

Nevertheless both parts are not independent of each other as Part I (2) Point (a) requires the product to be free of known exploitable vulnerabilities and thus requires the manufacturer to have a vulnerability handling process in place to mitigate known exploitable vulnerabilities before placing a PwDE on the market. Part II requires the manufacturer to identify, address and remediate vulnerabilities, this might include an update of the risk assessment of the PwDE and changes to the implementation of the requirements of Part I.

Part I (1) is the overarching requirement of the CRA and requires the manufacturer to ensure an appropriate level of cybersecurity of the PwDE based on a cybersecurity risk assessment. This includes identifying potential risks and implementing appropriate measures on the PwDE to mitigate these risks. Part I (2) supports the first requirement with high-level product requirements which have to be implemented into the PwDE based on the risk assessment and where applicable.

3.10 Consequences of Non-Compliance

PwDE placed on the market are subject to the corresponding market surveillance authorities. Manufacturers shall, upon a reasoned request from a market surveillance authority, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements.

Manufacturers are required to cooperate with the market surveillance authorities on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements which they have placed on the market.

Non-compliance with the obligations of the CRA can result in significant fines (up to €15 million or 2.5% of global annual turnover), market restrictions, or product recalls.

3.11 How to prepare for the CRA

Simplified the following aspects should be considered to prepare for the CRA even without specific regulatory guidance:

1. Perform an honest cybersecurity risk assessment for the PwDE including the assets which have to be protected by the PwDE and potential threats.
2. Mitigate identified risks to a tolerable level using appropriate security controls based on the essential requirements of the CRA
3. Keep your users in mind and communicate openly and transparent in the users' best interest
4. Maintain the security of the PwDE throughout its lifecycle and cooperate with the authorities on vulnerabilities
5. Use existing best practices and do not reinvent the wheel

Following these aspects every manufacturer, especially those already versed in cybersecurity, should be well equipped for the CRA.

This technical guideline will go more into detail to a potential implementation of the CRA especially for manufacturers new to the topic of cybersecurity.

4 Usage

This Technical Guideline is intended to be used for a self-assessment by the manufacturer or by a third party on behalf of the manufacturer. The following clarifications and assessment procedures have to be taken into account when performing the assessment.

4.1 Evaluator

The assessment is performed by an evaluator, which can be part of the manufacturer organisation or a third party. The following aspects have to be taken into account when selecting an evaluator:

- The evaluator needs sufficient technical knowledge as well as knowledge in assessment methods to perform the assessment in a qualified manner.
- The evaluator requires access to, or be provided with, all information required to perform the assessment
- The evaluator has to be impartial and should not be involved in the development of the PwDE, to facilitate an independent assessment.

It is always important to perform the assessment with an appropriately critical mindset and to stay objective, even if the evaluation is performed by the development team

4.2 Assessment Scope

The conformity assessment is performed on the design of the PwDE or an instance of the finished PwDE. The generic PwDE architecture in Figure 3 will be used.

The PwDE consists of the hardware and/or software components placed on the market according (Article 3(1) CRA). These "placed components" are distributed and placed under the control of a user.

Note A PwDE might have multiple users, e.g. an integrator installing the PwDE, an administrator configuring and maintaining the PwDE or an end-user actually using the functionality of the PwDE. A Distributor reselling the PwDE as is, is not regarded as a user, as the distributor does neither change the PwDE nor use it for one of its functionalities.

Where the PwDE provides the possibility to be altered by hardware or software components, placed on the market by, or under control of the manufacturer or other parties, these components do not have to be considered in the assessment. The interfaces to accommodate these components on the other hand are part of the PwDE and part of the assessment. Furthermore, the effects of possible additional components have to be considered in the risk assessment.

The same is true for PwDE that are supposed to be used in conjunction with other PwDE, placed on the market by, or under control of the manufacturer or other parties.

Additional components integrated by the user are not part of the PwDE, e.g. additional apps or services. Although these components not integrated by the manufacturer are not part of the PwDE, the associated risks still have to be taken into account when performing the risk assessment if the integration of third-party components by the user is within the intended purpose or foreseeable use of the PwDE.

Besides the software and hardware components placed on the market, the PwDE also contains remote data processing solutions (RDPS) designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions (Article 3(2) CRA).

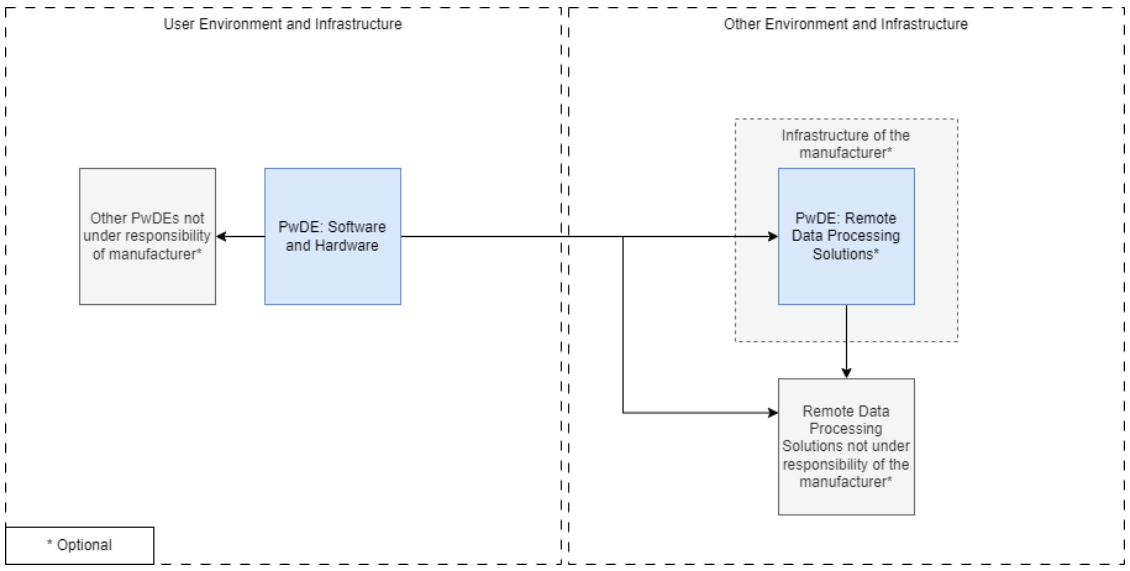


Figure 3 Generic PwDE architecture

According to CRA Article 26 additional guidance on the RDPS will be provided by the Commission. For the meantime this technical guideline will assume that every software designed and developed by or on behalf of the manufacturer, which provides a function used by the "placed components" are "RDPS" of the PwDE. Development also includes the customization of third-party software and implementation of new features used by the PwDE. The act of configuring a third-party software is not regarded as development.

This includes RDPS designed and developed by the manufacturer required for essential functionalities of the PwDE as well as RDPS necessary for other PwDE functionalities without importance for the user, like telemetry or advertisement, as these non-essential functions might also pose a risk to the PwDE. Software with no direct impact on the functionality of the PwDE is not part of the PwDE even if developed by the manufacturer, e.g. schedulers, backend logging frameworks, storage without business logic or other infrastructure services.

The infrastructure of an RDPS component, i.e. the hardware, third-party software and organisational measures required to operate the RDPS component, is not part of the PwDE. Nevertheless the manufacturer is responsible for the RDPS component and has to ensure secure operations by providing the necessary infrastructure.

4.3 Time of assessment

As it cannot be avoided that the PwDE is modified to an insecure state by the user, only the state after the initial configuration following the recommendations in the user's manual and (potential) update to the newest version is relevant for the assessment. This state can be achieved by executing the following steps:

- Obtaining a new product or resetting the product to its original state, e.g. factory reset or new installation.
- Start-up of the product and initial setup following the recommendations in the user's manual.
- Performing an update to the newest software version, if not already done during the initial setup.

4.4 Modal verbs

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED" and "OPTIONAL" in this document are to be interpreted as described in BCP 14 (RFC 2119, RFC 8174) when, and only when, they appear in all capitals, as shown here.

1. MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4.5 Control

The requirements of the CRA are dictated by the legislation itself. This technical guideline will set out controls with the goal to mitigate the cybersecurity risks of PwDE and fulfil the essential cybersecurity requirements of the CRA.

Each control consists of the following parts:

- **Input (Activity only):** Expected input for manufacturer activities
- **Risk scenario (Optional):** Risk-based scenario under which the control is applicable
- **Control:** has to be met by the PwDE or part thereof where applicable.
- **Output (Activity only):** Expected output of manufacturer activities
- **Target (Optional):** Type of component or function secured by the control.
- **Assessment Guidance (Optional):** Additional guidance for the assessment of the control. Depending on the associated risks different levels of assessment guidance might be provided.
- **Implementation Guidance (Optional):** Implementation specific information for the control, e.g. a specific cryptographic algorithm or a specific configuration of the PwDE. This is not a mandatory requirement, but rather a recommendation to implement the control in a specific way in accordance with the associated risk.
- **Compensation (Optional):** Alternative control for compensation if this control can not be fulfilled.
- **Reference CRA:** Essential requirement or other requirement of the CRA supported by the control. This reference can be used to identify the essential requirements implemented by the PwDE.

4.6 Assessment Procedure

This section specifies an assessment procedure on how to assess that the security controls stated in this Technical Guideline are met. For reproducibility and consistency every assessment step should be documented by the evaluator and included in the test report as defined in section 4.8.

The assessment is performed by evaluating the applicability and fulfilment of every control in this document based on the following rules:

Controls: Controls consist of a normative statement with MUST, the control is fulfilled (PASS) if the statement can be assessed as true, otherwise the control is not fulfilled (FAIL). A control can be marked as not applicable (N/A), if

- a referenced compensation is fulfilled instead,
- the target mechanism of the control does not exist in the PwDE,
- a "if" condition in the control statement does not apply,
- or the control is in conflict with other regulations.

Generally controls are specific enough for evaluation, if not the control will be supplemented by additional guidance which has to be used for assessing the control. Controls have to be at least assessed on a conceptional level based on the documentation of the PwDE. A functional assessment based on the behaviour of the PwDE or the manufacturer is recommended for additional assurance if possible, but not required.

Risk-based Controls: Risk-based controls consists of one or more risk-scenarios, a requirement and optional assessment criteria. Risk-based controls can be not applicable (N/A) if the risk does not apply to the product. Risk-based controls are fulfilled (PASS) if the underlying control is fulfilled by the PwDE or part thereof affected by the risk.

Generally the requirements of the CRA can be satisfied with any kind of control appropriate to sufficiently mitigate cybersecurity risks. This guideline uses the following types of controls for easier differentiation:

Activity: Activities are administrative controls consisting of an activity to be performed by the manufacturer as well as an expected input and output. Process controls are fulfilled (PASS) if the activity stated in the requirement is performed by the manufacturer and the required output is produced; otherwise, the control is not fulfilled (FAIL).

Mechanism: Mechanisms are active technical controls and are fulfilled (PASS) if the control is implemented as described by the PwDE, otherwise the control is not fulfilled (FAIL).

Documentation: Documentation is generated in the context of the PwDE but not direct part of the PwDE. Documentation controls are fulfilled (PASS) if the manufacturer provides the described documentation in the described manner for internal, external or public consumption. The assessment of documentation does not include the assessment of the underlying processes.

The assessment is preferably integrated into the development processes and continuous quality assurance processes, if possible in an automated manner.

The overall verdict "PASS" is given if all controls are marked as "PASS" or "N/A", otherwise "FAIL".

The assessment step might include one of the following terms, which have to be interpreted by the evaluator:

- **(Generally acknowledged) state of the art** refers to the current and generally acknowledged best practices within a specific field for a specific use case. This does generally not require the usage of the latest technology, but rather the usage of well-known and established technologies, methods and processes appropriate for a specific use case. If necessary examples or criteria for state of the art will be given.
- **(Generally acknowledged) State of the art cryptography** follows common and well-known cryptographic recommendations e.g. BSI TR-02102, SOG-IS Agreed Cryptographic Mechanisms or comparable standards meeting the requirements of ISO 18033-1 Annex A. A cryptographic mechanism can be considered state of the art if it is suitable for the corresponding use case and no feasible attack with current readily available technology is known.

- **Provide and publish** indicates the required distribution of an information. By default the manufacturer is not required to make documentation or other records available for third-parties if not otherwise specified with provide or publish. Providing means granting access to a document for a specific third-party, e.g. the user of the PwDE. Publish means that something is documented and available for free, easy and public access.
- **Support and implement** indicates if a functionality has to be implemented by the PwDE directly or only supported in the context of integration into another PwDE.
- **By default and always** indicates the validity of a configuration/policy of the PwDE. "by default" means the PwDE behaves in a described manner if not configured otherwise by the user. "Always" means the behaviour is enforced and cannot be changed by the user.

4.7 Interpretation of the overall verdict

The overall verdict is as an indicator if a PwDE is compliant with the requirements of this Technical Guideline, but is no direct statement of compliance with the CRA.

A "FAIL" does not necessarily mean the PwDE is not compliant with the CRA, as some requirements of this guideline might not be applicable for every product. Neither does a "PASS" mean that the PwDE is compliant with the CRA, as the PwDE might impose risks which are not covered by this Technical Guideline.

4.8 Test Report

Pursuant to Article 31 CRA the manufacturer must draw up technical documentation before placing a PwDE on the market. This includes, among other things:

- A general description of the product with digital elements, including its intended purpose, versions of software affecting compliance with essential cybersecurity requirements, user information and instructions as set out in Annex II as well as photographs or illustrations showing external features, marking, and internal layout in case of a hardware.
- A description of the design, development and production of the product with digital elements and vulnerability handling processes
- Necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;
- An assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced including how the essential cybersecurity requirements of Annex I Part I are applicable;
- Reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;

Using this Technical Guideline a test report can be generated to document the assessment of the PwDE. Based on the requirements for technical documentation the test report has to include at least the following information:

- Date of the assessment
- Identification of the PwDE, including at least:
  - Name and model of the PwDE

  - Description of the PwDE and intended purpose
  - Version of hardware and software
  - Software bill of materials (SBOM) where applicable
  - For hardware PwDE: Photographs or illustrations showing external features, marking and internal layout as well as hardware components with digital elements
- Risk assessment
  - Identified assets and threats
  - Evaluated risks
  - Accepted risks
- Design Documentation
  - Architecture of the PwDE, including hardware and software components with digital elements as well as network and physical interfaces
  - Applicable controls including mitigated risk and corresponding essential cybersecurity requirements
  - Description of implementation of selected controls
  - Verification processes for the selected controls
- Description of vulnerability handling activities
- Verification of vulnerability handling activities
- Provided user documentation

5 Risk-based Approach

5.1 Relevance of (Cybersecurity) Risks

According to Article 13 and Annex I Part 1 manufacturers shall ensure that their products are designed, developed and produced according to the essential cybersecurity requirements set out in Part I of Annex I in such a way that they ensure an appropriate level of cybersecurity based on the risks.

For this; manufacturers shall undertake an assessment of the (cybersecurity) risks associated with a PwDE and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks by preventing incidents and minimising (cybersecurity) their impact.

This approach is necessary to establish an appropriate level of cybersecurity for the broad spectrum of products covered by the CRA and to enable the manufacturer to exercise due diligence during the complete product lifecycles with the actions and processes fitting for its specific use case.

Risk Assessment is widely used in different use cases as every decision has an inherent risk. For the scope of this document the term "risk" is always used in the context of cybersecurity with the goal to reduce the risk to the PwDE, the user, the environment and networks connected to the PwDE to an acceptable level. The term "minimising" as stated in the legislation will not be used, as it is generally not the goal to reduce the associated risk to a minimum as that is generally not feasible and not necessary to handle risks in an appropriate manner.

5.2 Explanation on Risk-Terms

For the risk assessment the terms asset, (cybersecurity) threat, (cybersecurity) risk and (cybersecurity) incident will be used.

Asset: Assets are everything worth protecting which is created, processed, stored or otherwise influenced by the PwDE. This can be, among others, data, created, transmitted, stored or otherwise processed by the PwDE, network resources provided, used or otherwise influenced by the PwDE, physical or other assets as well as the integrity and proper function of the PwDE itself, privacy, safety and health of users of, and everybody affected by the PwDE.

(Cybersecurity) Incident: According to Article 3 an incident "is any event having an actual adverse effect on the security of network and information systems". Following this a (cybersecurity) incident is a single cybersecurity related event with an adverse effect on the security of assets of the PwDE.

(Cybersecurity) Threat: According to Article 3 a threat is "Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other person". A threat does only conclude that there is a potential for an incident and does not include the likelihood and potential impact of the threat. This abstraction is necessary as an incident can only be handled after it occurred, in contrast a threat can be used for evaluating potential cybersecurity measures to prevent, detect and correct incidents.

(Cybersecurity) Risk: According to Article 3 a cybersecurity risk is the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident. Adding the statements of likelihood and impact (magnitude of such loss or disruption) to a threat, makes it possible to plan appropriate security measures to prevent, detect and correct incidents and to prioritize their implementation.

As this technical guideline will only handle risks related to cybersecurity, the term cybersecurity will not be explicitly stated in conjunction with incident, threat and risk.

5.3 Tailoring of the risk-based approach

The appropriate handling of risks is highly specific to the type of PwDE and its intended purpose and foreseeable use. The risk handling in this technical guideline is based on the ISO 31000 and constitute a general set of activities common to risk-based approaches, which can be used for every kind of PwDE. To simplify the risk handling for a specific use case and to ease the implementation into existing processes the activities as well as the input and output can generally be customized, as long as it meets the general aspects and requirements set out in this document. The practice of customization to a specific use case is called "tailoring" and will be indicated throughout this document if encouraged.

It is generally advisable to use well known standards and frameworks for the tailoring of the risk based approach to incorporate existing sectorial knowledge about existing product specific risks and their appropriate treatment.

This guideline can be used standalone or in conjunction with other sector specific standards using the general activities laid out in this chapter.

5.4 Risk Handling

The minimal risk handling activities as shown in Figure 4 are risk assessment consisting of identification, analysis and evaluation of potential risks and the risk treatment to reduce risks to an acceptable level. Both activities are based on a risk context which describes the PwDE as well as criteria for the analysis and evaluation of risks.

The ISO 31000 uses the term risk management which also includes the activities "communication and consultation" for communicating and coordination risks with stakeholders, "review and monitoring" for reviewing the existing risks assessment and reacting to new risks as well as "recording and reporting" for the documentation of risks. Those activities are also partially included in the manufacturers obligations of updating the risk assessment and reporting risks and will be described separately, if needed.

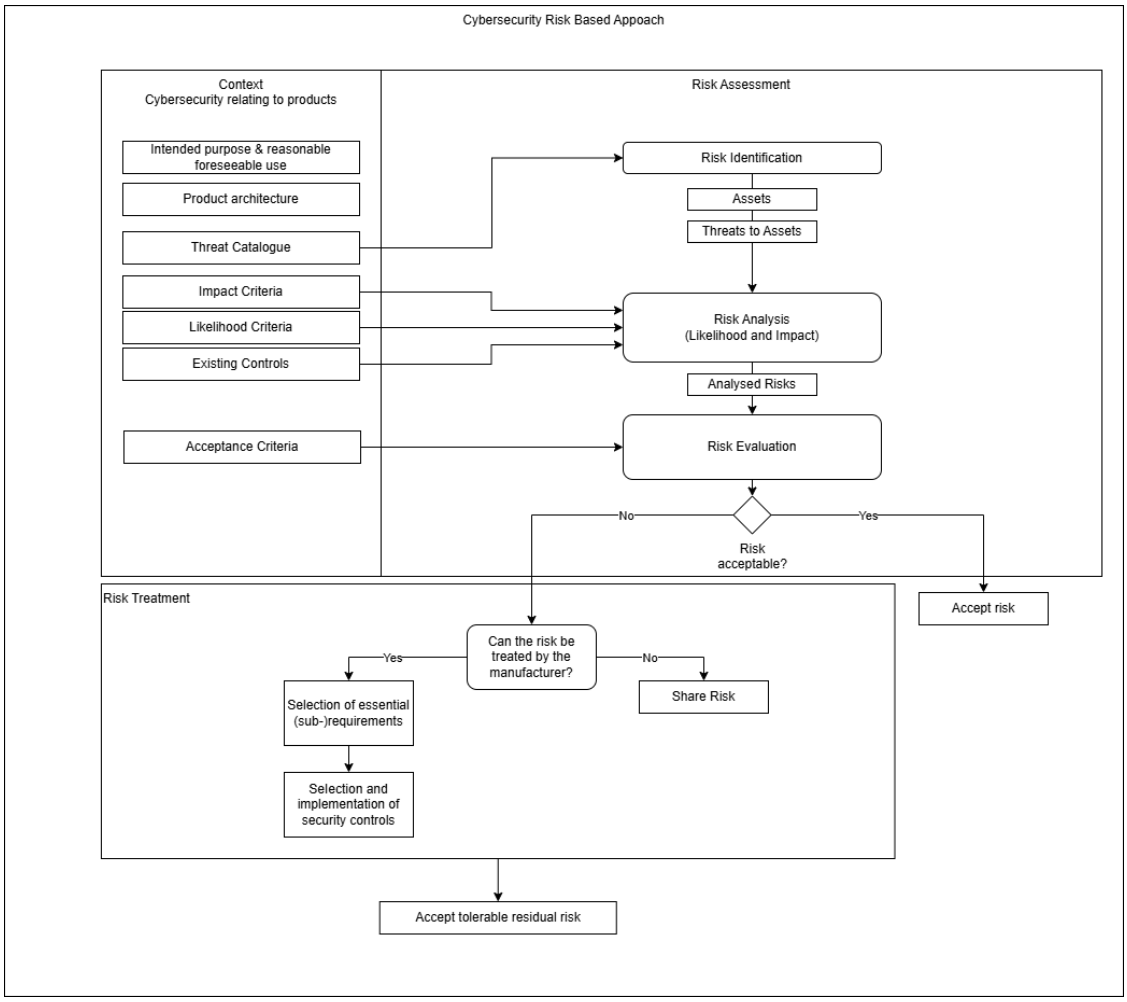


Figure 4 Risk Handling Overview

5.5 Risk handling as a process

Risk handling processes are individual based on the specific organisational needs. Generally there are some aspect to consider:

- Risk handling is iterative: It is not possible to handle all relevant risks in one go, as even with the most rigorous risk assessment there will still very likely still be risks not evaluated before as reality is complex and external factors can change often and risk mitigation measures will introduce new or affect existing interactions inside the PwDE, that have to be reassessed. Thus it is important to stay flexible by implementing usable and structured processes able to react to change and uncertainty. This applies to pre- as well as post-market.

- Risk handling is multi-layered: Risk handling is part of every part of a PwDEs lifecycle with different layers of granularity, based on the relevant stakeholders from governance, design, development, production and operations. This multi-layered approach will ensure an appropriate stakeholder engagement as well as multiple viewpoints necessary to get a good result. This guideline will stay on a level of granularity fit for product design as it is intended to help technical experts preparing for the CRA while simultaneously giving them the freedom for specific implementations.

- Risk handling is communication: The key to successful risk handling is communication as everyone involved in the PwDE is able to contribute with valuable insights and information necessary to handle risks appropriately. Thus it is important to be transparent on risks and communicate them with the relevant stakeholders.

5.6 Perspectives for risk handling

Risk handling is based on the expertise of the people involved as well as their perspective. Risk handling has to find an appropriate balance between the different perspectives. Common perspectives for risk handling are:

- Cyber Security perspective: The PwDE has to be protect the user or other stakeholders. Cybersecurity tries to assess what aspects of the PwDE are valuable and how to protect them. This perspective tries to represent the cybersecurity needs of the user or other entities affected by the PwDE and to reduce cybersecurity risks as much as possible.

- Developer perspective: The PwDE has to provide a function for the user. A developer has primarily the function in mind and thus risks have to be assessed and treated in harmony with the intended purpose of the PwDE. This perspective is needed to ensure that the PwDE stays usable and functional for the user.

- Attacker perspective: The PwDE is subject to potential attackers. An attacker tries to assess if a PwDE is worth attacking and how to do so. This perspective is important for the balance as it actively works against the interests of the user. Normally there is no real attacker involved in product development, consequently this can be emulated by internal expertise in offensive security, e.g. penetration testers or other cybersecurity experts.

5.7 Risk Context

The risk context contains all information necessary to perform the risk assessment. The risk context is highly individual for the specific product with digital elements and consists of the following components.

5.7.1 Intended purpose and foreseeable use

Risks which only impact the manufacturer, i.e. costs of necessary cybersecurity measures or the impact of cybersecurity measures on potential business opportunities, are generally not considered and are up to the manufacturer.

To assess the scope of the risk assessment it is necessary to define the context of the PwDE in regards to cybersecurity. Based on Article 13(1) products with digital elements shall be made available on the market only where they meet the essential cybersecurity requirements set out in Annex I Part I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Annex I Part I.

This means that the manufacturer can assume that their products are used for their intended purpose or other use cases that can be reasonably foreseen. 'reasonably foreseeable use' means use that is not necessarily the intended purpose supplied by the manufacturer, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions.

The CRA also addresses reasonably foreseeable misuse, which is in general not part of the risk assessment but has to be documented according to chapter 8 when posing a significant security risk. 'reasonably

foreseeable misuse' means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems. Intentionally malicious or detrimental actions by the users, which deliberately endanger the security of the PwDE or other systems, e.g. jailbreaking of a device or intentionally configuring a product to be insecure are generally not part of intended purpose or foreseeable use.

Based on this assumption the manufacturer can establish his risk assessment based on the intended purpose of the product as well as the reasonable foreseeable use. Following article 13 (3) this includes among other things

- The functionality of the product required to serve the intended purpose
- The potential degrees of freedom which will enable the use for a reasonable foreseeable use not included in the intended purpose
- The (operational) environment in which the product will be used (indoor or outside, private or office environment or other)
- The intended target user and usage scenarios (layman or professional users, single or multi user or other)
- Length of time the product is expected to be in use

5.7.2 Product architecture

Besides the intended purpose and foreseeable use a product architecture is also necessary to perform an effective risk assessment. The architecture is a high level technical description of the product and should include:

- The connective capabilities of the PwDE (WAN, Bluetooth, WLAN or other)
- The (potential) relation and communication of the PwDE with its remote data processing solutions
- The (potential) relation and communication to other PwDE
- The boundaries of the PwDE

Generally the risk context also includes the boundaries of the assessed PwDE as the risk assessment and especially the risk treatment can often only be sufficiently performed for products or components under the responsibility of the manufacturer. Risks associated with components outside of the PwDE might have to be handle by other entities. This is generally no problem for components in scope of the CRA as they are required to be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks for the intended purpose.

The manufacturer is generally responsible for third-party components integrated by the manufacturer itself and has to exercise due diligence according to CRA Article 13 (5). How to handle risks relating third-party components integrated by the manufacturer will be discussed in section 5.9.

5.7.3 Decision Criteria

The risk assessment aims to identify risks which have to be treated. The decision if a risk has to be treated depends on the potential impact of the risk and other factors. To establish a comprehensible and consistent

assessment the factors and criteria used for decision making have to be established as part of the risk context.

It is generally advisable to use existing specific standards based on existing sectorial knowledge and best practices.

For the risk assessment described in this document three types of criteria will be used:

- Impact criteria contain information on types of assets and the expected base impact of an incident, based on the type of affected asset and the loss of confidentiality, integrity and availability. The base impact can be raised depending the duration of the incident, the affected number of assets or on other factors.
- Likelihood criteria contain information on the estimated likelihood of an incident, based on existing compensation provided by the context of the product.
- Acceptance criteria define which risks are acceptable, based on the potential impact and likelihood of the risk.

A strategy on using these decision criteria as well as an initial set of criteria will be provided at the end of the chapter and can be tailored by the manufacturer for his specific use case based on its specific processes.

5.8 RH_RA.1 - Risk Assessment

Based on the context of the PwDE it is possible to identify and analyse potential cybersecurity risks to the PwDE. The following requirements are a general approach based on the ISO 31000 scoped for the purpose of assessing the cybersecurity risk of a PwDE in general manner. Risk assessment consists of risk identification, risk analysis and risk evaluation.

5.8.1 RH_RA.1.1 - Risk Identification

5.8.1.1 RH_RA.1.1.1 - Asset Identification (Activity)

5.8.1.1.1 General

To identify potential risks to a product it is necessary to identify the assets of the PwDE potentially affected by the realization of a risk. Assets are everything of the PwDE worth protecting.

This includes among others:

- The PwDE, its components and its functions
- Data assets collected, stored or otherwise processed by the PwDE

The list of asset should not include objects outside of the PwDE, as those can not be directly protected by the PwDE and will be unnecessary redundant, as everything outside of the PwDE which can be affected by the PwDE has a corresponding asset in the PwDE.

To keep the list of identified assets manageable it is advisable to group assets into categories based on the use case and general type of asset based on an asset catalogue. The list of assets in the impact criteria may be used as a base for the asset management.

5.8.1.1.2 Input

- Functionality of the product with digital elements based on the intended purpose and reasonable foreseeable use
- Recommended: Catalogue of common assets and asset categories

5.8.1.1.3 Control

The manufacturer MUST identify all assets of the PwDE

5.8.1.1.4 Output

- (Categorized) List of Assets of the PwDE

5.8.1.1.5 Reference CRA

- CRA Annex I Part I (1)

5.8.1.2 RH_RA.1.1.2 - Threat Modelling (Activity)

5.8.1.2.1 General

It is possible to identify the potential risks to the PwDE resulting from threats to the previously identified assets.

This includes all threats with potential adverse impact to the assets of the PwDE. This is independent of the likeliness or impact of an incident resulting from the threat as this will be considered when the to be identified risk are analysed and evaluated.

Generally threats are dependent on the intended purpose and reasonable foreseeable use of the PwDE without regards to a specific threat actor. It is generally advisable to use a structured approach for threat identification based on an existing threat catalogue.

As threats can affect different components of PwDE and there relations the threat identification can be supplemented by a data flow model for easier location of the affected components of the PwDE.

If components or RDPS of the PwDE are reused for other PwDEs, e.g. a companion app used for multiple IoT devices or a RDPS of the manufacturer used for multiple PwDE it is generally advisable to split threat modelling and the consequent risk assessment into components for easier reuse.

This way the risk handling for a common component can be done in one place and only has to be updated for each new related product if necessary.

5.8.1.2.2 Input

- Intended purpose and reasonable foreseeable use
- Product architecture
- List of assets
- (Optional: Threat catalogue)

5.8.1.2.3 Control

The manufacturer MUST identify threats to the assets and the potentially affected components of the PwDE.

5.8.1.2.4 Output

- List of identified risks consisting of threats to the assets and potentially affected components of the PwDE

5.8.1.2.5 Reference CRA

- CRA Annex I Part I (1)

5.8.2 RH_RA.1.2 - Risk Analysis (Activity)

5.8.2.1 General

The Analysis of an identified risks is necessary for the evaluation of the risk and includes the magnitude of the loss or disruption caused by an incident (impact) and the likelihood of occurrence of the incident. The impact is primarily defined through the value of the affected assets as an incident with a negative influence on an important asset has a higher impact than an incident affecting assets of lower importance. The impact can be determined based on impact criteria for the affected assets and additional amplifying factors, which can include the amount of affected assets and the duration of the adverse effect. Generally the value and consequently the potential impact on an assets is dependent on the usage of the product and the interests of the involved stakeholders, as businesses might have other priorities as a consumer.

The likelihood of an incident is influenced by several factors, which can include

- Attacker Motivation (Valuable assets raise the likelihood of an incident as there is a higher motivation for more qualified attackers)
- Communicative capabilities and communicative relations of the PwDE (Depending on the communicative capabilities and functionality communication which can be accessed by external actors, the products might be more likely to experience an incident)
- Potential exposure of the PwDE through existing vulnerabilities
- Potential exposure of the PwDE through the operational environment- Implemented or designed security controls

Generally, determining the likelihood of risks requires existing specific experience as well as applicable statistics and threat intelligence. To keep the estimation of likelihood comprehensible appropriate likelihood criteria have to be established. If the impact or likelihood of an identified risk can not be assessed, because it depends on additional parameters, e.g. attacker potential, duration of the incident, number of affected products, the identified risk should be split into multiple risks depending on the parameters. This will result in additional identified risks extending the list generated in RH_RA 1.1.2.

Note Rationale on impact and likelihood

The assessment of likelihood and impact can be performed using quantitative or qualitative methods or a mix of both. It is generally advisable to use sectorial appropriate methods for the risk analysis, fitting for the specific use case.

Generally, the analysis of risks is subjective and based on the experience of the person performing the risk analysis. Additional information to qualify or quantify the impact or likelihood of a risk enhance the reliability of the risk analysis, but rise the complexity and effort required for the risk analysis.

As it's generally not possible to completely, precisely and objectively assess the likelihood and impact of risks, the effort used for the risk analysis should be put into perspective to the effort

of treating a potential risk.The result of the risk analysis is the decision, if a risk has to be treated - Yes or No.

Consequently it might be more reliable and easier to handle a potential risk, instead of taking the effort to precisely assess the impact and likelihood. To support this statement and not give a false sense of numerical accuracy, this Technical does not use a quantitative approach. Instead a qualitative approach using parametrized risk scenarios will be used based on asset categories and operational environments.

5.8.2.2 Input

- List of identified risks
- Likelihood of an incident based on likelihood criteria
- Impact of a potential incident based on impact criteria

5.8.2.3 Control

The manufacturer MUST analyse the risks of the PwDE in regard to their likelihood and potential impact.

5.8.2.4 Output

- List of (analysed) risks including impact and likelihood

5.8.2.5 Reference CRA

- CRA Annex I Part I (1)

5.8.3 RH_RA.1.3 - Risk Evaluation (Activity)

5.8.3.1 General

After the risk have been analysed, the manufacturer needs to evaluate if the analysed risks have to be treated or can be accepted based on the impact and likelihood of a risk. This activity relies on acceptance criteria containing rules for the acceptance of a risk. As with other decision criteria these can be general, sector, organisation or product specific. As a general rule every risk which is plausible to happen and will exert a noticeable adverse effect for the user should be treated.

Note Rationale on Acceptance

It is generally possible to define multiple levels of acceptance criteria and to define risk acceptance for different use cases. It might be useful to establish risk acceptance levels for separate usage scenarios, e.g. consumer, business, government to handle multiple scenarios with one set of identified risk and for easier communication of the intended use of the product. This approach is not used in this guideline in order to keep the risk assessment flexible and generally applicable. Conceptually there is no difference as every additional parameter used to evaluate the risk acceptance can be reduced to impact and likelihood.

5.8.3.2 Input

- List of analysed risks
- Acceptance criteria

5.8.3.3 Control

The manufacturer MUST evaluate whether the analysed risks of the PwDE can be accepted or not.

5.8.3.4 Output

- List of (evaluated risk), which have to be treated or have been accepted

5.8.3.5 Reference CRA

- CRA Annex I Part I (1)

5.9 RH_RT.1 - Risk Treatment

Risks which a not accepted have to be treated. Treatment does not entail the complete eradication of a risk, as that is generally not possible. The goal of the treatment is to reduce the impact or likelihood of a risk to an acceptable level by implementing appropriate security measures based on the essential cybersecurity requirements of Annex I Part I.

The first essential cybersecurity requirement Part I (1) of Annex I states that "products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks". This entails that an appropriate risk treatment based on the risk is a required part of the product design. If the product design is properly implemented it will result in a secure development and production.

The treatment of risks is in the responsibility of the manufacturer and up to the process and used standard of the manufacturer. This document will define a strategy for selecting requirements and appropriate controls later on, which can be combined with existing standards and processes.

5.9.1 RH_RT.1.1 - Select appropriate controls (Activity)

5.9.1.1 General

The manufacturer has to meet the applicable requirements of Annex I Part I (2) on the basis of the cybersecurity risk assessment. This requires an initial selection of the corresponding requirements based on the risks to be treated. If a risk can not be effectively treated by the manufacturer on his one, risk sharing can be used.

Generally, the risk treatment can initially be performed independent of the essential cybersecurity requirements set out in Annex I Part I (2) as a product has to ensure an appropriate level of cybersecurity based on the risks according to Annex I Part I 1. Nevertheless the PwDE has to fulfil the applicable essential requirements to be compliant with the CRA.

The specific way to select the appropriate controls used in this guideline will be discussed in chapter 6.

5.9.1.2 Input

- List of evaluated risk, which have to be treated
- Essential cybersecurity requirements of Annex I Part I

5.9.1.3 Control

The manufacturer MUST select applicable essential cybersecurity requirements of Annex I Part I and appropriate controls to treat the evaluated risks and to reduce them to an acceptable level and include the selected controls in the design of the product.

5.9.1.4 Output

- List of selected controls and associated risks to be included in the design of the product

5.9.1.5 Reference CRA

- CRA Annex I Part I (1)
- CRA Annex I Part I (2)

5.9.2 RH_RT.1.2 - Risk Sharing

5.9.2.1 RH_RT.1.2.1 - Risk Sharing with Suppliers (Activity)

5.9.2.1.1 General

If the manufacturer is not able to effectively lower the risk on his own he can use risk sharing to reduce the risk to a acceptable level. The term risk transfer can be used synonymously, but will be avoided as it is generally not possible to transfer a risk completely to a third-party as the manufacturer is still responsible for addressing the risks of the PwDE and has to exercise due diligence according to CRA Article 13 (5) when integrating components.

Generally there a several way to share risk with suppliers:

- Sharing through compliance (with CRA): If the third-party component is subject to the CRA, the manufacturer can share risks if the intended purpose and foreseeable use as well as the associated handled risks of the component are sufficient for the integration in the PwDE. Other legislation with regard to cyber security, may also be suitable for risk sharing.
- Sharing through contract: If no regulation ensures that the shared risk are handled by the other party, the manufacturer can enforce the appropriate handling of risks by establishing a contract with the third-party manufacturer of a component to meet the requirements of the CRA. This approach can be combined with existing contractual frameworks like service level agreements, underpinning contracts or data processing agreements.

Financial risk sharing in the context of an insurance for cyber security related incident can also be additionally applied, but is generally not a valid approach to meet cyber security requirements.

Note: The sharing of risks when integrating free open source software (FOSS) is uncommon, as these software projects often neither have the capacity, resources and legal obligations to meet the requirements of the CRA. If the manufacturer is not able to treat the risk in relation to a FOSS component appropriately, he may rely on a third party acting as an open-source software steward providing support for the component. This will benefit the development of FOSS and can be a way to make FOSS viable for commercial usage.

5.9.2.1.2 Input

List of selected risks to share

5.9.2.1.3 Control

If sharing risks with a third-party supplier, the manufacturer MUST exercise due diligence by ensuring that the manufacturer of the integrated component is legally obliged, contractually required or otherwise able and willing to treat the risk accordingly.

5.9.2.1.4 Output

- List of shared risks including the actions taken by the manufacturer to exercise due diligence

5.9.2.1.5 Reference CRA

- CRA Annex I Part I (1)

5.9.2.2 RH_RT.1.2.2 - Risk Sharing with Users (Activity)

5.9.2.2.1 General

Risks can also be shared with the user by providing sufficient guidance for setting up and maintaining the product. In this case the manufacturer has to take into account the capabilities of the user and the infrastructure of the user. This can only be done if the shared risk meets the foreseeable expectations of the user, as the user is neither legally nor contractually obliged to share the risk. A common expectation for the end consumer context is that the PwDE is secure by default and the secure configuration and operation of the PwDE needs minimal user interaction. For other cases assuming a professional integrator or administrator more risks might be transferred if within the expectation of the user. This also includes providing PwDEs for integration in other PwDEs

5.9.2.2.2 Input

- List of selected risks to share

5.9.2.2.3 Control

If sharing the risk with the user, the manufacturer MUST ensure that the shared risks are within the foreseeable expectations of the user and that sufficient guidance documenting the risks and the expected mitigation by the user according to 8 is provided.

5.9.2.2.4 Output

- List of shared risks including the actions taken by the manufacturer to document shared risks

5.9.2.2.5 Reference CRA

- CRA Annex I Part I (1)

5.9.3 RH_RT.1.3 - Implementation and Verification (Activity)

5.9.3.1 General

The selected controls which were incorporated into the product design have to be implemented accordingly to be effective. This includes all measures necessary to perform the development and production according to the design of the product as well as the verification that the design is effective against the assessed risks and the implementation correct according to specification. The verification is part of the conformity assessment required for the CRA and depends on the used module and the

associated risk of the implemented control. The verification of effectiveness should at least be done on a conceptual level supported by a development process showing that the manufacturer develops and produces the PwDE correctly following the design. Generally higher risks might require additional or in depth verification.

5.9.3.2 Input

- List of selected controls and associated risks to be included in the design of the PwDE

5.9.3.3 Control

The manufacturer MUST implement the selected controls and verify their effectiveness and correctness, in accordance with the associated risk.

5.9.3.4 Output

- List of implemented controls and performed verification

5.9.3.5 Reference CRA

- CRA Annex I Part I (1)

5.10 RH_DOC.1 - Documentation of the risk assessment (Activity)

5.10.1 General

Following Article 13 (3) and (4) the cybersecurity risk assessment shall be documented and included in the technical documentation required pursuant to Article 31 and Annex VII. Besides that, the documentation of the risk assessment is in the interest of the manufacturer as a well structured and comprehensive documentation can be reused as basis for an update of the risk assessment. The usage of tools or templates for the documentation of the risk assessment is advisable.

5.10.2 Input

- Risk context
- Evaluated risks
- Shared risks
- Implemented controls
- Applicable essential cybersecurity requirements

5.10.3 Control

The manufacturer MUST document the results of the risk assessment in a comprehensive manner. This includes the risk context, the evaluated risks including the corresponding implemented controls and shared risks as well as the applicable essential cybersecurity requirements.

5.10.4 Output

- Documentation of the risk assessment

5.10.5 Reference CRA

- CRA Article 13 (3) & (4)

5.11 RH_UPD.1 - Update Risk Assessment (Activity)

5.11.1 General

The cybersecurity risk assessment has to be updated as appropriate during a defined support period according to Article 13 (3). An update is appropriate every time the existing risk assessment gets deprecated by an external or internal change in the threat context. This is at least the case in the following events:

- Update to the product with security implications
- New vulnerability becomes known
- New threat become known, e.g. new attack methods with potential impact on the product

Additionally, as not all relevant events can be monitored in all cases it is generally advisable to update the risk assessment in regular intervals.

5.11.2 Input

- Risk Assessment
- Optional: Event influencing the risk context

5.11.3 Control

The manufacturer MUST update the risk assessment when the risk context of the PwDE changes and treat new unaccepted risks accordingly.

5.11.4 Output

- Updated risk assessment

5.12 Decision Criteria

This guideline will work with decision criteria based on classification of the assets and the operational environment of the PwDE.

Decision criteria are a tool to simplify the analysis and evaluation of risks and should be defined on a on a sectorial, organisational or product level. Decision criteria condense existing knowledge in risk analysis and enable a reproducible and consistent risk assessment.

The risk assessment can be performed without detailed decision criteria as this will give additional freedom in performing the risk assessment, but might result in a higher effort necessary to perform a comprehensible and consistent risk assessment.

5.12.1 Impact Criteria

The impact of an incident is primarily dependent on the adversely affected assets. To estimate the potential impact of an incident the following scale will be used:

Impact:

- 1 - Negligible consequences
- 2 - Minor consequences
- 3 - Moderate consequences
- 4 - Major consequences
- 5 - Catastrophic consequences

The impact is estimated by selecting the base impact from the impact criteria in the following tables based on the affected assets and the type of loss in confidentiality ©, integrity (I) and availability (A). The criteria can be tailored if needed.

The base impact might not be representative based on the amount of affected Assets, in case of long time impact or other additional factors. In case an amplifier will be used in the context of this guideline a scenario/use case specific justification will be given.

```
Impact = BaseImpact * Amplifier
```

This guideline differentiates between assets to be protected and security assets required to protect the assets.

The impact of security assets is equal to impact the assets they protect, this will be implied by the impact X' with X equals C, I, A of the protected asset.

Data Assets

Asset	Confidentiality	Integrity	Availability	Rationale
PII.TechnicalNecessary	2	1	1	Technical necessary PII is data necessary for network communication and authentication related to a person with minor impact on confidentiality, which can not be protected without loss of function. This includes IP addresses and other technical identifiers

Asset	Confidentiality	Integrity	Availability	Rationale
PII.Generic	3	2	3	Generic PII with moderate impact in confidentiality, e.g. names, addresses, pictures or other
PII.Important	4	3	3	PII with a major impact on the associated person in case of information disclosure. This includes financial and health data. Note: This does not entail data, which is mixed with generic PII and can not be identified as important.
Other.Telemetric	1	1	1	Telemetric data containing no PII and no security relevant data have no relevant impact
Other.Configuration	1	3	1	Configuration containing no PII and no security relevant data might disturb the function of the PwDE if integrity is lost

Functional Assets

Asset	Confidentiality	Integrity	Availability	Rationale
Functions.Essential	-	-	3	Functions of the product which are required for its intended purpose and foreseeable use and whose availability has a moderate impact for the user
Functions.NonEssential	-	-	1	Functions of the product which might be part of the intended purpose and foreseeable use but whose availability have a negligible impact for the user, e.g. advertisement, additional information on a video stream, AI generated hints or other
Functions.Safety	-	-	5	Functions of the product in relation to safety whose availability have a major impact on the user

Asset	Confidentiality	Integrity	Availability	Rationale
Functions.Communication Network	-	3	-	Functions of the product in relation to the network might be tampered with and used to affect adjacent networks with generally more than two network peers. The base impact is estimated as moderate but can be amplified if needed.
Functions.Communication Local	-	2	-	Functions of the product in relation to connections with a peer in close proximity, generally this includes only one peer. The base impact is estimated as low.

Security Assets

Asset	Confidentiality	Integrity	Availability	Rationale
Security.Secrets	C' / I'	C' / I'	A'	Secrets (api-keys, passwords or other) used for ensuring confidentiality or integrity of a protected asset. The confidentiality and integrity impact of a secret is equal to the impact on either the confidentiality or integrity of the protected asset depending on the security mechanism. This also applies to availability as without secrets functionalities or access to assets can not be performed.
Security.Secrets.NetworkCredentials	3/4	A'	A'	Secrets (api-keys, passwords or other) used by the PwDE for authentication to networks or network resources. Generally the impact for loss of confidentiality is equal to the impact of an unauthorised access to the affected network or network resource using the disclosed secret. For secrets affecting the authentication to a complete network the impact 4 is assumed and for single network resources the impact 3 is taken as baseline, which can be changed based on the specific use case.
Security.PublicConfiguration	1	I' / C'	A'	Security relevant configuration, whose loss of confidentiality has no impact on the protected assets still needs to be protected in regard to integrity and availability depending on the confidentiality or integrity of the protected asset. This includes e.g. server certificates or cypher suites for cryptographic negotiation.

Asset	Confidentiality	Integrity	Availability	Rationale
Security.Logs	C'	I'	2	Security relevant logs contain information which might disclose security relevant data in case of an incident or might be manipulated to hide an incident. A short term loss of availability is of minor concern. If the long term loss of availability of security relevant log data is a major concern, an amplifier can be used.
Security.Mechanism	-	I' / C'	A'	Security relevant functions which needs to be protected in regard to integrity and availability depending on the confidentiality/integrity and availability of the protected asset.

5.12.2 Likelihood Criteria

To estimate the likelihood of an incident the following scale will be used:

Legend Likelihood:

1 - Risk scenario is highly unlikely to occur

2 - Risk scenario is unlikely to occur

3 - Risk scenario is somewhat likely to occur

4 - Risk scenario is highly likely to occur

5 - Risk scenario is almost certain to occur

Generally, likelihood is highly dependent on the specific risk and should be supported with sector specific knowledge and threat intelligence.

This guideline will use "environment" indicators for the likelihood of an incident based on the protection given by the expected operational environment of the PwDE or its components, lessening the likelihood of an incident. This approach can be used independent of a likelihood specific attacker profile, as this information is already included in the impact in so far that a higher impact results in a higher likelihood of attacks with higher motivation and capability.

Note The environment indicators can be tailored to the specific use case including more sophisticated approaches. The initially defined indicators are not including the consideration of attack chains or granular defence in depth strategies, as this would require assumptions of potentially broken environments or environment sensitive changes to asset impacts.

Indicators

Indicator	Rationale
Interface Restriction	Restriction on interfaces decrease the likelihood for an attack. This indicator shows the maximal assumed accessibility of the PwDE.

Indicator	Rationale
Access Restriction	Access restrictions have an impact on the number of potential attackers and the possible attack windows, lessening the likelihood of a successful attack.
User capabilities	Unskilled users have a higher likelihood to handle the product incorrectly or are more vulnerable too social engineering attacks. This indicator is only used, if the treatment of a risk depends on a user.

Interface Restriction

Value	Rationale
Physical	The PwDE communicates internally and can be accessed by physical manipulation. In case of software products this entails a manipulation of the internal communication/processing of the software. Attackers need direct access to the PwDE and manipulate it internally
Local	The PwDE communicates a short distance via a local interface, e.g. embedded user interface, nfc or short distance wired connection. In the case of software this also includes interprocess communication with other software PwDEs on the same device. Attackers need direct local access to the PwDE.
Dedicated known Network	The PwDE communicates with an adjacent network known and trusted by the user without intended connection to an external network. The network is dedicated to a use case and is as such expected to consists of limited number PwDE only using the network for the dedicated use case, e.g. local home bus system, peer-to-peer WLAN or bluetooth connection. Attackers have to be in proximity to the PwDE to access it via the network, access from an external network is not intended
Known network	The PwDE communicates with an adjacent multi-purpose network known and trusted by the user which is shared with other PwDEs for multiple use cases, e.g. home or office network. Attackers have to be in proximity to the PwDE to access it via the network, access from an external network is not intended
External Network	The PwDE communicates with a network not under the control of the user or the organisation of the user, e.g. mobile network, WAN or unknown WLANs. Attacker can potentially access the PwDE from anywhere as the topology of the external network is not known.

Access Restrictions

Value	Rationale
Restricted	The access to the PwDE is restricted, only a group of known people have access to the PwDE.
Public Restricted	Public access is intended or unavoidable, but the PwDE is normally supervised by an authorized person. The window for an attack is generally limited.
Movable	Public access is intended or unavoidable, but the PwDE is normally supervised by an authorized person. The PwDE is movable and can be removed by an attacker. The window for an attack is generally limited, but can be extended by moving the object.
Non-Restricted	No particular access restriction, there is no limitation on potential attacker and attack window. This also applies if the local access is restricted, but the attack can be executed without local access.

User Capability

Value	Rationale
Non-user-related	User Capabilities have no impact on the likelihood of an incident
Skilled	A skilled user, e.g. an IT professional, is not likely to exposed the product unnecessarily through insufficient handling and configuration and is able to enhance the security of the PwDE using his own expertise
Instructed	An instructed user, e.g. a craftsman or IT security savvy user who read the manual, is is not likely to exposed the product unnecessarily through insufficient handling and configuration
Layman	A not particular skilled user is likely to expose the product unnecessarily through insufficient handling and configuration

5.12.3 Acceptance Criteria

A risk can be classified and evaluated based on its likelihood and potential impact.

This guideline will use the following criteria for acceptance of risks:

- The risk for a moderate or higher impact of a local attack is not acceptable, if the access restrictions do not prevent the local access to potentially malicious actors with the capability to perform low complexity attacks.
- The risk for a high or higher impact of a local attack is not acceptable, if the access restrictions do not prevent local access to a known but potentially malicious group of actors with the capability to perform high complexity attacks.

- The risk for a moderate or higher impact of a network attack is not acceptable, if the network restrictions do not prevent the access to a unknown group of potentially malicious actors with the capability to perform low complexity attacks.
- The risk for a high or higher impact of a network attack is not acceptable, if the network restrictions do not prevent network access to a known limited group potentially malicious actors with the capability to perform high complexity attacks.
- The risk for a moderate or higher impact based on an initial misconfiguration of the PwDE is not acceptable, if the user is a layman.
- The risk for a high or very high impact based on an initial misconfiguration of the PwDE is not acceptable, if the user is a instructed tradesmen but not a skilled expert.

The acceptance of a risk can also be evaluated by using a scoring scheme and a risk matrix, as shown in Appendix B. This approach is highly experimental and will not be directly used in this guideline.

5.13 Risk handling in practice

Risk handling requires experience and is dependent on the product and the persons involved as such it not really feasible to describe risk handling in a way that detailed enough to be helpful but generic enough to be applicable to all products.

This guideline contains a simple example in Appendix A which can be used as an initial guidance for manufacturers without existing risk handling.

6 Working with Adaptable Risk-based Controls (ARC)

This technical guideline will use an approach called "Adaptable Risk-based Controls" (ARC) for selecting appropriate controls based on the associated risks. For this reason ARCs are always accompanied by one or more risk scenarios.

6.1 Risk Scenarios

A risk scenario contains the following information:

- Risk Scenario: Prose describing the risk scenario
- Assets: Affected Assets and Impact
- Environment: Environment parameters (Access Restriction, Interface Restriction, User Capabilities)

If a risk applies to the PwDE can be evaluated following these steps:

1. Perform the risk assessment as described in risk handling.
2. Categorize the assets identified in according to the impact criteria and the environment the component of the PwDe handling the asset in is. This will result in a mapping from asset to base impact in confidentially, integrity and availability and corresponding environment.
3. Separate the PwDE into different environments. Following the likelihood criteria the environment is a tuple of access restriction, user capability and interface restriction. Note the tuple describing the environment This can be started on a component basis and refined on a interface and functions basis later on. For RDPS under its responsibility the manufacturer is able to choose the environment it is willing to provide for the operation of the RDPS.
4. Select the controls based on the assets, impact and environment parameters given in the risk scenario of the control. A risk applies to the PwDE or part thereof if
   - the PwDE or part thereof handles or otherwise influences the listed assets
   - the PwDE or part thereof expects the access and communicative restriction as well as the user capability listed in the environment.

Example: A PwDE handling generic PIIs for the consumer market and indoor use with a RDPS operated by the manufacturer. The RDPS stores a huge amount of PII data sets.

Environment

A placed component with a layman consumer, restricted indoor access and connected to a remote network, resulting in (Layman, Restricted, External network) environment.

A RDPS component with a professional it operation, in a restricted data center and connected to a remote network, resulting in (Skilled, Restricted, External network) environment.

Impact categorisation

The placed component in the (Layman, Restricted, Network) environment handles PII.Generic with an impact of Confidentiality:3/Integrity:2/Availability:2.

The RDPS component in the (Layman, Restricted, Network) environment handles PII.Generic with an impact of Confidentiality:3/Integrity:2/Availability:2. As many data set might be affected a amplifier of 1 will be used resulting in Confidentiality:4/Integrity:3/Availability:3.

Selection of controls

Assume the following control:

Automatic Update Mechanism (Mechanism)

Risk Scenario: The PwDE handles Assets with moderate or higher impact which can not be protected if product integrity is lost. The user is a a layman not installing updates in regular intervals leaving the PwDE vulnerable to attack via external networks.

Assets:

- C(3)
- I(3)
- A(3)

Environment:

- Access Restriction: *
- Interface Restriction: External network
- User Capabilities: Layman

Control:

The update mechanism of the PwDE MUST include an automatic update mechanism able to check for new updates automatically.

Based on the parameters the control can be selected for different environments:

"Automatic Update Mechanism" does apply to PwDE handling assets with an impact of at least 3 over an external network without a skilled user. Consequently it applies in general to the exemplary PwDE handling generic PII and using a remote network access.

As the control also expects a layman user it only applies to the components of the PwDE administered by the Laymane and not the RDPS component as it is operated in a skilled environment. This applies to many security by default controls.

6.2 Rationale on ARCs

ARCs are an approach to select controls applicable to cybersecurity appropriate to the use case of the PwDE. There are two aspects affecting the appropriateness of cybersecurity:

- What must be protected?

  This is defined by the assets identified in asset identification and their potential impact. Following the impact categorization described step 2, an indicator for the amount of protection for confidentiality, integrity and availability can be derived.

- What must be protected against?

  This is defined by the threats identified in threat analysis and the likelihood of their occurrence. The categorization of assets into different impact classes also generates three generic threats, i.e.

loss of confidentiality, loss of integrity and loss of availability. This also includes the likelihood of occurrence of these threats as the impact has a direct relation to the motivation and consequently the potential capability of a malicious actors.

If nothing else is known about the product the worst case can be assumed, i.e. that all three threats apply and are likely relative to their potential impact. Generally this is not the case as based on the environment the PwDE already some level of protection and thus a reduced likelihood of an incident based on existing access restrictions, communicative restrictions or other security controls already realized and expected by the environment. A special environmental factor is the user capability, as a high user capability indicates an environment with mature administrative controls in place and the expected capability to set up certain restrictions or other technical/physical controls. Although not malicious an unskilled user will require additional support for the secure operation of the PwDE.

Environments can be used for composition of components of the PwDE. A component of the PwDE can expect an environment the manufacturer has provide when integrating the component. The manufacturer has to provide the expected expected environment in full or can delegate the expectation to the next user in the supply chain. If this is done, the manufacturer has to enable the next user to meet the expectations. This does at least include a transparent description of the delegated expectations as well as the means to meet the expectations, e.g. a configuration interface if some additional configuration is expected.

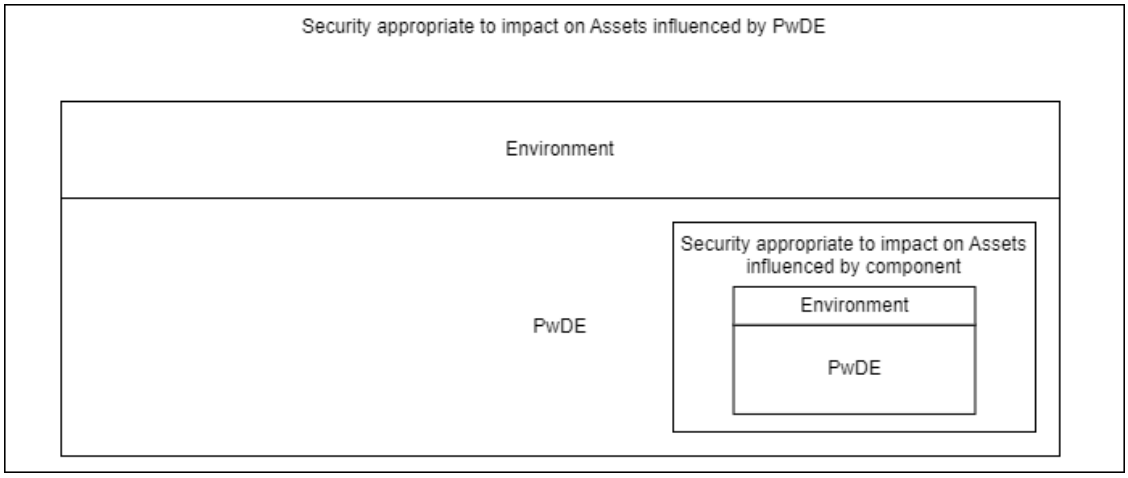


Figure 5: Composition of environments

In regards to the assessment of this technical guideline the composite property can be used for a top-down-approach, if the evaluator assumes that a control is not necessary or even detrimental for a part of the PwDE, e.g. an interface, an application or a function of the PwDE the evaluator can scope the used environment and assets specifically to that part of the PwDE and reevaluate the control.

7 Cybersecurity Controls

This guideline defines an initial set of controls for product security and vulnerability handling that are commonly used in order to ensure the cybersecurity of a PwDE.

These controls are generic and designed to be applicable for a wide range of products and are consequently rather high-level with the intent for further specification by the manufacturer depending on the use case and the specific type of PwDE.

The cybersecurity controls of this technical guideline are defined in the machine-readable format OSCAL in order to

- provide the capability for filtering of the appropriate controls for depending use cases
- simplify the reuse of existing controls and definition of custom control catalogs
- establish a structured format for documentation and assessment of the implemented controls

The OSCAL controls are provided via the Github-Repository: https://github.com/tr-03183/tr-03183-1

Access in conjunction with additional information on the usage of the repository and OSCAL will be provided upon request to tr-03183@bsi.bund.de.

8 User Documentation

User documentation is essential to enable the user to securely setup, maintain and decommission the PwDE. User documentation enables the manufacturer to communicate its expectation for secure use of the product to the user, thus reducing the risk of misuse and vulnerabilities resulting from user errors. It also provides the user with the necessary information to report vulnerabilities and security incidents to the manufacturer.

This section outlines the minimum user documentation which has to be provided with the PwDE as defined in Annex II of the CRA.

8.1 UD - User Documentation

8.1.1 UD.1.1 - Identification of the Manufacturer (Documentation)

8.1.1.1 Control

The user documentation related to the PwDE MUST contain the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website with the means to contact the manufacturer.

8.1.2 UD.1.2 - Identification of the PwDE (Documentation)

8.1.2.1 Control

The user documentation related to the PwDE MUST contain the name and type and any additional information enabling the unique identification of the PwDE.

8.1.3 UD.1.3 - Support Period (Documentation)

8.1.3.1 Control

The user documentation related to the PwDE MUST contain the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates.

8.1.4 UD.1.4 - Secure Setup (Documentation)

8.1.4.1 Control

The user documentation related to the PwDE MUST contain detailed information on the necessary measures during initial commissioning and throughout the lifetime of the PwDE to ensure its secure use.

8.1.5 UD.1.5 - Consequences of modifications (Documentation)

8.1.5.1 Control

The user documentation related to the PwDE MUST contain detailed information on how modifications to the PwDE can affect the security of data.

8.1.6 UD.1.6 - Installation of Updates (Documentation)

8.1.6.1 Control

The user documentation related to the PwDE MUST contain detailed information on how security relevant updates can be installed.

8.1.7 UD.1.7 - Secure Decommissioning (Documentation)

8.1.7.1 Control

The user documentation related to the PwDE MUST contain detailed information on the secure decommissioning of the product with digital elements, including information on how user data can be securely removed.

8.1.8 UD.1.8 - Automatic-Updates Opt-Out (Documentation)

8.1.8.1 Control

The user documentation related to the PwDE MUST contain detailed information on how the default setting enabling the automatic installation of security updates can be turned off.

8.1.9 UD.1.9 - Secure Integration (Documentation)

8.1.9.1 Control

The user documentation related to the PwDE MUST contain detailed information on where the PwDE is intended for integration into other products with digital elements and the information necessary for the integrator to comply with the essential requirements.

9 References

[1] REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf.

[2] European Parliamentary Research Service, EU Cyber Resilience Act - Briefing. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf.

[3] European Commission, The 'Blue Guide' on the implementation of EU product rules 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2022.247.01.0001.01.ENG.

[4] European Commission, New legislative framework. Available: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

[5] European Commission, Technical description of important and critical products with digital elements. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14449-Technical-description-of-important-and-critical-products-with-digital-elements_en.

[6] NIST, OSCAL: the Open Security Controls Assessment Language. Available: https://pages.nist.gov/OSCAL/.

Appendix A: Example

This example illustrates how the risk assessment for a product with digital elements might be performed, based on a simple network-connected camera. The example is not exhaustive and does not cover all possible threats, vulnerabilities, or controls that may be relevant for such a product. It is intended to provide a general idea of the risk assessment process and the types of considerations that may be involved.

A.1. Product description

Following is a brief description of the example product from the manufacturer's marketing material:

Simple Network Camera (SNC) X5 – Everyday Made Easy

Stay connected to your space with this easy-to-use network camera, designed for casual, everyday use. Whether you're checking in on pets, monitoring a room, or sharing live video with family or friends, this compact camera makes it simple.

Key Features:

- Clear HD **Video and Audio**: Stream in 1080p resolution for smooth, clear visuals—ideal for general viewing and sharing.
- Live Streaming Access: Connect to your **home network** and view the camera feed in real time from your phone, tablet, or computer via a web interface or streaming protocol.
- Flexible Mounting Options: Compact and lightweight, place it on a desk, shelf, or mount it to a wall with ease. Suitable for every kind of **indoor** use.
- Quick Setup: **No complicated** installation - just plug it in, **configure** with the **web interface**, connect to your **home Wi-Fi** and start streaming in minutes.
- Expandable Local Storage: **Insert** an **SD-Card** with up to 256GB and **save footage locally**, ensuring your videos are safe even if the network goes down.
- Everyday Monitoring: Perfect for **non-security applications** like checking in on a workspace, monitoring a hobby room, or staying in touch with loved ones remotely.

This simple network camera offers a convenient way to stay visually connected—without the complexity or features of a full security system.

Figure 6: Product image SNC X5

A.2. Risk context

For simplicity this example will derive a risk context from the product description above.

The risk context is a summary of the intended purpose, foreseeable user and environment of the product, as well as its main functions and interfaces. Implementation and design documents are normally a better source for this information than a marketing description.

The camera is intended to perform the following functions:

- capture video and audio data,
- store that data on a storage card locally inserted into the camera,
- stream that data over a home network to a user device using a web interface or streaming protocol,
- be configured and managed via a web interface,

The camera is intended to be operated

- by unskilled consumers,
- in a home network via WLAN and
- indoor in a restricted home environment

The camera is not intended

- for security applications,
- for professional or industrial environments,
- for public spaces.

The camera is a standalone device without need for a backend service or companion app.

The Camera possesses the following interfaces:

- Local card slot
- Wireless network (Wi-Fi)
  - Web interface (HTTP/HTTPS)
  - Streaming protocol (SRTP/RTP)
- Power supply (DC jack - no data transmission)

The communicative relationships of the camera as shown in Figure 7: are expected.

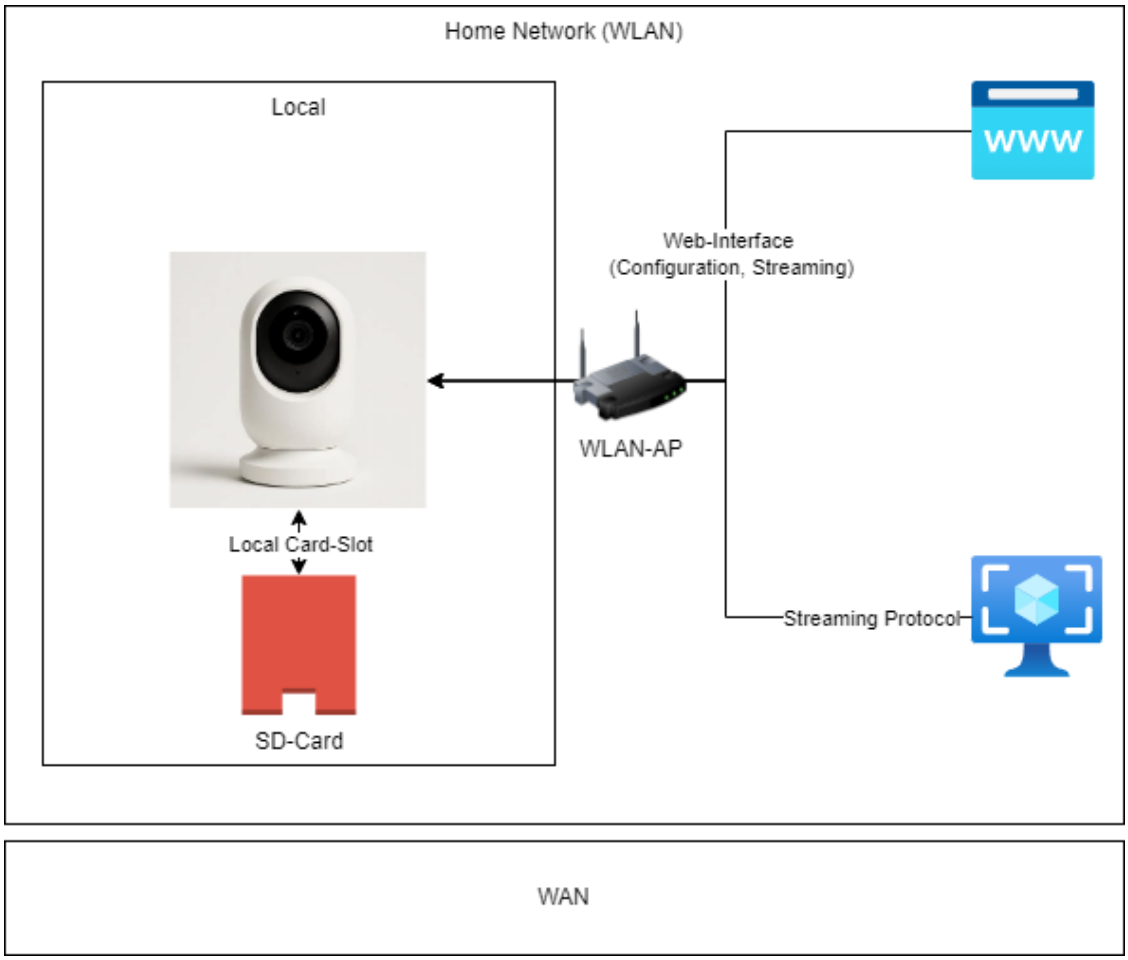


Figure 7: Network Architecture SNC X5

The camera is not intended to access the internet but is connected to a home network which presumably has internet access via a gateway. The home network is not dedicated to the camera and is shared with other devices.

The home network is expected to be protected by a home router with basic security features like WPA2/WPA3 authentication.

A.3. Asset identification (Initial)

From the risk context some initial assets and asset categories can be derived. This is important to assess what has to be protected.

Based on the further development of necessary security features there will be additional assets which can not directly derived from the pure functionality alone.

Data Assets

- Video and audio data (PII.Generic)
- Connection data (PII.TechnicalNecessary)
- General Configuration data (Other.Configuration)

Security Assets

- WPA-Key for WLAN access (Security.Secrets.NetworkCredentials)
- WLAN configuration besides WPA-Key (Security.PrivateConfiguration.Confidentiality)

Functional Assets

- Video and audio capturing function (Functions.Essential)
- Web-Interface Configuration (Functions.NonEssential)
- Web-Interface Streaming (Functions.Essential)
- Streaming Protocol (Functions.Essential)

A.4. Threat modelling

As the assets are not all handled the same way not all threats/attack scenarios apply to all kinds of assets.

To understand this a data flow diagram can be used including the data assets generated, stored and communicated by the PwDE. Especially important is the communication across (trust) boundaries between environments, this normally includes communication over interfaces of the PwDE with other systems, programs or users not part of the PwDE.

Functional assets are in the same way affected depending on the environment they are used in, e.g. a function only used internally is not directly affected by threats affecting network communication.

Communication not involving data assets can be ignored, in this case the power supply interface is not relevant as it does not involve data communication.

To the identified assets are stored and communicated as following this data flow diagram:

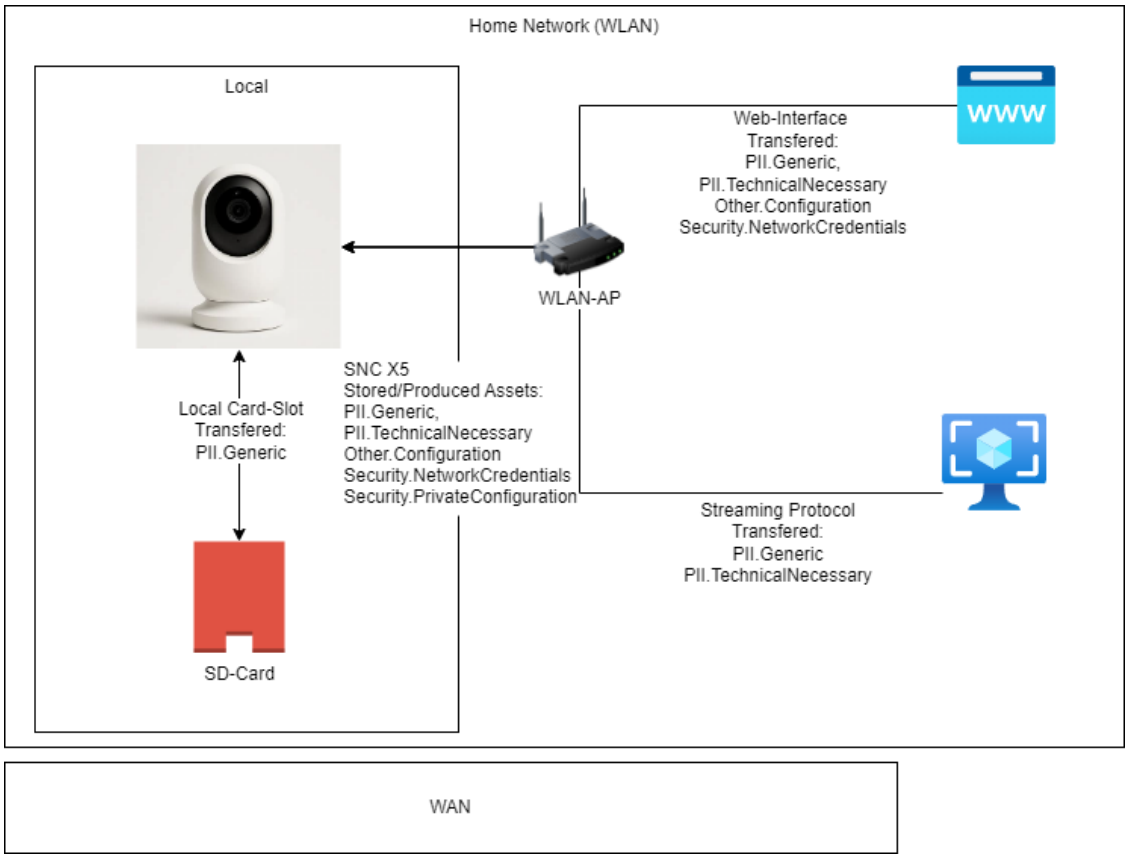


Figure 8: Data Flow Diagram SNC X5

Following this the PwDE has three different communicative environments:

- Internal (1): Everything stored and processed inside the camera
- Local (2): The local SD-Card interface
- Known network (3): The WLAN home network shared with other PwDEs of the user.

This results in the following asset - environment pairing

Data Assets

- Video and audio data (PII.Generic): Environment 1,2 & 3
- Connection data (PII.TechnicalNecessary): Environment 1 & 3
- General Configuration data (Other.Configuration): Environment 1 & 3

Security Assets

- WPA-Key for WLAN access (Security.Secrets.NetworkCredentials): Environment 1 & 3
- WLAN Configuration (Security.PrivateConfiguration): Environment 1

Functional Assets

- Video and audio capturing function (Functions.Essential): Environment 1 & 3
- Web-Interface Configuration (Functions.NonEssential): Environment 1 & 3
- Web-Interface Streaming (Functions.Essential): Environment 1 & 3
- Streaming Protocol (Functions.Essential): Environment 1 & 3

The simple list of threats can be generated from all possible combinations of assets, applicable environments as well as these generic threats:

For data assets

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability

For functional assets

- Loss of Integrity (Corruption of functional assets)
- Loss of Availability

This is not done verbosely here. Just a few threat examples:

- Loss of confidentiality of video and audio data based on local access to the SD-Card: PII.Generic.Local.Confidentiality
- Loss of integrity of security configuration data via the web-interface: Security.PrivateConfiguration.KnownNetwork.Integrity

- Loss of availability of the video streaming function via the web-interface: Function.Essential.KnownNetwork.Availability

These threats might be invoked by any events and are not necessarily attacker based. There are generally three types of events:

- Intentional attacks by malicious actors (Attack)
- Unintentional human errors (Misconfiguration)
- Natural or technical failures (Failure)

If necessary these events can be added to the threat description, e.g. PII.Generic.Local.Confidentiality.Attack.

A.5. Risk Evaluation

Based on the identified assets and their environments the risks can be evaluated in regards to their impact and likelihood.

Impact is based on the (C/I/A) values of the corresponding asset categories as described in 5.12.1.

Data Assets

- Video and audio data (PII.Generic): (3/2/3)
- Connection data (PII.TechnicalNecessary): (2/1/1)
- General Configuration data (Other.Configuration): (1/3/1)

Security Assets

- WPA-Key for WLAN access (Security.Secrets.NetworkCredentials): (4/3/3) Note: Integrity and availability is 3 because both will impact the availability of essential functions (A:3).
- WLAN Configuration (Security.PrivateConfiguration.Confidentiality): (3/3/3) Confidentiality and Integrity is 3 because both will impact the confidentiality of PII.Generic (C:3).

Functional Assets

- Video and audio capturing function (Functions.Essential): (-/-/3)
- Web-Interface Configuration (Functions.NonEssential): (-/-/1)
- Web-Interface Streaming (Functions.Essential): (-/-/3)
- Streaming Protocol (Functions.Essential): (-/-/3)

The likelihood of a threat is based on the environment the asset is handled in.

For assets handled in the internal environment (1) the following parameters apply:

- Access Restriction: Restricted
- Interface Restriction: Physical
- User Capability: Layman

For assets handled in the local environment (2) the following parameters apply:

- Access Restriction: Restricted
- Interface Restriction: Local
- User Capability: Layman

For assets handled in the known network environment (3) the following parameters apply:

- Access Restriction: Restricted
- Interface Restriction: Known Network
- User Capability: Layman

A.6. Risk Acceptance

Based on the impact and likelihood the risks can be evaluated in regards to their acceptance following the acceptance criteria in 5.12.3.

In the given example has generally assets with a moderate impact at best with an outliner of the WPA-Key with a high impact on confidentiality.

Local Threats to data assets with moderate impact can be accepted, as they are mitigated by the local access restriction. There are no threats with high or very high impact in the local environment.

Network Threats to data assets with moderate impact might be accepted, as they are mitigated by the closed network behind a gateway. As the network is not dedicated and might contain other potentially compromised devices, this is not advisable. As assets with a high impact are exchanged via the network, these threats are definitely not acceptable as an attacker might be motivated and capable enough to compromise the surrounding network.

Threats on misconfiguration can also not be accepted as the user is a layman and might easily misconfigure the device resulting in an adverse affect.

The results and rationale of risk acceptance are documented after performing the risk evaluation for all identified threats.

A.7. Mitigation of Risks

Unaccepted risks have to be mitigated by appropriate controls. The manufacturer decides to protect the confidentiality and integrity of the PwDEs assets against network threats.

This includes for example the following controls: - Use of encrypted protocols für the web interface and streaming protocol following the generally acknowledged state of the art (e.g. HTTPS, DTLS-SRTP) - Authentication for access to the web and streaming interface following the generally acknowledged state of the art (e.g. strong passwords, no default passwords) - Additional protection of the WPA-Key against information disclosure by storing in the PwDE with exclusive read-only access for the WLAN service and exclusive write-only access for configuration changes via the web interface.

Risks mitigated by these controls have to be re-evaluated in the updated risk assessment.

A.8. Updating the Risk Assessment

Following the implementation of the controls the risk assessment has to be updated to reflect the changed situation. This includes an update of the assets as the implementation of authentication and encryption made additional security asset necessary.

The encryption of the web and streaming interface is based on public and private keys provided by the manufacturer and stored on the PwDE. The public key

The HTTPS Key will protect the confidentiality of video and audio streams as well as configuration data in transit against eavesdropping, like the WPA-Key during set up. The WPA-Key has the highest confidentiality impact and will be used to calculate the impact of the HTTPS-keys:

- HTTPS-Private Key (Security.Secrets.Confidentiality): Environment 1: (4/4/3)
- HTTPS-Public Key (Security.PublicConfiguration): Environment 1 & 3: (1/4/3)

SRTP will protect the confidentiality of the video and audio stream. Based on the confidentiality impact of the video and audio data this will result in the following additional assets:

- SRTP-Private Key (Security.Secrets.Confidentiality): Environment 1: (3/3/3)
- SRTP-Public Key (Security.PublicConfiguration): Environment 1 & 3: (1/3/3)

To calculate the impact of the authentication data the functions accessible after authentication have to be evaluated. The authentication data is stored on the PwDE and transmitted during login and is as such subject to Environment 1 & 3

An authenticated user can access the configuration and streaming function. The authenticated user can read video and audio data as well as configuration data except the previously mentioned WPA-Key.

- User Credentials (Security.Secrets):Environment 1 & 3

Thus the impact of the user credentials used as a secret to protect the confidentiality is based on the confidentiality impact of video and audio data.

- User Credentials (Security.Secrets): Environment 1 & 3: (3/3/3)

The user credentials also protecting the integrity of the configuration and other data stored on the PwDE, which can be edited via the web interface. Taking the integrity of the protected assets into account this would yield the same result, as the maximum impact is 3 based on the integrity of the WPA-Key.

Besides the data assets the PwDE also has some new security relevant functions, protecting the confidentiality and integrity of the data assets, especially the WPA Key with the highest impact on confidentiality. Resulting in the following additional functional assets with network access (Environment 3) running on the PwDE (Environment 3):

- HTTPS encryption / Permission System (Security.Mechanism): Environment 1 & 3: (-/4/3)
- SRTP encryption (Security.Mechanism): Environment 1 & 3: (-/3/3)

These new assets result in additional threats, which have to be evaluated in the updated risk assessment and mitigated accordingly.

To reduce the number of these iterations

Appendix B: Risk Scoring

Instead of the binary acceptance criteria in 5.12.3 the acceptance of a risk can also be evaluated by using a scoring scheme and a risk matrix, as shown in this annex. This approach is highly experimental and will be developed further based on collected experience.

B.1. Environment Scoring

The mathematical interpretation is an experimental procedure which can be used to score the likelihood of an incident in a given environment.

The used environment indicators describe the maximum expected exposure of the PwDE to the minimum expected protection of the PwDE from network, physical or misuse threats in the expected operational environment and can be used for scoring of risks. This approach is loosely based on CVSS Environmental Metrics 6 and takes into account the different use cases a PwDE might be subject to.

Additional expectations for the operational environment can be included in this indicator for more specific scenarios. The environment indicator is estimated using the following formula:

```
environment = round(1 +  interface restrictions * access restriction * user capabilit
y) * 4)]
```

using the interface restriction, access restriction and user capability factors as defined below:

Interface Restriction

Value	Rationale	Base	Factor
Physical	The PwDE communicates internally and can be accessed by physical manipulation. In case of software products this entails a manipulation of the internal communication/processing of the software. Attackers need direct access to the PwDE and manipulate it internally	10%	38%
Local	The PwDE communicates a short distance via a local interface, e.g. embedded user interface, nfc or short distance wired connection. In the case of software this also includes interprocess communication with other software PwDEs on the same device. Attackers need direct local access to the PwDE.	20%	55%
Dedicated known Network	The PwDE communicates with an adjacent network known and trusted by the user without intended connection to an external network. The network is dedicated to a use case and is as such expected to consists of limited number PwDE only using the network for the dedicated use case, e.g. local home bus system, peer-to-peer WLAN or bluetooth connection. Attackers have to be in proximity to the PwDE to access it via the network, access from an external network is not intended	40%	70%

Value	Rationale	Base	Factor
Known network	The PwDE communicates with an adjacent multi-purpose network known and trusted by the user which is shared with other PwDEs for multiple use cases, e.g. home or office network. Attackers have to be in proximity to the PwDE to access it via the network, access from an external network is not intended	50%	80%
External Network	The PwDE communicates with a network not under the control of the user or the organisation of the user, e.g. mobile network, WAN or unknown WLANs. Attacker can potentially access the PwDE from anywhere as the topology of the external network is not known.	100%	100%

Access Restrictions

Value	Rationale	Base	Factor
Restricted	The access to the PwDE is restricted, only a group of known people have access to the PwDE.	10%	42%
Public Restricted	Public access is intended or unavoidable, but the PwDE is normally supervised by an authorized person. The window for an attack is generally limited.	20%	58%
Movable	Public access is intended or unavoidable, but the PwDE is normally supervised by an authorized person. The PwDE is movable and can be removed by an attacker. The window for an attack is generally limited, but can be extended by moving the object.	50%	81%
Non Restricted	No particular access restriction, there is no limitation on potential attacker and attack window. This also applies if the local access is restricted, but the attack can be executed without local access.	100%	100%

User Capability

Value	Rationale	Base	Factor
Non-user-related	User Capabilities have no impact on the likelihood of an incident	100%	100%
Skilled	A skilled user, e.g. an IT professional, is not likely to exposed the product unnecessarily through insufficient handling and configuration and is able to enhance the security of the PwDE using his own expertise	20%	58%

Value	Rationale	Base	Factor
Instructed	An instructed user, e.g. a craftsman or IT security savvy user who read the manual, is is not likely to exposed the product unnecessarily through insufficient handling and configuration	50%	81%
Layman	A not particular skilled user, is likely to expose the product unnecessarily through insufficient handling and configuration	100%	100%

Important The environment indicator is not a precise mathematical calculation of the likelihood of an incident, but rather a simplified indicator to support the risk assessment. The factors used for the parameters are a based on a subjective estimation of protection provided by the environment using the following rationales:

- Environments allowing an unregulated physical or logical access to the PwDE grant no protection from attackers have a factor of 100%, as they do not lessen the likelihood of an incident. Thus the likelihood of an incident can be directly based in the impact. Environments allowing only a limited physical or logical access to the PwDE grant some protection from attackers and have a factor less than 100%, as they lessen the likelihood of an incident. The factors are estimated based on potential number od entities known or unknown to the user with access to the environment.
- Environments without skilled personnel grant no protection against attacks facilitated by misconfiguration, social engineering attacks as well as attacks which can be avoided by manual monitoring of the PwDE and have a factor of 100%, as they do not lessen the likelihood of an incident. Environments with more skilled personnel are expected to be more aware and less likely subject to misconfiguration or other human errors, and thus making risks based on human error less likely.

As stated before the mathematical precise calculation of impact and especially likelihood is not particular feasible. The "calculated" likelihood in form of environment is just an indicator used to simplify risk the analysis and is not perfect. It is always possible to deviate from the calculated likelihood using a rationale based on experience and threat intelligence. Instead of the formula the environment indicator can also be expressed with a lookup table. This approach was not used as it will get increasingly confusing with additional parameters.

The factors used for the formula are derived the following approach:

- The fixed factors 1 and 4 are based on the number of the target scale 1 to 5.
- For every indicator a base is estimated using a value from 0 to 1. The estimation is based on the experience and evaluation of risk scenarios.

- The factor is calculated based on estimated base percentages b and f =(number of factors)^2 following the formula factor = Log_f((b*(f-1))+1). This is done in order to compensate the multiplication used in the calculation of the risk indicator.
- The factor 1 has no effect on the calculation and can also be used if a value has no impact on the calculation, e.g. Value "Non-user-related" for User Capabilities. Every lower factor has a beneficial impact on the likelihood.

B.2. Acceptance Criteria

A risk can be classified based on its likelihood and potential impact. The following scale will be used:

Risk Classification:

- 1 - Very Low
- 2 - Low
- 3 - Moderate
- 4 - High
- 5 - Very high

Acceptance Rule:

Every Low and Very Low Risk can be accepted, every other risk has to be treated.

Note Acceptance criteria are a tool for quick decision making, but not a substitute rationalized decision making process. Generally when accepting a risk the decision must be comprehensible justified and documented. Generally risks classified as moderate have to be treated during the course of development, but can be accepted in post-market if the effort of treatment is not in relation with the potential risk and the remaining product lifetime. High and very high risks are generally not acceptable and have to be treated.

	Impact 1	Impact 2	Impact 3	Impact 4	Impact 5
Environment 5	1	1	1	2	3
Environment 4	1	1	2	3	3
Environment 3	2	2	3	4	4
Environment 2	2	3	4	4	5
Environment 1	2	3	4	5	5