WHITEPAPER

Typische Audit-Prüffelder in der Cyber- und Informationssicherheit

Warum sich Wirksamkeit im Zusammenspiel der Prüffelder entscheidet und nicht im Einzelbefund

Carsten Beck

Cybersecurity Auditor | ISO/IEC 27001 & ISO 22301 Lead Auditor

MAS Information Systems Management

Erstveröffentlichung März 2026 · Version 1.1 (Oktober 2026)

Executive Briefing

Cyber- und Informationssicherheit ist eine Führungs- und Steuerungsaufgabe. Sie ist kein isoliertes IT-Thema, sondern integraler Bestandteil der Unternehmensstrategie. Ihre Wirksamkeit beruht auf dem Zusammenspiel klarer Verantwortlichkeiten, konsistenter Risikoentscheidungen und wirksamer technischer wie organisatorischer Kontrollen.

Erkenntnisse aus Prüfungen und Risikoanalysen zeigen ein wiederkehrendes Muster: Organisationen verfügen häufig über die einzelnen Bausteine, steuern sie aber nicht konsistent. Unklare Verantwortlichkeiten, fragmentierte Risikoentscheidungen, unvollständige Inventare, fragile Lieferketten oder unzureichend getestete Notfallfähigkeit verweisen auf strukturelle Governance-Schwächen, die sich mit technischen Mitteln allein nicht beheben lassen.

Diese Schwächen treffen auf eine Bedrohungslage, die hoch bleibt und sich laufend verändert. Ransomware, Angriffe über Lieferketten und gemeinsam genutzte Plattformen sowie KI-gestützte Angriffsmuster können Geschwindigkeit und Skalierbarkeit von Angriffen erhöhen. Wie gravierend die Folgen ausfallen, hängt auch davon ab, wie kohärent Governance, Risikomanagement und operative Umsetzung ineinandergreifen und wie gut sich kritische Leistungen im Ereignisfall fortführen lassen.

Dieses Whitepaper bündelt sieben zentrale Prüffelder, die regelmässig Gegenstand von Audits, Aufsichtsprüfungen und Risikoanalysen sind. Es richtet sich an Leitungs- und Aufsichtsgremien sowie an verantwortliche Funktionen in IT, Informationssicherheit, Datenschutz, Architektur, Business Continuity, Risiko und Compliance. Ziel ist nicht Checklisten-Compliance, sondern die Beurteilung, ob Governance, Risikosteuerung und operative Umsetzung als Gesamtsystem funktionieren, im Normalbetrieb ebenso wie im Vorfall.

Die Kernaussage lautet: Einzelne Kontrollen können für sich wirksam sein. Ob eine Organisation Angriffe und Ausfälle tatsächlich abwehren und bewältigen kann, entscheidet sich jedoch daran, ob Steuerung, Risikoentscheidungen und operative Umsetzung über die Prüffelder hinweg zusammenpassen.

Die Kapitel 3 bis 9 enthalten je einen Prüfnachweis und Leitfragen für die Führung. Kapitel 11 beschreibt die Anwendung und ihre Grenzen.

1 Ausgangslage: Von Lagebildern zu Prüffeldern

1.1 Governance-Schwächen als Muster hinter Vorfällen

Erkenntnisse aus der FINMA-Aufsicht und aus den Halbjahresberichten des Bundesamts für Cybersicherheit zeigen seit Jahren ein wiederkehrendes Muster: Schwerwiegende Vorfälle lassen sich oft nicht auf ein einzelnes technisches Defizit zurückführen. Regelmässig wirken technische Mängel mit strukturellen Schwächen der Governance-Architektur zusammen.[1]

Typische Befunde sind:

- unklare Verantwortlichkeiten zwischen IT, Cyber-/Informationssicherheit, Fachbereichen, Datenschutz und Geschäftsleitung
- fehlende oder unvollständige Inventare von kritischen Daten (einschliesslich Personendaten), Systemen und Dienstleistern
- unzureichende Identifikation und Bewertung von Risiken
- lückenhafte oder nicht getestete Notfall- und Wiederherstellungspläne
- Reporting, das relevante Risiken weder auf operativer noch auf Leitungsebene sichtbar macht

> **Regulatorischer Kontext**
>
> Regulatorische Rahmenwerke wie die FINMA-Aufsichtsmitteilung 03/2024, das DSG und die EU-DSGVO bilden den normativen Kontext, in dem sich die nachfolgenden Prüffelder bewegen. Sie gelten jeweils, soweit sie anwendbar sind, und werden in den Kapiteln dort referenziert, wo sie konkrete Anforderungen stellen. Die datenschutzrechtlichen Pflichten zur Datensicherheit und zur Auftragsbearbeitung (Art. 8 und 9 DSG, Art. 32 und 28 DSGVO) sind insbesondere für die Prüffelder Outsourcing und Informationswerte einschlägig. Die Meldepflichten für Cyberangriffe auf kritische Infrastrukturen (Art. 74a ff. ISG, CSV) und für Verletzungen der Datensicherheit (Art. 24 DSG) betreffen das Prüffeld Reporting.

1.2 Bedrohungslage, Verwundbarkeit und Kumulation

Die Halbjahresberichte des Bundesamts für Cybersicherheit (BACS) und der Lagebericht des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) dokumentieren eine anhaltend hohe Bedrohungslage. Der Meldeeingang beim BACS hat sich im ersten Halbjahr 2026 auf hohem Niveau stabilisiert, mit 27’128 freiwilligen Meldungen und 200 meldepflichtigen Cybervorfällen. Die Zahl der gemeldeten und beobachteten Ransomware-Vorfälle blieb konstant, während sich die Täterlandschaft fragmentierte: Die Zahl aktiver Ransomware-Familien in der Schweiz stieg von 21 auf 29, der Anteil der bislang führenden Gruppe sank deutlich. Mehrere Vorfälle zielten auf zentrale Plattformen, auf denen viele Systeme gemeinsam betrieben werden, sowie auf Dienstleister, bei denen ein einziger erfolgreicher Zugang die Daten zahlreicher Organisationen preisgibt.

[1] Zu den Befunden aus der Aufsichtstätigkeit: FINMA-Aufsichtsmitteilung 03/2024, Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, 7. Juni 2024. Zur Bedrohungslage: Bundesamt für Cybersicherheit, Halbjahresbericht 2026/1, 24. August 2026.

Lageeinschätzungen wie der Bericht «Sicherheit Schweiz 2026» des Nachrichtendienstes des Bundes (NDB) zeigen zudem ein strategisches Umfeld, das von einer verschärften geopolitischen Lage, einer zunehmenden Rivalität grosser Machtblöcke und einer Zunahme hybrider Aktivitäten geprägt ist. Dazu gehören auch Bedrohungen Kritischer Infrastrukturen.

Parallel dazu verändert der wachsende Einsatz von (generativer) KI sowohl die Angriffs- als auch die Verteidigungsseite und erhöht die Dynamik der Bedrohungslage. Angriffe können automatisierter, skalierbarer und schwerer erkennbar werden, während Verteidigungsfunktionen ihrerseits stärker von Datenqualität, Modellrisiken und regulatorischen Rahmenbedingungen abhängen.

Welche Rolle gemeinsame Abhängigkeiten spielen, zeigte unabhängig von gezielten Angriffen der CrowdStrike-Vorfall im Juli 2024. Die Ursachenanalyse des Herstellers dokumentiert Mängel bei Validierung, Test und gestaffelter Auslieferung eines Inhaltsupdates. Sie trifft keine Aussage über die Kontinuitätsplanung der betroffenen Organisationen. Für die nutzenden Organisationen ergibt sich daraus die Prüfungsfrage, ob sie gemeinsame Abhängigkeiten und einen breitflächigen Ausfall zentraler Sicherheitssoftware in ihrer Kontinuitätsplanung berücksichtigen.

Die Bedrohungslage bleibt hoch und verändert sich. Wie gravierend ihre Auswirkungen sind, hängt nicht allein von einzelnen Schutzmassnahmen ab, sondern davon, ob Governance, Risikosteuerung und Resilienz zusammenwirken und ob operative Schwächen isoliert bleiben oder sich kumulativ verstärken. Das folgende Prüfraster betrachtet diese Elemente in ihrem Zusammenspiel.

2 Das Prüfraster: Sieben Prüffelder

2.1 Überblick

Das Prüfraster umfasst sieben Prüffelder, die typischerweise Gegenstand von Aufsichtsprüfungen, internen Audits und Risikoanalysen sind. Es strukturiert Cyber- und Informationssicherheit entlang zentraler Steuerungs-, Risiko- und Umsetzungsthemen und richtet den Fokus auf die Qualität der Governance- und Steuerungsarchitektur. Die sieben Felder sind Steuerungsfelder. Technische Kontrollthemen wie Schwachstellen- und Patchmanagement, Protokollierung und Angriffserkennung oder Netzsegmentierung werden nicht als eigene Prüffelder geführt, sondern dort beurteilt, wo über sie entschieden wird: im Risikomanagement, im Identitäts- und Zugriffsmanagement, in der Outsourcing-Steuerung und im Business Continuity Management.

Die folgende Tabelle fasst die sieben Prüffelder und ihre jeweiligen Schwerpunkte zusammen. Sie dient als Orientierung für die nachfolgenden Kapitel, in denen die einzelnen Felder und ihre Schnittstellen vertieft werden.

Prüffeld	Kernfrage
Governance & Rollenmodell	Wer ist wofür verantwortlich, und wie werden Entscheidungen getroffen?
IT-/Cyber-Risikomanagement	Sind Risiken transparent, bewertet und mit Massnahmen hinterlegt?
Outsourcing & Drittparteien	Können ausgelagerte Leistungen tatsächlich gesteuert werden?
Identitäts- und Zugriffsmanagement (IAM)	Ist klar, wer auf welche Systeme und Daten zugreifen kann?

Prüffeld	Kernfrage
Informationswerte & Schutzbedarf	Sind kritische Informationen bekannt und die Systeme, die sie bearbeiten, ihrem Schutzbedarf entsprechend geschützt?
Business Continuity & Resilienz	Kann die Organisation kritische Leistungen im Ereignisfall aufrechterhalten und wiederherstellen?
Reporting & Eskalation	Erhalten Entscheider ein aussagekräftiges Lagebild mit klaren Eskalationswegen?

Tabelle 1: Die sieben Prüffelder und ihre Kernfragen

Für die Anwendung des Prüfrasters ist zunächst ein gemeinsames Verständnis der zentralen Begriffe erforderlich. Dazu gehört insbesondere die Kumulation von Kontrollschwächen: Schwächen in einzelnen Prüffeldern können sich über deren Schnittstellen hinweg verstärken.

Zentrale Begriffe

Schutzbedarf: Das erforderliche Schutzniveau eines Schutzobjekts, beispielsweise einer Anwendung, eines Systems oder einer ausgelagerten Leistung. Es wird für Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit getrennt bestimmt. Massgeblich sind die möglichen Folgen einer Beeinträchtigung der bearbeiteten Informationen und unterstützten Geschäftsleistungen sowie rechtliche und vertragliche Schutzpflichten.

Klassifizierung: Zuordnung von Informationen zu festgelegten Kategorien mit verbindlichen Vorgaben für ihre Behandlung. Die daraus folgenden Schutzpflichten fliessen in die Schutzbedarfsanalyse ein und können je nach Regelwerk ein Mindestschutzniveau für das bearbeitende Schutzobjekt vorgeben.

Werttransparenz: Das Wissen, welche Informationen welchen Wert haben, wer für sie verantwortlich ist und wo sie liegen.

Kumulation von Kontrollschwächen: Mehrere Defizite betreffen dieselbe Leistung, dieselben Informationen oder voneinander abhängige Kontrollen und erhöhen gemeinsam das Risiko. Ob eine solche Verstärkung vorliegt, ist anhand eines nachvollziehbaren Szenarios zu beurteilen.

Kumulationseffekt: Der Schutzbedarf einer gemeinsam genutzten Plattform kann für einzelne Schutzziele über dem der einzelnen darauf betriebenen Anwendungen liegen, wenn ihre gemeinsame Beeinträchtigung höhere Gesamtauswirkungen hat.

Konzentrationsrisiko: Mehrere kritische Leistungen hängen von derselben Ressource, demselben Dienstleister oder einer gemeinsamen Ausfallursache ab.

Im Weiteren bezeichnet «Kumulation» ohne Zusatz stets die Kumulation von Kontrollschwächen.

Entscheidend ist nicht die isolierte Betrachtung der sieben Prüffelder, sondern ihr Zusammenspiel. In der Praxis entstehen relevante Risiken dort, wo Steuerungsdefizite, unklare Werttransparenz oder operative Schwächen über mehrere Bereiche hinweg zusammenwirken.

Systemische Verwundbarkeit entsteht im Zusammenspiel, nicht im Einzelbefund.

Abbildung 1 verdichtet diesen Zusammenhang in einer dreistufigen Struktur und bildet die konzeptionelle Grundlage dieses Whitepapers.

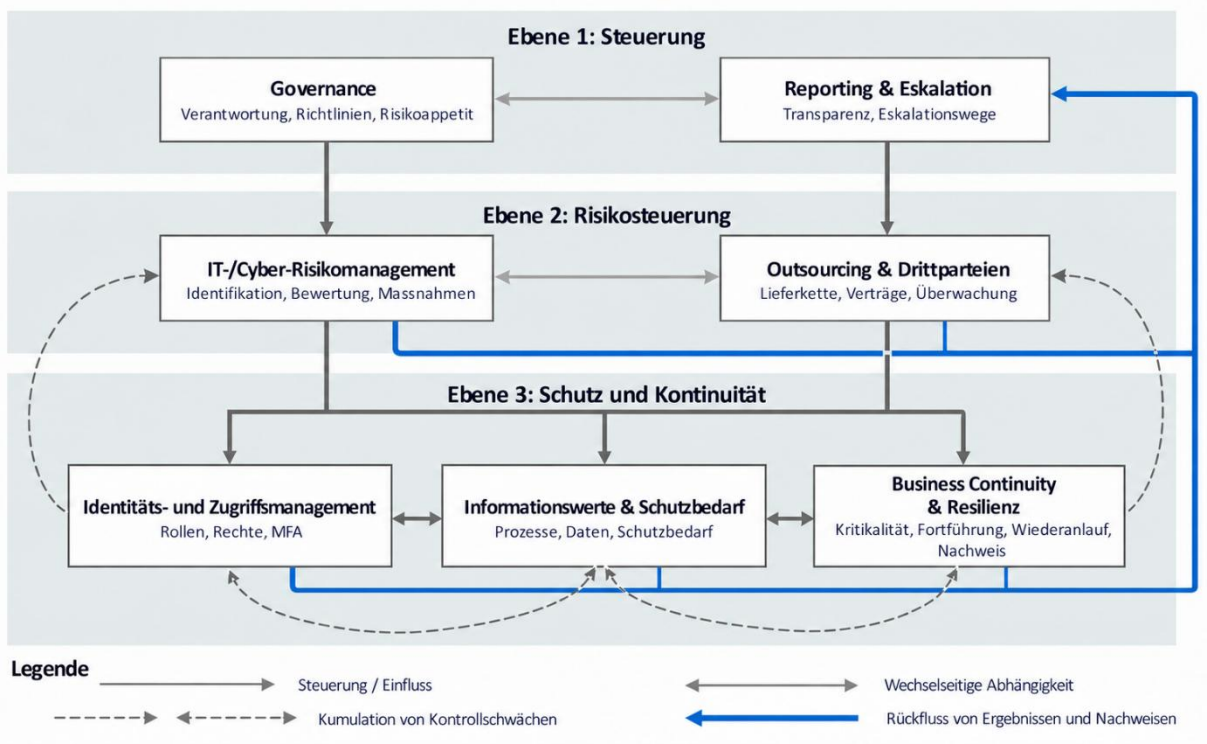


Abbildung 1: Governance- und Steuerungsmodell der sieben Prüffelder (eigene Darstellung). Dargestellt sind ausgewählte Wirkbeziehungen, nicht sämtliche Abhängigkeiten.

Die erste Ebene beschreibt den Steuerungsrahmen. Governance sowie Reporting und Eskalation legen fest, wer entscheidet, wie Risiken priorisiert werden und welche Themen auf welcher Ebene sichtbar sind. Fehlt hier Klarheit, bleibt auch die Risikosteuerung fragmentiert.

Die zweite Ebene umfasst die eigentliche Risikosteuerung. IT-/Cyber-Risikomanagement und die Steuerung von Outsourcing und Drittparteien übersetzen strategische Vorgaben in Bewertungen, Priorisierungen und Massnahmen.

Die dritte Ebene umfasst Schutz und Kontinuität. Identitäts- und Zugriffsmanagement, Informationswerte und Schutzbedarf sowie Business Continuity und Resilienz bestimmen, wie Schutzanforderungen konkret ausgestaltet und im Alltag durchgesetzt werden und wie sich kritische Leistungen im Ereignisfall fortführen lassen.

Die in Abbildung 1 dargestellten Verbindungen machen vier Wirkmechanismen sichtbar:

Top-down-Steuerung: Schwächen auf der Steuerungsebene wirken über die Risikosteuerung auf die nachgelagerten Prüffelder. Unklare Verantwortlichkeiten, fehlender Risikoappetit oder eine unzureichende Eskalationslogik führen dazu, dass Risiken operativ uneinheitlich adressiert werden.

Wechselseitige Abhängigkeiten: Innerhalb einer Ebene können sich Defizite gegenseitig verstärken. Ein unreifes IT-/Cyber-Risikomanagement erschwert die risikobasierte Steuerung von Auslagerungen.

Kumulation von Kontrollschwächen: Operative Schwächen bleiben selten isoliert. Überbreite Berechtigungen, ungeklärte Schutzanforderungen oder unzureichend getestete Notfallpläne mögen einzeln beherrschbar erscheinen. Betreffen sie dieselbe Leistung, können sie sich in einem gemeinsamen Szenario verstärken.

Rückfluss von Ergebnissen und Nachweisen: Ergebnisse aus der Risikosteuerung sowie aus Schutz und Kontinuität fliessen in Reporting und Eskalation zurück. Sie machen Risiken, Abweichungen und nachgewiesene Fähigkeiten für die zuständigen Entscheidinstanzen sichtbar.

2.2 Risikobasierte Auswahl der Prüffelder

Nicht jedes Prüffeld ist in jedem Kontext gleich relevant. Grösse, Regulierung, Reifegrad und aktuelle Risikolage einer Organisation bestimmen, wo der Prüffokus sinnvoll gesetzt wird.

In der Praxis werden aus diesen Prüffeldern kontextabhängig Schwerpunkte ausgewählt. Eine Vollprüfung sämtlicher Detailaspekte ist nicht in jedem Fall erforderlich. Entscheidend ist, ob die adressierten Themen konzeptionell tragfähig verankert, in Governance und Steuerung eingebettet und übergreifend anschlussfähig sind. Schwerpunkte sind zulässig und notwendig. Die Beurteilung kumulativer Effekte setzt jedoch voraus, dass die Verbindungen zu den nicht vertieft geprüften Feldern mitbetrachtet werden.

In jedem der folgenden sieben Prüffelder finden sich Leitfragen, die als Reflexionsanstoss dienen. Sie verstehen sich nicht als vollständiger Auditfragenkatalog, sondern als gezielte Denkanstösse für Leitungs- und Aufsichtsgremien sowie für verantwortliche Funktionen in IT, Informationssicherheit, Datenschutz, Architektur, Business Continuity, Risiko und Compliance. Sie sollen helfen, kumulative Effekte besser zu erkennen, ohne operative Detailprüfungen vorwegzunehmen.

Die Prüfnachweise zeigen beispielhaft, woran sich Aussagen zur Steuerung und Wirksamkeit überprüfen lassen. Auswahl, Umfang und Prüftiefe richten sich nach dem Prüfauftrag und dem Risikokontext.

3 Prüffeld Governance: Rollenmodell und Entscheidprozesse

Am Anfang steht die Frage, wer wofür verantwortlich ist. Ohne klare Governance bleibt jede noch so detaillierte Massnahme Stückwerk.

Ein reifes Governance-Setup umfasst:

- definierte Rollen für Informationssicherheit, Datenschutz, Risikomanagement, Business Continuity, IT, Fachbereiche und Lieferantensteuerung
- klare Zuständigkeiten und Stellvertretungen, dokumentiert und kommuniziert
- verbindliche Gremien (z.B. Security- oder Risiko-Board) mit Mandat, Traktandenplanung und Entscheidkompetenz
- sachliche Unabhängigkeit von Informationssicherheit, Datenschutz und Risikomanagement bei ihren Kontrollaufgaben sowie die Möglichkeit, Themen an die zuständige Leitung zu eskalieren, insbesondere wenn die CISO-Funktion organisatorisch der IT-Leitung unterstellt ist. Die interne Revision ist von Aufbau und Betrieb der Kontrollen unabhängig und berichtet an das zuständige Aufsichtsgremium
- festgelegte Grundsätze zu Risikoappetit und Priorisierung, abgeleitet aus der Unternehmensstrategie und verankert in den Entscheidprozessen

Prüfnachweis: Vorzulegen sind das Mandat des zuständigen Gremiums und seine Protokolle aus einem Jahr. Finden sich zu entscheidungsbedürftigen Sicherheitsrisiken nur Kenntnisnahmen, ist das ein Hinweis darauf, dass das Gremium seine Entscheidkompetenz nicht wahrnimmt.

3.1 Leitfragen für die Führung

- Sind unsere Rollen, Verantwortlichkeiten und Gremien nachvollziehbar beschrieben und werden sie tatsächlich gelebt?
- Haben wir einen klar definierten Ort, an dem über Sicherheitsrisiken, Massnahmen und Prioritäten entschieden wird, und kommen diese Entscheide im Betrieb an?
- Stellen wir sicher, dass kritische Risiken zeitnah die Geschäftsleitung und zuständigen Kontrollgremien erreichen?
- Haben wir die Unabhängigkeit unserer Überwachungs- und Kontrollfunktionen (z.B. Informationssicherheit, Datenschutz, Risikomanagement, interne Revision) organisatorisch so gesichert, dass Interessenkonflikte vermieden werden?
- Haben wir einen klar definierten Risikoappetit für Cyber- und Informationssicherheit und spiegelt er sich in unseren Entscheidungen zu Prioritäten und Ressourcen wider?

4 Prüffeld IT-/Cyber-Risikomanagement

Cyber- und Informationssicherheit ohne Risikoblick führt häufig zu wenig zielgerichteten, überbordenden oder aktionistisch geprägten Massnahmen, die nur teilweise wirksam sind. Statt die wesentlichen Risiken gezielt zu adressieren, werden Ressourcen mitunter nach dem Giesskannenprinzip in breit gestreute Security-Scans oder Penetrationstests investiert, ohne vorgängige Priorisierung entlang der zentralen Risikotreiber. Governance- oder Prozessrisiken bleiben dabei häufig nicht adressiert.

Ein strukturiertes Risikomanagement schafft Transparenz und Steuerbarkeit. Zentrale Elemente eines reifen IT-/Cyber-Risikomanagements sind:

- systematische Identifikation relevanter Risiken, einschliesslich Szenarien zu Ausfällen, Angriffen, Fehlkonfigurationen und Lieferkettenrisiken
- Verankerung von Cyber-Risiken in der übergeordneten Unternehmensrisikosteuerung als integrierter Bestandteil, nicht als isoliertes IT-Thema
- Bewertung nach Eintrittswahrscheinlichkeit und Auswirkungen sowie dokumentierte Entscheide zur Risikobehandlung (reduzieren, akzeptieren, übertragen, vermeiden), ergänzt durch szenariobasierte Ansätze und die Berücksichtigung von Konzentrationsrisiken, die über klassische Wahrscheinlichkeits-Schadens-Matrizen hinausgehen
- besondere Aufmerksamkeit für Szenarien mit geringer Eintrittswahrscheinlichkeit und hohem Schadensausmass oder systemischen Auswirkungen, etwa den Ausfall kritischer Infrastrukturen oder Dienstleister, breit angelegte Lieferkettenangriffe oder breitflächige Ransomware-Kampagnen. Solche Szenarien dürfen nicht allein wegen ihrer geringen Eintrittswahrscheinlichkeit vernachlässigt werden, gerade vor dem Hintergrund der angespannten geopolitischen Lage
- Verknüpfung mit Projekt-, Change- und Portfoliosteuerung, sodass neue Vorhaben und wesentliche Änderungen systematisch einem Risikoblick unterzogen werden
- regelmässige Aktualisierung bei veränderten Bedrohungslagen, neuen Schwachstellen oder organisatorischen Veränderungen

Im Geltungsbereich der FINMA-Aufsicht ist vorgegeben, Cyber-Risiken als eigenständige Risikokategorie im Management operationeller Risiken zu erfassen, in die übergeordnete Unternehmensrisikosteuerung

einzubetten und mit einem definierten Risikoappetit sowie klaren Toleranzgrenzen zu hinterlegen (FINMA-Aufsichtsmitteilung 03/2024, Abschnitt 2.2). Für andere Organisationen richtet sich die Ausgestaltung nach den jeweils geltenden rechtlichen Anforderungen und ihrer Organisationsverantwortung. Soweit Personendaten bearbeitet werden, sind insbesondere die anwendbaren Pflichten zur angemessenen Datensicherheit zu berücksichtigen (Art. 8 DSG, Art. 32 DSGVO).

Prüfnachweis: Für die Cyber-Risiken mit der höchsten Einstufung sind Risikobewertung, dokumentierter Behandlungsentscheid und die daraus abgeleitete Ressourcen- oder Investitionsentscheidung nebeneinanderzulegen. Lässt sich zu einem akzeptierten Risiko weder eine Entscheidinstanz noch ein Datum benennen, ist die Risikoakzeptanz nicht belegt.

4.1 Leitfragen für die Führung

- Sind Cyber- und Informationssicherheitsrisiken in unserer übergeordneten Unternehmensrisikosteuerung verankert oder werden sie organisatorisch isoliert als IT-Thema behandelt?
- Wie konsequent werden der definierte Risikoappetit und die Toleranzgrenzen in konkrete Priorisierungs- und Budgetentscheidungen übersetzt?
- Wie systematisch identifizieren und bewerten wir Szenarien, die technische Ausfälle, Angriffe, Lieferkettenrisiken und Fehlkonfigurationen verbinden, und fliessen diese in Planung, Projekte und Changes ein?

5 Prüffeld Outsourcing: Steuerung von Dienstleistern und Drittparteien

Mit jeder Auslagerung wandert ein Teil der operativen Kontrolle nach aussen. Die Verantwortung bleibt. Steuerungsfähigkeit gegenüber Dienstleistern wird damit zu einem eigenen Prüffeld.

Ein risikobasiertes Outsourcing-Setup umfasst:

- eine aktuelle Übersicht wesentlicher Dienstleister und Leistungen (Inventar mit Kritikalität und Datenarten) sowie risikobasierte Einstufung der Auslagerungen
- vertraglich verankerte Sicherheitsanforderungen, Reporting-, Audit- und Exit-Rechte sowie bei der Bearbeitung von Personendaten die Vergewisserung über die Datensicherheit beim Auftragsbearbeiter (Art. 9 DSG, Art. 28 DSGVO)
- Transparenz über Subdienstleister, insbesondere bei Cloud- und Infrastrukturprovidern
- gelebte Steuerungsgespräche mit systematischer Nachverfolgung von Massnahmen und Auffälligkeiten
- Konzentrations- und Abhängigkeitsanalysen zur Identifikation von «Single Points of Failure»

Wiederkehrende Befunde aus Aufsichtsmitteilungen sind: fehlende oder unvollständige Dienstleisterinventare, unklare Anforderungen an Informationssicherheit, mangelnde Transparenz über Subdienstleister sowie fehlende Definition kritischer Daten.

Wie kritisch unzureichend gesicherte Service- und Fernzugänge von IT-Dienstleistern sind, verdeutlicht ein Ransomware-Angriff auf einen Schweizer Softwareanbieter für Spitäler, der Ende Februar 2025 bekannt wurde. Der Anbieter wartet Systeme im Spitalumfeld über VPN-Zugänge. Nach Medienberichten, die sich

auf mehrere Quellen stützen, führten die Angreifer automatisierte Scans und Anmeldeversuche gegen angeschlossene Spitalsysteme durch. Der Anbieter erklärte, bei den durchgeführten Prüfungen sei keine Kompromittierung der Kundensysteme festgestellt worden.

Aus Sicht der Steuerung gilt: Gelingt es Angreifern in einer solchen Konstellation, den Zugang tatsächlich zu nutzen, sind potenziell mehrere Einrichtungen gleichzeitig betroffen, mit möglichen Auswirkungen auf Verfügbarkeit und Patientensicherheit. Ein kumulatives Risiko kann entstehen, wenn kompromittierte Dienstleisterzugänge, unzureichende Segmentierung und eine lückenhafte Steuerung von Drittzugriffen zusammenwirken.

Prüfnachweis: Vorzulegen sind das Dienstleisterinventar mit Kritikalitätseinstufung und wesentlichen Subdienstleistern sowie für eine kritische Auslagerung der Vertrag und das Protokoll des letzten Steuerungsgesprächs. Fehlt für kritische Auslagerungen die Übersicht über Subdienstleister, ist nicht belegt, dass die Abhängigkeiten bekannt sind.

5.1 Leitfragen für die Führung

- Haben wir ein klares Bild, bei welchen Dienstleistern sich unsere kritischsten Prozesse und Daten konzentrieren und welche «Single Points of Failure» daraus entstehen könnten?
- Inwieweit sind wir im Ernstfall tatsächlich steuerungsfähig gegenüber unseren wesentlichen Dienstleistern, oder sind wir faktisch abhängig von deren Prioritäten, Ressourcen und Krisenorganisation?
- Wie gut greifen vertragliche Regelungen, Reporting, Auditrechte und Exit-Szenarien als Gesamtsystem zusammen, und wo würden heute Lücken sichtbar, wenn ein zentraler Dienstleister ausfällt oder kompromittiert wird?

6 Prüffeld IAM: Identitäts- und Zugriffsmanagement

Wer worauf und mit welchen Rechten zugreifen darf, gehört zu den zentralen Stellschrauben der Informationssicherheit. Identitäts- und Berechtigungsmanagement ist damit eine eigene Systemebene und zugleich ein häufiger Schwachpunkt.

Kernelemente eines reifen IAM sind:

- eindeutige, einer Person oder einem System zurechenbare Identitäten und benannte Verantwortliche für technische Konten. Gemeinsam genutzte Personenkonten sind nur als begründete, geregelte und überwachte Ausnahme zulässig
- Rollenmodelle mit klar definierten Zugriffsrechten nach dem Prinzip «Need-to-Know / Least Privilege»[2]
- definierte Prozesse für Eintritte, Funktionswechsel und Austritte (Joiner / Changer / Leaver) und regelmässige Rezertifizierungen von Rechten
- Multi-Faktor-Authentifizierung (MFA) für kritische Systeme sowie Privileged-Access-Management für administrative Accounts (gesonderte Steuerung, Protokollierung und Überwachung weitreichender Systemzugriffe)

[2] «Need-to-Know» begrenzt den Kreis der Zugriffsberechtigten auf jene, die die Information für ihre Aufgabe benötigen. «Least Privilege» begrenzt den Umfang der eingeräumten Rechte auf das für die Aufgabe minimal Erforderliche. Beide Prinzipien wirken zusammen, beantworten aber unterschiedliche Fragen.

Typische Schwächen sind fehlende zentrale Übersichten, überbreite Berechtigungen, verwaiste Accounts, unvollständige MFA-Einführung sowie unzureichende Überwachung privilegierter Zugriffe. Ein Zero-Trust-orientierter Ansatz folgt dem Grundsatz «Nie vertrauen, immer prüfen»: Ein Zugriff gilt nicht schon deshalb als vertrauenswürdig, weil er aus dem eigenen Netz kommt. Geprüft werden Identität, Gerätezustand und weitere Umstände des Zugriffs, und zwar nicht nur bei der Anmeldung. Segmentierung begrenzt die Ausbreitung eines Angreifers im Netz. Die Entscheidung über Geltungsbereich und Tempo einer solchen Umstellung gehört in die Architektur- und Risikosteuerung, nicht in den Betrieb einzelner Systeme.

Prüfnachweis: Für eine kritische Anwendung sind die berechtigten Personen und technischen Konten mit Rollen und Verantwortlichen, das Ergebnis der letzten Rezertifizierung und die Auswertung der privilegierten Zugriffe vorzulegen. Finden sich Konten ohne Verantwortlichen oder ohne Bezug zu einer aktuellen Funktion, ist das ein Hinweis auf Lücken in der Rezertifizierung.

6.1 Leitfragen für die Führung

- Haben wir organisationsweit Transparenz darüber, welche Personen und Systeme mit welchen Rechten auf unsere kritischen Anwendungen und Daten zugreifen, einschliesslich privilegierter Zugriffe?
- In welchem Ausmass sind Rollenmodelle, die Prinzipien «Need-to-Know» und «Least Privilege» sowie Rezertifizierungen tatsächlich umgesetzt, und wo verlassen wir uns faktisch auf historisch gewachsene Berechtigungen?
- Wie eng ist IAM mit Informationswerten, Architektur (z.B. Segmentierung) und Outsourcing verzahnt, oder werden Zugriffsentscheidungen noch zu stark isoliert pro System oder Dienstleister getroffen?

7 Prüffeld Informationswerte: Schutzbedarf, Datenflüsse und Kumulation

Wiederkehrende Befunde aus Aufsichtsmitteilungen haben einen gemeinsamen Kern: Organisationen wissen nicht hinreichend genau, welche Informationen besonders kritisch sind und wo diese liegen. Ohne Werttransparenz und eine klare Schutzbedarfsdefinition bleiben weitere Steuerungs- und Schutzmassnahmen zufällig.

Fallvignette: Xplain

Der Cyberangriff auf den IT-Dienstleister Xplain zeigte exemplarisch, was fehlende Werttransparenz bedeutet: Grosse Mengen teils hochsensitiver Daten verschiedener Bundesämter und Behörden lagen auf Systemen des Dienstleisters, ohne dass Umfang, Sensitivität und Zweck ausreichend bekannt waren. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) bemängelte fehlende Vorgaben zu Übermittlung und Speicherung, eine unnötig lange Aufbewahrung und unzureichende Sicherheitsmassnahmen. Aus Sicht der Steuerung verdeutlicht der Fall, warum Zweck, Datenarten, Schutzanforderungen und Löschpflichten auch im Supportprozess und bei Dienstleistern geregelt, dokumentiert und überprüft werden müssen.

Ähnliche Muster zeigen sich in regulierten Finanzinstituten: Die FINMA hielt in einer Aufsichtsmitteilung fest, dass viele Institute nicht klar definiert hatten, welche Daten sie als kritisch einstufen. Das erschwerte sowohl den internen Schutz als auch die Einstufung von Dienstleistern und die Ableitung angemessener Kontrollmassnahmen.[3]

Ein reifer Ansatz zu Informationswerten umfasst drei Ebenen: Prozesse, Daten und Schutzbedarf. Ausgangspunkt ist eine Übersicht der wesentlichen Informationen mit ihrer fachlichen Bedeutung, ihren Verantwortlichen, ihren Bearbeitungsorten und den Geschäftsleistungen, die sie unterstützen.

Klassifizierungen regeln vor allem Kennzeichnung, Weitergabe und Ablage. Nach ISO/IEC 27001 können sie neben der Vertraulichkeit auch Integrität und Verfügbarkeit berücksichtigen. In der Praxis sind sie jedoch häufig auf Vertraulichkeit ausgerichtet und werden trotzdem als Schutzbedarf behandelt. Ein solches Schema sagt viel über den Umgang mit einem Dokument, aber wenig darüber, wie lange eine Anwendung ausfallen darf. Es ersetzt kein vollständiges Schutzbedarfsprofil.

Die Schutzbedarfsanalyse führt die Anforderungen aus dem Wert der Information einschliesslich der für sie geltenden Schutzpflichten aus Datenschutz, Geheimhaltung und Verträgen mit der Bedeutung der unterstützten Geschäftsleistungen zusammen. Daraus entsteht für die unterstützende Anwendung oder Plattform ein begründetes Schutzbedarfsprofil je Schutzziel, also für Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit.

Der definierte Schutzbedarf entfaltet seine Wirkung jedoch nur, wenn er mit den Anforderungen nachgelagerter Steuerungsbereiche verknüpft ist, insbesondere mit dem Business Continuity Management. Mit ihm werden vor allem die Anforderungen an Fortführung und Wiederanlauf abgestimmt. Verfügbarkeitseinstufung, Wiederanlaufziele und die nachgewiesene Fähigkeit von IT und Dienstleistern müssen zusammenpassen. Abweichungen sind zu bewerten und durch die zuständige Entscheidinstanz zu behandeln. Bei Auslagerungen und Cloud-Szenarien muss nachvollziehbar bleiben, wo die Informationen bearbeitet und wie ihre Schutzanforderungen entlang der Lieferkette umgesetzt werden.

7.1 Kumulation rund um Informationswerte

Das Prüffeld Informationswerte ist ein prototypisches Beispiel für Kumulation: fehlende Definition kritischer Daten, unvollständige Schutzbedarfsanalysen, lückenhafte Datenflussübersichten bei Auslagerungen und zugleich steigende Abhängigkeit von wenigen Dienstleistern. Jede Schwäche mag isoliert beherrschbar erscheinen. In Kombination kann systemische Verwundbarkeit entstehen.

Informationswerte sind kein isoliertes Prüffeld, sondern ein Querschnittsknoten: Wo Werttransparenz fehlt, können sich Schwächen in IAM, Outsourcing, BCM, Risikomanagement und Reporting gegenseitig verstärken. Die systemische Dimension dieser Kumulation wird in Kapitel 10 vertieft.

Prüfnachweis: Für die kritischsten Informationsbestände sind Eigner und Bearbeitungsorte einschliesslich Dienstleistern sowie das begründete Schutzbedarfsprofil der Anwendungen oder Plattformen, auf denen sie bearbeitet werden, vorzulegen. Lässt sich für einen dieser Bestände nicht benennen, wo er ausserhalb der eigenen Systeme bearbeitet wird, ist die Werttransparenz für diesen Bestand lückenhaft.

[3] vgl. FINMA-Aufsichtsmitteilung 03/2024, Abschnitt 2.1.

7.2 Leitfragen für die Führung

- Wissen wir organisationsweit, welche Informationsbestände und Systeme für unsere Wertschöpfung am kritischsten sind und wo diese konkret liegen, auch bei Dienstleistern und in der Cloud?
- Wie konsequent fliesst der Schutzbedarf der Systeme mit kritischen Informationen in Entscheidungen zu Outsourcing, IAM und Architektur ein, und ist er konsistent mit den Anforderungen aus dem Business-Continuity-Management verknüpft?
- Wo könnten heute Schwächen in der Werttransparenz (unklare Datenflüsse, ungeklärte Schutzanforderungen, veraltete Inventare) dazu führen, dass wir systemische Risiken unterschätzen?

8 Prüffeld Business Continuity: Resilienz statt nur Backup

Cyber- und Informationssicherheit endet nicht bei einem Ereignis, sondern umfasst auch die Fähigkeit zur Fortführung und Wiederherstellung kritischer Leistungen. Business Continuity wird in der Praxis jedoch häufig als Sammlung technischer Massnahmen verstanden und damit zu stark auf die IT verengt.

Tatsächlich handelt es sich um einen ausgeprägt Top-down-orientierten Managementprozess: Am Anfang stehen die Definition der Geschäftsprozesse und Leistungen, die Identifikation der kritischen Prozesse sowie deren Bewertung im Rahmen der Business-Impact-Analyse (BIA). Ohne diese Führungsperspektive droht BCM zu einem Technikprojekt zu werden, das an den eigentlichen Wertschöpfungs- und Entscheidungsstrukturen vorbeigeht. Die Vererbung nach unten ist dabei nur die eine Richtung. Den Anforderungen aus der Business-Impact-Analyse ist die nachgewiesene Fähigkeit von IT und Dienstleistern gegenüberzustellen: Übungen und Wiederherstellungstests zeigen, ob die vorgesehenen Leistungen innerhalb der Ziele und auf dem erforderlichen Mindestniveau wieder aufgenommen werden können. Ohne diesen Rückweg bleibt ein Wiederanlaufziel eine Absichtserklärung.

Ein belastbares BCM umfasst insbesondere:

- Business-Impact-Analysen (BIA) für kritische Leistungen und Prozesse als Grundlage für Wiederherstellungszeitziele (RTO) und Wiederherstellungspunkte (RPO)
- darauf aufbauende Business-Continuity-Strategien und -Pläne mit klar definierten Rollen, Abläufen und Eskalationswegen
- Notfall- und Wiederherstellungspläne für relevante Szenarien (z.B. Ransomware, Ausfall wesentlicher Dienstleister) sowie regelmässige Tests mit Auswertung von Lessons Learned
- eine robuste Backup-Strategie (z.B. 3-2-1-Regel), ergänzt um gegen Veränderung und Löschung geschützte Sicherungen sowie eine nachgewiesene Wiederherstellbarkeit[4]
- klare Krisenkommunikations- und Eskalationsprozesse

Prüfnachweis: Vorzulegen sind für eine kritische Leistung zwei Zahlen mit demselben Anfangs- und Endpunkt: das genehmigte Wiederanlaufziel und die zuletzt in einem Test oder Ereignis tatsächlich erreichte Wiederanlaufzeit samt Szenario, Umfang und erreichtem Mindestleistungsniveau. Fehlt ein geeigneter Nachweis, ist nicht belegt, dass die geforderte Wiederanlauffähigkeit erreicht wird.

[4] Die 3-2-1-Regel besagt: mindestens drei Kopien der Daten, auf zwei verschiedenen Medientypen, davon eine Kopie an einem externen Standort. Für Ransomware-Szenarien ist sie um gegen Veränderung und Löschung geschützte Sicherungen sowie einen dokumentierten Wiederherstellungstest zu ergänzen.

8.1 Leitfragen für die Führung

- Sind unsere definierten RTO-/RPO-Ziele und Notfallpläne auf breitflächige Ausfälle ausgelegt, auch auf den Ausfall kritischer Dienstleister oder Cloud-Plattformen, oder eher auf «klassische» Störungen zugeschnitten?
- Wie regelmässig üben wir realistische End-to-End-Szenarien mit Beteiligung von Business, IT, Dienstleistern und Führung, und leiten daraus konkrete Entscheide zu Architektur, Outsourcing oder Investitionen ab?
- Wo sehen wir heute Brüche zwischen Schutzbedarf, technischer Wiederherstellung und organisatorischer Krisenführung, also Stellen, an denen wir zwar Dokumente haben, aber keine gelebte Resilienz?
- Welche Rolle nimmt die Geschäftsleitung heute konkret in der Definition kritischer Geschäftsprozesse, der Genehmigung der BIA-Ergebnisse und der Auswahl der BCM-Strategie ein, und wo wurde diese Verantwortung faktisch an operative Ebenen delegiert?

9 Prüffeld Reporting: Lagebild und Eskalationslogik

Ohne strukturiertes Reporting bleibt Cyber- und Informationssicherheit unsichtbar oder taucht nur bei Vorfällen und Medienberichten auf. Ein klares Lagebild schliesst den Regelkreis zwischen Governance, Risiko und operativen Funktionen.

Bestandteile eines reifen Reporting-Ansatzes sind:

- regelmässige Berichte zu Risikolage, Vorfällen, Massnahmen, Prüfungen und Risikotrends (Key Risk Indicators)
- adressatengerechte Aufbereitung für operative Ebenen, Management und Aufsichtsgremien
- definierte Schwellenwerte und Kriterien für Eskalationen
- getrennte Kennzahlen zum Umsetzungsstand von Massnahmen, zur Risikolage (z.B. kritische Systeme ohne aktuellen Patchstand) und zur Wirksamkeit der Kontrollen (z.B. Mean Time to Detect/Respond, Ergebnisse von Tests und Übungen). Ein als erledigt gemeldeter Massnahmenstatus allein belegt keine Wirksamkeit
- Verknüpfung von Reporting-Erkenntnissen mit strategischer Planung und Ressourcenpriorisierung, sodass Lagebilder direkt in Massnahmen- und Budgetentscheide einfliessen

Gesetzliche und aufsichtsrechtliche Meldepflichten erfordern klare interne Meldewege und Eskalationskriterien. Behörden und Organisationen, die nach Art. 74b ISG meldepflichtig sind, müssen Cyberangriffe, welche die Voraussetzungen von Art. 74d ISG erfüllen, innert 24 Stunden nach ihrer Entdeckung dem BACS melden. Ausnahmen regelt die Cybersicherheitsverordnung (CSV). Hinzu kommen die Meldung von Verletzungen der Datensicherheit mit voraussichtlich hohem Risiko nach Art. 24 DSG sowie die jeweils anwendbaren sektorspezifischen Pflichten. Zuständigkeiten und Abläufe müssen die Einhaltung der jeweiligen Fristen ermöglichen. Ein gutes Lagebild kombiniert quantitative Kennzahlen mit qualitativer Einordnung.

Prüfnachweis: Vorzulegen sind die letzten Berichte an Geschäftsleitung und Aufsichtsgremium sowie für einen eskalationspflichtigen Sachverhalt die Zeitachse bis zur Befassung der zuständigen Ebene. Ist für entscheidungsbedürftige Themen keine Behandlung nachvollziehbar, ist nicht belegt, dass das Reporting die Steuerung erreicht.

9.1 Leitfragen für die Führung

- Erhalten Geschäftsleitung und Aufsichtsgremien ein Lagebild, das sie zu konkreten Priorisierungs- und Ressourcenentscheiden befähigt, oder eher eine Ansammlung technischer Kennzahlen?
- Wie stellen wir sicher, dass kritische Risiken, Vorfälle und Trendverschlechterungen schnell genug die richtige Führungsebene erreichen und dass Eskalationen nicht an Bereichsgrenzen hängen bleiben?
- Inwieweit verbindet unser Reporting Cyber-/Informationssicherheit mit Themen wie Outsourcing, Architektur, BCM und Risikoappetit, oder berichten wir diese Felder noch zu stark isoliert?

10 Kumulation von Kontrollschwächen als systemischer Risikotreiber

Isoliert betrachtet erscheinen einzelne Kontrollschwächen oft moderat. Kritisch werden sie dort, wo mehrere Schwächen entlang eines Prozesses oder einer Wertschöpfungskette zusammenwirken und so zu einem systemischen Risikotreiber werden.

Typische Hinweise auf Kumulation:

- Einzelbefunde tauchen in mehreren Prüffeldern mit ähnlichen Mustern auf, zum Beispiel unklare Verantwortlichkeiten in Governance, Outsourcing und BCM
- «Moderate» Risiken betreffen dieselben Prozesse, Daten oder Dienstleister
- wiederkehrende Feststellungen bleiben über mehrere Prüfzyklen hinweg offen oder werden in verschiedene Projekte «delegiert»
- Notfallübungen, Vorfälle oder Störungen bestätigen bekannte Schwächen, ohne dass die Governance-Architektur angepasst wurde

Diese Beobachtungen sind zunächst Hinweise. Der Nachweis einer gemeinsamen Wirkung entsteht erst durch den Bezug auf eine konkrete Leistung, eine gemeinsame Abhängigkeit oder ein nachvollziehbares Szenario. Auch wiederholt offene Feststellungen belegen für sich genommen noch keine Risikokumulation.

Wie aus Hinweisen ein Nachweis wird, zeigt ein vereinfachtes, fiktives Beispiel: Für eine Fachanwendung mit sensiblen Kundendaten sind Administratorkonten seit Jahren nicht rezertifiziert. Sie ermöglichen auch Zugriff auf nicht inventarisierte Dateiablagen mit Datenkopien, deren Schutzanforderungen und Überwachung ungeklärt sind. Die Notfallplanung ist genehmigt, getestet wurde aber nur die Wiederherstellung der Produktivdatenbank. Im Szenario eines kompromittierten Administratorkontos greifen die Befunde aus IAM, Informationswerten und BCM ineinander: Der Angreifer kann auf Anwendung und Datenkopien zugreifen und den Betrieb beeinträchtigen. Ob die unterstützte Leistung vollständig wieder aufgenommen werden kann, ist nicht belegt. Bei getrennter Bewertung kann das gemeinsame Schadenspotenzial für Vertraulichkeit und Leistungsfortführung unterschätzt werden.

Kernprinzip

Reife Governance rechnet mit Kumulation und richtet Prüfansatz, Steuerungsarchitektur und Berichterstattung darauf aus.

11 Anwendung des Prüfrasters

Das Prüfraster dient Leitungs- und Aufsichtsgremien sowie den verantwortlichen Fachfunktionen als Bezugsrahmen, um Prüfungsergebnisse und Risiken übergreifend einzuordnen. Prüfauftrag, Prüfprogramm und Methodik bestimmen weiterhin Umfang und Tiefe der konkreten Beurteilung.

Typische Einsatzformen sind: Self-Assessments zur Standortbestimmung je Prüffeld, die Vorbereitung auf Audits, regulatorische Prüfungen und Vor-Ort-Kontrollen bei externen Dienstleistern sowie die Strukturierung der Berichterstattung an Leitung und Aufsicht entlang der sieben Prüffelder. So lassen sich Lücken im Zusammenspiel der Bausteine identifizieren und Verbesserungsmassnahmen gezielt priorisieren.

Im Kern unterstützt das Prüfraster drei Leitfragen:

1. Haben wir ein klares Bild unserer Cyber- und Informationssicherheits-Architektur über alle sieben Prüffelder hinweg?
2. Wo kumulieren Kontrollschwächen zu systemischer Verwundbarkeit, und wie machen wir dies sichtbar?
3. Wie stellen wir sicher, dass Governance, Risiko, Lieferantensteuerung, IAM, Schutzbedarfsmanagement, Resilienz und Reporting als Gesamtsystem funktionieren, nicht nur auf dem Papier, sondern im gelebten Betrieb?

Fazit

Cyber- und Informationssicherheit entscheidet sich nicht an einzelnen Tools oder Projekten allein, sondern an der Qualität der Governance- und Steuerungsarchitektur. Einzelne technische Kontrollen können für sich wirksam sein. Ihre Schutzwirkung für die Organisation als Ganzes hängt aber davon ab, ob Rollen, Entscheidwege, Risikoappetit und Steuerungsmechanismen konsistent ausgestaltet sind und das Zusammenspiel dieser Elemente aktiv geführt wird.

Systemische Verwundbarkeit entsteht oft nicht durch das Fehlen einzelner Kontrollen, sondern durch die Kumulation moderater Kontrollschwächen entlang von Wertschöpfungs-, Daten- und Entscheidungsprozessen. Besonders kritisch wird es dort, wo mehrere Prüffelder isoliert betrachtet «ausreichend» erscheinen, ihr Zusammenspiel jedoch inkonsistent bleibt.

Resilienz in der Cyber- und Informationssicherheit ist daher keine technische Spezialdisziplin, sondern Ausdruck von Führungs- und Organisationsqualität. Sie zeigt sich in klarer Verantwortung, konsistenter Risikosteuerung, beherrschten Lieferketten, nachvollziehbarer Schutzbedarfs- und Berechtigungslogik, gelebter Wiederherstellungsfähigkeit und einem Lagebild, das Entscheide ermöglicht.

Abschliessender Gedanke

Die entscheidende Frage ist nicht, ob eine Organisation die richtigen Kontrollen implementiert hat, sondern ob ihre Governance-Architektur erkennt, wenn das Zusammenspiel dieser Kontrollen brüchig wird.

Quellen

Bundesamt für Cybersicherheit BACS, Halbjahresbericht 2026/1, 24. August 2026.

Bundesamt für Cybersicherheit BACS, Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain, 7. März 2024.

Bundesamt für Sicherheit in der Informationstechnik BSI, Die Lage der IT-Sicherheit in Deutschland 2025.

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1), insbesondere Art. 8, 9 und 24.

Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG, SR 128), Bestimmungen zur Meldepflicht für Cyberangriffe.

CrowdStrike, External Technical Root Cause Analysis – Channel File 291, 6. August 2024.

Cybersicherheitsverordnung (CSV), in Kraft seit 1. April 2025, Ausführungsbestimmungen zur Meldepflicht für Cyberangriffe.

Eidgenössische Finanzmarktaufsicht FINMA, Aufsichtsmitteilung 03/2024: Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, 7. Juni 2024, insbesondere Abschnitte 2.1 und 2.2.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Schlussbericht und Empfehlungen in Sachen Xplain AG, 25. April 2024.

inside-it.ch, «An einer Katastrophe vorbeigeschlittert», 19. März 2025.

ISO 22301:2019, Business continuity management systems – Requirements, sowie ISO/TS 22317:2021 zur Business-Impact-Analyse.

ISO/IEC 27001:2022, Information security management systems – Requirements, insbesondere Anhang A 5.12, sowie ISO/IEC 27002:2022, Information security controls.

Nachrichtendienst des Bundes NDB, Sicherheit Schweiz 2026. Lagebericht des Nachrichtendienstes des Bundes, 25. Juni 2026.

National Institute of Standards and Technology NIST, Special Publication 800-207, Zero Trust Architecture, August 2020.

Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), insbesondere Art. 28 und 32.

Hinweis

Dieses Whitepaper gibt ausschliesslich meine persönliche fachliche Einschätzung wieder und steht nicht für eine Behörde oder Aufsicht. Es darf unverändert weitergegeben und mit Quellenangabe zitiert werden. Kommerzielle Verwertung und Bearbeitungen bedürfen meiner vorherigen Zustimmung.



Fragen und Austausch willkommen

carsten@carsten-beck.ch

Alle Beiträge der Reihe

carsten-beck.ch/publikationen

linkedin.com/in/carstenbeck-grc