Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defense, Civil Protection, and Sport DDPS
National Cyber Security Center NCSC

November 20, 2025

Cybersecurity and Resilience Method (CSRM)

A structured approach to strengthening cybersecurity and resilience

Table of Contents

1 Introduction

In this document, the Swiss National Cyber Security Center (NCSC) proposes a structured approach to strengthening the cybersecurity and resilience of organizations and companies regardless of their size and industry, which is referred to below as the cybersecurity and resilience method (CSRM) or method, in short.[1]

The CSRM is based on relevant standards, recommendations, and best practices, in particular the NIST Cybersecurity Framework (CSF) [2] and the IT security procedures that have been successfully implemented in the Swiss federal administration.[2] It does not require a complete risk assessment, as is expected or required with all common frameworks for dealing with cyber risks[3], and aims to strengthen cybersecurity and cyber resilience in the simplest and most pragmatic way possible [6 – 8]. To this end, an extended baseline protection approach is pursued, whereby a baseline protection is defined by a set of best practices formulated as basic requirements (see Appendix C), which must be implemented in all cases. In addition, depending on the protection needs, additional technical and organizational measures (TOMs) must be implemented. The protection needs are determined by an assessment of the impact of potential IT security threats on the business and production process objectives of the organization or company.

The method is characterized by the following key features and characteristics:

- It is based on international standards (in particular, the NIST CSF) and the IT security procedures of the Swiss federal administration.
- Its overarching objectives are to safeguard important activities and corresponding business and production processes, protect the values of the organization or company, ensure compliance with laws and other regulatory requirements, and protect against disruptions and accidents. If necessary, additional TOMs may need to be implemented in addition to those that follow the baseline requirements.
- Although it does not require a complete risk assessment and particularly a quantification of risks, it is risk-based and is based on a qualitative assessment of IT security threats and their corresponding effects.
- It assumes that any number of hardware and software components can be aggregated into IT protection objects.[4] This aggregation option represents an important extension and refinement of the commonly used cyber security

[1] For the terms "cybersecurity" and "resilience," please refer to Appendix A and [1].

[2] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund.html. These requirements are available in German, French and Italian language only.

[3] Examples include ISO/IEC 27005 [2], NIST Risk Management Framework (RMF, https://csrc.nist.gov/projects/risk-management/) [3], and NIST SP 800-30 [4] with the corresponding tools. A more comprehensive overview of currently available and practically used framework models for dealing with cyber risks has been developed by the European Union Agency for Cybersecurity (ENISA) and is available at https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

[4] The term "IT protection object" has not yet been defined at this point. As explained later, an IT protection object is a set of IT resources (such as hardware and software components) that serve a common and defined purpose and therefore logically belong together.

frameworks . It allows for a coherent allocation of resources for the implementation of suitable TOMs.

- It enables reporting that allows organizations and companies to transparently demonstrate the security and resilience characteristics of each business or production process or product, thereby building trust with customers and society.

In the medium term, the CSRM is intended to offer an alternative to the ICT minimum standard [9] developed by the Federal Office for National Economic Supply (FONES) and declared mandatory by the respective regulators for parts of the Swiss economy, in particular operators of critical infrastructure in the electricity and gas sectors.

Figure 1: NIST Cybersecurity Framework (© N. Hanacek/NIST)

Various sections of this document refer to the NIST CSF, which is shown schematically in Figure 1. This applies, in particular, to the baseline requirements listed in Appendix C. The aim is to make it easier for users of the ICT minimum standard to switch to the CSRM. [10]

The next chapter provides an overview of the method, before the individual steps are explored in more detail in the following chapters 3 to 7. Chapter 8 outlines the control objectives for assessment and benchmarking, and Chapter 9 outlines current and future work related to CSRM. Finally, the An overview of the terms IT-, data- information- and cybersecurity is given in Appendix A, The security levels for authentication procedures, and services is provided in Appendix B and the baseline protection requirements are shown in Appendix C.

2 Overview

As mentioned, the CSRM is based on an (extended) baseline protection approach. This means that basic requirements are postulated, which must be implemented for each IT protection object with suitable TOMs (see Appendix C).[5]

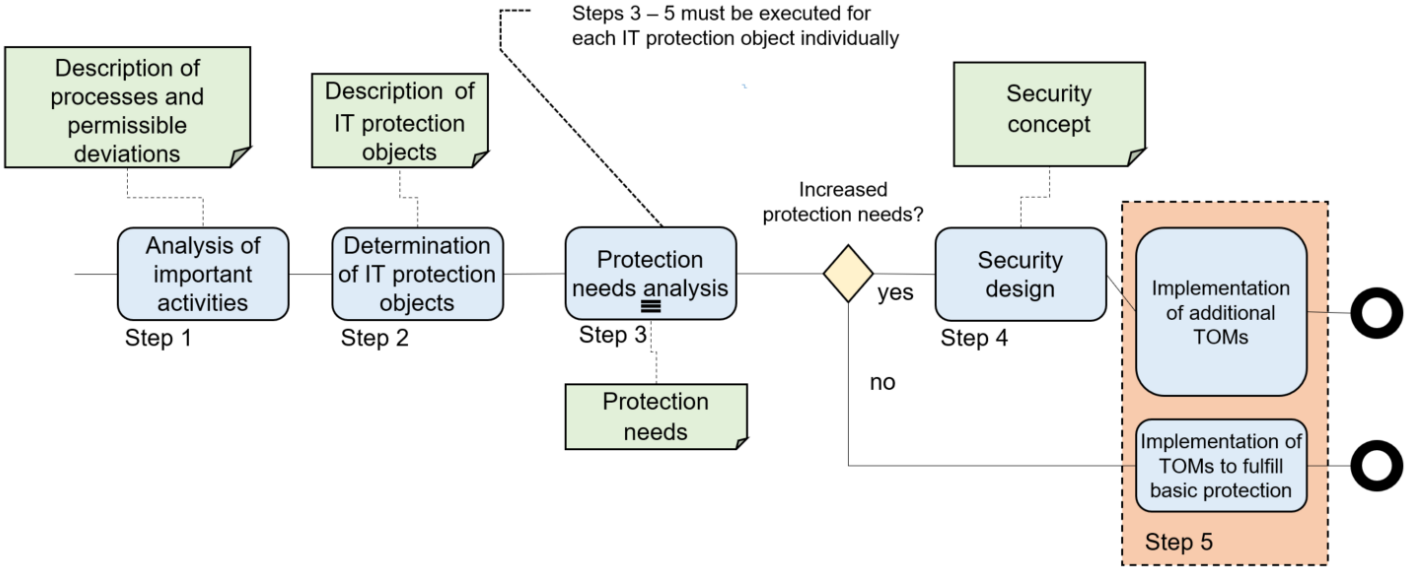

Figure 2: BPMN specification of CSRM

Beyond the baseline protection requirements, the method is based on a five-step process, which is limited to architectural security considerations for IT protection objects.[6] The steps of the CSRM are specified in Figure 2 using Business Process Model and Notation (BPMN) and can be summarized and described as follows:

- **Step 1 (Analysis of important business activities):** In order to use the method effectively, the organization or company must be familiar with and have a detailed understanding of its important activities and corresponding business and production processes, including their objectives and dependencies. Accordingly, this analysis represents the first step of the CSRM.
- **Step 2 (Determination of IT protection objects):** In the second step, the IT infrastructure used to perform the important activities analyzed in the first step is divided into a set of IT protection objects. These are then considered and documented individually. An IT protection object can consist of various IT resources, such as

[5] The implementation of the baseline protection requirements is fundamentally binding for all IT protection objects. Depending on the organization or company, justified and documented exceptions may be possible, whereby the corresponding exemption approval procedures and processes must be transparent and clearly defined.

[6] Vulnerabilities and weaknesses in specific implementations and products must be considered and addressed separately and outside the method, e.g., as part of vulnerability management. Such vulnerability management must be covered at the operational level and is not the subject of CSRM.

hardware[7] and software components, as well as data stored, processed, and transmitted therein. These resources serve a common and defined purpose and therefore belong together logically (e.g., an application for handling a business or production process or a platform used by multiple processes). Steps 3–5 are carried out individually for each object.

- **Step 3 (Protection needs analysis):** For each IT protection object identified in step two, step three must determine whether its protection needs are increased or not. This is achieved by mapping stored, processed and transmitted data to the business and protection processes that it enables, and then considering the impact that harm to its confidentiality, integrity or availability (IT protection goals) would have on the process objectives. If harm to any of these IT protection goals could result in an inability to achieve the process objectives, the protection needs are increased. This is essentially a binary decision that must be made independently of the baseline requirements.
- **Step 4 (Security design):** For each IT protection object with an increased protection need (according to the protection requirement analysis), step four must determine which additional TOMs beyond the baseline protection requirements are necessary or useful, and how these are to be implemented. An in-depth analysis of the IT protection object and its specific circumstances is required to select the appropriate TOMs. Typically, this analysis is based on a threat model. In either case, the outcome of this step is a security concept documenting both the IT protection object and its protection requirements, as well as the TOMs intended to fulfil these requirements.
- **Step 5 (Implementation):** In the fifth and final step, the TOMs must be implemented promptly for each IT protection object and transferred to regular operation. These TOMs either serve to fulfill the requirements of the baseline protection or are identified as additional TOMs in the IT security concept.

The organizational and administrative structure of the CSRM, as well as the corresponding responsibilities and accountabilities for establishing cybersecurity and resilience, depend on the organization or company in question and cannot be defined in a generally applicable manner within the scope of this document. However, it is certainly appropriate and advisable for management to issue a security policy that recommends or mandates the use of the method and ensure that the security concept of each IT protection object is brought to the attention of the management in a suitable form. This is in line with the fact that management is ultimately responsible for cybersecurity.

The following chapters provide a more detailed and in-depth explanation of the five steps of the CSRM, i.e., the analysis of important activities, the determination of IT protection objects, the protection needs analysis, the security design, and the implementation.

[7] The term "hardware components" also includes peripheral devices, i.e., external devices that are connected to an IT system to extend its functionality, such as keyboards, mice, printers, monitors, and external data storage devices.

3 Step 1: Analysis of Important Business Activities

The analysis of the activities that are important for the organization or company and the associated business and production processes forms the starting point for the CSRM. In a pharmaceutical company, for example, the manufacture and distribution of medicines are important activities, whereas in the IT industry it is more likely to be the development and maintenance of software and advising customers. In any case, the important activities must be supported by appropriate business and production processes (hereinafter referred to collectively as processes), whereby business processes involve the provision of (services) and production processes involve the manufacturing of goods. These processes vary from organization to organization and from company to company and must therefore be tailored to the organization or company and understood well for the CSRM to be used effectively.

3.1 Implementation

The analysis of important activities (step 1) essentially comprises two sub-steps: First, the processes relevant to the important activities of the organization or company must be identified[8] (sub-step 1) before these processes can then be analyzed and documented with regard to cybersecurity and resilience (sub-step 2).

Sub-step 1: Determining the relevant processes

In the first sub-step, the processes that are relevant to the performance of the organization's or company's important activities (and are therefore indispensable for achieving its strategic and economic goals) must be identified. To determine these processes, existing process descriptions or documentation, manuals, and standard operating procedures (SOPs) can be used[9] and/or interviews and workshops with employees (involved in the processes) can be conducted The number of relevant processes should be manageable and will depend on the organization or company. Normally, it will range from a few to a dozen, although in larger organizations or companies more might be needed.

Sub-step 2: Analysis and documentation of processes

The processes identified in sub-step 1 must be systematically analyzed and documented in sub-step 2 (with respect to cybersecurity and resilience). The analysis and documentation should primarily focus on the objectives (process objectives) and data (process data).

- The **process objectives** specify what is to be achieved with a process in concrete terms. They consist of a main or primary objective and several secondary objectives. While the primary objective is at the center of the process under consideration, the secondary objectives serve to ensure important conditions for this process. In a business process, for example, the primary objective will be the efficient provision of a service, while in a production process it will be more about

[8] Although the wording here is in the plural, it may be that in certain organizations or companies there is only one relevant business or production process.

[9] In this case, the existing standard operating procedures can be checked for validity at the same time.

manufacturing goods in the required quantities. In addition, a secondary objective may be the security of the process,[10] protection against disruptions and accidents (in terms of "safety"), the protection of intellectual property, or compliance with laws, regulations, standards, and best practices (in terms of "compliance"). Along with the (primary and secondary) process objectives, the maximum permissible deviations must also be defined. These permissible deviations are essential for the protection needs analysis carried out in step 3. The margins for deviations may also be small or non-existent (for example in the context of "compliance").

- **Process data** are metadata that summarize the process as completely as possible. This information will enable and simplify the subsequent steps of CSRM. Examples include data on the following process components:
  - Inputs (e.g., raw materials, suppliers, services, etc.)
  - Required resources (e.g., IT systems, machines, devices, etc.)
  - Procedures
  - Conditions (e.g., deadlines, lead times, etc.) and rules to be observed (e.g., legal and internal regulations, standards, quality specifications, etc.)
  - Dependencies (e.g., on other processes)
  - Problems and disruptions that may occur and must be anticipated (e.g., environmental damage, accidents, disclosure of trade secrets, etc.)[11]
  - Output and results (e.g., services or goods to be produced)

  In some cases, process data may already be specified as a primary or secondary objective, such as goods to be manufactured as the primary objective of a production process or environmental damage that must be minimized as part of a secondary objective.

3.2 Outputs

The processes derived from this analysis must be described and documented in an understandable form. For each process, the documentation consists of a graphical representation (e.g., flowchart or BPMN diagram) and a structured (e.g., tabular) description of the process objectives (with maximum permissible deviations) and the process data in accordance with section 3.1. Of course, unstructured additional information can also be included in the documentation, especially if it is suitable for supporting or simplifying the subsequent steps of this method.

4 Step 2: Identification of IT Protection Objects

Based on the processes analyzed in the first step, the second step involves determining the IT protection objects required by these processes. The necessary division of the IT infrastructure (consisting of hardware and software components, data, and other

[10] The secondary objectives of business or production processes that are relevant to security are collectively referred as protection objectives. IT-relevant contributions to the protection objectives are referred to as IT protection goals.

[11] This is not about performing a risk assessment. The aim is to assess whether the determined problems and disruptions can occur in principle, regardless of possible threats.

IT resources) into a set of IT protection objects is a difficult (architectural) task. On the one hand, it must be based on the relevant processes and an explicitly or implicitly given enterprise architecture (top-down approach). On the other hand, a meaningful aggregation of different hardware and software components into an IT protection object can also result from the interaction of these components in fulfilling a common function (e.g., platforms, cloud services, databases, etc.) ("bottom-up" approach). Taking both approaches into account and weighing them up is challenging and is not addressed in any of the current cyber security frameworks. Instead, these documents often refer to assets, i.e., properties that must be inventoried, but for which it is not specified whether they are individual IT resources or aggregated IT protection objects. In this sense, the definition of IT protection objects also represents an important extension and clarification of these frameworks. It allows the excessive number of IT resources and assets to be reduced to a manageable number of (aggregated) IT protection objects, thereby optimizing the overall effort.

It should be noted that there is not just one correct solution for determining IT protection objects, but many, each with different advantages and disadvantages. The assignment of IT resources to IT protection objects is not clear-cut, and accordingly there will be (many) IT resources that are simultaneously part of different IT protection objects. This will result in IT protection objects overlapping. It shall be the aim to keep the number of these overlaps as small as possible. Overlaps make it difficult to take a consistent approach to the selection and implementation of TOMs. For small organizations, there may also be cases where the entire IT infrastructure can be regarded and considered as a single IT protection object.

4.1 Implementation

There are various options or procedures for determining the components of IT protection objects. However, any sensible procedure will always consist at least of the three sub-steps outlined below.

Sub-step 1: Determination of applications (per process)

For each process, the applications that are necessary for achieving the corresponding primary and secondary objectives must be identified. With respect to primary objectives, these may be applications for supplier management or electronic commerce, while secondary objectives may include applications in the area of human resources or enterprise resource planning (ERP). In any case, the result of this step is a list of applications for the analyzed process.

Sub-step 2: Determination of IT resources (per application)

For each of the applications identified in sub-step 1, the IT resources they require must be determined. An IT resource can be a hardware and/or software component or data.[12]

[12] The software component may be the application determined in sub-step 1 itself or it may be the components and modules used by the application, if it is essential for securing the application to list them separately.

Sub-step 3: Review and simplification of IT protection objects

Finally, it must be checked whether all hardware and software components are assigned to at least one application and each application to at least one process. These assignments should be verified for further aggregation and simplification, such as combining several applications into a cross-application platform. A platform usually offers a range of cross-sectional functions that can be used by several applications simultaneously. Ultimately, each application or platform identified in this way represents an independent (aggregated) IT protection object. The number of IT protection objects should be limited to a few dozen at most.

4.2 Results

The aggregated IT protection objects identified in this step must be documented in a meaningful way. Documentation should include at least the following information relating to the IT protection object:

(1) Unique name or identifier
(2) Brief description (including any architectural sketches and platforms used)
(3) List of business and production processes served by the IT protection object
(4) Summary list of hardware and software used
(5) List of sensibly grouped and aggregated input and output data as well as data flows
(6) List of people and groups for whom the IT protection object is or may be relevant
(7) Physical conditions (e.g., buildings, machines, etc.) that may be relevant to cybersecurity
(8) Any other available information or condition (e.g., suppliers, geographical requirements, etc.)

Of course, any other information can also be included in the documentation of the IT protection object if it is useful for providing cyber security and resilience.

5 Step 3: Protection Needs Analysis

For each of the IT protection objects identified in the second step, the protection needs must be analyzed and defined in the third step. The analysis is based on the (primary and secondary) objectives of the processes the IT protection object supports as well as the maximum permissible deviations associated to these objectives (from step 1). If the IT protection object can result in at least one impermissible deviation, the protection needs of that object is increased. Only in the case of increased protection needs, additional security controls are to be evaluated in the fourth step (and a security concept will be developed). If there is no increased protection needs, this step is not needed, and the baseline protection requirements and the implementation of corresponding TOMs will suffice.

5.1 Implementation

For the protection needs analysis of an IT protection object to be carried out in a meaningful way, a data directory must be created. The input and output data identified in step two (i.e., in point (5) of section 4.2) can be used as a starting point. The directory

must contain the data that is either generated, stored, processed, and/or transmitted by the IT protection object or is required for the provision of the IT protection object. The data should be grouped in a meaningful way and supplemented with attributes. One such attribute could be, for example, whether the data group contains personal data and is therefore subject to personal data protection requirements.

For at least each data group (in the data directory) and, if necessary, for other IT resources (such as hardware or software components), it must be examined what effects a compromise could have with respect to the various IT protection goals. Specifically, the following questions must be answered: What would happen if a particular IT protection goal (e.g., confidentiality, integrity, availability, etc.) were violated, and how compatible would this be with the objectives defined for the underlying process, considering the permissible deviations? The answers to these questions should be compiled in a table, with the data groups and other IT resources listed as rows and the attributes listed as columns, together with the effects of a breach of IT protection goals. The table entries may contain full sentences or keywords. At a minimum it must be visible where the permissible deviations may be exceeded and where there is a resulting increased need for protection. A single possible impermissible deviation is sufficient for the whole IT protection object to have an increased need for protection. Detailed explanations throughout the table entries can help to create and improve the subsequent security concept.

Finally, the analysis must be verified for plausibility and consistency. This contains whether the reported possible effects are realistic, and if the assessments are comprehensible and well-founded. If necessary, other parties should also be consulted(such as the data protection advisor when working with personal data).

5.2 Results

The result of a protection needs analysis is a (binary) decision as to whether an IT protection object has an increased need for protection or not. As mentioned above, if the result is positive, a table with details on where deviations to the process goals are possible will also help with the next steps. The selection of suitable TOMs will depend largely on which IT protection goals are threatened and what these threats specifically look like (controls against availability needs are not the same as those for integrity or confidentiality needs). In any case, it makes sense to add the findings from the protection needs analysis in a suitable form to the documentation of the IT protection object from step two.

6 Step 4: Security Design

In the fourth step, a security concept must be developed for each IT protection object with increased protection needs. Among other things, this concept must specify which (additional) TOMs that go beyond the baseline protection requirements are necessary or useful, and how these TOMs are to be implemented without impairing the purpose of the underlying processes (security controls that impact the primary objectives are self-defeating and should be avoided). To select such TOMs, an in-depth analysis of the IT protection object and its specific circumstances is necessary.

The first step reveals, among other things, which objectives are to be achieved for a process (and its supporting IT protection object), and which deviations and

corresponding effects are therefore impermissible. The protection needs analysis carried out in the third step further reveals which of these effects are fundamentally possible. For these possible but impermissible effects, the aim is to select suitable TOMs to either eliminate the effects or reduce them to an acceptable level. This is the subject of the security design to be carried out in this step.

6.1 Implementation

Security design essentially consists of three sub-steps: threat modeling, the selection of suitable TOMs, and the creation of a security concept. Various methodical approaches are available for the first two sub-steps, the approach described below is recommended by this method. If an organization or company already successfully uses a different approach for threat modelling and selection of TOMs, it can of course continue using these.

Element	S	T	R	I	D	E	LM
Actor	x		x				
Prozess	x	x	x	x	x	x	x
Dataflow		x		x	x		
Datastore		x		x	x		
Basic measure	Authentication	Integrity check Hardening Message authentication	Logging	Encryption Access control Segmentation	Redundancy High availability	Access control Least Privilege	Autonomous protection of components

Table 1: Relevant threat categories according to STRIDE-LM (with basic measures)

Sub-step 1: Threat modeling

STRIDE or STRIDE-LM[13] is an approach to threat modeling that has proven itself in practice and is therefore also recommended as part of the CSRM. It involves systematically examining which architectural elements of an IT protection object are exposed

[13] STRIDE is an approach that was originally developed by Loren Kohnfelder and Praerit Garg for threat modeling at Microsoft and is now used worldwide [11]. The name is an acronym (artificial word) composed of the initial letters of the original six categories of security threats distinguished within STRIDE: Spoofing (identity concealment), Tampering (data manipulation), Repudiation (denial of having accessed a system or data), Information disclosure (violation of privacy or data leakage), Denial of service (prevent authorized access), and Elevation of privilege (extension of rights). Within the scope of STRIDE-LM, the model has been supplemented with the category "Lateral Movement" (LM) to include threats in networks. Although this category could also be subsumed under "privilege escalation," STRIDE-LM is used within this method.

to which threat categories and how these threat categories can be countered.[14] As shown in the upper (blue) part of Table 1,[15] the architectural elements can be viewed as rows and the threat categories as columns of a matrix. The basic architectural (data flow) elements are taken from the documentation of the IT protection object. These include actors, processes, data flows, and data storage. Different threat categories from STRIDE-LM are relevant for these elements, such as "spoofing" and "repudiation" for actors. The threat categories relevant to a specific architectural element are marked with an "x" in Table 1.

Sub-step 2: Selection of suitable TOMs

For each threat category relevant to a specific architectural element, it must be discussed with which basic measure (highlighted in orange) from Table 1 and its associated specific TOMs, the specific threats can be countered. This selection does not require probability-based estimates and risk calculations, but only qualitative and technological considerations in the form of heuristics[16] . If, for example, a relevant threat is that certain data can be intercepted during transmission, then the consistent use of encryption technologies is a sensible and appropriate (technical) measure to counter this threat. A similar heuristic applies to an Internet connection: if, for example, a specialist application can be accessed via the Internet as an IT protection object, the use of a firewall is always a sensible (technical) measure.

Heuristics must therefore be used to check whether the use of suitable TOMs from the basic measures listed in Table 1 can reduce the attack surface of the IT protection object and its critical elements to an acceptable level. Preventive and, in particular, detective and reactive TOMs should be used in such a way that they complement each other in a meaningful way.

Sub-step 3: Creation of a security concept

The TOMs selected must be specified and documented in a security concept. For certain situations and use cases, sets of suitable TOMs will emerge that are appropriate and can be standardized within context and sector specific recommendations.

6.2 Results

As a result of this step, all selected TOMs must be documented and specified in a security concept to be implemented as part of the next step. The specifications must

---

[14] In many process models, risks are modeled using a list of actual threats such as ransomware or DDoS attacks. The list of threat categories postulated within the framework of STRIDE simplifies this, as the actual threats can be assigned one or more of these categories. In the case of ransomware, these are "information disclosure" and "denial of service".

[15] This part of Table 1 is taken from https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach and supplemented in the last column.

[16] The term "heuristics" is derived from the Greek word "heuriskein," which can be translated as "to find" or "to discover." The aim is to find or discover a solution to a problem that cannot be formulated mathematically and solved precisely with the help of appropriate algorithms, but only approximately with the help of empirical values, rules of thumb, targeted simplifications, and shortcuts. A (solution) procedure is accordingly referred to as heuristic if it can find at least a sufficiently good or plausible solution to a problem with limited knowledge and time.

be sufficiently precise so that the TOMs can be used and operated effectively at the tactical and operational level.

7 Step 5: Implementation

In the fifth and final step of CSRM, the TOMs are to be initially implemented (from the outside in[17]) such that each IT protection object can be transferred to IT operations (who will monitor, maintain and improve these TOMs from thereon) . The TOMs either implement the baseline protection requirements (and are to be described as part of the baseline protection implementation documentation) or are specified in the security concept for those with increased protection needs. Who is responsible for implementation must be clearly identified for each TOM, i.e., it must be clear whether a TOM is to be implemented by the organization or the company itself or by a supplier or customer. In any case, IT operations must also cover its own operational processes, such as incident management, vulnerability management, supplier management, authorization management, and the management of awareness and training programs for employees. These operational processes are key to IT security.

In any case, operations should be understood as a circular process that includes permanent monitoring and improvement of TOMs. Ideally, operations should follow an explicitly or implicitly defined operating model, the form and content of which, however, are not the primary subject of CSRM and therefore of this document. In the simplest case, such a model can consist of policies[18] regarding the operational processes. These are then implemented as standards, procedures, defined roles and responsibilities, and rules, or as a list of activities to be carried out regularly. TOMs that prove to be ineffective must be removed in a timely manner.

8 Assessment and Benchmarking

IT security is a property that can only be measured and tested to a limited extent [12, 13]. Although this is similar for cybersecurity and cyber resilience [1], the latter is fundamentally better suited as a target function and basis for assessment and benchmarking. The reason for this is that, unlike cyber security, cyber resilience consists to a large extent of verifiable components (such as capabilities, processes, organization, and recovery mechanisms) that can be converted into defined control objectives and evaluated (see below).

Assessing and comparing one's own cyber resilience with that of comparable organizations and companies creates transparency on strengths and weaknesses in technology, organization, processes, and corporate culture. It helps those responsible to prioritize investments, implement targeted improvements, and align themselves with recognized standards and regulatory requirements. In this way, it also strengthens the reliability of services for customers, partners, and society as a whole.

---

[17] According to this heuristic, measures to protect the IT protection object from external access are implemented first, before measures aimed at internal protection are implemented. This heuristic therefore guides the prioritization when implementing measures.

[18] These policies do not have to be developed from scratch by each organization, as they will hardly differ for similar processes. Industry-wide templates can be developed and shared.

The assessment of an organization's or company's cyber resilience should be based on the following (six) control objectives:

1. The important business and production processes, along with their dependencies on IT protection objects, must be known, documented, and understood.
2. Responsibilities and accountabilities must be clarified, the necessary resources made available, and sustainably anchored within a security culture.
3. The threat situation must be analyzed and the protection needs understood for all IT protection objects.
4. Suitable TOMs must be implemented for all IT protection objects and brought together in a consistent security concept.
5. It must be ensured that security-related incidents can be detected and dealt with promptly. In particular, affected systems and applications must be able to be restored quickly.
6. All dependencies and risks arising from cooperation with third parties (e.g., from supply chains or through partners) must be controllable in order to avoid domino effects and ensure the resilience of whole value chains.

These control objectives establish the structure for a comprehensive benchmarking of cyber resilience. They ensure that technical, organizational, procedural, and cultural aspects are given equal consideration. With this in mind, the Swiss NCSC has developed cybersecurity and resilience test catalogues, which are currently being further refined and tested in collaboration with interested organizations and companies, with a focus on creating supporting resources and tools for this method.

9 Outlook

CSRM can be understood as a management system for cybersecurity and resilience along management systems that are similar but differ in their focus: data protection management systems (DSMS), business continuity management systems (BCMS), cybersecurity management systems[19] (CSMS) and, above all, information security management systems (ISMS). According to [14], an ISMS can be defined as "a system consisting of procedures and rules" that "can be used in an organization or company to ensure information security, i.e., to define concrete information security objectives and to plan, manage, and ensure their achievement."

Table 2 summarizes the various management systems [10] in terms of their coverage of the cyber resilience control objectives listed in Chapter 8. The CSRM does not provide complete coverage in all areas, as for example, control objective 6 shows. Classic BCM functions, such as recovery planning and sectoral crisis coordination, are not included in the CSRM in full depth. Organizations must additionally rely on established BCM methods.

However, a particular strength of CSRM is that it takes business and production processes as an essential starting point for assessing protection needs. Risks must

[19] This refers in particular to management systems in the field of OT that are aligned with relevant standards (e.g., IEC 62443).

always be assessed in the context of these processes. This also makes it possible to take data protection and operational safety requirements into account throughout the entire process.

While CSRM provides a method, the management systems mentioned above specialize in individual areas of focus: An ISMS, for example, is less firmly anchored in business processes and targets IT systems (as opposed to industrial OT systems). As a result, it is less effective at counteracting the effects of physical disruptions and accidents. A DPMS, on the other hand, focuses on the protection of personal data, the reporting of data breaches, and ensuring compliance with contractual provisions for the protection of personal data, regardless of the actual business and production processes. A BCMS, in turn, primarily affects control objectives 5 and 6, as well as knowledge of the actual business and production processes.

The CSRM offers convergence here and enables the establishment of a management system that combines ISMS, CSMS, DPMS, and in some cases even BCMS. In particular, however, it can enable the simple and pragmatic implementation of an ISMS.

Management system	**Cyber resilience control objectives**					
	1	**2**	**3**	**4**	**5**	**6**
CSRM Cybersecurity and Resilience Methodology		[20]				[21]
ISMS Information security management system			[22]	[23]		
DPMS Data protection management system						
BCMS Business Continuity Management System						

Fully covered

Partially covered

Not covered

Table 2: Coverage of cyber resilience (i.e., cyber resilience control objectives) by common management systems

[20] The method, like the compared management systems, states that ideally, operations must follow an explicitly or implicitly given operating model, the form and content of which, however, are not the primary subject of the CSRM.

[21] Supplier risk management is expected by CSRM as part of its baseline protection requirements, but is not explicitly part of the method.

[22] Risk identification in an ISMS is based on IT protection goals such as confidentiality, availability, and integrity, and not on the acceptable impact to business and production processes.

[23] The goal of an ISMS is to protect information and not to prevent data breaches or disruptions and accidents, so it is not a holistic approach.

Abbreviations

AAL	Authentication Assurance Level
BCM	Business Continuity management
BCMS	BCM-System
CCTV	Closed Circuit Television
CI/CD	Continuous Integration / Continuous Delivery
CSF	Cybersecurity Framework
CSMS	Cyber Security Management System
CSP	Cloud Service Provider
CSRM	Cybersecurity and Resilience Method
DSMS	Data Protection Management System
DDPS	Department of Defense, Civil Protection, and Sport
DTI	Digital Transformation and ICT Governance
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FIDO2	Fast IDentity Online 2
FONES	Federal Office for National Economic Supply
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ICT	Information and communication technology
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
LM	Lateral Movement
MFA	Multi-Factor Authentication
MITM	Mallory in the middle
MVSP	Minimum Viable Secure Product
NCSC	National Cyber Security Center
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OIDC	OpenID Connect
OT	Operational Technology
OTP	One-Time Password
PIN	Personal Identification Number
RFC	Request For Comments
RMF	Risk Management Framework
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SMS	Short Message Service
SOC	Security Operations Center
SOP	Standard Operating Procedure
SP	Special Publication
SSO	Single sign-on
STRIDE	Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege

TOM	Technical and organizational measures
TPM	Trusted Platform Module
XML	Extensible Markup Language

References

[1] NCSC, Technology Review «Cybersecurity and Cyber Resilience», November 2025

[2] NIST, The NIST Cyber Security Framework (CSF) 2.0, February 26, 2024

[3] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protectio— Guidance on managing information security risks

[4] NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations — A System Life Cycle Approach for Security and Privacy, December 2018

[5] NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, September 2012

[6] Rolf Oppliger and Andreas Grünert, How to Manage Cyber Risks: Lessons Learnt from Medical Science , IEEE Computer, Vol. 56, No. 1, January 2023, pages 117–119

[7] Rolf Oppliger and Andreas Grünert, How to Measure Cybersecurity and Why Heuristics Matter r, IEEE Computer, Vol. 57, No. 2, February 2024, pp. 111–115

[8] Andreas Grünert, James Bret Michael, Rolf Oppliger, and Ruedi Rytz, "Why Probabilities Cannot Be Used in Cyber Risk Management," IEEE Computer, Vol. 57, No. 10, October 2024, pp. 86–89.

[9] FONES, ICT minimum standards, 2023

[10] NCSC, «CSRM compared with well-known management systems», 2025

[11] Loren Kohnfelder and Praerit Garg, "The threats to our products," April 1, 1999

[12] Andreas Grünert, James Bret Michael, Rolf Oppliger, and Ruedi Rytz, "On the Measurability and Testability of IT Security," IEEE Computer, Vol. 58, No. 3, March 2025, pp. 120–126

[13] NCSC, Measurability and Testability of IT Security, June 10, 2025

[14] NCSC, Technology Review "Information Security Management and ISMS," July 2, 2025

[15] NIST SP 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management, June 2017

[16] NCSC, Technology Review "Passkeys," 2025

Appendix A: Terms

In computer science, the knowledge pyramid refers to the model shown in Figure 3, which schematically illustrates how information and knowledge can be acquired from data (upward direction) and how information and data can be acquired from knowledge (downward direction). Sometimes the model is supplemented with symbols at the bottom and wisdom or understanding at the top. Data is then composed of symbols, and wisdom or understanding arises (also) from knowledge. Reading downwards, it can be said that knowledge can be encoded as information and information as data. Data thus represents a form of encoded information designed especially for automated processing.

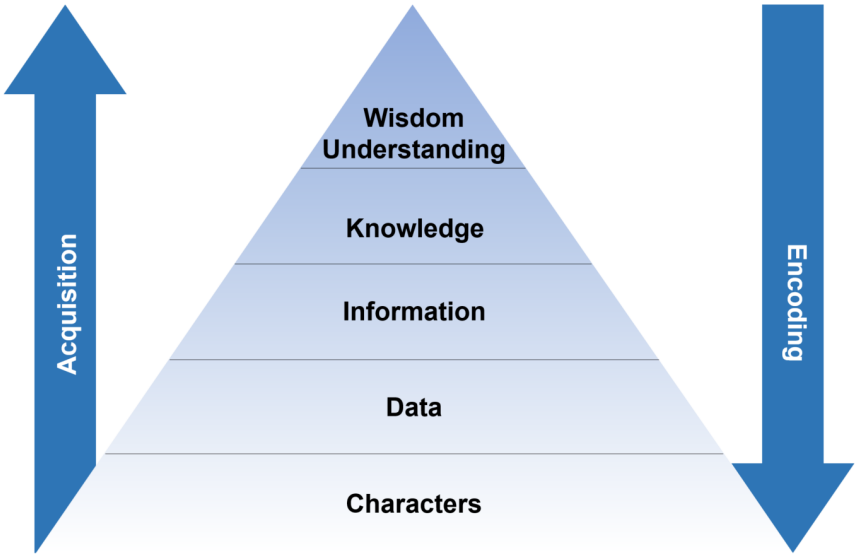

Figure 3: Knowledge pyramid

Although the terms *information* and *data* are often used synonymously in everyday life, this is incorrect and can lead to confusion or even misunderstandings in some circumstances. On the one hand, not all information is encoded as data. When you have a personal conversation, for example, you can glean information from the choice of words, facial expressions, and gestures that are not encoded in a protocol record, or at most only summarily. There are also other situations in everyday life that can be observed and are informative but are neither recorded nor encoded as data. On the other hand, there is data from which no information can be acquired. Think, for example, of randomly generated or encrypted data. In the second case, under certain conditions, it can even be mathematically proven that no information can be derived from encrypted data without knowledge of the keys used.[24]

Because of these differences, the terms information and data should be distinguished from each other, with the distinction also being carried over to the terms data security and information security.

[24] In this context, one also speaks of the information-theoretical security of encryption.

- **Data security** is about ensuring the security of data that is stored, (automatically) processed, and transmitted within the IT and OT systems. Security can also refer to various IT protection goals, such as the confidentiality, integrity, and availability of data.
- In contrast, **information security** is about ensuring the security of information which, as mentioned above, may also exist outside of IT in a form that is not designed for automated processing and is therefore encoded as data. Personal conversations and scenes from everyday life have already been mentioned as examples. Another example is paper archives with handwritten notes. Although the documents archived in this way are also coded, the corresponding coding is not designed for automated processing (even though today, increasingly such documents are being scanned and coded as data for automated processing).

The concept of **IT security** is like data security, but somewhat broader in scope. In addition to ensuring the security of data, this also involves ensuring the security of other IT resources, such as hardware and/or software components. This aspect plays an important role, particularly in the field of operational technology (OT) and in the use of smart devices, also known as the Internet of Things (IoT).[25] It should be noted that although OT and IoT use "normal" IT components, protocols, and architectures, a breach of the protection goals of confidentiality, availability, or integrity can have an impact not only on business and production processes (which may not be able to be continued), but also, on the real (physical) world (e.g., by opening valves, windows, or controlling a mechanical process), potentially causing accidents and injuries. CSRM makes it possible to protect OT and IT systems in a manner to make them resilient, thereby also supporting the methodical convergence of IT and OT in cybersecurity. [26]

[25] The threats to IoT devices, which are often standalone and exposed, differ from OT devices and components, which should be part of an environment equipped with additional safety systems. This difference has an impact on the implementation of the baseline requirements.

[26] The CSRM is designed to be applied not only to business processes, but also to production and OT management systems, process control systems, monitoring systems, digital actuators and sensors in industrial manufacturing processes. To this end, step 1 considers the objectives relating to protection against disruptions and accidents, step 2 considers the components of OT systems as part of the IT protection objects, and step 3 assesses whether a breach of the IT protection goals could lead to a breach of the process objectives, including protection against disruptions and accidents. Finally, the security concept according to step 4 and the baseline protection requirements must also be implemented for OT systems. A comparison of this method with the models from IEC 62443 is currently being developed.

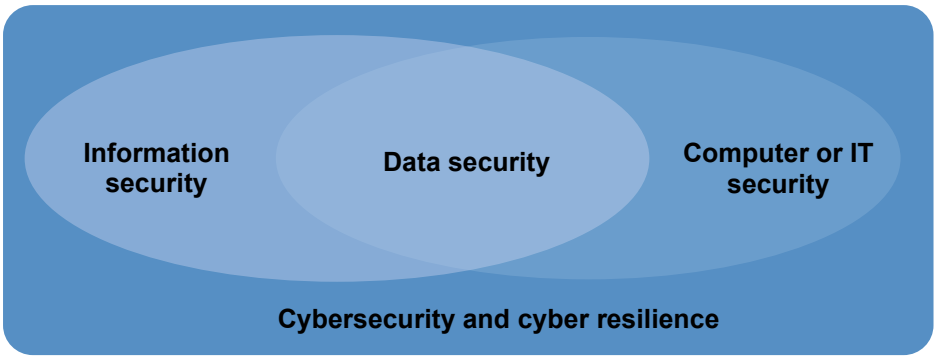

Figure 4: Security terms

The interaction between information, data, and IT security is shown schematically in Figure 4. In addition to these security terms, there are also the relatively new terms **cybersecurity and cyber resilience** [1]. However, the term Cybersecurity is not precisely defined and cannot be easily distinguished from the other security terms. Ultimately, however, cybersecurity is always about protecting IT infrastructures and the information and data directly associated with them. In contrast, **cyber resilience** describes the ability of an organization or company to maintain its essential business and production processes despite cyber threats and IT incidents, or to resume them as quickly as possible after an IT incident. The key factor here is not only the prevention of IT incidents (including attacks), but also the knowledge of which effects are unacceptable and the ability to remain capable of acting at all times, to effectively limit damage, and to return to normal operations quickly.

Appendix B: Security levels for authentication procedures, means, and services

There are many different methods, means, and services available on the market today that can be used for the direct or indirect authentication[27] of people or processes, and some of these differ considerably in terms of their security features. Without going into detail about the differences, this appendix proposes a rough classification with only three security levels ("low," "medium," and "high").[28] The classification is guided by the Authentication Assurance Levels (AAL) 1–3 from [15], is limited to knowledge-based approaches, is kept as simple as possible, and does not currently provide for formal testing or recognition.

- **Low:** The information on the basis of which (direct or indirect) authentication can take place is static and the same for every authentication transaction (e.g., a password or a cryptographic key). If this information is compromised, e.g., in a phishing attack or by recording data traffic on a network, it can be misused for identity theft. Typical examples are usernames and passwords, as well as bearer tokens that are not specifically protected by cryptography (e.g., cookies). The security level remains "low" even if the transmission takes place via a cryptographically secured connection (e.g., TLS). For security reasons, such authentication methods should not be used today, or only in exceptional cases.
- **Medium:** The information on the basis of which (direct or indirect) authentication can take place is dynamic and is regenerated for each authentication transaction. Accordingly, even if compromised, it cannot simply be misused for identity fraud. Usernames and passwords can still be used for direct authentication, but they must be secured by an additional security mechanism, such as device binding.[29] Better options here are OTP software solutions (e.g., Google or Microsoft Authenticator), software certificate-based authentication within using TLS, and FIDO2 implementations with synchronization and key export options (e.g., passkeys [16]). For indirect authentication, the certificates must be cryptographically secured (e.g., encrypted and/or digitally signed) and bound to the user context (e.g., the session) in

[27] Authentication is direct if it takes place directly between the authenticating entity (e.g., person or process) and another (authenticating) entity. If the authentication is moderated by a third party (e.g., an identity provider), it is indirect. In this case, the third party issues a certificate for one or more claims, which in this context is referred to as a *ticket* or *token* and is ideally cryptographically secured by itself. Authentication to the third party must meet the requirements of the corresponding security level.

[28] Accordingly, other approaches to authentication, such as biometric approaches and approaches based on "having something," as well as physical access control mechanisms, are not included in this classification.

[29] In principle, SMS verification codes also provide such security. However, the security of SMS-based authentication is questionable, so that this method should only be used if there is no better alternative.

a state-of-the-art manner.[30] Examples include Kerberos tickets, SAML and OIDC tokens,[31] and JSON Web Tokens (JWTs).

- **High:** The information on the basis of which (direct or indirect) authentication can take place is not only dynamic and is regenerated for each authentication transaction but also depends on a cryptographic key that is stored in a dedicated hardware module and cannot be extracted from there (with reasonable effort). In addition, the hardware module must be personal and must be issued as part of a defined and recorded registration process and handed over to a person in a controllable and recorded manner. Typical examples are OTP tokens (e.g., from RSA, Vasco, or other manufacturers), OTP solutions based on a TPM, hardware certificate-based authentication using TLS, FIDO2 implementations without synchronization and key export options, and authentication based on a Swisscom Mobile ID. For indirect authentication, the same requirements apply as to the "medium" security level, with the additional requirement that authentication with the identity provider (Kerberos tickets or other token-issuing third parties) must have taken place using a “high” security-level authentication transaction.

The examples mentioned are summarized in Table B.1 showing different variants for each security level. The list is not exhaustive.

Security level	Examples
Low	• Username and password • Bearer token (e.g., cookies)
Medium	• Username and password with SMS verification code • Username and password with device binding* • OTP software solution (e.g., Google or Microsoft Authenticator) • Software certificate-based authentication using TLS* • FIDO2 implementations with synchronization and key export capabilities (e.g., passkeys using synced authenticators*) • Kerberos tickets • SAML and ID and access tokens as part of OIDC and OAuth 2.0 • JWTs
High	• OTP tokens (e.g., RSA, Vasco, etc.) • OTP solution based on a TPM*

[30] Among other things, this requirement also implies that the validity period of such a token must not be excessively long in relation to its intended use.

[31] While SAML tokens refer to an older XML-based token format that has been in use since around 2005, in which entitlements are referred to as assertions and are used by service providers, OIDC tokens refer to a newer token format based on OAuth 2.0 and JSON. There the entitlements are referred to as claims and are used by relying parties. SAML tokens are typically used for enterprise-wide SSO solutions, while OIDC tokens are more commonly used for APIs providing authentication or authorization.

	• Hardware certificate-based authentication using TLS* • FIDO2 implementations without synchronization and key export capabilities (Passkeys with device-bound authenticators)* • Swisscom Mobile ID • Kerberos tickets and other tokens issued with a preceeding “high” security-level authentication

Table B.1: Security levels of authentication procedures, means, and services

In principle, combining several authentication procedures and means of a given security level does not increase the level, i.e., passkeys using synced authenticators remain at the "medium" security level even if they are combined with a username and password with an SMS verification code.

For (security-critical) applications where attackers are likely to attempt to take over authenticated sessions (session hijacking) and/or introduce real-time phishing or Mallory in the middle (MITM) in communication relationships, more advanced authentication procedures, means, and/or services are required. Device binding (i.e., binding the end devices to the session) protects against session hijacking attacks, while binding the authentication information to the session protects against MITM attacks. Authentication procedures, means, and services which support this are marked with an asterisk (*) in Table B.1. It should be noted that the procedures, means, and services may not be resistant to these attacks by default, but must be specifically configured.

Appendix C: Baseline protection requirements

The baseline protection requirements compiled and explained in this appendix are structured according to the functions of the NIST CSF. While the requirements of function 1 (GOVERN) relate to the organization or company that is responsible for an IT protection object, all other CSF functions (i.e., IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER) are to be implemented for each IT protection object. In contrast to the CSF, the RESPOND and RECOVER functions have been combined for the sake of simplicity (and color-coded to match RESPOND).

All requirements also apply along supply chains, whereby management must define the supply chain risk management method. Overall responsibility for security lies with management at all times.

The baseline protection requirements can be used independent to the CSRM method. When the five-step CSRM method is used, baseline requirements 1.2 and 2.1 are already covered. They are marked with an asterisk (*) accordingly.

Some specific implementation options are mentioned in individual sections. These options are to be understood as recommendations and do not exclude other implementation options. In any case, the quality of implementation must be based on the protection needs of the organization or company or the IT protection object.

1	GOVERN (GV)
1.1	**Security organization** The security organization must be defined and communicated to employees and must also be implemented in this form. In particular, the contact persons and their responsibilities for strategic and operational cybersecurity must be clearly defined.[32] These persons must have the technical expertise to fulfill their responsibilities.
1.2 *	**Cyber risk management** Cyber risk management must be defined and established, i.e., it must be clarified whether and how cyber risks are to be dealt with and how management (either directly or indirectly) is involved. Criteria must be defined for the assessment and classification of cyber risks, and adequate TOMs[33] must be determined and implemented for critical cyber risks. [34]

[32] Strategic cybersecurity includes the management of cybersecurity. In contrast, operational cybersecurity includes vulnerability, incident, supplier, training and awareness, and authorization management.

[33] Preventive, detective, and reactive TOMs are used to implement the PROTECT, DETECT, and RESPOND functions. These three functions are important and complement each other. Appropriate TOMs must be defined and implemented for each relevant risk, with detective and reactive TOMs being essential.

[34] A cyber risk is critical if the potential impact is severe and highly business critical.

1.3	**Screening of employees** The trustworthiness of employees[35] must be verified in accordance with their assigned tasks and responsibilities.
1.4	**Training and awareness** Employees must be made aware of and trained in cybersecurity issues in accordance with their assigned tasks and responsibilities. Where possible, the training must also discuss actual incidents and the conclusions that can be drawn from them for the organization or company.

2 IDENTIFY (ID)	
2.1 *	**IT protection objects** All (essential) hardware and software components must be documented with their input and output data, configurations, and data flows, and analyzed regarding their protection requirements.[36] Several logically related components (including peripherals) can be combined and aggregated into one IT protection object. The corresponding protection requirement analyses and documentation must include all implemented and yet-to-be-implemented TOMs and must always be kept up to date.
2.2	**Supply chains** All dependencies in the supply chains must be identified, assessed in terms of their significance for business activities (i.e., business and production processes), and monitored.[37] In particular, it must be ensured that suppliers of hardware and software components and services (e.g., SaaS services) that are essential to business and production processes, as well as suppliers with privileged access or access to sensitive data (e.g., for necessary monitoring and maintenance work), are themselves secured as best as possible and thus resilient through the implementation of adequate TOMs.

[35] External employees must be taken into account in the same way as internal employees.

[36] This requirement applies to all (essential) hardware and software components of the IT infrastructure, regardless of whether they are operated on-premises or obtained as a service from a cloud service provider (CSP). The need for protection relates to the importance of the hardware and software components or IT protection objects for the business and production processes they support, as well as the acceptability of the consequences of a breach of process objectives.

[37] This applies to both information technology (IT) and operational technology (OT) in accordance with Appendix A.

3	PROTECT (PR)
3.1	**Physical Protection, Configuration and operation** Each hardware and software component or each aggregated IT protection object must be configured and operated in such a way that its attack surface is kept as small as possible.[38] In particular, (a) adequate physical protection[39] must be provided, (b) the best possible logical isolation and separation (e.g., using virtualization technologies) must be achieved, and (c) technical hardening must have been carried out, whereby hardening means, among other things, that • predefined accounts are removed[40] and • unnecessary services are deactivated, and • changes to the security settings of physical devices require interactive confirmation (e.g., pressing a button), and (d) interlocking and independent components prevent the possibility of malfunctions and accidents as far as possible.
3.2	**Vulnerability and weakness management** Each hardware and software component or each aggregated IT protection object must be monitored and updated automatically as part of the lifecycle and regarding known weaknesses and vulnerabilities,[41] and must be maintained and kept as up to date as possible in accordance with the manufacturer's instructions (e.g. by promptly installing patches or replacing components). For networked devices, an automated firmware update mechanism must be available (if technically possible) and activated by default.
3.3	**Identity and access control management** Every hardware and software component or aggregated IT protection object must be integrated into a comprehensive identity and access control system that ensures that every access is authenticated and authorized.

[38] This requirement follows the motto: "Do not expose things on the Internet that do not need to be accessed by everyone."

[39] On the one hand, physical protection must protect against meteorological natural hazards such as hail, storms, rain, snow, or lightning strikes, gravitational natural hazards such as floods, mudslides, avalanches, or rockfalls, as well as tectonic and geological hazards such as earthquakes or radon emissions. On the other hand, physical protection must also control access to authorized persons only and monitor to ensure this, for example, using closed-circuit television (CCTV) cameras.

[40] This means that there are no predefined authentication credentials. If such credentials are required for activation, it must be generated at the time of activation and made available (only) to the user.

[41] Monitoring services such as Shadowserver (https://www.shadowserver.org) can be used to identify potential vulnerabilities and exposures. The Software Bill of Material (SBOM) provided by the manufacturer as well as blogs, RSS-Feeds and vendor information portals should be used for continuous monitoring of vulnerabilities.

	(a) It is authenticated if the identity of the accessing entity has been defined and verified using an authentication procedure, means, or service appropriate to the protection requirements.[42] (b) It is authorized if the access rights and privileges of the accessing entity permit access in this form. In this context, access rights and privileges must be assigned on a least privilege basis.
3.4	**Network security** Every hardware and software component or every aggregated IT protection object must be adequately protected against network-based attacks[43]. This can be achieved in two ways: • The component or IT protection object is operated in a separate network (segment),[44] which has suitable perimeter protection with restrictions on network services, protocols, and ports (in the sense of a firewall). • The component or IT protection object itself has suitable security mechanisms and precautions (in the sense of zero or minimal trust[45]).
3.5	**Malware protection** Every hardware and software component or aggregated IT protection object must be effectively protected against malicious software (malware) and data-driven attacks[46] using appropriate measures[47].

[42] Access can be interactive by a user or non-interactive by a service or process. Access can also be gained via a procedure for resetting authentication credentials. In all cases, the authentication requirements are the same. For knowledge-based authentication approaches, i.e., approaches based on users knowing something they can use to authenticate themselves (e.g., a password or cryptographic key), a possible classification into three security levels is proposed in Appendix B. In any case, authentication must be designed in such a way that it cannot be easily reset and thus circumvented. As an alternative to knowledge-based authentication approaches, the requirement can also be implemented using other authentication approaches or physical measures.

[43] This requirement is primarily intended to prevent pass-the-hash attacks and so-called lateral movements. The latter are also the subject of the extension from STRIDE to STRIDE-LM.

[44] As part of network segmentation, it should be ensured that at least IT and OT systems are separated from each other (i.e., operated in different segments).

[45] The usual term here is *zero trust*. However, because assumptions about trust relationships must always be made and these should be minimal, the term *minimal trust is* preferred and used accordingly in this context.

[46] In a data-driven attack, the attack takes place via data that is imported into an IT system or application and triggers a malfunction there.

[47] This requirement does not necessarily have to be met with the help of additional software. In many cases, it is sufficient to use the on-board tools of the operating systems if they are used and configured accordingly. In addition, protection can also be provided by checking data and/or blocking unnecessary data during transmission (i.e., before it reaches the end systems).

3.6	**Encryption and deletion of data** During storage, processing, and transmission, data must be adequately protected in terms of confidentiality and integrity (e.g., using appropriate cryptographic methods). Data that is no longer needed must be deleted in accordance with its protection and regulatory requirements.[48] This requirement applies not only to IT operations, but also to development of systems and applications.
3.7	**Data backup** All data relevant to important business and production processes must be backed up regularly. Ideally, a backup concept should be implemented that provides for online/offline data storage in multiple generations at multiple locations. In addition, it must be possible to restore the data as quickly and completely as possible at any time, and data recovery must be practiced periodically.
3.8	**Development** Cybersecurity must be considered from the start when developing hardware and software components. This includes, for example, threat modeling during architecture planning, compliance with guidelines[49] and best practices during implementation (including the avoidance of unsafe practices), the use of a CI/CD platform that includes continuous security checks, the design of interfaces (especially graphical user interfaces) that do not lead to mistakes, and the security-conscious use of integrated development environments and corresponding plugins by developers. In any case, development and production environments must be separated.
3.9	**Availability** Every hardware and software component or aggregated IT protection object must be secured in terms of its availability. In particular, sufficient computing, storage, and transmission capacities must be available, and important components must also be redundant whenever appropriate.

[48] Above a certain level of protection, logical deletion at the operating system level is not sufficient. Instead, the data to be deleted must be overwritten several times with randomly selected data.

[49] For software development, the Minimum Viable Secure Product (MVSP) guideline (https://mvsp.dev) is a good option. Basically, the principles *of security by design and security by default* must be incorporated into the development process. Security *by default* means that IT resources are developed, configured, and operated in such a way that all security measures that are appropriate in a specific environment are activated by default and can take effect without users having to worry about them. Security *by design* requires that security be considered an integral part of development from the start.

4	DETECT (DE)
4.1	**Recording and monitoring** For each hardware and software component or each aggregated IT protection object (and in particular for networks), security-related activities, incidents, and events must be recorded[50] and promptly (and if possible in an automated way) evaluated for attacks that may have occurred (e.g., by a Security Operation Center - SOC).
4.2	**Reporting center** For each hardware and software component or each aggregated IT protection object, it must be clear how outsiders can report vulnerabilities and security-related incidents.[51]

5	RESPOND (RS) and RECOVER (RC)
5.1	**Incident management** Incidents and malfunctions detected that could affect relevant business and production processes must be triaged and resolved as quickly as possible.
5.2	**Contingency planning** The restoration of operational capability must be ensured for every hardware and software component and every aggregated IT protection object.[52] To this end, emergency and recovery plans[53] must be defined, prioritized, regularly practiced, and, if necessary, improved. These plans must be integrated into an overarching emergency plan for the entire organization or company.
5.3	**Communication** The responsibilities and objectives on how communication should take place must be known for all plans to be created in accordance with requirement 5.2.

[50] The records must be stored in a suitable form for an appropriate period in an unalterable form and must be made available again to ensure the traceability of security-related activities. Canaries should also be used here to detect possible compromises.

[51] This can be done by making a security.txt file available on the web in accordance with RFC 9116.

[52] This must also take into account the dependencies in the IT/OT supply chains in accordance with baseline requirement 2.2 and the recoverability of the secured data in accordance with baseline requirement 3.7.

[53] The findings and lessons learned from previous security incidents and any simulations must be considered in these plans.