STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

Leitfaden Risikomanagement-massnahmen (CSG/CSV)



Inhaltsverzeichnis

Einleitung 4

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen 6
   1.1 Risikoanalyse 6
   1.2 Sicherheitsrichtlinie 7
   1.3 Überprüfungsplan der Netz- und Informationssysteme 8
   1.4 Ressourcenmanagement/Asset Management 9
   1.5 Personal, Cyberhygiene und Schulungen 10
   1.6 Bewertung der Wirksamkeit der Risikomanagementmassnahmen 12

2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement) 13
   2.1 Identifikation und Authentifikation 13
   2.2 Privilegierte Konten 14
   2.3 Systeme und Anwendungen zur Systemadministration 15
   2.4 Multi-Faktor-Authentifizierung 16

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung 17
   3.1 Sicherheit der Netz- und Informationssysteme 17
   3.2 Fernzugriff 18
   3.3 Konfigurationsmanagement 19
   3.4 Netzwerksegmentierung 20
   3.5 Kryptographie 21
   3.6 Updatemanagement 22
   3.7 Schwachstellenmanagement 23

4. Sicherheitsmassnahmen bei Erwerb und Entwicklung 24
   4.1 Beschaffungsmanagement 24
   4.2 Projekt- und Entwicklungsmanagement 25
   4.3 Änderungsmanagement 26

5. Sicherheit der Lieferkette 27
   5.1 Verzeichnis der Lieferanten, Anbieter und Diensteanbieter 27
   5.2 Beziehungen zu unmittelbaren Anbietern und Diensteanbietern 28
   5.3 Leistungsvereinbarungen mit Lieferanten, Anbietern und Diensteanbietern 29

6. Physische Sicherheit 30

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung) 31
   7.1 Protokollierung und Monitoring 31
   7.2 Erkennung, Korrelation und Analyse 32
   7.3 Sicherheitsvorfallsreaktion 33
   7.4 Sicherheitsvorfallsmeldung 34
   7.5 Sicherheitsvorfallsanalyse 35

8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall 36
   8.1 Unterstützende Versorgungsleistungen 36
   8.2 Betriebskontinuitätsmanagement 37
   8.3 Notfallmanagement 38
   8.4 Backup-Management 39

9. Krisenmanagement 40

Änderungsverzeichnis

Datum	Version	Änderung	Autor
21.09.2026	0.3	Erstfassung	SCS
24.11.2026	1.0	Fassung nach öffentlicher Konsultation	SCS

Disclaimer

Dieser Leitfaden versteht sich als Unterstützung für die praktische Umsetzung und erhebt keinen Anspruch auf Vollständigkeit oder uneingeschränkte Korrektheit. Die Risikobeschreibungen sind im jeweiligen Kontext zu prüfen und die Massnahmen gegebenenfalls an die konkreten Gegebenheiten anzupassen.

Einleitung

Mit dem revidierten Cyber-Sicherheitsgesetz (CSG)[1] wurde die Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)[2] in Liechtenstein national umgesetzt. Das aktuelle CSG trat am 1. Februar 2025 mit der entsprechenden Cyber-Sicherheitsverordnung (CSV)[3] in Kraft.

Der gegenständliche Leitfaden erläutert die Anforderungen für wesentliche und wichtige Einrichtungen die sich aus Art. 4 CSG in Verbindung mit Art. 3 CSV samt Anhang ergeben und dient als Auslegungshilfe und der Orientierung. Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismässige technische, operative und organisatorische Massnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen.[4]

Die zu ergreifenden Massnahmen müssen unter Berücksichtigung des Stands der Technik, der Umsetzungskosten und gegebenenfalls der einschlägigen europäischen und internationalen Normen ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist. Bei der Bewertung sind das Ausmass der Risikoexposition und die Grösse der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen, einschliesslich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.[5]

Welche Themen die ergriffenen Massnahmen zumindest umfassen müssen, regelt Art. 4 Abs. 3 CSG. Die Massnahmen müssen etwa auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen.

Der Anhang der CSV konkretisiert diese gesetzliche Pflicht. So sieht dieser für wesentliche und wichtige Einrichtungen vor, dass jedenfalls Risikomanagementmassnahmen in folgenden Bereichen zu ergreifen sind:

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen;
2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement);
3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung;
4. Sicherheitsmassnahmen bei Erwerb und Entwicklung;
5. Sicherheit der Lieferkette;
6. Physische Sicherheit;
7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung);
8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall;
9. Krisenmanagement.

Bei der Implementierung der konkreten technischen, operativen und organisatorischen Massnahmen betrachten und berücksichtigen die wesentlichen und wichtigen Einrichtungen jeweils die eigenen Netz- und Informationssysteme sowie das Ergebnis der eigenen Risikoanalyse. Es steht jeder wesentlichen und wichtigen Einrichtung frei, für die sie betreffenden identifizierten individuellen Risiken, geeignete und verhältnismässige, dem jeweiligen Risiko angemessene, Risikomanagementmassnahmen zu ergreifen.

Die Verbindlichkeit ist nicht absolut im Sinn einer ausnahmslosen Pflicht, jede einzelne Massnahme des Anhangs der CSV umzusetzen. Hält eine wesentliche oder wichtige Einrichtung es etwa für nicht angemessen, nicht anwendbar oder nicht durchführbar, bestimmte im Anhang vorgesehene technische, operative und organisatorische Risikomanagementmassnahmen zu ergreifen, hat die betreffende Einrichtung eine

[1] Cyber-Sicherheitsgesetz vom 5. Dezember 2024, LGBl. 2025 Nr. 111, https://gesetze.li/konso/2025111000
[2] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie); https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555.
[3] Cyber-Sicherheitsverordnung vom 14. Januar 2025, LGBl. 2025 Nr. 163, https://gesetze.li/konso/2025163000.
[4] Art. 4 Abs. 1 CSG.
[5] Art. 4 Abs. 2 CSG.

diesbezügliche Begründung in verständlicher Weise zu dokumentieren.[6] Die ab Kapitel 1 aufgeführten zeitlichen Intervalle zur Überprüfung von Risikomanagementmassnahmen stellen keine verbindlichen Vorgaben dar, sondern sind unter Berücksichtigung des jeweiligen Risikoprofils anzuwenden und als Best-Practice-Empfehlungen zu verstehen.

Stellt eine Einrichtung fest, dass sie den vorgeschriebenen Massnahmen nicht nachkommt, ergreift sie unverzüglich alle erforderlichen, angemessenen und verhältnismässigen Korrekturmassnahmen.[7] In diesem Zusammenhang wird darauf hingewiesen, dass geeignete kombinierte Übungen insbesondere in den Bereichen der Kapitel 7, 8 und 9 zur Erfüllung mehrerer Anforderungen beitragen können, sofern die relevanten Prüfziele adressiert und die erzielten Ergebnisse transparent und nachvollziehbar dokumentiert werden.

Eine angemessene und aktuelle Dokumentation der verwendeten Netz- und Informationssysteme sowie der implementierten Risikomanagementmassnahmen ist für einen sicheren Betrieb der Netz- und Informationssysteme unerlässlich. Die erforderliche Dokumentation kann im Rahmen eines bestehenden Managementsystems, beispielsweise eines Information Security Management System nach ISO/IEC 27001, geführt werden. Ungeachtet dessen ist im Einzelfall sicherzustellen und nachzuweisen, dass sämtliche Anforderungen des CSG und der CSV erfüllt werden, da eine ISO/IEC-27001-Zertifizierung allein keine vollständige CSG-Konformität begründet.

Die Genauso bedeutsam für den Schutz gegen Cyberbedrohungen ist die gelebte Praxis. Nur beides zusammen, vollständige Dokumentation und gelebte Praxis, kann den Schutz der Netz- und Informationssysteme angemessen sicherstellen.

Die Durchführungsverordnung (EU) 2024/2690[8] konkretisiert die Anforderungen der NIS-2-Richtlinie für bestimmte Arten von Einrichtungen im Bereich der digitalen Infrastruktur. Sie gilt für: DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen (CDN-Anbieter), Anbieter verwalteter Dienste (Managed Service Provider, MSP), Anbieter verwalteter Sicherheitsdienste (Managed Security Service Provider, MSSP), Anbieter von Online-Marktplätzen, Online-Suchmaschinen, Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter. Für diese Einrichtungen legt die erwähnte Verordnung technischen und methodischen Anforderungen der in Art. 21 Abs. 2 der NIS-2-Richtlinie bzw. Art. 4 Abs. 3 CSG genannten Massnahmen fest. Auch für andere wesentliche und wichtige Einrichtungen, die nicht unmittelbar in den Anwendungsbereich der Verordnung fallen, können die dort konkretisierten Anforderungen als Orientierung für die angemessene und verhältnismässige Umsetzung der Risikomanagementmassnahmen herangezogen werden.

[6] Art. 3 Abs. 2 CSV.
[7] Art. 4 Abs. 5 CSG.
[8] Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmassnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt; https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2690.

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.1 Risikoanalyse

Eine Risikoanalyse der Netz- und Informationssysteme ist periodisch durchzuführen, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu ermitteln, zu beurteilen und zu behandeln. Die Ergebnisse der Risikoanalyse sind zu dokumentieren. Auf Grundlage der Ergebnisse ist ein Risikobehandlungsplan zu erstellen, umzusetzen und zu überwachen.

Referenz CSG	Art. 4 Abs. 3 Bst. a CSG Konzepte in Bezug auf die Risikoanalyse für Informationssysteme

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 1.1 (Konzept für die Sicherheit von Netz- und Informationssystemen)
	  ○ Ziff. 2.1 (Risikomanagementrahmen)
	• ISO/IEC 27001:2022, Pkt. 6.1.2, 6.1.3, 7.5, 9.1, 9.3, 10.1
	• BSI IT-Grundschutz[9], ISMS.1, ORP.5, DER.3.1, DER.3.2, DER.4
	• IKT-Minimalstandard[10], ID.RA-1 bis ID.RA-6

Risiko	Die Risikoanalyse bildet die Grundlage für die Festlegung, Priorisierung und Ausgestaltung sämtlicher Cybersicherheits-Risikomanagementmassnahmen. Das CSG schreibt keine bestimmte Methode hinsichtlich der Risikoanalyse vor. Die Ergebnisse sind jedoch nachvollziehbar zu dokumentieren. Durch das Fehlen einer Risikoanalyse steigt die Wahrscheinlichkeit von Sicherheitsvorfällen, da die mit dem Betrieb der Netz- und Informationssysteme verbundenen Risiken nicht ermittelt (identifiziert), beurteilt und behandelt werden können. Das Ergebnis wäre eine ineffiziente oder fehlgeleitete IT-Sicherheit.
Checkliste	☐ Eine Risikoanalyse der Netz- und Informationssysteme wurde durchgeführt; ☐ Die Ergebnisse der Risikoanalyse sind dokumentiert; ☐ Die Risiken für die Sicherheit von Netz- und Informationssystemen wurden ermittelt, beurteilt und behandelt; ☐ Ein Risikobehandlungsplan wurde erstellt und umgesetzt; ☐ Die Aktivitäten im Zusammenhang mit dem Risikobehandlungsplans werden überwacht;
Periodisch zu überprüfen	Die Risikoanalyse der Netz- und Informationssysteme ist periodisch durchzuführen. Das CSG legt dazu keinen Zeitraum fest, doch ist eine jährliche Überprüfung in der Regel angemessen und verhältnismässig. Längere Intervalle sind in begründeten Fällen möglich. Die Ergebnisse der letzten Risikoanalyse sollten ebenfalls zeitnah in jenen Fällen überprüft werden, wenn sich die Betriebsumstände oder die eingesetzten Netz- und Informationssysteme sowie verwendete Infrastruktur wesentlich ändern, z. B. beim Einsatz neuer Technologien.

[9] IT-Grundschutz-Kompendium, Edition 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1

[10] Version Mai 2023, mit Update NIST SP 800-53 Rev. 5 und ISO 27001:2022, https://www. bacs.admin.ch/de/ikt-minimalstandards.

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.2 Sicherheitsrichtlinie

Eine Sicherheitsrichtlinie ist zu erstellen, periodisch zu überprüfen und gegebenenfalls zu aktualisieren.

Referenz CSG	Art. 4 Abs. 3 Bst. a CSG Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme Art. 5 Abs. 1 Bst. a CSG Leitungsorgane wesentlicher und wichtiger Einrichtungen sind verpflichtet, die ergriffenen Risikomanagementmassnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 1 (Konzept für die Sicherheit von Netz- und Informationssystemen)
	  ○ Ziff. 2 (Konzept für das Risikomanagement);
	• ISO/IEC 27001:2022, 5.1, 5.2, 7.3, 7.4, 7.5, 9.3, 10.1
	• BSI IT-Grundschutz, ISMS.1, ORP.1, ORP.5
	• IKT-Minimalstandard, ID.GV-1 bis ID.GV-4

Risiko	In der Sicherheitsrichtlinie werden die Regeln, Verfahren und Massnahmen festgelegt, die eine Einrichtung implementiert, um ihre Netz- und Informationssysteme vor Bedrohungen und Sicherheitsvorfällen zu schützen. Sie stellt sicher, dass die Risikomanagementmassnahmen innerhalb der Einrichtung einheitlich, klar und aktuell sind. Dadurch werden Fehlentscheidungen sowie technische, operative und organisatorische Schwachstellen und Sicherheitslücken infolge fehlender Governance reduziert. Alle Regelungsinhalte können in einer einzigen, monolithischen, Richtlinie zusammengefasst werden. In der Praxis wird die Sicherheitsrichtlinie mehrheitlich in verschiedene Dokumente aufgeteilt, um die Lesbarkeit und Verständlichkeit zu erhöhen. Die Sicherheitsrichtlinie ist durch die Leitungsorgane der Einrichtung zu billigen und im Unternehmen entsprechend zu kommunizieren.
Checkliste	☐ Eine Sicherheitsrichtlinie wurde erstellt; ☐ Die Sicherheitsrichtlinie wurde von den Leitungsorganen der Einrichtung gebilligt; ☐ Die Sicherheitsrichtlinie ist in der Einrichtung kommuniziert; ☐ Diese Sicherheitsrichtlinie wird periodisch überprüft und ggf. aktualisiert;
Periodisch zu überprüfen	Die Häufigkeit, mit der die Sicherheitsrichtlinie aktualisiert werden muss, hängt von verschiedenen Faktoren ab, wie bspw. von technologischen Entwicklungen, neuen Bedrohungen und Veränderungen in den Geschäftsprozessen. Jährliche Überprüfungen und Aktualisierungen stellen in der Regel sicher, dass die Sicherheitsrichtlinie wirksam bleibt und den jeweils aktuellen Anforderungen entspricht.

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.3 Überprüfungsplan der Netz- und Informationssysteme	
Die periodische Überprüfung der Sicherheit der Netz- und Informationssysteme ist zu planen und durchzuführen.	
Referenz CSG	Art. 4 Abs. 3 Bst. a CSG Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 2.2 (Überwachung der Einhaltung);
	  ○ Ziff. 2.3 (Unabhängige Überprüfung der Netz- und Informationssicherheit)
	• ISO/IEC 27001:2022, Pkt. 7.5, 9.1, 9.2, 9.3, 10.1, 10.2
	• BSI IT-Grundschutz, ISMS.1, DER.3.1, DER.3.2
	• IKT-Minimalstandard, PR.IP-7, PR.IP-8, DE.DP-2, DE.DP-3, RS.IM-1, RC.IM-1

Risiko	Die periodischen Überprüfungen der Sicherheit der Netz- und Informationssysteme zielen darauf ab, die Anwendung, Wirksamkeit und Angemessenheit der implementierten Risikomanagementmassnahmen zu validieren. Konkrete Anforderungen ergeben sich aus der Risikoanalyse. Es existiert ein Prüfplan, der zumindest folgende Punkte enthält: • Umfang und Prüfinhalte (inkl. Prüfungstiefe) • Prüfmethode (Audit, Schwachstellenscan, Penetrationstest usw.) • Festlegung von Prüfintervallen • Verantwortlichkeiten • Terminplanung • Ableitung und Nachverfolgung von Massnahmen • Dokumentation, wie Prüfungsergebnis festgehalten werden soll Ohne Prüfplan bleiben Schwachstellen, Sicherheitsmängel, Fehlkonfigurationen und Kontrolllücken unentdeckt. Audits erfolgen reaktiv statt risikobasiert. Zudem ist eine kontinuierliche Verbesserung nicht möglich. Das Sicherheitsniveau stagniert oder verschlechtert sich. Die Massnahme reduziert insbesondere das Risiko eines schleichenden Sicherheitsverlusts aufgrund fehlender Überwachung und Kontrolle.
Checkliste	☐ Die Sicherheit der Netz- und Informationssysteme wird periodisch überprüft; ☐ Für die Überprüfung der Sicherheit der Netz- und Informationssysteme existiert ein Prüfplan;
Periodisch zu überprüfen	Jährlicher Prüfplan, wobei kritische Netz- und Informationssysteme häufiger zu prüfen sind. Nach wesentlichen Änderungen oder Sicherheitsvorfällen sind die Prüfprozesse zu überprüfen und bei Bedarf anzupassen.

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.4 Ressourcenmanagement/Asset Management

Ein vollständiges, genaues, aktuelles und kohärentes Inventar der Netz- und Informationssysteme und anderer zugehöriger Anlagen und Werte, die die Abläufe und die Dienste der betreffenden Einrichtung unterstützen, ist zu führen. Alle Ressourcen, die erforderlich sind, um die Sicherheit von Netz- und Informationssystemen zu gewährleisten, sind im Hinblick auf kurz-, mittel- und langfristige Kapazitätsanforderungen einzuplanen und auf einem festgelegten Schutzniveau sicherzustellen.

Referenz CSG	Art. 4 Abs. 3 Bst. i CSG Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 12 (Anlagen- und Wertemanagement) • ISO/IEC 27001:2022, Pkt. 6.1.2, 6.2, 7.1, 7.5, 8.1, 9.1, 9.3 • ISO/IEC 27002:2022, Pkt. 5.9, 5.10, 5.11, 5.12, 5.13, 5.14 • BSI IT-Grundschutz, ORP.1, OPS.1.1.7, SYS.1.1, SYS.2.1, SYS.3.2.1, SYS.3.2.2, NET.1.1, NET.3.4, INF.1, INF.2 • IKT-Minimalstandard, ID.AM-1 bis ID.AM-6
Risiko	Unvollständige Inventare verhindern ein wirksames Schwachstellen-, Patch-, Zugriffs- und Notfallmanagement. Durch fehlende Transparenz ist die Risikoanalyse unvollständig und fehlerbehaftet. Durch mangelnde Ressourcenplanung kann in der Regel das festgelegte Sicherheitsniveau nicht erreicht werden, da die für den sicheren Betrieb der Netz- und Informationssysteme benötigten finanziellen, personellen sowie technischen Ressourcen nicht bereitgestellt werden können.
Checkliste	☐ Ein Inventar der Netz- und Informationssysteme ist vorhanden; ☐ Das Inventar enthält neben den Netz- und Informationssystemen, ebenso andere zugehörige Anlagen und Werte, die die Abläufe und die Dienste der betreffenden Einrichtung unterstützen; ☐ Das Inventar ist vollständig, genau, aktuell und kohärent (widerspruchsfrei); ☐ Das Schutzniveau der Netz- und Informationssysteme ist festgelegt; ☐ Alle Ressourcen sind identifiziert, die erforderlich sind, um das festgelegte Sicherheitsniveau von Netz- und Informationssystemen zu gewährleisten; ☐ Kurz-, mittel- und langfristige Kapazitätsanforderungen sind eingeplant;

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.5 Personal, Cyberhygiene und Schulungen

Sicherheitsrelevante Aspekte, einschliesslich allfälliger Zuverlässigkeitsüberprüfungen, sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen. Regelmässig sind Sensibilisierungsmassnahmen und Schulungen in den Bereichen der Cybersicherheit und Cyberhygiene bei den Mitarbeitenden durchzuführen.

Referenz CSG	Art. 4 Abs. 3 Bst. g CSG Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit; Art. 5 Abs. 1 Bst. b CSG Leitungsorgane wesentlicher und wichtiger Einrichtungen sind verpflichtet, an Schulungen teilzunehmen und allen Mitarbeitern regelmässig entsprechende Schulungen anzubieten.

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 8.1 (Sensibilisierungsmassnahmen und grundlegende Verfahren im Bereich der Cyberhygiene)
	  ○ Ziff. 8.2 (Sicherheitsschulungen)
	  ○ Ziff. 10.1 (Sicherheit des Personals)
	• ISO/IEC 27001:2022, Pkt. 5.3, 7.2, 7.3, 7.4, 7.5, 9.1, 10.1
	• ISO/IEC 27002:2022, Pkt. 6.1 bis 6.8
	• BSI IT-Grundschutz, ORP.2, ORP.3, ORP.4, ORP.5
	• IKT-Minimalstandard, PR.AT-1 bis PR.AT-5

Risiko	Die Einrichtung stellt sicher, dass Mitarbeitende in sensiblen Funktionen eine geeignete und verhältnismässige Zuverlässigkeitsüberprüfung durchlaufen. Beispielsweise wenn Mitarbeitende berechtigt sind, über einen Fern- oder direkten Zugriff auf für die Einrichtung kritische Netz- und Informationssysteme zuzugreifen. Bei der Ausgestaltung und Durchführung von Zuverlässigkeitsüberprüfungen sind insbesondere die datenschutzrechtlichen sowie arbeitsrechtlichen Anforderungen einzuhalten. Die Anforderung zur Berücksichtigung sicherheitsrelevanter Aspekte im Personalwesen, einschliesslich allfälliger Zuverlässigkeitsüberprüfungen, zielt insbesondere auf das Risiko von Insider-Handlungen, Missbrauch privilegierter Zugänge und ungeeigneten Personen in sicherheitskritischen Funktionen ab. Die Schulungen zielen darauf ab, ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. Die Vorgabe zu Sensibilisierungsmassnahmen und Schulungen adressiert das Risiko menschlicher Fehler, unsicherer Verhaltensweisen und einer unzureichenden Cyberhygiene der Mitarbeitenden.
Checkliste	☐ Sicherheitsrelevante Aspekte sind in den Prozessen im Personalwesen berücksichtigt und umgesetzt; ☐ Mitarbeitende in sensiblen Funktionen haben eine geeignete und verhältnismässige Zuverlässigkeitsüberprüfung durchlaufen; ☐ Mitarbeitende besuchen regelmässig Sensibilisierungsmassnahmen und Schulungen in den Bereichen der Cybersicherheit und Cyberhygiene; ☐ Leitungsorgane nehmen regelmässig an Schulungen teil;

Periodisch zu überprüfen	Alle Mitarbeitenden nehmen regelmässig, in der Regel jährlich, an Schulungen teil. Die Schulungsinhalte sind aktuell bzw. zielgruppengerecht aufbereitet.

1. Risikoanalyse und Sicherheit von Netz- und Informationssystemen

1.6 Bewertung der Wirksamkeit der Risikomanagementmassnahmen

Konzepte liegen vor und Verfahren legen fest, um zu bewerten, ob die ergriffenen Risikomanagementmassnahmen im Bereich der Cybersicherheit wirksam umgesetzt sind.

Referenz CSG	Art. 4 Abs. 3 Bst. f CSG Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit; Art. 5 Abs. 1 Bst. a CSG Leitungsorgane sind verpflichtet, die Umsetzung der ergriffenen Risikomanagementmassnahmen im Bereich der Cybersicherheit zu überwachen.
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 7 (Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit); • ISO/IEC 27001:2022, Pkt. 6.1.3, 7.5, 9.1, 9.2, 9.3, • ISO/IEC 27002:2022, Pkt. 5.35, 5.36 und 8.34 • BSI IT-Grundschutz, DER.3.1, DER.3.2, DER.4 • IKT-Minimalstandard, DE.CM-1 bis DE.CM-8, DE.DP-5, RS.IM-2, RC.IM-2
Risiko	Massnahmen können formal bestehen, während ihre tatsächliche Wirksamkeit jedoch unbekannt bleibt. Ohne Kennzahlen fehlen Steuerung und Nachweisbarkeit. Konzepte und Verfahren zur Bewertung der Wirksamkeit sollen verhindern, dass unwirksame, unvollständig umgesetzte oder veraltete Risikomanagementmassnahmen ein falsches Sicherheitsgefühl vermitteln und bestehende Risiken unerkannt fortbestehen.
Checkliste	☐ Konzepte zur Bewertung der Wirksamkeit der Risikomanagementmassnahmen liegen vor; ☐ Die Bewertung umfasst sämtliche Risikomanagementmassnahmen im Bereich der Cybersicherheit; ☐ Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmassnahmen wurden festgelegt;
Periodisch zu überprüfen	Die Konzepte und Verfahren werden regelmässig auf Aktualität und Anwendbarkeit überprüft und bei Bedarf angepasst. Die Überprüfungsintervalle richten sich nach dem Risiko, haben in der Regel jährlich zu erfolgen oder nach wesentlichen Änderungen und Sicherheitsvorfällen.

2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement)

2.1 Identifikation und Authentifikation

Es sind Verfahren umzusetzen und Technologien einzusetzen, die die logische und physische Kontrolle des Zugangs zu den Netz- und Informationssystemen mittels Identifikation und Authentifikation von Nutzern und Diensten gewährleisten. Die Zuweisungen von Zugangs- und Zugriffsrechten sind periodisch zu überprüfen und gegebenenfalls anzupassen.

Referenz CSG	Art. 4 Abs. 3 Bst. i CSG Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690:
	  o Ziff. 11 (Zugriffskontrolle);
	  o Ziff. 13.3 (Perimeter und physische Zutrittskontrolle)
	• ISO/IEC 27002:2022, Pkt. 5.15 bis 5.18
	• BSI IT-Grundschutz, ORP.4, NET.3.4
	• IKT-Minimalstandard, PR.AC-1, PR.AC-6, PR.AC-7;

Risiko	Die mangelnde Umsetzung führt zu einem grundlegenden Kontrollverlust darüber, wer, was, wann und mit welchen Rechten auf Netz- und Informationssysteme zugreift. Unzureichende Identifikation und Authentifikation sowie nicht regelmässig überprüfte Zugriffsrechte erhöhen das Risiko von unbefugtem Zugriff, Identitätsmissbrauch, Datenabfluss, Manipulationen und nicht nachvollziehbaren Sicherheitsvorfällen. Dadurch werden Vertraulichkeit, Integrität und Verfügbarkeit der Netz- und Informationssysteme gefährdet. Zur Identifikation richtet die Einrichtung entsprechend einem definierten und dokumentierten Verfahren eindeutige Konten für Benutzer oder für automatisierte Prozesse ein, die auf Netz- und Informationssysteme zugreifen müssen. Es ist ein Verfahren für den Benutzer-Lebenszyklus zu definieren. Ein regelmässiger Überprüfungsprozess ist zu etablieren. Es werden Technologien eingesetzt, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten.
Checkliste	☐ Es sind Verfahren umgesetzt, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten. ☐ Es werden Technologien eingesetzt, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten. ☐ Zugewiesene Benutzerberechtigungen werden periodisch überprüft und angepasst.
Periodisch zu überprüfen	Die Prüffrequenz sollte risikobasiert festgelegt werden und je nach Risikoausprägung und Stabilität der IT-Landschaft zwischen quartalsweisen und jährlichen Prüfungen liegen.

2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement)

2.2 Privilegierte Konten

Administrative Zugangs- und Zugriffsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.

Referenz CSG	Art. 4 Abs. 3 Bst. i CSG Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 11.3 (Privilegierte Konten und Systemverwaltungskonten); • ISO/IEC 27002:2022, Pkt. 8.18, 8.2 • BSI IT-Grundschutz, ORP.4, OPS.1.1.2 • IKT-Minimalstandard, PR.AC-4, PR.AC-5, PR.AC-6;
Risiko	Privilegierte Konten sind ein bevorzugtes Ziel von Angreifern, weil sie vielfach Zugriff auf zentrale Systeme, Verzeichnisse, Administrationswerkzeuge, Sicherheitslösungen, Datenbanken oder Cloud-Umgebungen ermöglichen. Wenn solche Konten nicht konsequent nach dem Minimalrechtsprinzip vergeben und regelmässig überprüft werden, entsteht ein erhöhtes Risiko für: • Manipulation von Sicherheits- und Protokolldaten; • Unterbrechung kritischer Netz- und Informationssysteme; • Datenabfluss; • Ausweitung eines Cyberangriffs auf weitere Netz- und Informationssysteme.
Checkliste	☐ Personen mit administrativen oder privilegierten Zugangs- und Zugriffsrechten sind bekannt; ☐ Es sind Verfahren umgesetzt, die sicherstellen, dass administrative Zugangs- und Zugriffsrechte nach dem Minimalrechtsprinzip zugewiesen werden; ☐ Diese Zuweisungen werden periodisch überprüft und ggf. angepasst;
Periodisch zu überprüfen	Die Prüffrequenz muss risikobasiert festgelegt, dokumentiert und begründet werden. Beispielsweise sind hochkritische (z. B. Notfall-/Break-Glass-Konten) und externe privilegierte Rechte mindestens halbjährlich zu prüfen.

2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement)

2.3 Systeme und Anwendungen zur Systemadministration

Systeme und Anwendungen zur Systemadministration sind ausschliesslich für Tätigkeiten zum Zweck der Systemadministration zu verwenden.

Referenz CSG	Art. 4 Abs. 3 Bst. i CSG Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 11.4 (Systemverwaltungssysteme); • ISO/IEC 27002:2022, Pkt. 5.37, 8.2, 8.18, 8.9 • BSI IT-Grundschutz, OPS.1.1.1, OPS.1.1.2, OPS.1.1.7, SYS.1.1, SYS.2.1 • IKT-Minimalstandard, PR.IP-1 bis PR.IP-3; PR.MA-1; PR.MA-2
Risiko	Systeme und Anwendungen zur Systemadministration ermöglichen vollumfänglichen Zugriff auf die Netz- und Informationssysteme einer Einrichtung. Werden diese Systeme und Anwendungen unzureichend abgesichert und erlangt eine unberechtigte Person Zugriff auf diese Werkzeuge, kann sie damit weitreichende Berechtigungen erhalten und sämtliche Schutzziele der Informationssicherheit gefährden. Eine Möglichkeit der Absicherung zur Minimierung dieses Risikos ist die strikte Trennung zwischen administrativen Tätigkeiten und normaler Nutzung auf Ebene der Systeme und Anwendungen. Dies mit dem Ziel, Missbrauch administrativer Privilegien zu verhindern. Dazu beschränken und kontrollieren die betreffenden Einrichtungen die Nutzung von Systemen und Anwendungen zur Systemadministration im Einklang mit Ziff. 2.2. (Privilegierte Konten).
Checkliste	☐ Die Systeme und Anwendungen zur Systemadministration sind bekannt; ☐ Die Systeme und Anwendungen zur Systemadministration werden ausschliesslich für Tätigkeiten zum Zweck der Systemadministration verwendet;

2. Berechtigungsmanagement (Identitäts- und Zugriffsmanagement)

2.4 Multi-Faktor-Authentifizierung

Authentifizierungsmethoden sind der Kritikalität der Netz- und Informationssysteme angemessen. Dies umfasst unter anderem eine Multi-Faktor-Authentifizierung.

Referenz CSG	Art. 4 Abs. 3 Bst. k CSG Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 11.7 (Multi-Faktor-Authentifizierung); • ISO/IEC 27002:2022, Pkt. 5.17, 8.5 • BSI IT-Grundschutz, ORP.4, NET.3.3, NET.3.4, SYS.2.1, SYS.3.2.1 • IKT-Minimalstandard, PR.AC-7
Risiko	Ohne risikoadäquate Multi-Faktor-Authentifizierung besteht ein erhöhtes Risiko von unberechtigten Zugriffen auf Netz- und Informationssysteme.
Checkliste	☐ Die Kritikalität der Netz- und Informationssysteme wurde beurteilt; ☐ Je nach Kritikalität der Netz- und Informationssysteme wurden angemessene Authentifizierungsmethoden festgelegt; ☐ Angemessene Authentifizierungsmethoden sind implementiert; ☐ Bei entsprechender Kritikalität der Netz- und Informationssysteme ist eine Multi-Faktor-Authentifizierung vorhanden;

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.1 Sicherheit der Netz- und Informationssysteme

Technische, operative und organisatorische Massnahmen zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen. Diese Massnahmen umfassen unter anderem den Schutz gegen Schadsoftware.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 6 (Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen)
	  ○ Ziff. 13 (Sicherheit des Umfelds und physische Sicherheit)
	• ISO/IEC 27002:2022, Pkt. 5.37, 8.1, 8.7, 8.15, 8.16, 8.19;
	• BSI IT-Grundschutz, OPS.1.1.1, OPS.1.1.4, OPS.1.1.5, SYS.1.1, SYS.2.1, NET.3.2, NET.3.4;
	• IKT-Minimalstandard, DE.CM-4, DE.CM-5

Risiko	Ohne sicheren Systembetrieb von Netz- und Informationssystemen und wirksamen Schutz vor Schadsoftware steigt die Wahrscheinlichkeit von Kompromittierungen, Betriebsunterbrechungen, Datenverlust und Sicherheitsvorfällen.
Checkliste	☐ Technische, operative und organisatorische Massnahmen zur Gewährleistung eines sicheren Systembetriebs der Netz- und Informationssysteme wurden festgelegt; ☐ Technische, operative und organisatorische Massnahmen zur Gewährleistung eines sicheren Systembetriebs der Netz- und Informationssysteme wurden eingeführt/implementiert; ☐ Diese Massnahmen umfassen den Schutz gegen Schadsoftware; ☐ Die Überprüfungsintervalle sind definiert;
Periodisch zu überprüfen	Die Überprüfungsintervalle sind risikobasiert festzulegen. Beispielsweise kann eine allgemeine Überprüfung (Management-Review, internes Audit) jährlich erfolgen, wohingegen eine Überprüfung der eingesetzten Massnahmen zur Gewährleistung eines sicheren Systembetriebs von kritischen Netz- und Informationssystemen (Domain Controller, Backups usw.) in kürzeren Abständen zu erfolgen hat.

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.2 Fernzugriff

Fernzugriffe sind eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 6.4 (Änderungsmanagement, Reparatur und Wartung);
	  ○ Ziff. 6.7 (Netzsicherheit)
	• ISO/IEC 27002:2022, Pkt. 6.7, 5.15, 5.18, 8.5, 8.20, 8.21, 8.22;
	• BSI IT-Grundschutz, OPS.1.2.5, NET.3.3, NET.3.4, IND.3.2, INF.2;
	• IKT-Minimalstandard, PR.AC-3, PR.MA-2;

Risiko	Eine mangelhafte Absicherung von Fernzugriffen führt zu Kontrollverlust über externe Zugänge zu Netz- und Informationssystemen. Unzureichend abgesicherte oder uneingeschränkt vergebene Fernzugriffsrechte erhöhen das Risiko von unbefugtem Zugriff, Missbrauch privilegierter Zugänge, Datenabfluss und der Kompromittierung der Netz- und Informationssysteme.
Checkliste	☐ Prozesse zur Vergabe und Verwaltung von Fernzugriffen sind etabliert; ☐ Fernzugriffsrechte werden eingeschränkt nach dem Minimalrechtsprinzip vergeben; ☐ Fernzugriffe werden zeitlich beschränkt vergeben; ☐ Vergebene Fernzugriffsrechte werden periodisch überprüft; ☐ Fernzugriffsrechte werden bei Bedarf angepasst; ☐ Die Sicherheit des Fernzugriffs ist gewährleistet;
Periodisch zu überprüfen	Sofern für Fernzugriffsrechte kein Ablaufdatum definiert ist, sollte deren Notwendigkeit mindestens einmal pro Quartal überprüft werden.

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.3 Konfigurationsmanagement	
Netz- und Informationssysteme sind sicher zu konfigurieren. Die Konfigurationen sind zu dokumentieren. Die Dokumentation ist aktuell zu halten.	
Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 6.3 (Konfigurationsmanagement); • ISO/IEC 27002:2022, Pkt. 8.9, 8.32; • BSI IT-Grundschutz, OPS.1.1.2, OPS.1.1.3, OPS.1.1.7, SYS.1.1, SYS.2.1, NET.1.2, NET.3.1, NET.3.4; • IKT-Minimalstandard, PR.IP-1, PR.IP-3, PR.PT-3
Risiko	Die mangelnde Umsetzung führt zu einem Kontrollverlust über die sicherheitsrelevanten Einstellungen der Netz- und Informationssysteme. Ursachen für Sicherheitsvorfälle können unter anderem unsichere oder nicht ausreichend gehärtete Systemkonfigurationen sein. Fehlkonfigurationen erhöhen das Risiko von Ausfällen der Netz- und Informationssysteme.
Checkliste	☐ Die Konfigurationsmöglichkeiten der Netz- und Informationssysteme sind bekannt; ☐ Die Netz- und Informationssysteme sind sicher konfiguriert / gehärtet; ☐ Die Konfigurationen der Netz- und Informationssysteme sind nachvollziehbar dokumentiert; ☐ Die Dokumentation der Konfigurationen ist aktuell;
Periodisch zu überprüfen	Die Überprüfungsintervalle des Konfigurationsmanagements sind risikobasiert festzulegen. Die sichere Konfiguration von Netz- und Informationssystemen sollte jedoch mindestens einmal jährlich überprüft werden. Bei wesentlichen Änderungen der Systeme oder nach Sicherheitsvorfällen ist eine anlassbezogene Überprüfung vorzunehmen. Die Konfigurationsdokumentation ist laufend aktuell zu halten.

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.4 Netzwerksegmentierung	
Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.	
Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 6.8 (Netzwerksegmentierung); • ISO/IEC 27002:2022, Pkt. 8.22 • BSI IT-Grundschutz, NET.1.1, NET.1.2, NET.3.1, NET.3.2, NET.3.3, NET.3.4, IND.1; • IKT-Minimalstandard, PR.AC-5
Risiko	Ohne angemessene Netzwerksegmentierung kann aus einem einzelnen kompromittierten System schnell ein organisationsweiter Sicherheitsvorfall entstehen, da Netzwerke nicht ausreichend nach Schutzbedarf, Kritikalität und Vertrauenszonen getrennt sind und Angreifer sich somit leichter von einem System zu anderen Systemen bewegen können. Auch Schadsoftware kann sich ungehindert über Netzbereiche hinweg verbreiten.
Checkliste	☐ Der Schutzbedarf der Netz- und Informationssysteme ist festgelegt; ☐ Die Netzwerke sind abhängig vom Schutzbedarf segmentiert; ☐ Die Segmentierung erfolgt innerhalb der Netz- und Informationssysteme;

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.5 Kryptographie

Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.

Referenz CSG	Art. 4 Abs. 3 Bst. h CSG Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 9 (Kryptografie); • ISO/IEC 27002:2022, Pkt. 8.24 • BSI IT-Grundschutz, CON.1, CON.8, NET.3.2, NET.3.3, SYS.1.1, SYS.2.1; • Technische Richtlinie, BSI TR-02102-1[11] • IKT-Minimalstandard, PR.DS-2, PR.DS-6
Risiko	Der Einsatz kryptographischer Verfahren schützt die Vertraulichkeit, Authentizität und Integrität von Informationen während der Speicherung, Verarbeitung oder Übertragung. Auf Netz- und Informationssysteme soll nicht unbefugt zugegriffen, verarbeitete Daten eingesehen oder verändert werden können.
Checkliste	☐ Vertraulichkeit, Authentizität und Integrität von Informationen sind sichergestellt; ☐ Kryptographische Verfahren und Technologien werden eingesetzt; ☐ Die eingesetzten kryptographischen Verfahren und Technologien sind angemessen und wirksam;

[11] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2026-01 vom 23. Januar 2026, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html.

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.6 Updatemanagement

Verfügbare Sicherheitsupdates sind zeitnah zu testen, zu bewerten und einzuspielen.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 6.4 (Änderungsmanagement, Reparatur und Wartung)
	  ○ Ziff. 6.6 (Sicherheitspatch-Management)
	• ISO/IEC 27002:2022, Pkt. 8.8, 8.19, 8.32
	• BSI IT-Grundschutz, OPS.1.1.3, OPS.1.1.6, SYS.1.1, SYS.2.1, NET.1.2, NET.3.1;
	• IKT-Minimalstandard, PR.IP-2, PR.IP-7, PR.IP-12, DE.CM-8

Risiko	Die mangelnde Umsetzung führt dazu, dass bekannte Sicherheitslücken und Schwachstellen in Netz- und Informationssystemen bestehen bleiben. Nicht zeitnah getestete, bewertete oder eingespielte Sicherheitsupdates erhöhen das Risiko der Kompromittierung von Netz- und Informationssystemen und Systemausfällen.
Checkliste	☐ Ein Inventar der Netz- und Informationssysteme ist vorhanden;[12] ☐ Verfügbarkeit von Sicherheitsupdates der eingesetzten Netz- und Informationssysteme wird überwacht; ☐ Verfügbare Sicherheitsupdates werden zeitnah getestet und bewertet; ☐ Verfügbare Sicherheitsupdates werden zeitnah eingespielt;

[12] Siehe ebenso Checkliste zu Pkt. 1.4 (Ressourcenmanagement/Asset Management)

3. Sicherheitsmassnahmen im laufenden Betrieb und bei der Wartung

3.7 Schwachstellenmanagement

Mögliche Datenlecks sowie öffentlich bekannte Sicherheitslücken in eingesetzter Software und Hardware sind zu identifizieren. Gegen Verwundbarkeiten und bekannte Schwachstellen der Netz- und Informationssysteme sind im laufenden Betrieb geeignete Massnahmen zu ergreifen.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 6.5 (Sicherheitsprüfung);
	  ○ Ziff. 6.6 (Sicherheitspatch-Management);
	  ○ Ziff. 6.10 (Behandlung und Offenlegung von Schwachstellen);
	• ISO/IEC 27002:2022, Pkt. 5.7, 8.8, 8.16, 8.19
	• BSI IT-Grundschutz, OPS.1.1.3, OPS.1.1.6, DER.1, DER.2.1, NET.1.2, NET.3.1, NET.3.4
	• IKT-Minimalstandard, PR.IP-12, DE.CM-8, ID.RA-1, ID.RA-2

Risiko	Fehlendes Schwachstellenmanagement führt dazu, dass Verwundbarkeiten und Schwachstellen in den eingesetzten Netz- und Informationssystemen unerkannt oder unbehandelt bleiben. Verwundbarkeiten und Schwachstellen können von Angreifern ausgenutzt werden. Die Wahrscheinlichkeit erfolgreicher Cyberangriffe und Sicherheitsvorfälle steigt signifikant. Ohne systematisches Schwachstellenmanagement bleiben bekannte Angriffsvektoren offen. Dadurch steigt das Risiko, dass Angreifer bekannte Schwachstellen für die initiale Kompromittierung von Netz- und Informationssystemen ausnutzen.
Checkliste	☐ Ein Inventar der eingesetzten Hard- und Software ist vorhanden;[13] ☐ Verfügbare Sicherheitsupdates werden zeitnah eingespielt;[14] ☐ Verwundbarkeiten und Schwachstellen in der eingesetzten Hard- und Software werden zeitnah identifiziert; ☐ Gegen Verwundbarkeiten und bekannte Schwachstellen in der eingesetzten Hard- und Software werden bis zur Verfügbarkeit von Sicherheitsupdates ausgleichende und geeignete Massnahmen ergriffen.

[13] Vgl. dazu Checkliste zu Pkt. 1.4 (Ressourcenmanagement/Asset Management)
[14] Siehe ebenso Checkliste zu Pkt. 3.6

4. Sicherheitsmassnahmen bei Erwerb und Entwicklung

4.1 Beschaffungsmanagement

Es sind Verfahren und Massnahmen für das Management der Risiken festzulegen und periodisch zu überprüfen, die sich aus der Beschaffung von IKT-Diensten oder IKT-Produkten ergeben, die auf die Sicherheit der Netz- und Informationssysteme der betreffenden Einrichtungen einen Einfluss haben.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang zur Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 6.1 (Sicherheitsmassnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten);
	  ○ Ziff. 6.4 (Änderungsmanagement, Reparatur und Wartung);
	  ○ Ziff. 6.5 (Sicherheitsprüfung);
	  ○ Ziff. 6.7 (Netzsicherheit);
	  ○ Ziff. 13 (Sicherheit des Umfelds und physische Sicherheit);
	• ISO/IEC 27002:2022, Pkt. 5.19, 5.20, 5.21, 5.23, 8.30
	• BSI IT-Grundschutz, ORP.5, OPS.2.2, OPS.2.3, NET.1.1, NET.3.1, NET.3.4, IND.1
	• IKT-Minimalstandard, PR.IP-2, PR.MA-1, PR.IP-12, PR.PT-3, ID.SC-1 bis ID.SC-5

Risiko	Die mangelnde Umsetzung führt dazu, dass Risiken aus der Beschaffung von IKT-Diensten und IKT-Produkten unzureichend berücksichtigt werden. Dadurch können unsichere Produkte und Dienstleistungen sowie Lieferanten mit unzureichendem Sicherheitsniveau die Sicherheit der Netz- und Informationssysteme beeinträchtigen und neue Angriffsflächen schaffen. Werden Sicherheitsanforderungen nicht bereits im Beschaffungsprozess berücksichtigt, werden Risiken häufig erst nach der Einführung erkannt, wenn deren Behebung mit erheblichem Aufwand oder mit zusätzlichen Risiken verbunden ist.
Checkliste	☐ IKT-Dienste und IKT-Produkte, die auf die Sicherheit der Netz- und Informationssysteme Einfluss haben, sind bekannt; ☐ Für die Risiken, die sich aus der Beschaffung von IKT-Diensten oder IKT-Produkten ergeben, wurden Verfahren und Massnahmen für das Management dieser Risiken festgelegt; ☐ Die Verfahren und Massnahmen werden periodisch überprüft;
Periodisch zu überprüfen	Die Verfahren und Massnahmen für das Management der Risiken sollten mindestens einmal jährlich überprüft werden. Bei Beschaffungen mit erhöhtem Risiko für die Sicherheit der Netz- und Informationssysteme, wesentlichen Änderungen der Bedrohungslage oder der Einführung kritischer IKT-Dienste oder IKT-Produkte, sollte die Überprüfung anlassbezogen erfolgen.

4. Sicherheitsmassnahmen bei Erwerb und Entwicklung

4.2 Projekt- und Entwicklungsmanagement

Die Sicherheit von Netz- und Informationssystemen ist in den Prozessen des Projektmanagements, insbesondere bei der Entwicklung, entsprechend zu berücksichtigen.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  o Ziff. 6.4 (Änderungsmanagement, Reparatur und Wartung)
	  o Ziff. 6.2 (Sicherer Entwicklungszyklus)
	  o Ziff. 6.7 (Netzsicherheit);
	• ISO/IEC 27002:2022, Pkt. 5.8, 8.25, 8.26, 8.27, 8.28, 8.29, 8.30
	• BSI IT-Grundschutz, CON.8, CON.10, APP.7
	• IKT-Minimalstandard, PR.IP-1, PR.IP-2, PR.IP-7, PR.IP-12, PR.DS-7

Risiko	Die Anforderung verankert Security-by-Design im Projektmanagement. Die mangelnde Umsetzung führt dazu, dass Sicherheitsaspekte bei Projekten und der (Weiter-)Entwicklung von Netz- und Informationssystemen unzureichend berücksichtigt werden. Dadurch werden Schwachstellen oder unsichere Architektur- oder Designentscheidungen bereits bei der Entstehung von Systemen nicht entdeckt. Die Risiken werden häufig erst im laufenden Betrieb sichtbar, wenn ihre Behebung zumeist mit erheblichem Aufwand verbunden ist.
Checkliste	☐ Prozesse für das Projektmanagement sind festgelegt; ☐ Die Sicherheit der Netz- und Informationssysteme wird in den Prozessen des Projektmanagements berücksichtigt (Security by Design); ☐ Prozesse für die Entwicklung von Netz- und Informationssystemen oder deren Elemente (Komponenten) sind festgelegt; ☐ Die Sicherheit der Netz- und Informationssysteme wird in den Entwicklungsprozessen berücksichtigt;

4. Sicherheitsmassnahmen bei Erwerb und Entwicklung

4.3 Änderungsmanagement

Die Sicherheit der Netz- und Informationssysteme ist in den Prozessen des Änderungsmanagements entsprechend zu berücksichtigen. Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden dokumentiert, bewertet, getestet, genehmigt, umgesetzt und überprüft.

Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 6.4 (Änderungsmanagement, Reparatur und Wartung); • ISO/IEC 27002:2022, Pkt. 8.9, 8.19, 8.32 • BSI IT-Grundschutz, OPS.1.1.3, OPS.1.1.6, NET.1.2, NET.3.4 • IKT-Minimalstandard, PR.IP-3, PR.IP-7, PR.IP-12, PR.MA-1
Risiko	Änderungen an Netz- und Informationssystemen haben kontrolliert und unter ausreichender Berücksichtigung der Sicherheitsanforderungen zu erfolgen. Nicht dokumentierte, unzureichend bewertete oder getestete Änderungen können zu Verwundbarkeiten führen sowie Fehlkonfigurationen oder Betriebsstörungen verursachen. Dadurch steigt das Risiko von Sicherheitsvorfällen und Systemausfällen.
Checkliste	☐ Prozesse für das Änderungsmanagement sind festgelegt und dokumentiert; ☐ Die Sicherheit der Netz- und Informationssysteme wird in den Prozessen des Änderungsmanagements berücksichtigt; ☐ Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden dokumentiert und bewertet; ☐ Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden getestet, genehmigt und umgesetzt; ☐ Änderungen an den Netz- und Informationssystemen, insbesondere auch sicherheitsrelevante Konfigurationsänderungen, werden überprüft;

5. Sicherheit der Lieferkette

5.1 Verzeichnis der Lieferanten, Anbieter und Diensteanbieter

Es ist ein Verzeichnis zu führen und laufend zu aktualisieren, welches die Lieferanten, die unmittelbaren Anbieter und Diensteanbieter samt Kontaktdaten enthält.

Referenz CSG	Art. 4 Abs. 3 Bst. d CSG Sicherheit der Lieferkette, einschliesslich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 5.2 (Verzeichnis der Anbieter und Diensteanbieter); • ISO/IEC 27002:2022, Pkt. 5.19, 5.21, 5.22, 5.23 • BSI IT-Grundschutz, OPS.2.2, OPS.2.3, ORP.5 • IKT-Minimalstandard, ID.SC-1, ID.SC-2
Risiko	Die Beziehungen zu Lieferanten, Anbietern und Diensteanbietern können nur wirksam gesteuert werden, wenn der Einrichtung bekannt ist, wer sicherheitsrelevante Leistungen erbringt. Ein unvollständiges oder veraltetes Verzeichnis führt dazu, dass Abhängigkeiten, Zuständigkeiten und Risiken in der Lieferkette nicht erkannt werden.
Checkliste	☐ Ein Verzeichnis der Lieferanten, Anbieter und Diensteanbieter ist vorhanden; ☐ Das Verzeichnis ist vollständig und aktuell; ☐ Das Verzeichnis beinhaltet zumindest die Kontaktdaten sowie eine Beschreibung der erbrachten Dienstleistung(en);
Periodisch zu überprüfen	Das Verzeichnis ist laufend zu aktualisieren und Änderungen sind umgehend einzupflegen. Eine periodische Überprüfung wird jährlich empfohlen, ist jedoch mindestens alle zwei Jahre durchzuführen.

5. Sicherheit der Lieferkette

5.2 Beziehungen zu unmittelbaren Anbietern und Diensteanbietern	
Anforderungen an unmittelbare Anbieter und Diensteanbieter für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.	
Referenz CSG	Art. 4 Abs. 3 Bst. d CSG Sicherheit der Lieferkette, einschliesslich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern Art. 4 Abs. 4 CSG Die Einrichtungen berücksichtigen bei der Erwägung geeigneter Massnahmen (nach Abs. 3 Bst. d) bei den einzelnen unmittelbaren Anbietern und Diensteanbietern die spezifischen Schwachstellen; die Gesamtqualität der Produkte sowie die Cybersicherheitspraxis, einschliesslich die Sicherheit der Entwicklungsprozesse.

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 5.1 (Konzept für die Sicherheit der Lieferkette);
	  ○ Ziff. 6.7 (Netzsicherheit)
	• ISO/IEC 27002:2022, Pkt. 5.19, 5.20, 5.21, 5.22, 5.23
	• BSI IT-Grundschutz, OPS.2.2, OPS.2.3, ORP.5
	• IKT-Minimalstandard, ID.SC-3, ID.SC-4, ID.SC-5

Risiko	Anforderungen an Lieferanten, unmittelbare Anbieter und Diensteanbieter müssen festgelegt und regelmässig überprüft werden. Beispielsweise können fehlende oder unzureichende Sicherheitsanforderungen dazu führen, dass Lieferanten, Anbieter oder Diensteanbieter unsichere Zugänge betreiben oder Sicherheitsmassnahmen auf einem unzureichenden Niveau umsetzen. Dadurch steigt das Risiko von Sicherheitsvorfällen, unbefugten Zugriffen und der Kompromittierung von Netz- und Informationssystemen.
Checkliste	☐ (Sicherheits-)Anforderungen an unmittelbare Anbieter und Diensteanbieter für den Betrieb von Netz- und Informationssystemen sind festgelegt; ☐ (Sicherheits-)Anforderungen an unmittelbare Anbieter und Diensteanbieter für den Zugang zu Netz- und Informationssystemen sind festgelegt; ☐ (Sicherheits-)Anforderungen an unmittelbare Anbieter und Diensteanbieter für den Zugriff auf Netz- und Informationssystemen sind festgelegt; ☐ Sämtliche (Sicherheits-)Anforderungen werden periodisch überprüft;
Periodisch zu überprüfen	Die (Sicherheits-)Anforderungen sowie die Einhaltung dieser Anforderungen durch die unmittelbaren Anbieter und Diensteanbieter sind periodisch, in der Regel mindestens jährlich, zu überprüfen.

5. Sicherheit der Lieferkette

5.3 Leistungsvereinbarungen mit Lieferanten, Anbietern und Diensteanbietern	
Die Leistungsvereinbarungen mit Lieferanten, unmittelbaren Anbietern und Diensteanbietern sind periodisch zu überprüfen und zu überwachen.	
Referenz CSG	Art. 4 Abs. 3 Bst. d CSG Sicherheit der Lieferkette, einschliesslich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 5.1 (Konzept für die Sicherheit der Lieferkette); • ISO/IEC 27002:2022, Pkt. 5.20, 5.22, 5.23 • BSI IT-Grundschutz, OPS.2.2, OPS.2.3, ORP.5 • IKT-Minimalstandard, ID.SC-3, ID.SC-5, RS.CO-4
Risiko	Leistungsvereinbarungen mit Lieferanten, Anbietern und Diensteanbietern müssen regelmässig überprüft und überwacht werden, damit die vereinbarten Leistungen ordnungsgemäss erbracht werden. Nicht überprüfte oder unzureichend überwachte Leistungen können dazu führen, dass Sicherheitsmängel unentdeckt bleiben. Dadurch steigt das Risiko von Sicherheitsvorfällen und Betriebsstörungen. Ebenso ergeben sich aufgrund fehlender Nachweise erhöhte Betriebs- sowie Compliance-Risiken.
Checkliste	☐ Leistungsvereinbarungen mit Lieferanten, Anbietern und Diensteanbietern sind vorhanden; ☐ Die Leistungsvereinbarungen werden periodisch (inhaltlich) überprüft; ☐ Die Einhaltung der mit Lieferanten, Anbietern und Diensteanbietern vereinbarten Leistungen wird überwacht
Periodisch zu überprüfen	Die Leistungsvereinbarungen sind periodisch, zumindest in der Regel jährlich, zu überprüfen. Die Einhaltung der vereinbarten Leistungen ist laufend zu überwachen.

6. Physische Sicherheit

Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor Naturkatastrophen oder unbefugtem Zutritt und Zugang, ist zu gewährleisten.	
Referenz CSG	Art. 4 Abs. 3 Bst. e CSG Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung von Schwachstellen. Art. 4 Abs. 3 Bst. i CSG Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen.

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 13 (Sicherheit des Umfelds und physische Sicherheit)
	  ○ Ziff. 13.2 (Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds)
	• ISO/IEC 27002:2022, Pkt. 7.1 bis 7.14
	• BSI IT-Grundschutz, INF.1, INF.2, INF.5, INF.6, INF.7, INF.12, INF.13
	• IKT-Minimalstandard, PR.AC-2, PR.IP-5, PR.PT-4

Risiko	Der physische Schutz von Netz- und Informationssystemen hat angemessen gewährleistet zu sein. Fehlende oder unzureichende Schutzmassnahmen gegen Naturereignisse sowie unbefugten Zutritt oder Zugang können zu Manipulationen, Diebstahl, Beschädigungen oder Ausfällen von Netz- und Informationssystemen führen.
Checkliste	☐ Netz- und Informationssysteme sind vor physischen Gefährdungen geschützt; ☐ Schutzmassnahmen gegen Naturereignisse (z. B. Feuer, Wasser, Stromausfall) sind umgesetzt; ☐ Der Zutritt zu den Netz- und Informationssystemen ist auf berechtigte Personen beschränkt; ☐ Der physische Zugang zu Netz- und Informationssystemen ist gegen unbefugte Nutzung geschützt;

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)

7.1 Protokollierung und Monitoring

Mechanismen zur Protokollierung und zum Monitoring von Aktivitäten in den Netz- und Informationssystemen sind umzusetzen.

Referenz CSG	Art. 4 Abs. 3 Bst. b CSG Bewältigung von Sicherheitsvorfällen;
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 3.2 (Überwachung und Protokollierung); • ISO/IEC 27002:2022, Pkt. 8.15, 8.16, 8.17 • BSI IT-Grundschutz, OPS.1.1.5, DER.1, NET.1.2 • IKT-Minimalstandard, PR.PT-1, DE.CM-1, DE.CM-2, DE.CM-6, DE.CM-7
Risiko	Aktivitäten in Netz- und Informationssystemen sind angemessen zu protokollieren und zu überwachen, sodass sicherheitsrelevante Ereignisse frühzeitig erkannt und ggf. nachvollzogen werden können. Fehlende oder unzureichende Protokollierung und Überwachung können dazu führen, dass Cyberbedrohungen oder -angriffe unentdeckt bleiben oder Sicherheitsvorfälle nicht oder nur unzureichend aufgeklärt werden können. Bei der Ausgestaltung und Umsetzung zur Protokollierung und zum Monitoring von Aktivitäten sind insbesondere die datenschutzrechtlichen sowie arbeitsrechtlichen Anforderungen einzuhalten.
Checkliste	☐ Die Protokollierungs- und Monitoringmechanismen sind umgesetzt; ☐ Die zu protokollierenden Aktivitäten in den jeweiligen Netz- und Informationssystemen sind festgelegt; ☐ Die Protokolldaten sind für die Auswertung, Untersuchung und Aufklärung nach Sicherheitsvorfällen geeignet;

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)

7.2 Erkennung, Korrelation und Analyse

Mechanismen zur Erkennung und Bewertung von Sicherheitsvorfällen, gegebenenfalls durch die Korrelation und Analyse der ermittelten Protokolldaten, sind umzusetzen.

Referenz CSG	Art. 4 Abs. 3 Bst. b CSG Bewältigung von Sicherheitsvorfällen;

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 3.2 (Überwachung und Protokollierung)
	  ○ Ziff. 3.4 (Bewertung und Klassifizierung von Ereignissen)
	• ISO/IEC 27002:2022, Pkt. 5.25, 8.15, 8.16
	• BSI IT-Grundschutz, DER.1, DER.2.1, OPS.1.1.5
	• IKT-Minimalstandard, DE.AE-1 bis DE.AE-5, DE.CM-1 bis DE.CM-3, DE.DP-2

Risiko	Sicherheitsrelevante Ereignisse und Auffälligkeiten in den Protokolldaten müssen erkannt werden, damit auf Cyberbedrohungen und -angriffe sowie Sicherheitsvorfälle so rasch als möglich reagiert werden kann. Fehlende oder unzureichende Mechanismen zur Erkennung können dazu führen, dass Cyberbedrohungen und -angriffe, verdächtige Aktivitäten oder sicherheitsrelevante Zusammenhänge unentdeckt bleiben. Dadurch steigt das Risiko von Sicherheitsvorfällen aufgrund verspäteter Reaktion auf Cyberbedrohungen und -angriffe oder andere sicherheitsrelevante Ereignisse. Bei der Ausgestaltung und Umsetzung zur Korrelation und Analyse von Protokolldaten sind insbesondere die datenschutzrechtlichen sowie arbeitsrechtlichen Anforderungen einzuhalten.
Checkliste	☐ Mechanismen zur Erkennung und Bewertung von Sicherheitsvorfällen sind umgesetzt; ☐ Vorhandene Protokolldaten werden *(falls erforderlich)* zur Erkennung und Bewertung von Sicherheitsvorfällen korreliert und analysiert; ☐ Die Korrelation und Analyse der ermittelten Protokolldaten ist geeignet, Sicherheitsvorfälle zu erkennen oder zu bewältigen;

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)

7.3 Sicherheitsvorfallsreaktion

Prozesse zur Reaktion auf Sicherheitsvorfälle sind zu erstellen (Konzept für die Bewältigung von Sicherheitsvorfällen), periodisch zu überprüfen, gegebenenfalls zu aktualisieren sowie zu erproben.

Referenz CSG	Art. 4 Abs. 3 Bst. b CSG Bewältigung von Sicherheitsvorfällen;
Referenzen zu Rechtsnormen und Standards	• Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 3.5 (Reaktion auf Sicherheitsvorfälle); • ISO/IEC 27002:2022, Pkt. 5.24, 5.26, 5.28 • BSI IT-Grundschutz, DER.2.1, DER.2.2, DER.2.3 • IKT-Minimalstandard, RS.RP-1, RS.CO-1 bis RS-CO-5
Risiko	Auf Sicherheitsvorfälle muss koordiniert und zeitnah reagiert werden können. Fehlende oder unzureichende Prozesse zur Reaktion auf Sicherheitsvorfälle können dazu führen, dass Sicherheitsvorfälle nicht rechtzeitig erkannt werden oder Gegenmassnahmen verspätet, ungeeignet oder unkoordiniert erfolgen. Dadurch steigt das Risiko einer Eskalation von Sicherheitsvorfällen, von Betriebsunterbrüchen sowie weiterer Schäden für die betroffene Einrichtung und Dritte.
Checkliste	☐ Prozesse zur Reaktion auf Sicherheitsvorfälle wurden erstellt (Konzept für die Bewältigung von Sicherheitsvorfällen); ☐ Das Konzept für die Bewältigung von Sicherheitsvorfällen ist aktuell; ☐ Die Prozesse zur Reaktion auf Sicherheitsvorfälle werden periodisch überprüft; ☐ Die Reaktion auf Sicherheitsvorfälle wird periodisch erprobt / geübt;
Periodisch zu überprüfen	Die Prozesse zur Reaktion auf Sicherheitsvorfälle sollten mindestens einmal jährlich auf Aktualität, Vollständigkeit und Wirksamkeit überprüft werden. Eine zusätzliche Überprüfung sollte anlassbezogen erfolgen, insbesondere nach wesentlichen Änderungen der Netz- und Informationssysteme, nach Sicherheitsvorfällen oder bei Veränderungen der Bedrohungslage. Übungen sollten ebenfalls mindestens einmal jährlich durchgeführt werden. Bei kritischen Netz- und Informationssystemen oder erhöhtem Risikoprofil kann eine häufigere Durchführung, beispielsweise halbjährlich, angemessen sein.

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)

7.4 Sicherheitsvorfallsmeldung

Prozesse zur internen und externen Meldung von Sicherheitsvorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.

Referenz CSG	Art. 4 Abs. 3 Bst. b CSG Bewältigung von Sicherheitsvorfällen; Art. 6 Abs. 1 in Verbindung mit Abs. 2 CSG Unverzügliche Meldung (innerhalb 24 Stunden) sowie weitere Fristen und Inhalte der Meldung
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 3.3 (Meldung von Ereignissen); • ISO/IEC 27002:2022, Pkt. 5.5, 5.24, 5.25, 6.8 • BSI IT-Grundschutz, DER.2.1, ORP.3 • IKT-Minimalstandard, RS.CO-2, RS.CO-3, DE.DP-4
Risiko	Sicherheitsvorfälle müssen intern und extern zeitnah gemeldet werden können. Fehlende oder unzureichende Meldeprozesse können dazu führen, dass sicherheitsrelevante Informationen nicht rechtzeitig an die zuständigen Stellen gelangen oder gesetzlichen Berichts- und Meldepflichten[15] nicht entsprochen wird. Dadurch steigt einerseits das Risiko einer verspäteten Reaktion auf Sicherheitsvorfälle sowie andererseits entstehen zusätzliche Betriebs- und Compliance-Risiken sowie die Gefahr von Reputationsschäden. Externe Meldungen sind über das auf der Website der SCS verfügbare Online-Meldeformular einzureichen.[16]
Checkliste	☐ Der Prozess für interne Meldungen von Sicherheitsvorfällen ist festgelegt; ☐ Der Prozess für externe Meldungen von Sicherheitsvorfällen ist festgelegt; ☐ Kriterien für die Meldung von Sicherheitsvorfällen sind vorhanden; ☐ Der interne und externe Meldeprozess wird *(regelmässig)* erprobt;

[15] Vgl. dazu Art. 6 CSG (Berichtspflichten).
[16] Siehe https://www.llv.li/de/landesverwaltung/stabsstelle-cybersicherheit/it-sicherheitsvorfall-melden

7. Bewältigung von Sicherheitsvorfällen (Erkennung und Bewältigung)

7.5 Sicherheitsvorfallsanalyse

Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.

Referenz CSG	Art. 4 Abs. 3 Bst. b CSG Bewältigung von Sicherheitsvorfällen;
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 3.6 (Überprüfungen nach Sicherheitsvorfällen); • ISO/IEC 27002:2022, Pkt. 5.25, 5.27, 5.28 • BSI IT-Grundschutz, DER.2.1, DER.2.2, DER.2.3, DER.3.1 • IKT-Minimalstandard, RS.AN-1, RS.AN-3, RS.AN-4
Risiko	Sicherheitsvorfälle müssen analysiert und bewertet werden, damit aus ihnen gelernt und die Cybersicherheit verbessert werden kann. Fehlende oder unzureichende Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen können dazu führen, dass Ursachen und Auswirkungen unentdeckt sowie sicherheitsrelevante Erkenntnisse ungenutzt bleiben. Dadurch steigt das Risiko wiederkehrender Sicherheitsvorfälle sowie das Fortbestehen von Verwundbarkeiten und Schwachstellen in den Netz- und Informationssystemen.
Checkliste	☐ Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen sind festgelegt; ☐ Prozesse zur Sammlung relevanter Informationen, insbesondere von Kompromittierungsindikatoren, zu oder nach Sicherheitsvorfällen sind festgelegt; ☐ Sicherheitsvorfälle werden hinsichtlich ihrer zugrunde liegenden Ursache, den (grenzüberschreitenden) Auswirkungen und Schweregrad bewertet; ☐ Aus den Analysen und Erkenntnissen vergangener Sicherheitsvorfälle werden Verbesserungsmassnahmen abgeleitet; ☐ Die Prozesse werden regelmässig überprüft und erprobt;
Periodisch zu überprüfen	Die Prozesse zur Analyse und Bewertung von Sicherheitsvorfällen und zur Sammlung relevanter Informationen sollten mindestens einmal jährlich überprüft werden. Eine zusätzliche Überprüfung sollte nach wesentlichen Sicherheitsvorfällen oder bei erheblichen Änderungen der Netz- und Informationssysteme erfolgen. Die praktische Erprobung der Prozesse sollte ebenfalls mindestens einmal jährlich stattfinden. Erkenntnisse aus Sicherheitsvorfällen und Übungen sind zu dokumentieren und für den kontinuierlichen Verbesserungsprozess zu nutzen.

8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall

8.1 Unterstützende Versorgungsleistungen

Verluste, Schäden oder Beeinträchtigungen von Netz- und Informationssystemen oder Unterbrechungen ihres Betriebs aufgrund des Ausfalls oder der Störung unterstützender Versorgungsleistungen sind zu verhindern.

Referenz CSG	Art. 4 Abs. 3 Bst. c CSG Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 13.1 (Unterstützende Versorgungsleistungen) • ISO/IEC 27002:2022, Pkt. 7.5, 7.11, 8.14 • BSI IT-Grundschutz, INF.2, INF.5, INF.12, INF.13 • IKT-Minimalstandard, PR.IP-5, RC.RP-1
Risiko	Die Verfügbarkeit von Netz- und Informationssystemen hängt von unterstützenden Versorgungsleistungen ab. Typische unterstützende Versorgungsleistungen sind: Stromversorgung (Notstromversorgung), Kühlung/Klimatisierung, Telekommunikations- und Internetanbindungen, Wasserversorgung (sofern relevant). Fehlende oder unzureichende Massnahmen zum Schutz vor Ausfällen oder Störungen dieser Versorgungsleistungen können zu Beeinträchtigungen oder Ausfällen von Netz- und Informationssystemen führen. Dadurch steigt das Risiko von Betriebsunterbrüchen und der eingeschränkten Verfügbarkeit von Diensten.
Checkliste	☐ Unterstützende Versorgungsleistungen für die Netz- und Informationssysteme sind identifiziert; ☐ Risiken aufgrund des Ausfalls oder der Störung unterstützender Versorgungsleistungen sind bekannt und berücksichtigt; ☐ Massnahmen zur Verhinderung des Ausfalls oder der Störung unterstützender Versorgungsleistungen sind umgesetzt; ☐ Unterstützende Versorgungsleistungen werden überwacht, gewartet und periodisch getestet;

8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall

8.2 Betriebskontinuitätsmanagement

Die Wiederherstellung der Netz- und Informationssysteme auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.

Referenz CSG	Art. 4 Abs. 3 Bst. c CSG Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690
	  ○ Ziff. 4.1 (Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs)
	  ○ Ziff. 4.2 (Backup-Sicherungs- und Redundanzmanagement)
	• ISO/IEC 27002:2022, Pkt. 5.29, 5.30
	• BSI IT-Grundschutz, DER.4, CON.3, ISMS.1
	• IKT-Minimalstandard, PR.IP-4, PR.IP-9, RC.RP-1

Risiko	Netz- und Informationssysteme müssen nach einem Sicherheitsvorfall auf einem festgelegten Qualitätsniveau wiederhergestellt werden können. Fehlende oder unzureichende Vorkehrungen zur Wiederherstellung können dazu führen, dass Netz- und Informationssysteme länger als notwendig nicht verfügbar sind oder nicht vollständig wiederhergestellt werden können. Dadurch steigt das Risiko von Betriebsunterbrüchen sowie finanziellen, betrieblichen und reputationsbezogenen Schäden.
Checkliste	☐ Ein Qualitätsniveau der Netz- und Informationssysteme für den Fall der Wiederherstellung nach einem Sicherheitsvorfall ist festgelegt; ☐ Die Wiederherstellung der Netz- und Informationssysteme nach einem Sicherheitsvorfall ist gewährleistet;

8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall

8.3 Notfallmanagement

Notfallpläne für die Aufrechterhaltung und Wiederherstellung des Betriebs nach einem Sicherheitsvorfall sind zu erstellen, anzuwenden, regelmässig zu bewerten und zu erproben.

Referenz CSG	Art. 4 Abs. 3 Bst. c CSG Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 4.1 (Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs) • ISO/IEC 27002:2022, Pkt. 5.29, 5.30, 8.13 • BSI IT-Grundschutz, DER.4, CON.3, ISMS.1 • IKT-Minimalstandard, PR.IP-9, RC.RP-1, RC.CO-1
Risiko	Zur Aufrechterhaltung und Wiederherstellung des Betriebs der Netz- und Informationssysteme sind Notfallpläne zu erstellen. Fehlende, unvollständige oder nicht erprobte Notfallpläne können dazu führen, dass bei einem Sicherheitsvorfall unkoordiniert, verspätet oder unzureichend reagiert wird. Dadurch steigt das Risiko von länger andauernden Betriebsunterbrüchen, Wiederherstellungsverzögerungen und erhöhten Schäden. <u>Abgrenzung zwischen 8.2 und 8.3:</u> • Pkt. 8.2 adressiert das Risiko, dass Systeme nicht wiederhergestellt werden können. • Pkt. 8.3 adressiert das Risiko, dass es keine ausreichende organisatorische Vorbereitung und Notfallplanung für die Wiederherstellung des Betriebs gibt.
Checkliste	☐ Notfallpläne für die Aufrechterhaltung des Betriebs der Netz- und Informationssysteme nach einem Sicherheitsvorfall sind vorhanden; ☐ Notfallpläne für die Wiederherstellung des Betriebs der Netz- und Informationssysteme nach einem Sicherheitsvorfall sind vorhanden; ☐ Die Notfallpläne werden bei Sicherheitsvorfällen angewendet; ☐ Die Notfallpläne werden regelmässig bewertet und erprobt;
Periodisch zu überprüfen	Die Notfallpläne sollten mindestens einmal jährlich bewertet werden. Zudem sollten sie nach wesentlichen Änderungen der Netz- und Informationssysteme, nach Sicherheitsvorfällen oder nach organisatorischen Änderungen überprüft und gegebenenfalls angepasst werden. Die Erprobung der Notfallpläne sollte ebenfalls mindestens einmal jährlich erfolgen. Bei besonders kritischen Systemen kann eine häufigere Durchführung von Übungen angemessen sein.

8. Aufrechterhaltung des Betriebs und Wiederherstellung nach einem Notfall

8.4 Backup-Management

Sicherungskopien sämtlicher relevanter Daten (einschliesslich Konfigurationsdaten) sind zu erstellen. Die Wiederherstellung innerhalb eines festzulegenden Zeitraums ist gewährleistet. Es werden regelmässig Integritätsprüfungen der Sicherungskopien durchgeführt.

Referenz CSG	Art. 4 Abs. 3 Bst. c CSG Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 4.2 (Backup-Sicherungs- und Redundanzmanagement) • ISO/IEC 27002:2022, Pkt. 8.13, 5.30 • BSI IT-Grundschutz, CON.3, OPS.1.1.7, SYS.1.8 • IKT-Minimalstandard, PR.IP-4, PR.IP-10, RC.RP-1
Risiko	Verarbeitete Daten und Konfigurationsdaten müssen regelmässig gesichert und innerhalb eines festgelegten Zeitraums wiederhergestellt werden können. Fehlende, unvollständige oder nicht überprüfte Sicherungskopien können zu Datenverlusten führen, oder dass Systeme nach einem Sicherheitsvorfall nicht rechtzeitig wiederhergestellt werden können. Ein zusätzlicher Aspekt der gegenständlichen Anforderung ist die Integritätsprüfung der Sicherungskopien. Vorhandene Backups sind wertlos, wenn sie beschädigt, manipuliert oder nicht wiederherstellbar sind.
Checkliste	☐ Sicherungskopien sämtlicher relevanter Daten (einschliesslich relevanter Konfigurationsdaten) werden erstellt; ☐ Für die Wiederherstellung der Daten und Konfigurationsdateien wurde ein Zeitraum festgelegt (RTO, Recovery Time Objective); ☐ Die Wiederherstellung der gesicherten Daten und Konfigurationsdateien ist gewährleistet; ☐ Dazu werden regelmässig Integritätsprüfungen (z. B. in Form von Wiederherstellungstests) der Sicherungskopien durchgeführt;
Periodisch zu überprüfen	Intervalle für Integritätsprüfungen von Sicherungskopien haben risikobasiert zu erfolgen. Die Wiederherstellbarkeit der Backups sollte mindestens einmal jährlich anhand eines Restore-Tests nachgewiesen werden. Bei kritischen Netz- und Informationssystemen oder häufigen Änderungen an den relevanten Daten kann eine häufigere Überprüfung angemessen sein.

9. Krisenmanagement

Rahmenbedingungen und Verfahren des Krisenmanagements sind für die Netz- und Informationssysteme vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen, zu erproben und periodisch zu überprüfen.	
Referenz CSG	Art. 4 Abs. 3 Bst. c CSG Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
Referenzen zu Rechtsnormen und Standards	• Anhang der Durchführungsverordnung (EU) 2024/2690 ○ Ziff. 4.3 (Krisenmanagement) • ISO/IEC 27002:2022, Pkt. 5.24, 5.26, 5.29, 5.30 • BSI IT-Grundschutz, DER.4, DER.2.1, DER.2.3, ISMS.1 • IKT-Minimalstandard, RC.RP-1, RC.IM-1, RC.CO-1, RS.IM-1
Risiko	Erhebliche Sicherheitsvorfälle müssen auch unter Krisenbedingungen koordiniert, wirksam und zeitnah bewältigt werden können. Fehlende oder unzureichende Rahmenbedingungen und Verfahren des Krisenmanagements können dazu führen, dass Verantwortlichkeiten unklar sind, Entscheidungen verzögert getroffen werden und die Bewältigung eines Sicherheitsvorfalls unkoordiniert erfolgt. Dadurch steigt das Risiko einer Eskalation von Sicherheitsvorfällen, länger andauernder Betriebsunterbrüche sowie erheblicher finanzieller, rechtlicher und reputationsbezogener Schäden für die betroffene Einrichtung und Dritte.
Checkliste	☐ Rahmenbedingungen für das Krisenmanagement von Netz- und Informationssystemen sind definiert; ☐ Verfahren für das Krisenmanagement von Netz- und Informationssystemen sind definiert; ☐ Die Rahmenbedingungen und Verfahren des Krisenmanagements sind umgesetzt; ☐ Die Rahmenbedingungen und Verfahren werden erprobt. ☐ Die Rahmenbedingungen und Verfahren werden periodisch überprüft.
Periodisch zu überprüfen	Die Rahmenbedingungen und Verfahren des Krisenmanagements werden mindestens jährlich überprüft und mindestens jährlich in Form einer Stabs- oder Tabletop-Übung erprobt. Kontakt- und Eskalationslisten sind aktuell und werden mindestens quartalsweise aktualisiert. Nach Sicherheitsvorfällen, Krisenübungen oder wesentlichen Änderungen erfolgt eine anlassbezogene Überprüfung und Anpassung.