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

CSRM compared with well-known management systems

1 Introduction

This text provides a concise overview of three approaches to cyber resilience: the ICT minimum standard (or NIST Cyber Security Framework CSF), ISO/IEC 27001, and the Cyber Security and Resilience Method CSRM. CSRM is compared with the other two methods in terms of content and form and compared in terms of its suitability as a method for managing, controlling, and verifying the cyber resilience of organizations or companies.

It is aimed in particular at members of business and divisional management, CISOs, risk owners, and service and asset owners. It is intended for organizations and companies that already apply the ICT minimum standard or ISO/IEC 27001 and now wish to evaluate the transition or addition to CSRM.

The purpose of this document is to provide clear, comparative guidance: What is the logic, strengths, and limitations of the ICT minimum standard and ISO/IEC 27001, what makes CSRM different methodically, in decisions and documentation and what practical added value does it bring? At the same time, the text serves as a decision-making aid by showing how existing implementations can be transferred to CSRM.

2 Minimum ICT standard and NIST CSF

The ICT minimum standard is based on the NIST CSF and supplements it with OT-specific protection aspects. Due to the minor deviations from the NIST CSF (version 1.1), no distinction is made between the two in the following. Unless otherwise noted, the following considerations apply to both frameworks.

The ICT minimum standard describes a series of organizational and technical measures that must be implemented in accordance with the identified protection requirements. There are no fixed minimum requirements. The protection requirements are determined using a probability-based risk assessment. For this purpose, NIST recommends using the NIST Risk Management Framework (RMF)[1]. Dependencies between IT systems and business processes are considered separately as part of risk management.

[1] 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

A central component of implementation is the establishment of internal policies and strategies, the consistent implementation of which must be ensured within the organization. However, this makes it difficult to compare implementations between different organizations. The ICT minimum standard itself acts as a framework that allows organizations, associations, or regulators to create specific profiles. [2] These profiles define which measures are to be implemented and to what extent using fixed "tiers".

From the NCSC perspective, certain requirements should always be implemented as baseline measures, while others – especially when increased protection is warranted – should be context-specific, depending on data, systems, and IT architectures. Profiles can map such requirements, but do not offer a method for deriving additional requirements in cases of increased protection needs. Due to the large number of requirements (108 subcategories in NIST CSF v1.1 and the ICT minimum standard), profiles are often very extensive and therefore difficult to implement in practice, especially for smaller organizations. In addition, the use of profiles as a reference makes it difficult to compare different organizations.

On the one hand, the ICT minimum standard addresses IT and information security, in particular the protection of IT systems, infrastructures, and processed and transmitted information. On the other hand, it attempts to cover aspects of operational security (OT) with the same requirements without sufficiently taking into account the specific characteristics of this area[3] . The NIST CSF covers segmentation, secure transitions, physical security, hardening, and monitoring in a technology-neutral manner; the OT-specific features remain deliberately abstract and can only be specified to a limited extent in a profile.

In summary, the ICT minimum standard is a framework but not a step-by-step process model. It requires a risk-based decision as to which requirements apply and which measures are to be implemented. Profiles serve to bundle these requirements; the associated tier model describes their degree of implementation and supports internal self-assessment.

3 ISO/IEC 27001

The ISO/IEC 27001 standard enables companies to establish and operate an information security management system (ISMS). An ISMS in accordance with ISO/IEC 27001 comprises policies, procedures, guidelines, and the associated resources and activities that are controlled by an organization to protect its information assets. It thus represents a systematic model for the introduction, implementation, operation, monitoring, review, maintenance, and continuous improvement of information security with the aim of supporting the organization's business objectives.

The ICT minimum standard can also support the development of an ISMS, but is primarily designed as a framework for managing cyber risks. In contrast to the ICT minimum standard, ISO/IEC 27001 provides a process model based on a control loop. This is usually referred to as the PDCA cycle (Plan–Do–Check–Act). The standard describes the step-by-step development and operation of an ISMS: from planning security objectives and measures to their implementation and continuous monitoring to regular reviews and improvements. The process model thus promotes an iterative improvement process.

---

[2] Protection profiles A, B, C: Electricity Supply Ordinance (StromVV), Art. 5a in conjunction with Annex 1a: Binding nature of the minimum ICT standard "in accordance with the respective protection level".

[3] OT differs from IT in terms of long life cycles and manufacturer lock-in, limited patchability with narrow change windows, and high availability/real-time requirements, among other things.

In addition, ISO/IEC 27001 aims to ensure auditability and certifiability.[4] The standard contains requirements that external auditors can use to assess the effectiveness and conformity of the ISMS. This structural auditability clearly distinguishes ISO/IEC 27001 from the ICT minimum standard, which does not provide for formalized certification.

However, the two standards have many other aspects in common:

- In both approaches, a risk- and probability-based assessment determines which requirements apply and which measures (from the respective catalog) are to be implemented.
- The catalogs of measures do not define any mandatory baseline requirements that need to be implemented regardless of the risk.
- The additional internal policies and strategies to be established are the main basis for the implementation of measures, not the requirements from the standard itself.
- The focus is on the information security of the organization. Protection against disruptions and accidents are not central objectives. The focus is on protecting the confidentiality, integrity, and availability of information and information-processing systems – rather than protecting the business and production processes themselves.

A key difference from the ICT minimum standard is the documentation and verification requirement. Unlike the ICT minimum standard, ISO/IEC 27001 does not have tiers or implementation levels. Instead, all measures must be described in a "Statement of Applicability" (SoA) and assigned in a comprehensible manner.

4 Cybersecurity Risk Management (CSRM)

The differences and strengths of the CSRM compared to the above approaches are summarized in the following sections.

Baseline requirements and procedure for increased protection needs

The CSRM defines 20 baseline requirements for all IT and OT systems as well as a method for threat modeling in cases of increased protection needs. The baseline requirements are formulated in such a way that they are understandable for IT specialists, verifiable by these specialists and relevant for cybersecurity and resilience. Requirements that do not directly contribute to improving resilience were not taken into account. The clear language facilitates practical implementation and enables companies and public authorities to achieve effective foundational protection. The threat modeling method complements these baseline requirements and enables the selection of additional measures depending on the context, architecture, and protection needs.

Risk assessments in relation to business and production processes

The overarching objectives of the CSRM is to ensure the continuity of important activities and corresponding business and production processes, protect the values of the organization or company, comply with laws and regulatory requirements, and protect against disruptions and accidents. If necessary, in addition to the technical and organizational measures (TOMs) that meet the baseline requirements, further (additional) TOMs must also be defined and implemented.

[4] National Cyber Security Center (NCSC), Technology Review – Measurability and Testability of IT Security, Bern, June 10, 2025. Available online at: ncsc.admin.ch.

Procedural model, not framework

CSRM focuses on a step-by-step approach to achieving cybersecurity and resilience. A probability-based risk assessment is deliberately not taken into account. Nevertheless, the method is risk-based: it relies on the qualitative assessment of IT security threats and their potential impact on business processes in order to identify intolerable deviations at an early stage and manage them appropriately.

Protected objects, not assets

The method assumes that hardware and software components (including OT and peripheral devices) can be aggregated into IT protection objects. This aggregation option represents an important extension and refinement to commonly used cyber security standards for dealing with cyber risks, particularly for practical use, and allows for a coherent allocation of resources for the implementation of suitable TOMs. ISO/IEC 27001 and the ICT minimum standard are based on individual assets (also referred to as "values") that must be protected individually.

Information security guidelines

Another strength of the CSRM is that its implementation does not require every organization to create and document its own policies on information security or cyber risk management. This represents a significant difference from the ICT minimum standard and the ISO/IEC 27001 standard, where the implementation of measures often has to be reviewed in the context of organization-specific policies.

In comparison, CSRM can be understood as an overarching guideline and policy. Technical standards and acceptable use policies for predominantly operational activities – such as vulnerability management, incident management, supplier management, training and awareness, or authorization management – remain necessary. The NCSC recommends developing sector-wide templates for this purpose in order to harmonize these.

It is a key aspect of this method that companies and authorities can focus on implementing measures and documenting systems and responsibilities without first having to develop their own methods and policies. This increases the efficiency of security controls while at the same time strengthens cybersecurity and resilience.

IT/OT convergence

A key concern in the development of CSRM was the creation of a uniform method that links IT and OT (operational technologies) systems. The aim is to take account of the increasing convergence of IT and OT in the area of preventive cybersecurity.

The CSRM is designed to be applied not only to business logic, but also to production and operational management systems, process control systems, control and monitoring systems, and 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 protected 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 requirements must also be implemented for OT systems.

A comparison of this method with the models and requirements of IEC 62443 is in preparation.

Implementation of an ISMS

Compared to ISO/IEC 27001, the CSRM method presents an alternative and simpler approach to establishing an information security management system (ISMS). However, this does not rule out the possibility of implementing ISO/IEC 27001 – for example, if this is necessary due

to compliance requirements. The NCSC has published its own technology review on the topic of information security management and ISMS[5] .

Reporting and resilience assessment

The NIST CSF enables reporting on the implementation status using Tiers. The ICT minimum standard expands on this concept by also allowing the quantitative evaluation and calculation of the measures implemented in order to create an average maturity level.

The CSRM itself does not define the form of reporting. However, the NCSC is aware that standardized reporting is of central importance. For this reason, a resilience assessment[6] is being developed in a separate project, which is currently in the pilot phase. This assessment is intended to enable organizations and companies to transparently demonstrate the security and resilience characteristics for each business or production process or product, thereby strengthening the trust of customers and society.

In contrast, this transparency is often lacking in the ICT minimum standard and ISO/IEC 27001, as the associated implementation documentation (e.g., the "Statement of Applicability" according to ISO/IEC 27001) is not usually shared with customers. In addition, the implementation is usually done at the organizational level and not for each business or production process or product.

Consideration of safety as a corporate goal

Safety-[7], that is the protection of people and the environment from unintended harm resulting from technical risks, natural hazards, or similar influences is often considered secondary in information- and cybersecurity, which is also reflected in existing standards. CSRM, on the other hand, considers safety to be an integral part of the process. Unacceptable incidents and accidents must be taken into account both in the analysis of business and production processes and in the assessment of protection needs. Requirements for protection against natural events, aging, or wear and tear of technical components are anchored in the baseline requirements of CSRM. This makes the method suitable for use in technical infrastructures and industrial facilities.

5 Simultaneous Implementation of ICT minimum standard, ISO/IEC 27001 and CSRM

5.1 Duplication

Parallel implementation of CSRM and the ICT minimum standard or ISO/IEC 27001 is possible in principle, but leads to duplication in reporting and potentially also in cyber risk management. The supplementary implementation of a probability-based risk analysis offers only limited added value. Although it can be used to identify additional measures, it must not be used to reject measures defined within the CSRM.

CSRM stipulates that if measures are not implemented, the relevant business and production process objectives must be adjusted accordingly. This approach supports governance, as the

[5] National Cyber Security Center (NCSC), Technology Review – Information Security Management and ISMS, Bern, July 2, 2025. Available online at: ncsc.admin.ch.

[6] This assessment is based on the UK Cyber Assessment Framework and findings on the measurability and testability of IT security (footnote 4).

[7] In contrast to safety, security is intended to protect systems and data from deliberate attacks and manipulation. More on that in National Cyber Security Center (NCSC), Technology Review – Cybersecurity and Resilience, Bern, November, 2025. Available online at: ncsc.admin.ch.

effects are immediately visible, and simplifies decision-making by allowing management to focus on assessing acceptable effects without having to deal with technical details.

5.2 What is new with CSRM?

By applying CSRM, the following additional work for managing and controlling information security is expected:

- Business and production processes must be assessed in terms of the acceptable impact in order to determine the need for protection.
- It must be defined how hardware and software components can be aggregated into IT protection objects.
- Existing information security policies and technical implementation standards must be reviewed to ensure that they take into account the baseline requirements of the CSRM. The method provides numerous implementation recommendations that can be adopted directly and goes beyond existing requirements of NIST CSF or ISO/IEC 27001 in individual points – for example, with regarding the requirements for system hardening (baseline requirement 3.1), the obligation to perform offline backups (baseline requirement 3.7), and specifications for secure software development (baseline requirement 3.8).
- Since CSRM covers both IT and OT systems, as well as elements of the business continuity process, closer cooperation between teams that previously worked separately may be necessary.

In addition, the method brings about a change in mindset: the focus is no longer primarily on information security or compliance, but declares cyber resilience as the overarching goal.

6 Useful information for companies and public authorities that currently implement the ICT minimum standard

With the exception of a few requirements, CSRM covers all aspects of the ICT minimum standard. Implementing CSRM therefore generally also leads to compliance with the requirements of the ICT minimum standard. This section looks at those subcategories of the ICT minimum standard that require special attention (in addition to the methodical differences in cyber risk management explained above):

- ID.BE-2 requires *that the importance of the organization as part of critical infrastructure and its role within the respective sector be identified and communicated*. This identification and communication takes place outside the scope of CSRM.
- ID.RA-2 requires *that up-to-date information on cyber threats be obtained through regular exchanges in forums and expert committees*. RS.CO-5 requires *that information be exchanged regularly and voluntarily with external actors in order to raise awareness of the current cybersecurity situation*. The CSRM does not explicitly stipulate these requirements, as cyber resilience must be ensured regardless of the current threat situation. However, the method recommends to take these aspect into account in the design of operational processes, for example in vulnerability and incident management.
- ID.SC-3 requires *that contracts with suppliers and third parties oblige them to implement and comply with the measures necessary to achieve the objectives of the organization's supply chain risk management program*. In this context, the CSRM requires that supply chain dependencies be identified, monitored, and appropriate protective measures

implemented (baseline requirement 2.2). Contractual agreements are not explicitly required by the method, but are implicitly considered a possible measure. The argument here is that contracts alone do not establish cybersecurity or resilience, but primarily serve as legal protection.

- PR.AT-3 requires *that all stakeholders outside the organization (suppliers, customers, partners) are aware of their roles and responsibilities.* The CSRM does not explicitly stipulate this requirement, as it is hard to implement and does not directly impact cyber resilience of the organization itself.
- PR.DS-8 requires *organizations to establish a process for verifying the integrity of the hardware used.* Hardware verification is not a baseline requirement in the method, but can be taken into account with additional measures if there is an increased need for protection.
- PR.IP-1 requires *that a standard configuration be created for the information and communication infrastructure and for industrial control systems in order to ensure compliance with basic security principles*. The method does not explicitly stipulate such a requirement, as the baseline requirements of the CSRM itself are considered a fundamental security baseline. An additional, company-specific baseline is not necessary and would unnecessarily complicate implementation. However, system-specific configuration standards – for example, for firewall or network configurations – must be developed and taken into account as part of appropriate operational processes.
- PR.IP-3 requires *that a process for controlling configuration changes be established*. The CSRM does not explicitly require this. However, in accordance with baseline requirement 4.1, it must be ensured that security-related changes are recorded and evaluated. Detailed specifications for configuration management should be defined and implemented as part of operational processes.
- PR.IP-7 requires *that information security processes be continuously developed and improved*. CSRM does not rule out continuous improvement, but does not explicitly require it. The goal is to establish and implement a cybersecurity process structure that ensures the organization's resilience to cyber risks. Continuous improvement is therefore not mandatory – effective and stable processes are sufficient. What is more important is to regularly review the effectiveness of existing measures and promptly withdraw those measures that prove to be ineffective in operation. This aspect is an integral part of the fifth step of CSRM.
- RS.AN-3 requires *forensic analyses to be carried out after an incident has occurred.* CSRM only requires an incident management exists, that promptly triages and resolves incidents and detected disruptions (baseline requirement 5.1). An obligation to carry out forensic analyses should be taken into account through specific requirements in cases of increased protection needs.
- RC.CO-2 requires *that*, *after a cybersecurity incident has occurred, the organization should ensure that it is perceived positively again.* The CSRM does not take this into account in such concrete terms, but requires in baseline requirement 5.3 that communication and its objectives in emergencies must be known. In the event of incidents, lessons learned are not explicitly mentioned as a baseline requirement. The method assumes that communication is part of the incident management process that must be established.