Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

24. November 2025

CSRM im Vergleich mit bekannten Managementsystemen

1 Ausgangslage

Dieses Dokument bietet einen kompakten Überblick über drei Ansätze zur Cyberresilienz: den IKT-Minimalstandard (respektive das NIST Cyber Security Framework CSF), ISO/IEC 27001 und die Cyber Security and Resilience Method CSRM. Die CSRM wird inhaltlich und formal den beiden anderen Methoden gegenübergestellt und in ihrer Eignung als Methode für Führung, Steuerung und Nachweise der Cyberresilienz von Organisationen oder Unternehmen eingeordnet.

Angesprochen sind insbesondere Mitglieder der Geschäfts- und Bereichsleitung, CISO, Risk Owner sowie Service- und Asset-Owner. Er richtet sich an Organisationen und Unternehmen, die den IKT-Minimalstandard oder ISO/IEC 27001 bereits anwenden und nun die Umstellung beziehungsweise Ergänzung hin zur CSRM bewerten möchten.

Zweck dieses Dokumentes ist eine klare, vergleichende Orientierung: Wo liegen Logik, Stärken und Grenzen von IKT-Minimalstandard und ISO/IEC 27001, was macht das CSRM anders – methodisch, in Entscheidungen und Nachweisen – und welchen praktischen Mehrwert bringt es. Zugleich dient der Text als Entscheidungshilfe, indem er aufzeigt, wie bestehende Umsetzungen in die CSRM überführt werden können.

2 IKT-Minimalstandard und NIST CSF

Der IKT-Minimalstandard orientiert sich am NIST CSF und ergänzt es um OT-spezifische Schutzaspekte. Wegen der geringen Abweichungen zum NIST CSF (Version 1.1) wird im Folgenden nicht zwischen beiden unterschieden; die nachstehenden Überlegungen gelten – sofern nicht anders vermerkt – für beide Rahmenwerke.

Der IKT-Minimalstandard beschreibt eine Reihe organisatorischer und technischer Massnahmen, die gemäss dem identifizierten Schutzbedarf umzusetzen sind. Dabei bestehen keine festgelegten Minimalanforderungen. Die Bestimmung des Schutzbedarfs erfolgt über eine wahrscheinlichkeitsbasierte (probabilistische) Risikobewertung. Zu diesem Zweck empfiehlt NIST die Verwendung des NIST Risk Management Framework (RMF)[1]. Abhängigkeiten

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

zwischen IT-Systemen und geschäftskritischen Prozessen werden im Rahmen des Risikomanagements gesondert betrachtet.

Ein zentraler Bestandteil der Umsetzung ist die Etablierung interner Richtlinien und Strategien, deren konsequente Umsetzung in der Organisation sicherzustellen ist. Dies erschwert jedoch die Vergleichbarkeit der Implementierungen zwischen verschiedenen Organisationen. Der IKT-Minimalstandard selbst fungiert als Rahmenwerk, das es Organisationen, Verbänden oder Regulatoren erlaubt, spezifische Profile[2] zu erstellen. Diese Profile definieren, welche Massnahmen in welcher Ausprägung umzusetzen sind; im Standard werden hierfür feste „Tiers" verwendet.

Aus Sicht des BACS sollten bestimmte Anforderungen stets als Basis-Massnahmen implementiert werden, andere – insbesondere bei erhöhtem Schutzbedarf – hingegen kontextspezifisch, abhängig von Daten, Systemen und IT-Architekturen. Profile können solche Basisanforderungen abbilden, bieten jedoch keine Methodik zur Ableitung zusätzlicher Anforderungen bei erhöhtem Schutzbedarf. Aufgrund der Vielzahl an Anforderungen (108 Subkategorien im NIST CSF v1.1 und IKT-Minimalstandard) sind Profile oftmals sehr umfangreich und damit in der praktischen Umsetzung, vor allem für kleinere Organisationen, schwer zu handhaben. Zudem erschwert die Nutzung von Profilen als Basisreferenz die Vergleichbarkeit zwischen verschiedenen Organisationen.

Der IKT-Minimalstandard adressiert einerseits die IT- und Informationssicherheit, insbesondere den Schutz von IT-Systemen, Infrastrukturen sowie verarbeiteten und übertragenen Informationen. Andererseits versucht er mit denselben Anforderungen auch Aspekte der Operational Security (OT) abzudecken, ohne den spezifischen Eigenheiten dieses Bereichs[3] ausreichend Rechnung zu tragen. Das NIST CSF deckt Segmentierung, gesicherte Übergänge, physische Sicherheit, Härtung und Monitoring technologie-neutral ab; die OT/ICS-spezifischen Besonderheiten bleiben dabei bewusst abstrakt und sind in einem generischen Profil nur eingeschränkt konkretisierbar.

Zusammenfassend stellt der IKT-Minimalstandard zwar ein Rahmenwerk aber kein schrittweises Vorgehensmodell dar. Er erfordert eine risikobasierte Entscheidung, welche Anforderungen gelten und welche Massnahmen umzusetzen sind. Profile dienen der Bündelung dieser Anforderungen; das zugehörige Tier-Modell beschreibt deren Ausprägungsgrad und unterstützt die interne Selbstbeurteilung (Self-Assessment).

3 ISO/IEC 27001

Die Norm ISO/IEC 27001 ermöglicht es Unternehmen, ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen und zu betreiben. Ein ISMS gemäss ISO/IEC 27001 umfasst Politik, Verfahren, Richtlinien sowie die zugehörigen Ressourcen und Aktivitäten, die von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen. Es stellt somit ein systematisches Modell für die Einführung, Umsetzung, den Betrieb, die Überwachung, Überprüfung, Pflege und kontinuierliche Verbesserung der Informationssicherheit dar, mit dem Ziel, die Geschäftsziele der Organisation zu unterstützen.

Der IKT-Minimalstandard kann ebenfalls beim Aufbau eines ISMS unterstützen, ist jedoch primär als Rahmenwerk zum Management von Cyberrisiken konzipiert. Im Unterschied zum

[2] Schutzprofile A, B, C: Stromversorgungsverordnung (StromVV), Art. 5a i.V.m. Anhang 1a: Verbindlichkeit des IKT-Minimalstandards „gemäss dem jeweiligen Schutzniveau" und Definition der Schutzniveaus

[3] OT unterscheidet sich von der IT u. a. durch lange Lebenszyklen und Herstellerbindung, eingeschränkte Patchbarkeit mit engen Change-Fenstern, sowie hohe Verfügbarkeits-/Echtzeitanforderungen.

IKT-Minimalstandard bringt ISO/IEC 27001 ein Vorgehensmodell auf Basis eines Regelkreises mit. Meistens wird dabei vom PDCA-Zyklus (Plan–Do–Check–Act) gesprochen. Der Standard beschreibt den schrittweisen Aufbau und Betrieb eines ISMS: von der Planung der Sicherheitsziele und -massnahmen über deren Umsetzung und kontinuierliche Überwachung bis hin zu regelmässigen Überprüfungen und Verbesserungen. Das Vorgehensmodell fördert damit einen iterativen Verbesserungsprozess.

Darüber hinaus verfolgt ISO/IEC 27001 das Ziel, Auditierbarkeit und Zertifizierbarkeit sicherzustellen.[4] Die Norm enthält Anforderungen, anhand derer externe Prüfstellen die Wirksamkeit und Konformität des ISMS bewerten können. Diese strukturelle Prüfbarkeit unterscheidet ISO/IEC 27001 deutlich vom IKT-Minimalstandard, der keine formalisierte Zertifizierung vorsieht.

In vielen weiteren Aspekten weisen beide Standards jedoch Gemeinsamkeiten auf:

- Welche Anforderungen gelten und welche Massnahmen (aus dem jeweiligen Katalog) umzusetzen sind, wird in beiden Ansätzen durch eine risiko- und wahrscheinlichkeitsbasierte Bewertung gesteuert.
- Die Massnahmenkataloge definieren keine obligatorischen Basisanforderungen oder einen Grundschutz, der unabhängig vom Risiko umzusetzen wäre.
- Die zusätzlich zu etablierenden internen Richtlinien und Strategien sind die Hauptgrundlage für die Umsetzung von Massnahmen, nicht die Anforderungen aus dem Rahmenwerk selbst.
- Der Schwerpunkt liegt auf der Informationssicherheit der Organisation. Sicherheit vor Stör- und Unfällen sind nicht zentrale Zielsetzungen. Im Vordergrund steht der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und informationsverarbeitenden Systemen – weniger der Schutz der Geschäfts- und Produktionsprozesse selbst.

Ein wesentlicher Unterschied zum IKT-Minimalstandard besteht in der Dokumentations- und Nachweispflicht. Anders als beim IKT-Minimalstandard gibt es bei ISO/IEC 27001 keine Tiers oder Umsetzungsgrade., Dafür müssen sämtliche Massnahmen in einem „Statement of Applicability“ (SoA) beschrieben und nachvollziehbar zugeordnet werden.

4 Cybersicherheits- und Resilienz Methode (CSRM)

Die Unterschiede und Stärken des CSRM im Vergleich zu obgenannten Ansätzen sind in den nun folgenden Abschnitten zusammengefasst.

Basisanforderungen und Vorgehen bei erhöhtem Schutzbedarf

Die CSRM definiert 20 Basisanforderungen für alle IT- und OT-Systeme sowie eine Methode zur Bedrohungsmodellierung bei erhöhtem Schutzbedarf. Die Basisanforderungen sind so formuliert, dass sie für IT-Fachpersonen verständlich, sowie für die Cybersicherheit und Resilienz relevant und überprüfbar sind. Anforderungen, die keinen direkten Beitrag zur Verbesserung der Resilienz leisten, wurden nicht berücksichtigt. Durch die kompakte und klare Sprache wird die praktische Umsetzbarkeit erleichtert und es wird Unternehmen wie Behörden ermöglicht, einen wirksamen Grundschutz zu erreichen. Die Methode zur Bedrohungsmodellierung ergänzt diese Basisanforderungen und ermöglicht die Ausarbeitung zusätzlicher Massnahmen in Abhängigkeit von Kontext, Architektur und Schutzbedarf.

[4] Bundesamt für Cybersicherheit (BACS), Technologiebetrachtung – Mess- und Prüfbarkeit der IT-Sicherheit, Bern, 10. Juni 2025. Online verfügbar unter: ncsc.admin.ch.

Risikobeurteilungen in Bezug zu den Geschäfts- und Produktionsprozessen

Die übergeordneten Ziele der CSRM sind die Sicherstellung der wichtigen Tätigkeiten und entsprechenden Geschäfts- und Produktionsprozessen, der Schutz der Werte der Organisation oder des Unternehmens, die Einhaltung von Gesetzen und anderen regulativen Vorschriften, sowie der Schutz vor Stör- und Unfällen. Falls erforderlich sind dazu neben den technischen und organisatorischen Massnahmen (TOMs), mit denen die Basisanforderungen erfüllt werden, auch noch weitere (zusätzliche) TOMs zu definieren und umzusetzen.

Vorgehensmodell nicht Framework

Bei der CSRM steht das schrittweise Vorgehen zur Erreichung von Cybersicherheit und Resilienz im Vordergrund. Eine wahrscheinlichkeitsbasierte (probabilistische) Risikoeinschätzung wird dabei bewusst nicht berücksichtigt. Trotzdem ist die Methode risikobasiert: Sie stützt sich auf die qualitative Beurteilung von IT-Sicherheitsbedrohungen und deren potenzielle Auswirkungen auf Geschäftsprozesse, um nicht tolerierbare Abweichungen frühzeitig zu erkennen und angemessen zu steuern.

Schutzobjekte nicht Assets

Die Methode geht davon aus, dass Hard- und Softwarekomponenten (inklusive OT und Peripheriegeräten) zu Informatikschutzobjekten aggregiert werden können. Diese Aggregationsmöglichkeit stellt eine insbesondere für den praktischen Einsatz wichtige Erweiterung und Präzisierung der gängigen Rahmenmodelle für den Umgang mit Cyberrisiken dar und erlaubt eine kohärente und nachvollziehbare Allokation von Ressourcen für die Umsetzung von geeigneten TOMs. ISO/IEC 27001, sowie der IKT-Minimalstandard gehen von einzelnen Assets (auch als «Werte» bezeichnet) aus, die es individuell zu schützen gilt.

Informationssicherheitsrichtlinien

Eine weitere Stärke der CSRM besteht darin, dass ihre Umsetzung nicht voraussetzt, dass jede Organisation eigene Richtlinien zur Informationssicherheit oder zum Cyber-Risikomanagement erstellen und dokumentieren muss. Dies stellt einen wesentlichen Unterschied zum IKT-Minimalstandard und zum ISO/IEC 27001-Standard dar, bei denen die Umsetzung der Massnahmen oft im Kontext organisationsspezifischer Richtlinien zu prüfen ist.

Die CSRM kann im Vergleich dazu selbst als übergeordnete Richtlinie verstanden werden. Technische Standards sowie Umsetzungs- und Einsatzrichtlinien für überwiegend operative Aufgaben – wie Schwachstellenmanagement, Vorfallmanagement, Lieferantenmanagement, Schulungs- und Sensibilisierungsmassnahmen oder Berechtigungsmanagement – bleiben dennoch erforderlich. Das BACS empfiehlt hierfür sektorweite Vorlagen zu entwickeln, um diese Aufgaben zu harmonisieren und den Aufwand für einzelne Organisationen zu verringern.

Im Kern der Methode liegt der Ansatz, dass sich Unternehmen und Behörden auf die Umsetzung von Massnahmen sowie auf die Dokumentation von Systemen und Verantwortlichkeiten konzentrieren können, ohne zunächst eine eigene Methodik entwickeln zu müssen. Dies erhöht die Effizienz der Umsetzung und stärkt zugleich die Cybersicherheit und Resilienz.

IT/OT Konvergenz

Ein zentrales Anliegen bei der Entwicklung der CSRM war die Schaffung einer einheitlichen Methode, die IT- und OT-Systeme (Operational Technologies) miteinander verknüpft. Ziel ist es, der zunehmenden Konvergenz von IT und OT auch im Bereich der präventiven Cybersicherheit Rechnung zu tragen.

Die CSRM ist darauf ausgelegt, nicht nur auf die Kerntätigkeiten und Geschäftsprozesse von Unternehmen angewendet zu werden, sondern ebenso auf Produktions- und Betriebsführungssysteme, Prozessleitsysteme, Steuerungs- und Überwachungssysteme sowie digitale Aktoren und Sensoren industrieller Fertigungsprozesse. Das Vorgehensmodell der Methode

berücksichtigt diese Integration schrittweise: Schritt 1 definiert die Schutzziele unter Berücksichtigung des Schutzes vor Störfällen und Unfällen; Schritt 2 bezieht die Komponenten der OT-Systeme ausdrücklich in die Schutzobjekte ein und Schritt 3 bewertet, ob eine Verletzung der IT-Schutzziele zu einer Beeinträchtigung der Prozessziele sowie des Schutzes vor Störfällen und Unfällen führen kann. Schritt 4 und 5 fordert die Erstellung Umsetzung der Sicherheitskonzeption und die Umsetzung der Basisanforderungen auch für OT-Systeme.

Ein detaillierter Vergleich dieser Methode mit den Modellen und Anforderungen der IEC 62443 ist in Vorbereitung.

Umsetzung eines ISMS

Im Vergleich zu ISO/IEC 27001 stellt die CSRM-Methode einen alternativen und zugleich einfacheren Ansatz zur Etablierung eines Informationssicherheitsmanagementsystems (ISMS) dar. Dies schliesst jedoch nicht aus, dass ergänzend auch eine Umsetzung nach ISO/IEC 27001 erfolgen kann – etwa dann, wenn dies aufgrund von Compliance-Anforderungen erforderlich ist. Zum Thema Informationssicherheitsmanagement und ISMS veröffentlichte das BACS eine eigene Technologiebetrachtung[5].

Reporting und Resilienz Assessment

Das NIST CSF ermöglicht eine Berichterstattung über den Umsetzungsstand mithilfe von Stufen, den sogenannten „Tiers“. Der IKT-Minimalstandard erweitert dieses Konzept, indem er zusätzlich die Bewertung und Verrechnung der umgesetzten Massnahmen erlaubt, um einen durchschnittlichen Reifegrad zu berechnen.

Die CSRM selbst definiert die Form der Berichterstattung nicht. Dem BACS ist jedoch bewusst, dass im Zusammenhang mit der Einführung der Methode ein standardisiertes Reporting von zentraler Bedeutung ist. Aus diesem Grund wird in einem separaten Vorhaben ein Resilienz-Assessment[6] entwickelt, das sich derzeit in der Pilotphase befindet. Dieses Assessment soll es Organisationen und Unternehmen ermöglichen, die Sicherheits- und Resilienzeigenschaften pro Geschäfts- oder Produktionsprozess beziehungsweise pro Produkt transparent auszuweisen und dadurch das Vertrauen von Kunden und Gesellschaft zu stärken.

Im Gegensatz dazu fehlt diese Transparenz beim IKT-Minimalstandard und bei ISO/IEC 27001 häufig, da die zugehörigen Umsetzungsdokumentationen (beispielsweise das „Statement of Applicability“ nach ISO/IEC 27001) in der Regel nicht mit Kunden geteilt werden. Zudem erfolgt die Dokumentation dort meist auf Organisationsebene und nicht pro Geschäfts- oder Produktionsprozess beziehungsweise Produkt.

Berücksichtigung der Safety als Unternehmensziel

Safety[7] – also der Schutz von Menschen und Umwelt vor unbeabsichtigten Schäden infolge technischer Risiken, Naturgefahren oder ähnlicher Einflüsse – wird in der Informations- und Cybersicherheit häufig als nachrangig betrachtet, was sich auch in bestehenden Rahmenwerken widerspiegelt. Die CSRM hingegen berücksichtigt den Aspekt der Safety als integralen Bestandteil. Nicht akzeptierbare Störfälle und Unfälle sind sowohl bei der Analyse der Geschäfts- und Produktionsprozesse als auch bei der Beurteilung des Schutzbedarfs mit einzubeziehen. Anforderungen an den Schutz vor natürlichen Ereignissen, Alterung oder Verschleiss technischer Komponenten sind in den Basisanforderungen der CSRM verankert.

---

[5] Bundesamt für Cybersicherheit (BACS), Technologiebetrachtung – Informationssicherheitsmanagement und ISMS, Bern, 2. Juli 2025. Online verfügbar unter: ncsc.ch.

[6] Wir orientieren uns bei diesem Assessment am UK Cyber Assessment Framework, sowie an den Erkenntnissen zur Mess- und Prüfbarkeit der IT-Sicherheit (Fussnote 4)

[7] Im Gegensatz zur Safety soll die Security, Systeme und Daten vor absichtlichen Angriffen und Manipulationen schützen. Technologiebetrachtung: Cybersicherheit und -resilienz. Online verfügbar unter: ncsc.ch.

Dadurch eignet sich die Methode auch für den Einsatz in technischen Infrastrukturen und industriellen Anlagen.

5 Gleichzeitige Umsetzung des IKT-Minimalstandards, ISO/IEC 27001 und der CSRM

5.1 Doppelspurigkeiten

Eine parallele Umsetzung der CSRM und des IKT-Minimalstandards oder von ISO/IEC 27001 ist grundsätzlich möglich, führt jedoch zu Doppelspurigkeiten in der Berichterstattung und potenziell auch im Cyber-Risikomanagement. Die ergänzende Durchführung einer wahrscheinlichkeitsbasierten Risikoanalyse bietet dabei nur begrenzten Mehrwert. Sie kann zwar zur Identifikation zusätzlicher Massnahmen herangezogen werden, darf jedoch nicht dazu dienen, im Rahmen der CSRM definierte Massnahmen abzulehnen oder als Restrisiken auszuweisen.

Die CSRM sieht vor, dass bei einer Nichtumsetzung von Massnahmen die betroffenen Geschäfts- und Produktionsprozessziele entsprechend angepasst werden müssen. Dieser Ansatz unterstützt die Governance, da die Auswirkungen unmittelbar sichtbar werden, und vereinfacht die Entscheidungsfindung, indem sich die Geschäftsleitung auf die Bewertung akzeptabler Auswirkungen konzentrieren kann, ohne technische Detailfragen behandeln zu müssen.

5.2 Was kommt mit dem CSRM neu dazu?

Durch die Anwendung der CSRM erwartet das BACS folgende zusätzliche Aufwände bei der Steuerung und Lenkung der Informationssicherheit:

- Geschäfts- und Produktionsprozesse müssen hinsichtlich der akzeptierbaren Auswirkungen bewertet werden, um den Schutzbedarf festzulegen.
- Es ist zu definieren, wie Hard- und Softwarekomponenten sinnvoll zu Schutzobjekten aggregiert werden können.
- Bestehende Informationssicherheitsrichtlinien und technische Umsetzungsstandards sind darauf zu prüfen, ob sie die Basisanforderungen der CSRM berücksichtigen. Die Methode liefert hierzu zahlreiche Umsetzungsempfehlungen, die direkt übernommen werden können, und geht in einzelnen Punkten darüber hinaus – etwa mit Anforderungen an die Systemhärtung (Basisanforderung 3.1), der Pflicht zu einem Offline-Backup (Basisanforderung 3.7) und Vorgaben zur sicheren Softwareentwicklung (Basisanforderung 3.8).
- Da die CSRM sowohl IT- als auch OT-Systeme, sowie Elemente des Business Continuity Prozesses abdeckt, kann eine engere Zusammenarbeit bisher getrennt arbeitender Teams erforderlich werden.

Darüber hinaus bewirkt die Methode eine Veränderung des Bewusstseins: Im Mittelpunkt steht nicht mehr primär die Informationssicherheit oder Compliance, sondern die Cyberresilienz als übergeordnetes Ziel.

6 Wissenswertes für Unternehmen und Behörden, welche heute den IKT-Minimalstandard umsetzen

Mit Ausnahme weniger Anforderungen deckt die CSRM sämtliche Aspekte des IKT-Minimalstandards ab. Eine Umsetzung der CSRM führt somit in der Regel auch zur Erfüllung der meisten Anforderungen des IKT-Minimalstandards. Im Folgenden werden jene Subkategorien des IKT-Minimalstandards betrachtet, die – zusätzlich zu den methodischen Unterschieden im Cyber-Risikomanagement – einer gesonderten Beachtung bedürfen:

- ID.BE-2 fordert, *dass die Bedeutung der Organisation als Teil kritischer Infrastrukturen sowie ihre Rolle innerhalb des jeweiligen Sektors identifiziert und kommuniziert wird*. Diese Identifikation und Kommunikation erfolgen ausserhalb des Anwendungsbereichs der CSRM.
- ID.RA-2 verlangt, *dass aktuelle Informationen zu Cyberbedrohungen durch regelmässigen Austausch in Foren und Fachgremien eingeholt werden*. Respektive RS.CO-5 verlangt, *dass regelmässig freiwillig Informationen mit externen Akteuren ausgetauscht werden, um das Bewusstsein hinsichtlich der aktuellen Cybersicherheitssituation zu steigern*. Die CSRM sieht diese Anforderungen nicht ausdrücklich vor, da Cyberresilienz grundsätzlich unabhängig von der aktuellen Bedrohungslage gewährleistet werden muss. Das BACS berücksichtigt diesen Aspekt jedoch im Rahmen der Ausgestaltung der Betriebsprozesse, beispielsweise beim Schwachstellen- und Vorfallmanagement.
- ID.SC-3 fordert, *dass Verträge mit Lieferanten und Drittparteien diese verpflichten, die zur Erreichung der Ziele des Cybersicherheitsprogramms der Organisation notwendigen Massnahmen umzusetzen und einzuhalten*. Die CSRM verlangt in diesem Zusammenhang, dass Abhängigkeiten identifiziert, überwacht und angemessene Schutzmassnahmen umgesetzt werden (Basisanforderung 2.2). Vertragsvereinbarungen werden durch die Methode nicht explizit gefordert, gelten jedoch implizit als mögliche Massnahme. Das BACS begründet dies damit, dass Verträge allein keine Cybersicherheit oder Resilienz herstellen, sondern vor allem der rechtlichen Absicherung dienen.
- PR.AT-3 verlangt, *dass alle beteiligten Akteure ausserhalb ihres Unternehmens (Lieferanten, Kunden, Partner) ihrer Rolle und Verantwortung bewusst sind.* Die CSRM sieht diese Anforderung nicht ausdrücklich vor, da ihre praktische Umsetzung in der Regel nur eingeschränkt möglich ist.
- PR.DS-8 verlangt, *dass die Organisationen einen Prozess etablieren, um die eingesetzte Hardware hinsichtlich ihrer Integrität zu verifizieren.* Die Verifikation von Hardware ist in der Methode keine Basisanforderung, kann aber bei erhöhtem Schutzbedarf mit zusätzlichen Massnahmen berücksichtigt werden.
- PR.IP-1 fordert, *dass für die Informations- und Kommunikationsinfrastruktur sowie für industrielle Kontrollsysteme eine Standardkonfiguration erstellt wird, um die Einhaltung grundlegender Sicherheitsprinzipien sicherzustellen*. Das BACS sieht eine solche Anforderung nicht ausdrücklich vor, da die Basisanforderungen der CSRM selbst als grundlegende Sicherheits-Baseline gelten. Eine zusätzliche, unternehmensspezifische Baseline ist nicht erforderlich und würde die Umsetzung unnötig verkomplizieren. Systemspezifische Konfigurationsstandards – etwa für Firewall- oder Netzwerkkonfigurationen – müssen jedoch entwickelt und im Rahmen geeigneter operativer Prozesse berücksichtigt werden.
- PR.IP-3 fordert, *dass ein Prozess zur Kontrolle von Konfigurationsänderungen etabliert wird*. Die CSRM verlangt dies nicht ausdrücklich. Im Sinne der Basisanforderung 4.1 ist jedoch sicherzustellen, dass sicherheitsrelevante Änderungen aufgezeichnet und

ausgewertet werden. Detaillierte Vorgaben zum Konfigurationsmanagement sollten im Rahmen der operativen Prozesse festgelegt und umgesetzt werden.

- PR.IP-7 fordert, *dass Prozesse zur Informationssicherheit kontinuierlich weiterentwickelt und verbessert werden*. Die CSRM schliesst eine kontinuierliche Verbesserung zwar nicht aus, verlangt sie jedoch nicht ausdrücklich. Ziel ist die Etablierung und Umsetzung einer Cybersicherheitsprozessstruktur, welche die Resilienz der Organisation gegenüber Cyberrisiken sicherstellt. Eine fortlaufende Verbesserung ist daher nicht zwingend erforderlich – wirksame und stabile Prozesse genügen. Entscheidend ist vielmehr die regelmässige Überprüfung der Wirksamkeit bestehender Massnahmen und das zeitnahe Zurückziehen solcher Massnahmen, die sich im Betrieb als ineffektiv erweisen. Dieser Aspekt ist integraler Bestandteil des fünften Schrittes der CSRM.
- RS.AN-3 verlangt, *dass nach einem eingetretenen Vorfall forensische Analysen durchgeführt werden.* Die CSRM verlangt nur das ein Vorfallmanagement existiert, welches Vorfälle und erkannte Störungen zeitnah triagiert und behebt (Basisanforderung 5.1). Eine Pflicht zu forensischen Analysen sollte durch gezielte Anforderungen bei erhöhtem Schutzbedarf berücksichtigt werden.
- RC.CO-2 verlangt, *dass die Organisation nach einem eingetretenen Cybersecurityvorfall sicherstellen soll, dass sie wieder positiv wahrgenommen wird.* Das CSRM berücksichtigt dies nicht so konkret, verlangt aber in Basisanforderung 5.3, dass die Kommunikation und deren Zielsetzung in Notfällen bekannt sein muss. Bei Vorfällen ist das Lessons Learnt nicht explizit als Basisanforderung erwähnt. Die Methode geht davon aus, dass die Kommunikation Teil des zu etablierenden Vorfallmanagementprozesses ist.