Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr,
Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilung Sicherheit

Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.

Herausgeber Bundesamt für Verkehr, 3003 Bern
Abteilungen Infrastruktur und Sicherheit

Verteiler: Veröffentlichung auf der BAV-Internetseite (www.bav.admin.ch)

Verfügbare Sprachen: Deutsch (Original)
Französisch
Italienisch

Inkrafttreten: 01.07.2024

Bundesamt für Verkehr
Abteilung Infrastruktur

Remund Zuffi Anna Barbara G0BQTG
26.09.2023

Info: admin.ch/esignature | validator.ch

Anna Barbara Remund
Vizedirektorin

Abteilung Sicherheit

Sperlich Rudolf 7OUWIO
25.09.2023

Info: admin.ch/esignature | validator.ch

Dr. Rudolf Sperlich
Vizedirektor

Ausgaben / Änderungsgeschichte

Version	Datum	Ersteller	Änderungshinweise	Status
V0.4	15.12.2022	Bundesamt für Verkehr	Überarbeitung nach SI/st Review (BAV)	Review in der Branche
V0.5	27.03.2023	Bundesamt für Verkehr	Überarbeitung nach Review in der Branche	abgelöst
V0.7	20.07.2023	Bundesamt für Verkehr	Nach Lektorat durch Redguard AG und anschliessender Bereinigung	abgelöst
V1.0	22.09.2023	Bundesamt für Verkehr	Bereinigung nach der Übersetzung	publiziert

[x] folgende Status sind vorgesehen: in Arbeit; in Review; publiziert; in Kraft/mit Visum; abgelöst

Inhaltsverzeichnis

1 Ausgangslage

Die Verfügbarkeit und die Korrektheit von Daten und Informationen sind ein wesentlicher Erfolgsfaktor für alle Geschäftsprozesse im Bereich des öffentlichen Verkehrs. Die fortschreitende Digitalisierung führt dazu, dass Informationen heute überwiegend elektronisch verarbeitet und gespeichert werden. Gleichzeitig werden immer mehr und immer unterschiedlichere Systeme miteinander vernetzt. Die Grenzen zwischen Informatikanwendungen, Kommunikations-, Industrie- und Eisenbahnanlagen, wie sie im öffentlichen Verkehr zur Anwendung kommen, verschwinden zunehmend.

Daraus resultiert eine hohe Abhängigkeit von informationsverarbeitenden Systemen und Anwendungen. Die zunehmende Vernetzung eröffnet zwar neue unternehmerische Möglichkeiten und Chancen. Durch die damit verbundene erhöhte Anfälligkeit für Cyberangriffe verändert sich jedoch auch ständig das Gefährdungsbild. Gleiches gilt für das potenzielle Schadensausmass bei einem Angriff. Die öffentliche Wahrnehmung von Cyberbedrohungen hat sich jedoch in den letzten Jahren stark verändert, da die Auswirkungen von Cyberangriffen zunehmend sichtbar und spürbar geworden sind.

2 Ziel und Zweck der Richtlinie

Das vorliegende Dokument konkretisiert die AB-EBV zu Art. 5c Abs. 1, AB 5c.1 [2] hinsichtlich der minimalen Ausgestaltung des Informationssicherheitsmanagementsystems (ISMS).

Informationen, Daten und Systeme sollen entsprechend ihrem Schutzbedarf und unter Berücksichtigung der spezifischen Risikosituation geschützt werden.
Dieser risikobasierte Ansatz ist die Grundlage für die Anwender dieser Richtlinie.

Dieser Ansatz besagt, dass Massnahmen zur Risikominderung und etwaige Lücken zwischen der aktuellen Risikominderung und dem vertretbarem Risikoniveau festzulegen sind, nachdem die wichtigsten Geschäftsrisiken in Bezug auf Vorschriften, operationellen und finanzielle Risiken oder Reputationsrisiken ermittelt wurden (siehe bspw. ISO/IEC 27005:2022, Kapitel 6.4).
Das Erkennen von Bedrohungen und das Ermitteln von Risiken sowie deren Umgang sind deshalb zentrale Themen in einem ISMS und in dieser Richtlinie.

Die Verweise auf bestehende Hilfsmittel (Anhang 3) sollen bei der Implementierung eines ISMS unterstützen.

Werden die Vorgaben der Richtlinie durch das Eisenbahnunternehmen eingehalten, können die erarbeiteten ISMS-Grundlagen in methodischer Hinsicht durch das BAV akzeptiert werden. Abweichungen von den Vorgaben der Richtlinie sind zulässig, wenn das von Gesetz und der Verordnung verfolgte Ziel auf andere Weise erreicht wird.

Die Richtlinie dient zudem als Grundlage für die Prüfungen im Rahmen der Aufsichtstätigkeit des BAV.

Da sich Mittel und Vorgehensweisen von Cyberkriminellen wandeln und professionalisieren, wird sich diese Richtlinie im Laufe der Zeit weiterentwickeln.

3 Grundlagen / Referenzen

Das vorliegende Dokument basiert auf den nachfolgenden rechtlichen Grundlagen, Normen und Standards:

[1] Eisenbahngesetz (EBG), SR 742.101[1]

[2] Eisenbahnverordnung (SR 742.141.1)[2] und deren Ausführungsbestimmungen (primär AB-EBV Art. 5c.1), SR 742.141.11[3]

[3] Delegierte Verordnung (EU) 2018/762 DER KOMMISSION vom 8. März 2018 über gemeinsame Sicherheitsmethoden bezüglich der Anforderungen an Sicherheitsmanagementsysteme gemäss der Richtlinie (EU) 2016/798 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EU) Nr. 1158/2010 und (EU) Nr. 1169/2010 (CSM zum SMS)[4]

[4] Verordnung über vorrangige Transporte in Ausnahmesituationen (VVTA), SR 531.40[5]

[5] Datenschutzgesetz (DSG), SR 235.1[6]

[6] Informationssicherheitsgesetz (ISG)[7] – Die Artikel mit der Meldepflicht bei Cyberangriffen ist noch nicht in Kraft (Stand September 2023).

[7] Verordnung über die Sicherheitsuntersuchung von Zwischenfällen im Verkehrswesen (VSZV), SR 742.161[8]

[8] SN ISO/IEC 27001:2022 (Übersicht siehe Anhang 2, Kapitel 11)[9]

[9] SN ISO/IEC 27002:2022

[10] NIST Cybersecurity Framework CSF 1.1[10]

[11] CLC/TS 50701:2023[11]

[12] IEC 62443[12]

[13] Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs (Handbuch VöV vom 2020)[13]

[1] https://www.fedlex.admin.ch/eli/cc/1958/335_341_347/de

[2] https://www.bav.admin.ch/bav/de/home/rechtliches/rechtsgrundlagen-vorschriften/ab-ebv.html

[3] https://www.fedlex.admin.ch/eli/cc/1983/1902_1902_1902/de

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0762&qid=1659537640455

[5] https://www.fedlex.admin.ch/eli/cc/2019/517/de

[6] https://www.fedlex.admin.ch/eli/cc/2022/491/de

[7] https://www.fedlex.admin.ch/eli/oc/2022/232/de und https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/vernehmlassung-meldepflicht.html

[8] https://www.fedlex.admin.ch/eli/cc/2015/26/de

[9] Die Norm ISO/IEC 27001 steht auf der VöV-Normenplattform exklusiv den Mitarbeitenden der beteiligten Schweizer Eisenbahnunternehmen (ohne SBB), sowie BAV und ZVV zur Verfügung: www.voev.ch/normenplattform

[10] https://www.nist.gov/cyberframework

[11] Die Norm CLC/TS 50701 steht auf der VöV-Normenplattform exklusiv den Mitarbeitenden der beteiligten Schweizer Eisenbahnunternehmen (ohne SBB), sowie BAV und ZVV zur Verfügung: www.voev.ch/normenplattform

[12] Teile dieser Norm stehen auf der VöV-Normenplattform exklusiv den Mitarbeitenden der beteiligten Schweizer Eisenbahnunternehmen (ohne SBB), sowie BAV und ZVV zur Verfügung: www.voev.ch/normenplattform

[13] https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/oeffentlicher_verkehr.html

[14] SN EN 50159:2010[14]

[15] BDEW Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Version 2.0 05/2018)[15]

[16] Verordnung über die Videoüberwachung im öffentlichen Verkehr – VüV-ÖV[16]

[17] Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA[17] (nur in deutscher Sprache vorhanden)

Welche Normen sind vorzuziehen?

Für die Erstellung und Aufrechterhaltung eines ISMS hat sich die ISO/IEC 27001 als international anerkannte Norm etabliert. Die ISO/IEC 27002 ist der Leitfaden für Massnahmen (Controls), die aus den Anforderungen der ISO/IEC 27001 risikobasiert umzusetzen sind.

Die IEC 62443 Normen basieren auf den ISO 27000 Normen und erweitern diese mit den Unterschieden und Spezifika der industriellen Automation. Die CLC/TS 50701 basieren auf den IEC 62443 Normen mit Spezifika der Eisenbahnsysteme und Fahrzeuge (siehe auch Abbildung 1 in [11]).

Im Bereich der elektrischen Anlagen sind das referenzierte BDEW Whitepaper [15] und die ISO/IEC 27019 weit verbreitet.

Für den Einstieg in das Thema Cybersicherheit bei Eisenbahnen eignet sich das Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs [13]. Dieses enthält auch ein Hilfsmittel zur Selbsteinschätzung.

[14] Diese Norm steht auf der VöV-Normenplattform exklusiv den Mitarbeitenden der beteiligten Schweizer Eisenbahnunternehmen (ohne SBB), sowie BAV und ZVV zur Verfügung: www.voev.ch/normenplattform

[15] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

[16] https://www.fedlex.admin.ch/eli/oc/2009/736/de

[17] https://www.isaca.de/sites/default/files/isaca_implementierungsleitfaden_isms_2022.pdf

4 Aufbau dieser Richtlinie

Das **Kapitel 5** beschreibt den Geltungsbereich dieser Richtlinie und gibt einige Hinweise zur Abgrenzung der beschriebenen Mindestanforderungen.

Das **Kapitel 6** hebt die Bedeutung einer angemessenen Integration des ISMS in bestehende Prozesse und in die Sicherheitskultur des Unternehmens hervor. Es stellt den Bezug zu anderen Managementsystemen und bestehenden Normen und Standards her.

Die beschriebenen Mindestanforderungen gliedern sich in zwei Teile:

- **Kapitel 7:** Enthält Anforderungen an das ISMS mit dem Ziel, die Aspekte der Informationssicherheit systematisch und unter Berücksichtigung aller Vorgaben und Bedürfnisse auszurichten und zu steuern. Das Kapitel 7 konkretisiert den Artikel 5c.1.2 der Ausführungsbestimmungen zur EBV (AB-EBV [2]) und definiert die Mindestanforderungen an ein ISMS. Dabei stehen die prozessualen Anforderungen an das Managementsystem im Fokus.

- **Kapitel 8:** Umfasst technische und organisatorische Massnahmen (sogenannte «Controls») zur Gewährleistung eines angemessenen Informationssicherheitsniveaus für den Eisenbahnsektor, als Teil der kritischen Infrastrukturen der Schweiz. Es werden sowohl generelle Massnahmen, die für alle Systeme und Anwendungen gelten, als auch spezifische Massnahmen für den Bereich Operational Technology (OT) und spezifische Massnahmen für die Fahrzeugsysteme aufgeführt.

Der **Anhang 1** gibt einen kurzen Überblick über den Bezug eines ISMS zu anderen Managementsystemen als Teil eines Integrierten Managementsystems (IMS).

Der **Anhang 2** gibt einen kurzen Überblick über die Normen ISO/IEC 27001 und 27002, welche für den Aufbau und die Weiterentwicklung eines ISMS von zentraler Bedeutung sind.

Der **Anhang 3** verweist auf Hilfsmittel für die Implementierung eines ISMS.

Anhang 4 enthält das Gesuchformular zur Befreiung von der ISMS-Pflicht für EVU resp. ISB gemäss dem Geltungsbereich in Kapitel 5.

5 Geltungsbereich

Die Mindestanforderungen gelten für folgende Organisationen und Unternehmen:

- **Eisenbahninfrastrukturbetreiberinnen (ISB):** Unternehmen, die über eine Konzession und eine Sicherheitsgenehmigung nach Art. 5 Eisenbahngesetz (EBG) für den Bau und Betrieb einer Eisenbahninfrastruktur verfügen. Die Eisenbahninfrastruktur umfasst die Betriebsanlagen der Eisenbahn einschliesslich der Bahnstromanlagen.

- **Eisenbahnverkehrsunternehmen (EVU):** Unternehmen, die über eine Sicherheitsbescheinigung nach Art. 8c EBG verfügen.

Die enthaltenen Bestimmungen beziehen sich auf alle Prozesse, Informationsverarbeitungssysteme und Datennetzwerke, die im Rahmen der oben genannten Tätigkeiten eingesetzt werden oder diese Tätigkeiten indirekt ermöglichen.
Werden einzelne Tätigkeiten an Dritte übertragen (z.B. Lieferanten, Hersteller, Instandhaltungsbetriebe, für die Instandhaltung zuständige Stellen, Schienenfahrzeughalter, Dienstleister und Beschaffungsstellen), gelten diese Bestimmungen ebenfalls. Die Verantwortung für die Einhaltung der Bestimmungen verbleibt bei den ISB bzw. EVU.

Die Bestimmungen gelten für alle Informationsverarbeitungssysteme (HW + SW) und Datennetzwerke in den Bereichen Informationstechnologie (IT), Operational Technology (OT) der ortsfesten Anlagen sowie für Systeme auf Fahrzeugen.

EVU und ISB, die keine oder eine vernachlässigbare Angriffsfläche im Bereich der Informationssicherheit haben (beispielsweise historische Bahnen), können beim BAV eine Befreiung von der ISMS-Pflicht beantragen. Dazu ist das Gesuch im Anhang 4 auszufüllen und dem BAV über die E-Mail-Adresse _BAV-WeiterentwicklungRegelwerke@bav.admin.ch oder das Portal eGesuche (https://www.bav.admin.ch/bav/de/home/kontakt/e-gesuche.html) einzureichen[18].

5.1 Abgrenzungen

Die Verantwortung für den angemessenen Schutz ihrer Daten und Informationen liegt gemäss Geltungsbereich bei der jeweiligen ISB bzw. EVU. Das vorliegende Dokument grenzt sich dabei wie folgt ab:

- Die Bestimmungen enthalten Massnahmen zur Gewährleistung eines minimalen Informationssicherheitsniveaus.

- Abhängig von organisationsspezifischen Gegebenheiten, sowie resultierend aus Risikobewertungen, können weitergehende Massnahmen notwendig sein.

- Die Umsetzung der hier enthaltenen Bestimmungen ist nicht ausreichend, um eine Zertifizierung zu erlangen (z.B. ISO/IEC 27001).

[18] Das neue eGesuch-Formular wird bis zum Inkrafttreten der Richtlinie auf bav.admin.ch aufgeschaltet. Bis auf weiteres ist das Gesuch an folgende Adresse zuzustellen: _BAV-WeiterentwicklungRegelwerke@bav.admin.ch

6 Bezug zu anderen Managementsystemen

Bei der Ausgestaltung und Umsetzung des ISMS ist zu berücksichtigen, dass bei den betroffenen Unternehmen gegebenenfalls bereits andere Managementsysteme bestehen. Das ISMS ist so zu implementieren, dass keine Konflikte mit bestehenden Managementsystemen entstehen. Sind Konflikte mit bestehenden Managementsystemen unvermeidbar oder sind potenzielle Konflikte erkennbar, so ist dies zu dokumentieren. Soweit möglich und sinnvoll, sollen vorhandene Elemente und damit verbundene Synergien aus bereits bestehenden Managementsystemen genutzt werden. Ein integriertes Managementsystem (IMS) ist anzustreben (siehe Anhang 1).

7 Minimale Anforderungen an das Managementsystem für Informationssicherheit (ISMS)

Dieses Kapitel umfasst die Anforderungen an das ISMS mit dem Ziel, die Aspekte der Informationssicherheit systematisch und unter Berücksichtigung aller Vorgaben und Bedürfnisse auszurichten und zu steuern. **Zudem konkretisiert dieses Kapitel den Artikel 5c.1.2 der Ausführungsbestimmungen zur EBV** (AB-EBV [2]) **und definiert die Mindestanforderungen an ein ISMS**. Der Fokus liegt dabei auf den prozessualen Anforderungen an das Managementsystem. In **Kapitel 8** werden konkrete Massnahmen (Controls) beschrieben, **die zur Erfüllung der in diesem Kapitel beschriebenen Anforderungen beitragen**.

In der Spalte «Verweis» wird auf bestehende Normen, Standards, hoheitliche Vorgaben verwiesen und mögliche Synergien zur VO 2018/762 [3], Anhänge I und II aufgezeigt[19]. In der Spalte «Controls Kapitel 8» wird auf die mit der Anforderung verbundenen Massnahmen verwiesen.

Die Eisenbahnunternehmen sind verpflichtet, einen verbindlichen Zeitplan für die Umsetzung der nachfolgend beschriebenen Anforderungen an das ISMS zu führen und diesen dem BAV auf Verlangen zur Verfügung zu stellen.

Nr.	Anforderung	Verweis	Controls Kapitel 8
A-01	**Informationssicherheitsstrategie** Die oberste Führungsebene muss festlegen, welche Ziele mit der Informationssicherheit erreicht werden sollen. Die Ziele müssen mit der strategischen Ausrichtung des Unternehmens und den Interessen der interessierten Parteien vereinbar sein. Die oberste Führungsebene muss gewährleisten, dass die zur Zielerreichung notwendigen Ressourcen zur Verfügung stehen. Zudem muss definiert werden, welche Geschäftsbereiche das ISMS abdeckt und wo es keine Anwendung findet. Der minimale Geltungsbereich des ISMS kann Kapitel 5 entnommen werden.	ISO/IEC 27001 Kapitel 5.1 NIST CSF 1.1 ID.BE-3 ID.GV-1 Handbuch VöV Kapitel 3.2.1 und 3.2.3 VO 2018/762 Kapitel 1 Kapitel 2.1	B-01 B-04 B-05 B-06 B-08 B-09 B-20
A-02	**Rollen und Verantwortlichkeiten** Die Verantwortlichkeiten und Befugnisse der Rollen mit Bezug zur Informationssicherheit müssen klar definiert und zugewiesen sein. Für das Unternehmen ist eine informationssicherheitsbeauftragte Person zu benennen und dem BAV bekannt zu geben.	ISO/IEC 27001 Kapitel 5.3 NIST CSF 1.1 ID.GV-2 Handbuch VöV Kapitel 3.2.2 VO 2018/762 Kapitel 2.3	B-01 B-02 B-04 B-06 B-08 B-09 B-10 B-12 B-16 B-22 B-23 B-28

[19] Die Anhänge I und II der VO 2018/762 sind inhaltlich identisch. Daher wird nicht unterschieden.

Nr.	Anforderung	Verweis	Controls Kapitel 8
A-03	**Richtlinien und Organisation** **Die oberste Führungsebene muss gewährleisten, dass das ISMS in die Geschäftsprozesse des Unternehmens integriert ist** (siehe Beispiel in Abbildung 1, Anhang 1)**.** Hierfür müssen Informationssicherheitsrichtlinien erstellt, von der Führungsebene bzw. den verantwortlichen Personen freigegeben und innerhalb des Unternehmens sowie bei involvierten externen Stellen bekannt gemacht werden.	ISO/IEC 27001 Kapitel 5.2 NIST CSF 1.1 ID.GV-3 ID.GV-4 Handbuch VöV Kapitel 3.2.3 VO 2018/762 Kapitel 2.1-2.4	B-02 B-03 B-04 B-05 B-06 B-07 B-08 B-09 B-10 B-11 B-12 B-15 B-16 B-18 B-20 B-22
A-04	**Regelmässige Überprüfung der Informationssicherheit / Audits** Die Durchführung regelmässiger Audits liefert Informationen darüber, in welchen Bereichen die Informationssicherheit zu verbessern ist. Dabei sind auch Lieferanten und Dienstleister zu berücksichtigen. Die zu prüfenden Themenbereiche und die Periodizität der Audits sind in einem Auditprogramm festzuhalten. Daraus resultierende Massnahmen sind nach einer vorgenommenen Priorisierung umzusetzen.	ISO/IEC 27001 Kapitel 9.1 Kapitel 9.2 NIST CSF 1.1 ID.SC-4 PR.PT-1 VO 2018/762 Kapitel 6.1 Kapitel 6.2	B-04 B-05 B-06 B-08 B-09 B-10 B-14 B-20
A-05	**Kontinuierliche Verbesserung** Das Unternehmen muss die Eignung und Wirksamkeit ihres ISMS kontinuierlich verbessern. Diese Prüfung erfolgt mindestens einmal jährlich.	ISO/IEC 27001 Kapitel 5.1 Kapitel 9.3 Kapitel 10 NIST CSF 1.1 RS.IM-1 VO 2018/762 Kapitel 6.3 Kapitel 7	B-04 B-08 B-14

Nr.	Anforderung	Verweis	Controls Kapitel 8
A-06	**Dokumentation** Sämtliche relevanten Aktivitäten und Ergebnisse im Zusammenhang mit dem ISMS müssen dokumentiert und protokolliert werden. D.h. insbesondere: a) Die Beschreibung der Prozesse und Aktivitäten im Zusammenhang mit der Informationssicherheit des Eisenbahnbetriebs, einschliesslich sicherheitsrelevanter Aufgaben und der damit verbundenen Verantwortlichkeiten; b) Identifizierung der Auftragnehmer, Partner und Zulieferer mit Beschreibungen der Art und des Umfangs der erbrachten Dienstleistungen; c) Identifizierung der vertraglichen und sonstigen geschäftlichen Vereinbarungen zwischen dem Unternehmen und der anderen unter Buchstabe b genannten Beteiligten, die für die Beherrschung der durch das Unternehmen und den Einsatz von Auftragnehmern entstehende Sicherheitsrisiken erforderlich sind; Die Dokumentation und die Protokolle sind vor unbefugter Einsichtnahme und vor Verlust zu schützen.	ISO/IEC 27001 Kapitel 4.1 Kapitel 4.2 Kapitel 7.5 NIST CSF 1.1 ID.GV-1 ID.GV-3 VO 2018/762 Kapitel 4.5	B-02 B-04 B-06 B-08 B-09 B-13 B-18 B-20 B-21 B-22 B-23 B-24 B-25 B-26 B-27 B-28 B-29
A-07	**Risikobeurteilung und –behandlung** Das Unternehmen muss einen Prozess zur Beurteilung von Informationssicherheitsrisiken festlegen und anwenden. Es müssen Kriterien für die Risikoakzeptanz und die Durchführung von Risikobeurteilungen definiert werden. Der Prozess muss folgende Punkte beinhalten: **a) Risiken identifizieren** Risiken, die sich aus dem Ausfall oder Beeinträchtigung von Informationssystemen ergeben, sind im Hinblick auf Integrität, Verfügbarkeit und Vertraulichkeit zu ermitteln. Es sind Personen zu bestimmen, die als Risikoeigner fungieren. **b) Risiken analysieren** Die möglichen Folgen bei Eintritt der identifizierten Risiken und deren Eintrittswahrscheinlichkeit sind abzuschätzen. **c) Risiken bewerten** Die Ergebnisse der Risikoanalyse (Risk Assessment) müssen mit den definierten Risikokriterien verglichen und eine Priorisierung für die Risikobehandlung durchgeführt werden. **d) Risiken behandeln** Basierend auf den Ergebnissen der Risikobeurteilung muss das Unternehmen angemessene Massnahmen zur Risikobehandlung auswählen und deren Umsetzung planen und durchführen. Die Risikoeignerin bzw. der Risikoeigner muss diesen Plan genehmigen, die Restrisiken dokumentieren, ggf. akzeptieren und die Mitarbeitenden sowie externe Beteiligte informieren. Es ist sicherzustellen, dass diese Schritte bei relevanten Änderungen sowie bei einer Verschlechterung der Bedrohungslage wiederholt werden. Mindestens einmal jährlich sind die Schritte a) bis d) zu wiederholen, um neue Risiken zu identifizieren, bestehende Risiken ggf. neu zu bewerten und die Wirksamkeit der umgesetzten Massnahmen auf die Risiken zu beurteilen.	AB-EBV Artikel 5c.1 ISO/IEC 27001 Kapitel 6.1.2 Kapitel 6.1.3 NIST CSF 1.1 ID.RM-1 ID.RM-2 ID.RM-3 Handbuch VöV Kapitel 3.3 VO 2018/762 Kapitel 3.1 (Eingang in SMS von relevanten Bedrohungen aus der Risikoanalyse der Cybersicherheit) Hilfsmittel zum Risikomanagement siehe Anhang 3	B-04 B-13 B-15 B-16 B-19 B-20 B-27

8 Controls (Basismassnahmen)

Die in diesem Kapital aufgeführten Massnahmen tragen dazu bei, die Anforderungen des Kapitels 7 zu erfüllen und ein minimales Niveau an Informationssicherheit im Eisenbahnsektor zu erreichen.

Die Umsetzung der Massnahmen bzw. deren Priorisierung hat risikobasiert zu erfolgen. Dies bedeutet, dass aufgrund der Risikoanalyse und des Schutzbedarfs der Systeme zusätzliche Massnahmen erforderlich sein können oder einzelne der hier aufgeführten Massnahmen nicht zielführend sind.
Es ist zulässig, andere Kompensationsmassnahmen zu realisieren oder auf Zielkonflikte zu reagieren, sofern damit das von Gesetz und Verordnung verfolgte Ziel erreicht wird (siehe auch [11]). Die Kompensationsmassnahmen sind schriftlich festzuhalten.

8.1 Organisatorische, personelle, physische und technologische Controls für IT, OT, Datennetzwerke, inkl. Eisenbahnfahrzeuge

Dieses Kapitel umfasst organisatorische, personelle, physische und technologische Massnahmen (Controls) zur Gewährleistung eines angemessenen Informationssicherheitsniveaus für den Eisenbahnsektor als Teil der kritischen Infrastrukturen der Schweiz.

In Kapitel 8.1 sind die Controls aufgeführt, die für alle Systeme und Anwendungen gelten. In Kapitel 8.2 sind die spezifischen Controls für den Bereich Operational Technology (OT) und in Kapitel 8.3 die spezifischen Controls für die Fahrzeugsysteme aufgeführt.

In der Spalte «Control» werden konkrete Massnahmen beschrieben. Diese orientieren sich unter anderem an der ISO/IEC 27001:2022 [8] bzw. ISO/IEC 27002:2022 [9]. In der Spalte «Verweis» wird der Bezug zu bestehenden Normen, Standards, Hilfsmitteln und hoheitlichen Vorgaben hergestellt. Die letzte Spalte soll mögliche Synergien zum SMS [3] aufzeigen.

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-01	**Festlegung von Rollen und Verantwortlichkeiten** Es müssen Rollen und Verantwortlichkeiten für den Bereich der Informationssicherheit definiert werden. Die einzelnen Aufgabenbereiche müssen Personen mit den entsprechenden Fachkenntnissen zugewiesen werden.	ISO/IEC 27002:2022 Kapitel 5.2 NIST CSF 1.1 ID.GV-2	Kapitel 2.3 Kapitel 4.1 Kapitel 4.2
B-02	**Zugriffs- und Identitätsmanagement** Identitäten von Personen und Systemen, die Zugriff auf Informationen oder anderen Assets haben, müssen verifiziert und verwaltet werden. a) Eine Identität muss immer nur einer Person oder einem System zugeordnet werden. b) Es ist festzulegen, welche Identitäten welche Berechtigungen und Zugriffe erhalten. c) Dabei sind die Grundsätze des "Need-to-know-" und des "Least-privilege-Prinzips" anzuwenden. d) Die vergebenen Berechtigungen müssen regelmässig überprüft und den aktuellen Begebenheiten angepasst werden. e) Nicht mehr aktive Identitäten sind zu deaktivieren.	ISO/IEC 27002:2022 Kapitel 5.3 Kapitel 5.15 Kapitel 5.16 Kapitel 5.17 Kapitel 5.18 NIST CSF 1.1 PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-6	

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-03	**Asset Management** a) Es muss ein Inventar von Daten, Informationen und informationsverarbeitenden Systemen erstellt werden. b) Für jedes Asset resp. jede Kategorie ist eine verantwortliche Person zu benennen. c) Es ist ein Verfahren zu implementieren, das gewährleistet, dass neue Assets aufgenommen werden und das Inventar aktualisiert wird. d) Die Assets bzw. die Kategorien sind hinsichtlich ihres Schutzbedarfs in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu klassifizieren.	ISO/IEC 27002:2022 Kapitel 5.9 Kapitel 5.11 Kapitel 5.12 Kapitel 7.8 Kapitel 7.14 NIST CSF 1.1 ID.AM-1 ID.AM-2 ID.AM-5 Handbuch VöV Kapitel 3.3.1 TS50701:2023 Kapitel 4.2	Kapitel 5.2
B-04	**Lieferantenmanagement** Gemäss dem Geltungsbereich in Kapitel 5 ist sicherzustellen, dass die Informationssicherheit bei der Zusammenarbeit mit Lieferanten berücksichtigt wird. a) Sämtliche Lieferanten sowie deren Beitrag zur Informationssicherheit müssen erfasst und beurteilt sein. b) Je nach Schutzbedarf (Kritikalität) der verarbeiteten Daten sind Lieferanten im Rahmen ihrer Leistungserbringung zur Einhaltung der relevanten Informationssicherheitsvorgaben zu verpflichten. Diese Verpflichtung ist auch auf deren Mitarbeitende und allfällige Unterlieferanten zu übertragen. c) Darüber hinaus sind die Mitarbeitenden der Lieferanten durch regelmässige Schulungen über die gesetzlichen und internen Vorgaben zum Schutz von Informationen und zum sicheren Umgang mit informationsverarbeitenden Systemen zu informieren und zu schulen. d) Sofern die Nachweise nicht anderweitig ausreichend vorliegen, ist vertraglich ein Auditrecht vorzusehen. e) Es muss regelmässig überprüft werden, ob die vertraglich definierten Bestimmungen eingehalten werden.	ISO/IEC 27002:2022 Kapitel 5.18 Kapitel 5.19 Kapitel 5.20 Kapitel 5.21 DSG NIST CSF 1.1 ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 Handbuch VöV Tabelle 6 Kapitel 3.6 Siehe auch Anhang 3 Hilfsmittel	Kapitel 2.4 Kapitel 5.3

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-05	**Informationssicherheit in Projekten mit IT- und OT-Bezug** (einschliesslich Beschaffungen) sowie bei Prozess- und Organisationsentwicklungen. a) Das Projekt hat einer definierten Projektmanagementmethode zu folgen. b) Informationssicherheit ist ein Bestandteil der Projektmanagementmethode. c) Zu Beginn des Projektes sind der Schutzbedarf und relevante Informationssicherheitsanforderungen festzulegen. d) Während des Projekts ist der Erfüllungsgrad der vorgenannten Anforderungen zu überprüfen und zu dokumentieren. e) Nicht umgesetzte Anforderungen oder bekannte Risiken sind innerhalb des Unternehmens bekannt zu machen. f) Informationssicherheitsanforderungen müssen frühzeitig in Projekte integriert werden. Deren Einhaltung ist zu dokumentieren und an relevante Interessengruppen zu berichten.	ISO/IEC 27002:2022 Kapitel 5.2 Kapitel 5.8 NIST CSF 1.1 ID.RA-4 TS50701:2023 Abbildung 6	
B-06	**Massnahmen im Bereich Cloud** Es ist sicherzustellen, dass beim Bezug von Cloud-Diensten die Anforderungen an die Informationssicherheit berücksichtigt und Massnahmen zum Schutz umgesetzt werden. Cloud-Dienste, die geschäftskritische Prozesse oder personenbezogene Daten betreffen, sind im Rahmen eines internen Freigabeprozesses regelmässig auf ihre Eignung zu prüfen. a) Es muss eine Übersicht über alle verwendeten Cloud-Dienste geführt werden. Jedem Cloud-Dienst ist eine verantwortliche Person zuzuordnen. b) Die Verantwortlichkeiten des Cloud Anbieters und Cloud Nutzers müssen klar definiert werden (Shared Responsibility Model). c) Vor der Verwendung von Cloud-Diensten ist zu prüfen, welche Daten dort gespeichert und verarbeitet werden. Es ist eine Risikoanalyse durchzuführen und zu beurteilen, ob die vorhandenen bzw. die vom Cloud-Anbieter angebotenen Schutzmassnahmen ausreichend sind.	DSG ISO/IEC 27002:2022 Kapitel 5.23 Kapitel 8.27 Handbuch VöV Kapitel 3.6.3 Siehe auch Anhang 3 Hilfsmittel	
B-07	**Überwachung (security monitoring)** Systeme und Netzwerke sind so aufzubauen und zu konfigurieren, dass Angriffe und Anomalien zeitnah erkannt und ausgewertet werden können.	ISO/IEC 27002:2022 Kapitel 8.15 Kapitel 8.16 NIST CSF 1.1 DE.AE Handbuch VöV Kapitel 3.6.4	

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-08	**Management von Informationssicherheitsvorfällen** a) Verfahren, wie mit Informationssicherheitsvorfällen umgegangen wird, sind zu etablieren. Der Prozess muss das Vorgehen bei einem Sicherheitsvorfall beschreiben und die Verantwortlichkeiten und Kommunikationswege festlegen. b) Der Prozess stellt sicher, dass geeignete Massnahmen zur Reaktion und Wiederherstellung getroffen und umgesetzt werden. c) Bei der Behandlung von Vorfällen sind die einzelnen Bearbeitungsschritte zu dokumentieren. d) Geltende Meldepflichten gegenüber Behörden und Dritten (z.B. EDÖB[20], NCSC[21]) müssen eingehalten werden. e) Aus Informationssicherheitsvorfällen müssen entsprechende Erkenntnisse und Verbesserungen gezogen werden.	ISO/IEC 27002:2022 Kapitel 5.24 Kapitel 5.25 Kapitel 5.26 Kapitel 5.27 Kapitel 5.28 NIST CSF 1.1 RS.RP-1 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RC.RP-1 RC.IM-1 RC.IM-2 DSG ISG (Zukunft) VSZV	Kapitel 7 Kapitel 7.1. Kapitel 7.2.
B-09	**Business Continuity Management** Es ist ein Prozess zu erstellen, welcher die Fortführung der Betriebstätigkeit bei Ausfall kritischer Komponenten oder eines Systems gewährleistet. Dies betrifft neben den Informations- und Kommunikationstechnologien auch Technologien der OT und den Bereich der Fahrzeuge. a) Kritische Komponenten oder Systeme sind bekannt und beurteilt. b) Für alle kritischen Komponenten und Systeme muss ein Notfall- und Wiederherstellungsplan erstellt werden. c) Diese Pläne werden regelmässig oder nach weitreichenden Änderungen getestet und geübt.	VVTA Art.8 ISO/IEC 27002:2022 Kapitel 5.29 Kapitel 5.30 NIST CSF 1.1 ID.RA-4 RS.RP-1 Handbuch VöV Kapitel 3.3.5	Kapitel 5.5
B-10	**Beschäftigung von Mitarbeitenden**	ISO/IEC	

[20] www.edoeb.admin.ch

[21] www.ncsc.admin.ch

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
	Vor und während der Beschäftigung einer Person im Unternehmen sind folgende Massnahmen durchzuführen: a) Insbesondere bei Mitarbeitenden mit sicherheitsempfindlichen Tätigkeiten: Durchführung einer angemessenen Sicherheitsüberprüfung unter Berücksichtigung relevanter gesetzlicher Bestimmungen und der vorgesehenen Funktion. b) Die Mitarbeitenden werden durch regelmässige Schulungen über die gesetzlichen und internen Vorgaben zum Schutz von Informationen und zum sicheren Umgang mit informationsverarbeitenden Systemen informiert. c) In den vertraglichen Vereinbarungen werden die Mitarbeitenden zur Einhaltung der gesetzlichen und internen Informationssicherheitsvorgaben verpflichtet. d) Personen, die mit schützenswerten Informationen arbeiten oder Zugang zu solchen haben, müssen vertraglich zur Geheimhaltung verpflichtet werden (Geheimhaltungsverpflichtung) Änderung und/oder Beendigung der Beschäftigung: e) Zugänge zur Unternehmensinfrastruktur müssen für austretende Personen zeitnah deaktiviert werden. f) Es ist ein Prozess zu etablieren, der die Rückgabe oder Vernichtung entsprechender Daten, Informationen und informationsverarbeitender Geräte bei Beschäftigungswechsel (Übertritt und insbesondere Austritt) regelt.	27002:2022 Kapitel 6.1 Kapitel 6.2 Kapitel 6.3 Kapitel 6.4 Kapitel 6.5 Kapitel 6.6 NIST CSF 1.1 PR.AC-1 PR.AT-1 PR.AT-2 PR.AT-3 PR.IP-11 Handbuch VöV Kapitel 3.7	Kapitel 4.2 Kapitel 4.3 Kapitel 4.4
B-11	**Betreiben von Systemen und Datennetzwerken** Systeme und Datennetzwerke sind so zu konfigurieren bzw. zu schützen, dass ungeplante Beeinträchtigungen oder Ausfälle vermieden werden. a) Für eine Übersicht des vorhandenen Netzes müssen aktuelle Netzwerkpläne vorliegen. b) Netzwerke müssen in sinnvollem Mass und unter Berücksichtigung der Grösse segregiert werden. Hierfür ist ein Netzwerkkonzept zu erstellen, das spezifische Massnahmen zum Informationsschutz beschreibt. c) Falls eine Vernetzung von OT- und IT-Diensten z.B. mit Public-Cloud Anwendungen so zunimmt, dass Netzübergänge nicht mehr sicher nach dem klassischen Zonenkonzept «Zones and Conduits» betrieben und verwaltet werden können, ist eine geeignete Sicherheitsarchitektur z.B. nach dem Zero-Trust-Prinzip zu etablieren. d) Informationssicherheitsrelevante Aktivitäten und Änderungen an den Systemen müssen gemäss dem Änderungsmanagementprozess protokolliert werden.	ISO/IEC 27002:2022 Kapitel 5.2 Kapitel 7.11 Kapitel 8.9 Kapitel 8.14 Kapitel 8.20 Kapitel 8.22 NIST CSF 1.1 PR.AC-5 PR.IP-1 PR.IP-3 PR.PT-4 Handbuch VöV Kapitel 3.5	Kapitel 3.1.2

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-12	**Erstellen von Richtlinien (policies) für die Authentifizierung bei Systemen** a) Es sind Richtlinien zu etablieren, die beschreiben, wie sich Benutzer an den Systemen anmelden. b) Die Richtlinien beschreiben, welche Authentifizierungsverfahren verwendet werden müssen (z.B. Zwei-Faktor-Authentisierung) und wie diese korrekt zu verwenden sind. c) Die Sicherheitsanforderungen an die Authentifizierungsverfahren sind nach Möglichkeit technisch durchzusetzen (z.B. Mindestanforderungen an Passwörter, Änderung von Initialpasswörtern). d) Wo möglich, sind starke Authentifizierungsverfahren zu verwenden (z.B. Zwei-Faktor-Authentisierung, tokenbasierte oder biometrische Verfahren, etc.).	ISO/IEC 27002:2022 Kapitel 5.17 NIST CSF 1.1 PR.AC-1 PR.AC-4 PR.AC-7 Handbuch VöV Kapitel 3.5 Siehe auch Anhang 3 Hilfsmittel	
B-13	**Massnahmen zum Schutz von Endgeräten** Verwendete Endgeräte im Bereich IT, OT oder für Fahrzeuge müssen die folgenden Sicherheitsanforderungen erfüllen: a) Die Konfiguration und die Verwendung erfolgen gemäss definierten Richtlinien. b) Bei der Nutzung privater Endgeräte im Unternehmenskontext ist darauf zu achten, dass diese mindestens die Anforderungen der in a) erstellten Richtlinie erfüllen. c) Auf Systemen und Endgeräten müssen sicherheitsrelevante Patches zeitnah installiert werden. d) Können keine sicherheitsrelevanten Patches innerhalb nützlicher Frist installiert werden, sind entsprechend der Risiken andere Massnahmen zu treffen (z.B. Einschränkungen bei Fernzugriffen, Optimierung des Sicherheitsmonitorings, um eine Ausnutzung der Schwachstelle zeitnah erkennen zu können). Siehe auch B-20 b).	ISO/IEC 27002:2022 Kapitel 8.1 NIST CSF 1.1 PR.DS-1 PR.DS-5 DE.AE-1 TS50701:2023 Kapitel 10.2 Kapitel 10.3 Handbuch VöV Kapitel 3.5 Tabelle 6	
B-14	**Schutz vor Schadsoftware (malware)** Es müssen Schutzmassnahmen zum präventiven Schutz und zur Erkennung von Schadsoftware auf Systemen implementiert werden. Die Implementierung kann je nach verwendeten Technologien und Zweck des Systems durch den Einsatz entsprechender Software oder durch eine Härtung des Systems erfolgen (z.B. Perimeterschutz, Defence-in-depth). Für OT: siehe auch B-25	ISO/IEC 27002:2022 Kapitel 6.3 Kapitel 8.7 NIST CSF 1.1 DE.CM-1 DE.CM-4 DE.AE-2 TS50701:2023 B.4.4, C.3 Handbuch VöV Kapitel 3.5	

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-15	**Konfigurations- und Änderungsmanagement** Bei der Konfiguration von Hardware, Software, innerhalb von Netzwerken sowie im Bereich OT und für Fahrzeuge müssen Informationssicherheitsanforderungen erfüllt werden. a) Änderungen müssen nach einem definierten Prozess autorisiert und umgesetzt werden. b) Bei der Konfiguration ist sicherzustellen, dass nur Personen Konfigurationseinstellungen durchführen dürfen, die für die Tätigkeit autorisiert sind. c) Standardpasswörter müssen vor der Inbetriebnahme geändert werden.	ISO/IEC 27002:2022 Kapitel 5.22 Kapitel 8.9 Kapitel 8.32 NIST CSF 1.1 PR.IP-1 PR.IP-3 Handbuch VöV Kapitel 3.5	Kapitel 5.2 Kapitel 5.4
B-16	**Fernarbeit (remote work)** Fernarbeit liegt dann vor, wenn Mitarbeitende oder externe Dienstleister von einem Ort ausserhalb des Unternehmensgeländes arbeiten und dabei über ICT-Geräte auf Informationen zugreifen. a) Wenn Mitarbeitende oder externe Dienstleister über ICT-Geräte aus der Ferne auf Informationen zugreifen, müssen Richtlinien definiert werden, wie die Fernarbeit im Kontext der Informationssicherheit zu erfolgen hat. b) Es ist zu definieren, welche Authentifizierungsmechanismen zur Durchführung von Fernarbeit verwendet werden. c) Mitarbeitende müssen für das Thema Fernarbeit sensibilisiert werden und entsprechende Informationen (z.B. Umgang mit persönlichen Accounts) erhalten. d) Massnahmen, die gewährleisten, dass nur berechtigte Personen über das Internet auf Informationen zugreifen können (z.B. über VPN), sind zu forcieren.	ISO/IEC 27002:2022 Kapitel 6.7 NIST CSF 1.1 PR.AC-3 PR.AT-1 PR-AT.3	
B-17	**Einsatz von kryptografischen Verfahren** Falls in Applikationen kryptografische Verfahren zur Anwendung kommen, müssen diese auf anerkannten und geprüften Algorithmen und einer sicherer Schlüsselgenerierung basieren.	TS50701:2023 SR 4.2 SR 4.3 NIST CSF 1.1 PR.DS-1 Siehe auch Anhang 3 Hilfsmittel	

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-18	**Schutz der Daten und Informationen** Daten- und Informationen müssen geschützt werden, um die Anforderungen von Gesetzen, Behörden oder anderen Verträgen zu erfüllen. Es bedarf einer Richtlinie, welche die Regeln und Verfahren zum Schutz der Daten und Informationen definiert. a) Daten- und Informationen sind bei der Speicherung und Übertragung entsprechend ihrem Schutzbedarf zu schützen. Die Schutzmassnahmen und die Verfahren sind zu dokumentieren. b) Schützenswerte Daten (z.B. personenbezogene Daten, Zugangsdaten) sind durch technische Massnahmen zu schützen (beispielsweise durch Verschlüsselung). c) Es müssen Massnahmen zum Schutz vor Datenverlust in Systemen, Netzwerken und anderen Geräten implementiert werden (beispielsweise die Überwachung von Zugriffen auf Daten mit hohem Schutzbedarf). d) Sicherungskopien von Daten, Informationen, Software und Systemen sind regelmässig durchzuführen und zu testen. e) Auf Geräten oder Speichermedien gespeicherte und nicht mehr verwendete Daten bzw. Informationen müssen entsprechend ihrem Schutzbedarf gelöscht werden. Für die Vernichtung von Speichergeräten empfiehlt sich der Einsatz von zugelassenen, zertifizierten Anbietern von sicheren Entsorgungsdienstleistungen.	ISO/IEC 27002:2022 Kapitel 5.24 Kapitel 5.31 Kapitel 8.10 Kapitel 8.11 Kapitel 8.12 Kapitel 8.13 Kapitel 8.24 NIST CSF 1.1 PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6 PR.PT-2 SN EN 50159: 2010 DSG Handbuch VöV Kapitel 3.5	Kapitel 4.5
B-19	**Zutrittsschutz zu Gebäuden und Fahrzeugen** Gebäude, Räume und Bereiche mit sicherheitsrelevanten Systemen in Anlagen, Aussenanlagen und in Fahrzeugen sind, soweit möglich und verhältnismässig, gegen unbefugten Zutritt zu schützen.	ISO/IEC 27002:2022 Kapitel 5.15 Kapitel 7.1 Kapitel 7.2 Kapitel 7.3 Kapitel 7.4 NIST CSF 1.1 PR.AC-2 Handbuch VöV Kapitel 3.5.5	Kapitel 5.2
B-20	**Schwachstellenmanagement** Es muss ein Schwachstellenmanagement eingerichtet werden, dass alle Systeme berücksichtigt und die folgenden Kriterien erfüllt: a) Die Verantwortlichkeiten im Zusammenhang mit der Identifizierung und Meldung von Schwachstellen, sind zwischen dem Betreiber, dem Systemintegrator, dem Hersteller und in den Service Level Agreements (SLA) für jedes System klar zu definieren. b) Wird eine Schwachstelle identifiziert, muss das hierdurch entstehende Risiko durch die verantwortliche(n) Stelle(n) bewertet und auf dieser Basis entschieden werden, ob und welche Sofortmassnahmen getroffen werden können und wann resp. unter welchen Bedingungen ein Sicherheitspatch einzuspielen ist. Dabei kann ein temporäres Risiko bestehen, das ggf. getragen werden muss.	ISO/IEC 27002:2022 Kapitel 8.8 TS50701:2023 Kapitel 10.2 Kapitel 10.3 NIST CSF 1.1 PR.IP-12	

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-21	**Trennung von Entwicklungs-, Test- und Produktionsumgebungen** a) Entwicklungs-, Test- und Produktionssysteme sind voneinander zu trennen. b) Änderungen an Produktionssystemen müssen zunächst in einer Testumgebung durchgeführt werden, bevor diese auf Produktionssysteme angewendet werden dürfen.	ISO/IEC 27002:2022 Kapitel 8.29 Kapitel 8.31 NIST CSF 1.1 PR.DS-7	

8.2 Spezifische Controls im Bereich Operational Technology (OT)

In diesem Kapitel beziehen sich die Controls sowohl auf OT-Systeme ortsfester Anlagen als auch auf OT-Systeme auf Eisenbahnfahrzeugen.
Bei den OT-Systemen ist davon auszugehen, dass insbesondere die Verfügbarkeit und die Integrität der Systeme im Fokus stehen und die Vertraulichkeit eine untergeordnete Rolle spielt. Daher ist bei der Umsetzung der Security-Massnahmen im OT-Bereich immer zu prüfen, ob diese die Funktionssicherheit (Safety) oder die Betriebsfähigkeit des jeweiligen Systems beeinflussen oder indirekte Auswirkungen auf diese haben. Die Implementierung von Security-Massnahmen ist immer in enger Zusammenarbeit und Abstimmung mit dem Safety-Management zu entscheiden und durchzuführen, um mögliche Wechselwirkungen angemessen zu berücksichtigen (Rückwirkungsfreiheit) und Risiken identifizieren zu können.

Die Rückwirkungsfreiheit (d.h. Abwesenheit von Rückwirkungen, was bedeutet, dass die Funktion andere sicherheitsbezogene Funktionen nicht beeinträchtigt) muss nachgewiesen werden. Fallspezifisch sind für diesen Nachweis sowohl analytische Methoden wie auch Regressionstests anzuwenden.

Signifikante resp. wesentliche Änderungen an bestehenden Systemen sind gemäss EBV Art. 8 [2] genehmigungspflichtig. Im Zweifelsfall ist das BAV zu kontaktieren.

Nr.	Control	Verweis
B-22	**Installation von Software auf OT** Aufgrund der Kritikalität (Schutzbedarf) der OT-Systeme müssen Softwareinstallationen überwacht und kontrolliert werden. a) Die Installation von Updates auf OT-Systemen dürfen nur von qualifiziertem Personal durchgeführt werden. b) Es muss sichergestellt werden, dass Softwareupdates der Hersteller für die OT-Systeme in einem vorgängig mit dem Hersteller definierten Zeitraum zur Verfügung gestellt werden. c) Für die Installation von Updates muss ein Genehmigungsverfahren durchlaufen werden, an dem auch das Safety-Management involviert ist. d) Vor der Installation von Updates auf OT-Systemen ist die Software umfangreich zu testen. Für die Tests sind Testprotokolle zu führen, mit denen die getesteten Funktionen und eventuelle Auffälligkeiten dokumentiert werden. Bei Problemen darf keine Installation respektive Update durchgeführt werden. e) Es muss im Voraus eine Rollback-Strategie definiert und getestet werden. Dies bedeutet, dass die OT-Systeme bei Nichtfunktionalität auf den ursprünglichen, funktionierenden Zustand zurückgeführt werden können. f) Es ist zu protokollieren, von wem und aus welchem Grund Updates oder Software installiert werden. g) Ältere Softwareversionen müssen zusammen mit den notwendigen Informationen und Parametern archiviert werden.	TS50701:2023 Kapitel 9 Kapitel 10.2 Kapitel 10.3 NIST CSF 1.1 PR.DS-6 PR.MA-1

Nr.	Control	Verweis
B-23	**Identifikation und Authentifikation** In Bezug auf Benutzerverwaltung und Authentifizierungsmöglichkeiten sind OT-Systeme im Vergleich zu klassischen IT-Systemen oft stark eingeschränkt oder diese sind aufgrund hoher Verfügbarkeitsanforderungen nicht gemäss Stand der Technik realisierbar. Dem ist mit entsprechenden Gegenmassnahmen zu begegnen. a) Kompensierende Massnahmen für die eingeschränkten Authentifizierungsmöglichkeiten bei vielen OT-Systemen müssen risikobasiert getroffen werden. Z.B. Starke Authentisierung an der Netzzonengrenze durch einen Policy Enforcement Point (z.B. Proxy oder VPN-Endpunkt), verstärkte Überwachung der Systemzugriffe mittels Access Logs, etc. b) Endgeräte, die im Kontext von OT-Systemen verwendet werden, sind entsprechend ihres Schutzbedarfs zu schützen.	TS50701:2023 SR 1.4 SR 1.11 SR 1.7 SR 2.3 NIST CSF 1.1 PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4
B-24	**Überwachung (security monitoring)** Die sicherheitsrelevanten Systemprotokolle der vernetzten Systeme müssen an ein zentrales System zur Loganalyse übertragen und dort entsprechend den unternehmensinternen Vorgaben bzw. dem Logging-Konzept aufbewahrt werden. Siehe auch B-07	TS50701:2023 SR 2.1 SR 2.8 NIST CSF 1.1 DE.AE-3 DE.AE-4 PR.PT-1
B-25	**Systemintegrität** Zum Schutz vor Malware kann oft keine entsprechende Erkennungssoftware auf den Systemen installiert werden. Als Gegenmassnahmen sollten präventive Mechanismen implementiert werden. Dazu gehören z.B. Richtlinien für den Umgang mit Wechseldatenträgern und Endgeräten in Verbindung mit vorgelagerten Erkennungsmechanismen (z.B. IDS).	TS50701:2023 SR 3.2 NIST CSF 1.1 DE.CM-1 DE.CM-2 DE.CM-7 PR.PT-2
B-26	**Einschränkung des Datenflusses** Ausgehend vom Schutzniveau der Systeme und der durchgeführten Risikoanalyse sind die Netze sinnvoll zu segmentieren. Dabei ist zu beachten, dass Netzwerkzonen im Notfall vom restlichen Netzwerk getrennt werden können, um den Schaden zu minimieren. Es ist daher zu prüfen, welche zentralen Dienste in mehreren Zonen redundant bereitgestellt werden müssen (z.B. DHCP, DNS, etc.). Insbesondere Systeme, die für die funktionale Sicherheit (Safety) relevant sind, sollten soweit möglich und sinnvoll von anderen Netzwerken isoliert sein, um Schäden zu begrenzen.	TS50701:2023 SR 5.1 NIST CSF 1.1 PR.AC-5 RS.MI-1
B-27	**Verfügbarkeit** a) Es ist ein angemessener Schutz vor Denial-of-Service-Angriffen zu implementieren. Angriffe dürfen sich nicht über mehrere Systeme oder Netzwerkbereiche ausbreiten können. b) Für relevante Daten und Dateien muss ein geeignetes Backupverfahren definiert und implementiert werden. Für die Wiederherstellung von Backups ist eine Wiederherstellungsstrategie zu entwickeln. Darüber hinaus ist die Rückspielbarkeit von Backups regelmässig zu testen, um eine sichere und konforme Wiederherstellung der Daten gewährleisten zu können. c) Systeme und OT-Anwendungen müssen so ausgelagert werden, dass die Verfügbarkeit bei einem Ausfall durch ein redundantes System gewährleistet ist. Das Unternehmen sollte Verfahren für die Aktivierung redundanter Komponenten und Verarbeitungseinrichtungen planen und umsetzen.	TS50701:2023 SR 7.1 SR 7.2 SR 7.3 SR 7.4 SR 7.5 ISO/IEC 27002:2022 Kapitel 8.14 NIST CSF 1.1 PR.IP-4 PR.IP-7 PR.IP-9

8.3 Spezifische Controls bei ICT-Systemen auf Eisenbahnfahrzeugen

Nr.	Control	Verweis
B-28	**Identifikation und Authentifikation** In Fahrzeugen dürfen Authentifizierungsverfahren den schnellen Zugriff auf Systeme nicht verhindern. Systeme, die der Lokführer für den Betrieb des Fahrzeugs benötigt, dürfen nach der initialen Identifikation, z.B. durch Schlüssel oder Badge, nicht automatisch gesperrt werden. Der Zugriffsschutz muss zusätzlich durch physische Massnahme (z.B. verschlossene Türen zum Führerstand) sichergestellt werden. Für sonstige Arbeiten, die nicht während des Regelbetriebs durchgeführt werden, z.B. Änderungen von Softwarekonfigurationen oder Parametern, ist ein striktes Identifikations- und Authentifizierungsmanagement anzustreben.	TS50701:2023 SR 1.4 NIST CSF 1.1 PR.AC-1
B-29	**Physischer Schutz** a) Es ist durch geeignete Massnahmen (z.B. abschliessbarer Schrank) sicherzustellen, dass schützenswerte Komponenten vor physischer Manipulation geschützt sind. b) Falls kein wirksamer physischer Schutz realisiert werden kann, sind andere Massnahmen wie z.B. ein Fahrzeugüberwachungssystem zu etablieren.. c) Für die Überwachung sind Alarmsysteme (z.B. durch Videoüberwachung, Überwachung von Abdeckungen bei schützenswerten Komponenten) zu konfigurieren und entsprechend zu schützen (siehe folgender Punkt). d) Überwachungssysteme sollten sich in einem Bereich befinden, der für die Person, die den Alarm auslöst, nicht zugänglich ist. e) Die Überwachungssysteme müssen über manipulationssichere Mechanismen verfügen und regelmässig getestet werden.	ISO/IEC 27002:2022 Kapitel 7.4 NIST CSF 1.1 PR.AC-2 Videoüberwachung: VüV-ÖV [16]

9 Begriffe

Begriff	Definition
Asset	Ein Asset ist alles, was Wert für die Organisation hat (auch Informationsgut und Informationswert genannt). Es gibt viele Asset-Typen, etwa: Informationen, Software, Hardware, Services, Menschen mit ihren Qualifikationen, Kompetenzen und Erfahrungen sowie immaterielle Werte, wie Reputation und Image. ISO/IEC 27005:2022 unterscheidet zwischen primären und sekundären Assets. Die primären Assets sind Assets, die unbedingt zu schützen sind. Sie stellen den eigentlichen Wert einer Organisation oder eines Unternehmens dar. Das sind z.B. Geschäftsprozesse und -Geheimnisse, Stammdaten, Reputation eines Unternehmens, etc.. Sekundären Assets sind Assets die benötigt werden, damit die primären Assets ihre Wertschöpfung entfalten können. Das sind z.B. IKT-Betriebsmittel (Hardware, Software), Immobilien, Personal, Websites.
Asset Owner	Asset Owner ist die Person, die für die tägliche Verwaltung der Assets verantwortlich ist. Dazu gehören nicht nur elektronische und gedruckte Informationen, sondern auch Hardware, Software, Dienstleistungen und Einrichtungen.
Authentifizierung / Authentisierung (englisch «authentication»)	Die Begriffe Authentisierung und Authentifizierung werden im allgemeinen Sprachgebrauch oft synonym verwendet, beschreiben aber verschiedene Teilprozesse z.B. eines Anmeldevorgangs. Ein Benutzer AUTHENTISIERT sich an einem System mittels eindeutiger Anmeldeinformationen (z.B. Passwort oder Chipkarte). Das System überprüft daraufhin die Gültigkeit der verwendeten Daten, es AUTHENTIFIZIERT den Nutzer oder die Nutzerin.
Autorisierung	Unter Autorisierung versteht man in der Informationstechnologie die erstmalige Vergabe und die wiederholte Überprüfung von Zugriffsrechten auf Daten und Dienste mittels spezieller Methoden. Die zwei häufigsten Formen sind: • der autorisierte Zugriff auf Ressourcen (z. B. auf Verzeichnisse oder Dateien) in einem Computernetzwerk. • die Autorisierung zur Installation oder Nutzung von Computerprogrammen.
BAV	**Bundesamt für Verkehr**
BSI	**Bundesamt für Sicherheit in der Informationstechnik**
CLC	**CENELEC**: Comité Européen de Normalisation Électrotechnique
Controls	Controls sind Massnahmen, die der Erreichung von Massnahmenzielen dienen und Risiken der Informationssicherheit signifikant reduzieren.
CSM	**Common safety method** CSM der ERA (European Union Agency for Railways)
Cyberangriff	Jede Form böswilliger Aktivitäten, die von Unbefugten absichtlich ausgelöst werden und sich gegen Informationstechnologie oder Personen richten, die diese nutzen.
Cyberbedrohung	Jeder Umstand oder jedes Ereignis, das zu einem Cybervorfall führen kann.

Cybersicherheit	Technologien, Dienste, Strategien, Praktiken und Richtlinien zum Schutz von Systemen bzw. Netzwerken der Informationstechnologie vor Angriffen böswilliger Akteure.
Cybervorfall	Ereignis beim Betrieb von Informatikmitteln, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Verarbeitung beeinträchtigen kann. Siehe auch CLC TS 50701:2023, Kapitel 3.1.32 resp. CLC TS 50501:2021, Kapitel 3.1.29.
ECM	**Entity in Charge of Maintenance** Für die Instandhaltung zuständige Stelle im Eisenbahnverkehr
EVU	**Eisenbahnverkehrsunternehmen** (mit einer Konzession)
Fernzugriff	Der Fernzugriff soll Mitarbeitenden und ausgewählten externen Dienstleistern (z.B. für Wartungszwecke) einen sicheren Zugang zum Netz eines Unternehmens resp. zu einem OT-Netz ermöglichen, so dass bestimmte Anwendungen auch von ausserhalb genutzt werden können. Für den Fernzugriff steht ein entsprechend ausgestattetes Endgerät zur Verfügung. Es muss in der Lage sein, eine sichere Kommunikationsbeziehung über einen Netzzugang (z. B. DSL, WLAN, Mobilfunk) und ein Transfernetz (z. B. Internet) zum Unternehmensnetz aufzubauen.
ICS	**Industrial Control System** – Steuerungssysteme in industriellen Anlagen (anderer Begriff für OT)
IDS	**Intrusion Detection System**. Systeme zur Erkennung unautorisierte Zugriffe auf Daten oder Rechner.
Informationssicherheit	Informationssicherheit dient der Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit von informations- und Kommunikationstechnischen Systemen und der darin verarbeiteten bzw. gespeicherten Daten.
Informationsverarbeitende Systeme / Anwendungen	Systeme und Anwendungen, in denen Informationen verarbeitet oder gespeichert werden.
Integrität	Gewährleistung der Korrektheit bzw. Unversehrtheit von Daten sowie des korrekten Funktionierens von Systemen.
IMS	Das **Integrierte Managementsystem** fasst Methoden und Instrumente zur Erfüllung von Anforderungen aus verschiedenen Bereichen, die der Corporate Governance dienen (z.B. Qualität, Sicherheit, Informationssicherheit, Instandhaltung), in einer einheitlichen Struktur zusammen. Durch die Nutzung von Synergien und die Bündelung von Ressourcen ist im Vergleich zu einzelnen, isolierten Managementsystemen ein schlankeres und effizienteres Management möglich.
ISB	**Infrastrukturbetreiberinnen** (der Eisenbahn, d.h. landseitige Systeme)
ISMS	**Information Security Management System** – Teil des übergreifenden Managementsystems, basierend auf einem Geschäftsrisiko-Ansatz, zur Etablierung, Implementierung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit. Das Managementsystem beinhaltet die Organisationsstruktur, Policies, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Prozesse und Ressourcen.
IT	**Informationstechnologie** Alle Techniken und die dazu verwendete Hard- und Software im Zusammenhang mit der elektronischen Datenverarbeitung. Gegenüberstellungen zwischen IT resp. IKT und OT siehe Handbuch VöV, Tabelle 5 [13].

ICS	**Industrial Control System** (industrielles Kontrollsystem; wird im vorliegenden Dokument als Synonym zu den Abkürzungen «OT» und «SCADA» verwendet).
ICT / IKT	**Informations- und Kommunikationstechnologien** sind Technologien, die zur Abwicklung von Kommunikationsprozessen wie Telekommunikation, Rundfunk, intelligente Gebäudemanagementsysteme, audiovisuelle Verarbeitungs- und Übertragungssysteme sowie netzbasierte Steuerungs- und Überwachungsfunktionen eingesetzt werden.
ISACA	**Information Systems Audit and Control Association**
Least-privilege-Prinzip, Need-to-know-Prinzip	Ein System oder eine Person erhält nur Zugriff zu den Informationen, die sie zur Erfüllung ihrer Aufgaben benötigt. Unterschiedliche Aufgaben oder Rollen führen zu unterschiedlichen Need-to-know-Informationen und damit zu unterschiedliche Zugangsprofilen.
NCSC	**Nationales Zentrum für Cybersicherheit**
OT	**Operational Technology** bezeichnet die Hardware und Software, die die Leistung physischer Geräte überwacht und steuert. In der Vergangenheit bezog sich OT hauptsächlich auf Steuerungs- und Überwachungssysteme in Fertigungs-, Transport- und Versorgungsunternehmen. Gegenüberstellungen zwischen IT und OT siehe Handbuch VöV, Tabelle 5 [13].
RTE	**Regelwerk Technik Eisenbahn**. Ein Regelwerk des VöV (Verband öffentlicher Verkehr).
Rückwirkungsfreiheit	Nachweis, dass sich die vorgenommenen Anpassungen ausschliesslich auf die betroffenen Systeme, Komponenten oder Funktionen inkl. der Schnittstellen gemäss der Änderungsbeschreibung auswirken. Resp. dass die Funktion andere sicherheitsbezogene Funktionen nicht beeinträchtigt.
Schutzbedarf (Klassifikation eines Schutzobjekts)	Der Schutzbedarf eines Objekts orientiert sich am Ausmass des Schadens, der bei einer Verletzung der Informationssicherheit droht. Dies können Verletzungen der Vertraulichkeit, der Integrität und der Verfügbarkeit sein. Üblich sind mindestens folgende Schutzbedarfskategorien: • **normal:** Schadensauswirkungen sind begrenzt und beherrschbar. • **hoch:** Schadensauswirkungen können beträchtlich sein. • **sehr hoch:** Schadensauswirkungen können existenzbedrohende und katastrophale Ausmasse erreichen. •
Segregation of Duties (SoD)	Auch bekannt als „Prinzip der Funktionstrennung“.
SiBe	Die **Sicherheitsbescheinigung** im Eisenbahnverkehr bestätigt, dass das Unternehmen aufgrund seiner Organisation in der Lage ist, mit geeignetem Personal und Fahrzeugen sicher auf fremder Infrastruktur zu fahren.
SiGe	Die **Sicherheitsgenehmigung** umfasst die Bestätigung der Zweckmässigkeit des Sicherheitsmanagementsystems der Infrastrukturbetreiberin und die Akzeptanz der Vorkehrungen, die die Infrastrukturbetreiberin getroffen hat, um einen sicheren Betrieb auf ihren Strecken zu gewährleisten.
SMS	**Safety Management System** gemäss [3]
SR	**System Requirement** gemäss CLC/TS50701:2023, Tabelle 6 [11], resp. IEC 62443-3-3 [12]

SR	**Systematische Rechtssammlung** (Schweizer Recht)
Verfügbarkeit	Ist die Fähigkeit eines Systems, zu einem bestimmten Zeitpunkt oder während eines bestimmten Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen zu erfüllen, sofern die erforderlichen Mittel bereitgestellt werden [5].
Vertraulichkeit	Vertraulichkeit bedeutet, dass Daten nur von autorisiertem Personal eingesehen oder weitergegeben werden können. Dazu ist klar zu definieren, wer wie darauf zugreifen kann. Siehe auch [5].
VO	Verordnung (EU)
VöV	**Verband öffentlicher Verkehr** (www.voev.ch)
VVTA	**Verordnung über vorrangige Transporte in Ausnahmesituationen** (SR 531.40).
Zero-Trust-Prinzip	Ansatz, bei dem jeder Zugriff auf Ressourcen eine Authentifizierung erfordert. Jeder einzelne Datenfluss wird dabei auf Vertrauenswürdigkeit überprüft (siehe auch Positionspapier Zero Trust auf www.bsi.bund.de oder die NIST Special Publication 800-207 auf https://nvlpubs.nist.gov/).

Weitere Cyber-Begriffe sind auf https://www.ncsc.admin.ch/ncsc/de/home/glossar.html zu finden.

10 Anhang 1 – Integriertes Managementsystem und ISMS

Mit einem Integrierten Managementsystem (IMS) können bestehende Instrumente zur Erfüllung von Anforderungen aus verschiedenen Bereichen in einer einheitlichen und schlankeren Struktur zusammengefasst werden. Durch eine ganzheitlichere Darstellung können Synergien genutzt und Ressourcen gebündelt werden.

Nachfolgende Managementsysteme verfügen über Schnittstellen und damit über mögliches Synergiepotential:

- Sicherheitsmanagementsystem (CSM SMS)
- Qualitätsmanagementsystem (QMS)
- ECM Instandhaltungsmanagementsystem (CSM ECM)
- Compliancemanagementsystem (CMS)
- Risikomanagementsystem (RMS)
- Internes Kontrollsystem (IKS)

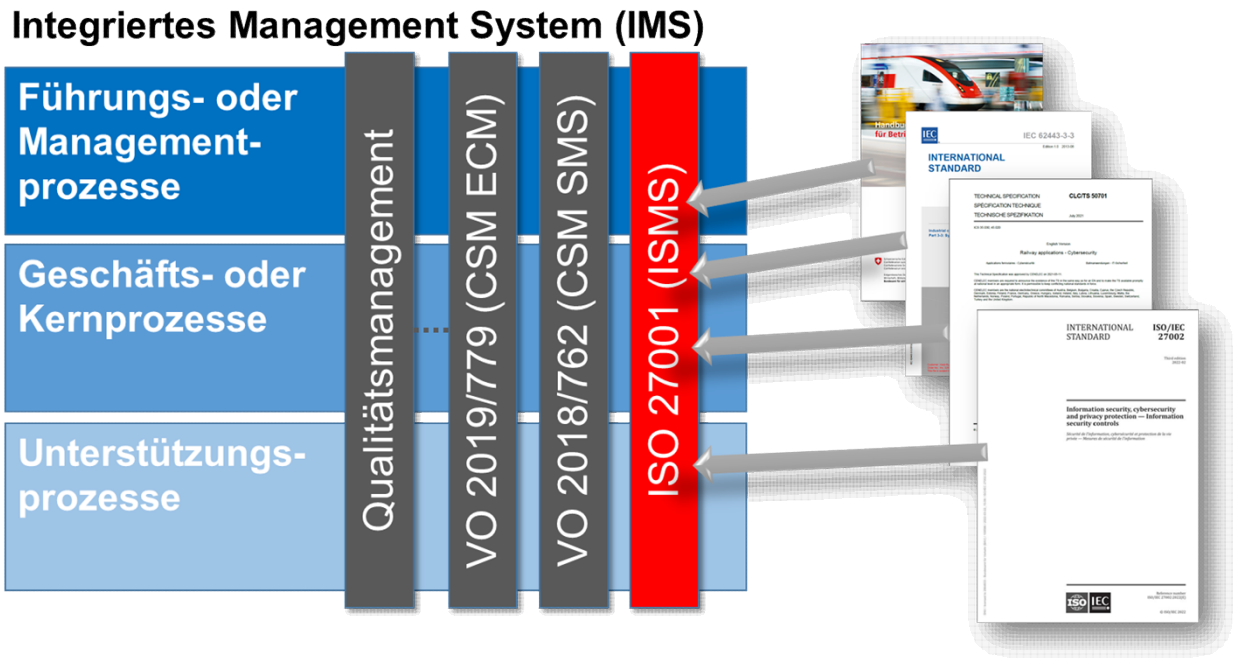
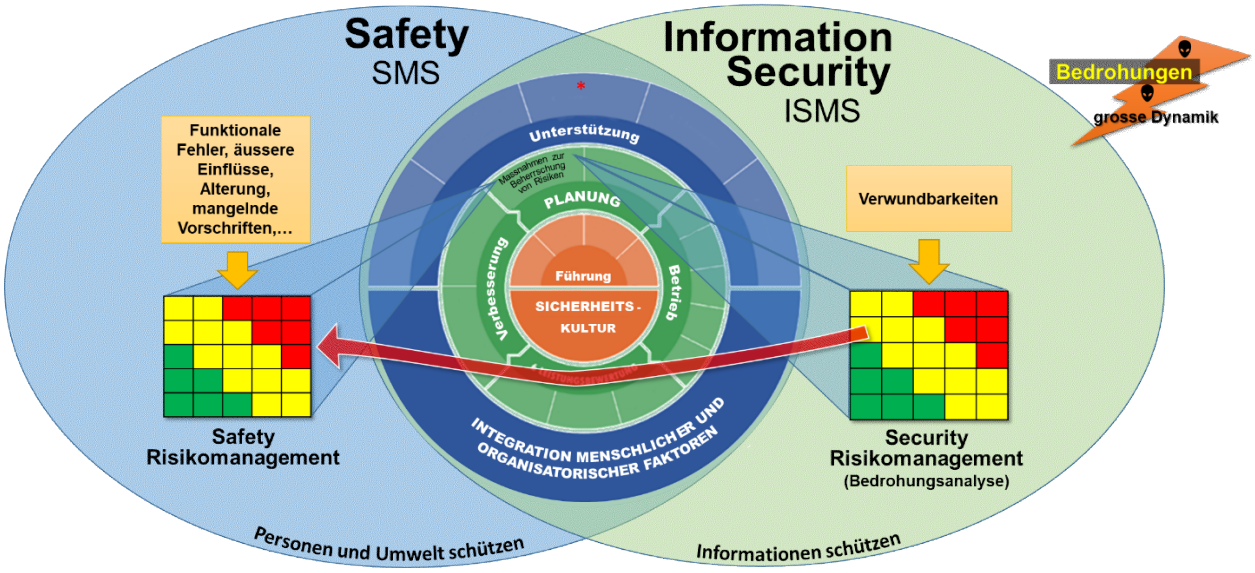


Abbildung 1 - Typisches IMS einer mittleren bis grösseren Transportunternehmung mit Bezug der Unternehmensprozesse zu Normen/Standards mit Sicherheitsanforderungen

Unter dem Gesichtspunkt der Sicherheit haben ISMS und Sicherheitsmanagementsysteme (SMS) eine gemeinsame Schnittstelle. Bei beiden Systemen steht die Risikominimierung im Vordergrund, um das Sicherheitsniveau kontinuierlich zu verbessern. Dazu müssen Risiken im Vorfeld identifiziert und kommuniziert werden.

Die wichtigste Schnittstelle zwischen einem ISMS und einem SMS ist demzufolge das Risikomanagement. Erkenntnisse aus der Bedrohungsanalyse eines ISMS müssen gemäss Abbildung 2 in das Risikomanagement des SMS einfliessen. Die für die Safety als relevant bewerteten Risiken sind im Gefährdungslogbuch (vgl. bspw. Hazard-Log gemäss SN EN 50126:2017) zu führen.



* https://www.era.europa.eu/sites/default/files/activities/docs/guide_sms_requirements_en.pdf

Abbildung 2 - ISMS Bezug zu SMS (Vereinfachte Darstellung mit der wichtigsten Nahtstelle ISMS-SMS)

11 Anhang 2 – Überblick der ISO/IEC 27001 und ISO/IEC 27002

Die Normenreihe ISO/IEC 27000 umfasst mehrere Teilnormen zum Thema Informationssicherheitsmanagement.
Die zentrale Norm ist die ISO/IEC 27001. Sie besteht aus einem Hauptteil mit allgemeinen Anforderungen an ein ISMS und einem umfangreichen Anhang A mit spezifischen Massnahmenzielen. Der Anwendungsbereich eines ISMS ist meist das gesamte Unternehmen. Wichtige Aufgaben eines ISMS sind:

- Formulierung von Sicherheitszielen
- Bestimmung der Assets
- Risikobeurteilung
- Risikobehandlung
- Kontinuierliche Verbesserung (z.B. nach dem PDCA-Zyklus – Plan-Do-Check-Act)

Gemäss ISO/IEC 27001 sollen alle relevanten Informationen, Daten und datenverarbeitende Systeme eines Unternehmens erfasst bzw. inventarisiert werden. Informationen, Daten oder datenverarbeitende Systeme mit vergleichbarem Wert und mit vergleichbaren Risiken können zusammengefasst und als ein Wert betrachtet werden.

Der **Anhang A der ISO/IEC 27001:2022** ist ein Katalog, der aus vier Sicherheitsthemen (Control Clauses) und 93 Controls besteht. Die vier Sicherheitsthemen sind:

- Organizational Controls - organisatorische Massnahmen (5.1 - 5.37)
- People Controls - personelle Massnahmen (6.1 - 6.8)
- Physical Controls - physische Massnahmen (7.1 - 7.14)
- Technological Controls - technologische Massnahmen (8.1 - 8.34)

Erläuterungen zur Umsetzung der 93 Controls und Massnahme-Beispiele finden sich in der ISO 27002.

Der **Anhang A der ISO/IEC 27002:2022** führt die Controls in einer Matrixdarstellung mit ihren jeweiligen Attributwerten auf. Die Matrixdarstellung ermöglicht eine Gruppierung und Filterung der Sicherheitsanforderungen, die ein Unternehmen erfüllen sollte.

Weiterführende Informationen zu Normen und Standards sind im Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs (Kapitel 6.2 in [13]) und auf verschiedenen Webseiten zu finden.[22]

[22] Beispielsweise https://en.wikipedia.org/wiki/IT_security_standards

12 Anhang 3 – Hilfsmittel für die Umsetzung eines ISMS

Hilfsmittel	Bemerkung
Handbuch Cybersecurity für Betriebe des öffentlichen Verkehrs (Handbuch VöV vom 2020) [13]	Das Handbuch VöV dient als Einführung in die Informationssicherheit im ÖV-Sektor und ermöglicht den Unternehmen eine Selbsteinschätzung durchzuführen. Das Handbuch basiert auf dem branchenübergreifenden IKT-Minimalstandard des Bundesamts für wirtschaftliche Landesversorgung (BWL[23]).
Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA (siehe [17])	Dient als Hilfsmittel zur Implementierung eines ISMS.
ICS Security Kompendium: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html	Mit dem ICS Security Kompendium veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Grundlagenwerk für die IT-Sicherheit in ICS.
Schwachstellen- und Lieferantenmanagement: ENISA: - Good Practices for Supply Chain Cybersecurity - Threat Landscape for Supply Chain Attacks	
Aktuelle Bedrohungen: www.ncsc.admin.ch	Unternehmen können sich beim Cyber Security Hub nach erfolgter Registrierung anmelden. Das NCSC informiert darin über aktuelle Bedrohungen. Registrierte Nutzer und Nutzerinnen haben die Möglichkeit, aktiv Informationen auf dieser Plattform auszutauschen. Anträge für die Registrierung nimmt das NCSC unter folgender Adresse entgegen: ncsc-useraccounts@gs-efd.admin.ch
Hilfsmittel für Risikoanalysen (Risk Assessments): - ISO/IEC 27005 - IEC 62443-3-2 - CLC/TS 50701:2023, Kapitel 6 und 7	Siehe auch: http://www.enisa.europa.eu ➔ Risk Management und eisenbahnspezifisch: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
Hilfsmittel für die Netzwerksegmentierung: - IEC 62443-3-2 und IEC 62443-3-3 - CLC/TS 50701 - Zoning and Conduits for Railways (ENISA, ER-ISAC)	
NIST Cryptography: www.nist.gov/cryptography	Informationen bezüglich Kryptografie-Standards.
BSI Empfehlungen zu kryptographischen Verfahren und Schlüssellängen: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html	
IEEE Cryptography:	

[23] www.bwl.admin.ch

https://standards.ieee.org/	
Passwortschutz und weiterführende Informationen zur Mitarbeitersensibilisierung: http://www.s-u-p-e-r.ch/de/tipps/e-wie-einloggen/	U.a. hilfreiche Hinweise für die Passwort-wahl.
Hilfsmittel für die Maturität der Cybersicherheit in einer Organisation zu bestimmen: IKT-Minimalstandard – Assessment Tool	RAILplus bietet ein eigenes Hilfsmittel zur Bestimmung der Maturität der Informations-sicherheit.
Hilfsmittel zum Thema Cloud: - Cloud Security Alliance - ENISA: Cloud Cybersecurity Market Analysis - BSI: Mindeststandard des BSI zur Nutzung externer Cloud-Dienste - BSI: Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)	
Mapping-Tabellen für verschiedene Normen: - IKT-Minimalstandard – Assessment Tool - Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur - Mapping Tabelle von ENISA für spezifische Sektoren	Die Aktualität der Mapping-Tabellen ist nicht immer gegeben.

Weitere Hilfsmittel siehe https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html

13 Anhang 4 – Checkliste und Gesuch zur Befreiung der ISMS-Pflicht für EVU und ISB

Namen und Unternehmens-Identifikationsnummer (UID) des Gesuchstellers: ☐ EVU ☐ ISB

Kontaktperson (Vor-, Nachnahme, E-Mail, Telefon Nr., Funktion):

Nr.	Prüfpunkt	Antwort	Erläuterungen / Referenzen
1	Wir haben folgende Systeme/Fahrzeuge im Geltungsbereich der AB-EBV im Einsatz:		
2	Es existieren digitale Schnittstellen zu folgenden betrieblichen und technischen Systemen (insbesondere zu Zugsicherungs- und Zugbeeinflussungssystemen)[24]: Bemerkung: bitte auch die Art der Schnittstelle beschreiben (z.B. TCP/IP Schnittstelle)		
3	Wir sind für den Betrieb gemäss der in Frage 2 aufgeführten Systeme auf folgende Dienstleister angewiesen[25]:		
4	Sind die Dienstleister (gem. Frage 3) vertraglich verpflichtet, Mindestanforderungen der Cybersicherheit für ihre Lieferanteile zu erfüllen?	☐ ja ☐ nein Wenn ja, welche Mindestanforderungen? Bemerkungen:	
5	Ohne unsere IT-Systeme[26] können wir unseren Betrieb … Stunden aufrechterhalten.	Anzahl Stunden: Begründung:	

[24] Als Übersicht kann die Abbildung 5 im Handbuch VöV [13] dienen.

[25] Als Dienstleister sind primär solche im IT- und OT-Bereich wie auch Eigentümer von gemieteten Anlagen und Rollmaterial denkbar.

[26] Unter IT-Systeme fallen unter anderem die Business-IT und Datenablagen.

Nr.	Prüfpunkt	Antwort	Erläuterungen / Referenzen
		Betriebsrelevante IT-Systeme (z.B. Dispo-System):	
6	Wir haben folgende Vorkehrungen getroffen, damit digital gespeicherte Informationen, welche relevant für unseren Betrieb und die Instandhaltung sind, jederzeit verfügbar sind[27]:		
7	Wir haben folgende Änderungen/Erneuerungen geplant, welche hinsichtlich der Cybersicherheit relevant sind / sein könnten.		
8	Vorhandene Grundlagen (z.B. Risikoanalysen, Systembeschreibungen) welche für die Beurteilung dieses Gesuchs hilfreich sind (bitte beilegen):		
9	Begründung des Gesuchstellers, wieso die Erstellung und Pflege eines ISMS für sein Unternehmen als nicht notwendig erachtet wird:		

Kriterien für eine Befreiung der ISMS-Pflicht:

1. Der Informationsschutzbedarf der vorhandenen IT- und OT-Systeme des Antragstellers für einen sicheren und zuverlässigen Betrieb (Kritikalität).

2. Bedeutsamkeit des Antragstellers (EVU resp. ISB) für die Landesversorgung und im Verbund mit anderen Transportunternehmen.

3. Wie die Sicherheitsziele **ohne ein ISMS mit den vorhandenen Managementsystemen** wie z.B. dem SMS erreicht werden können.

Bemerkungen: Der Antrag für eine Befreiung der ISMS-Pflicht ist alle 5 Jahre zu erneuern. Dies in Koordination mit den Prozessen SiBe/SiGe (413/414). Falls bei der Antragstellerin Änderungen erfolgen, welche hinsichtlich der Cybersicherheit relevant sein können, ist ein aktualisiertes Gesuch spätestens zum Zeitpunkt der Inbetriebnahme der Neuerung dem BAV einzureichen.

Ort, Datum:

Name, Vorname und Unterschrift[28]:

[27] z.B. offline Backup, welches regelmässig überprüft wird

[28] Funktionsträger nach Art. 14 Abs. 4 EBV, SR 742.141.1