Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports,
de l'énergie et de la communication DETEC

Office fédéral des transports OFT
Division Sécurité

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

Directive

Cybersécurité chemins de fer

Dir. CySec-Rail

Sur la base de l'art. 5*c* de l'ordonnance du 23 novembre 1983 sur les chemins de fer (OCF ; *RS 742.141.1*) et des dispositions d'exécution de l'OCF.

Éditeur : Office fédéral des transports, 3003 Berne
Divisions Infrastructure et sécurité

Distribution : Publication sur le site Web de l'OFT (www.bav.admin.ch)

Versions linguistiques : Allemand (version originale)
Français
Italien

Entrée en vigueur : 1er juillet 2024

Office fédéral des transports
Division infrastructure

Remund Zuffi Anna Barbara G0BQTG
26.09.2023

Info: admin.ch/esignature | validator.ch

Anna Barbara Remund
Sous-directrice

Division Sécurité

Sperlich Rudolf 7OUWIO
25.09.2023

Info: admin.ch/esignature | validator.ch

Rudolf Sperlich
Sous-directeur

Éditions / Historique des modifications

Version	Date	Auteur	Modifications	État*
V0.4	15.12.2022	Office fédéral des transports	Refonte suite à une révision par SI/st (OFT)	Révisé par la branche
V0.5	27.03.2023	Office fédéral des transports	Refonte suite à une révision par la branche	Remplacé
V0.7	20.07.2023	Office fédéral des transports	Après relecture par Redguard AG et mise au point	En révision
V1.0	22.09.2023	Office fédéral des transports	Mise au point après traduction	Publié

* Les états suivants sont prévus : en cours, en révision, publié, en vigueur/avec visa, remplacé

Table des matières

1 Contexte 4
2 Objectifs et utilité de la directive 4
3 Bases / référence 5
4 Structure 7
5 Champ d'application 8
5.1 Délimitations 8
6 Rapport avec les autres systèmes de gestion 9
7 Exigences minimales auxquelles doit répondre un SGSI 10
8 Contrôles (mesures de base) 13
8.1 Contrôles organisationnels, personnels, physiques et technologie pour les TI et les TO, réseaux de données, y compris les véhicules ferroviaires 13
8.2 Contrôles spécifiques dans le domaine des TO 22
8.3 Contrôles spécifiques pour des systèmes TIC embarqués 24
9 Glossaire 25
10 Annexe 1 – Système de gestion intégré et SGSI 29
11 Annexe 2 – Aperçu de la norme ISO/IEC 27001 et ISO/IEC 27002 31
12 Annexe 3 – Auxiliaires pour la mise en œuvre d'un SGSI 32
13 Annexe 4 – liste de contrôle et demande d'exemption de l'obligation de devoir mettre en place un SGSI pour des ETF et des GI 34

1 Contexte

La disponibilité et l'exactitude des données et des informations sont un facteur de réussite essentiel pour tous les processus commerciaux dans le domaine des transports publics. En raison de la numérisation croissante, les informations sont aujourd'hui traitées et stockées principalement sous forme électronique. Parallèlement, de plus en plus de systèmes d'une diversité croissante sont mis en réseau. Les limites entre les applications informatiques, les installations de communication, industrielles et ferroviaires, telles qu'elles sont utilisées dans les transports publics, tendent de plus en plus à disparaître.

Il en résulte une forte dépendance des systèmes et applications de traitement des informations. Bien que l'interconnexion croissante offre de nouvelles possibilités et chances entrepreneuriales, la vulnérabilité accrue aux cyberattaques qui en découle modifie constamment la menace. Il en va de même pour l'ampleur des dommages potentiels en cas d'attaque. La perception publique des cybermenaces a fortement évolué au cours des dernières années, car les risques de cyberattaques sont devenus de plus en plus visibles et tangibles.

2 Objectifs et utilité de la directive

Le présent document concrétise la DE ad art. 5c, al. 1, DE-OCF [2] en ce qui concerne la configuration minimale du système de gestion de sécurité de l'information (SGSI).

Les informations, les données et les systèmes doivent être sécurisés en fonction de leur besoin de protection et en tenant compte de la situation de risque spécifique.
Cette approche basée sur les risques constitue la base pour les utilisateurs de la présente directive.

Selon cette approche, les mesures d'atténuation des risques et les écarts éventuels entre l'atténuation actuelle des risques et le niveau de risque acceptable doivent être déterminés après identification des principaux risques commerciaux en termes de prescriptions, de risques opérationnels et financiers ou de risques de réputation (cf. par ex. ISO/IEC 27005:2022, ch. 6.4).
L'identification de menaces et la détermination des risques ainsi que leur traitement sont des thèmes essentiels dans un SGSI et dans la présente directive.

Les références aux auxiliaires existants (annexe 3) sont destinées à aider à implémenter un SGSI.

Si l'entreprise ferroviaire respecte les prescriptions de la directive, les bases du SGSI qui ont été élaborées peuvent être acceptées par l'OFT d'un point de vue méthodologique. Des écarts par rapport aux prescriptions de la directive sont autorisés si l'objectif fixé par la loi et l'ordonnance est atteint d'une autre manière.

La directive sert, en outre, de base aux contrôles effectués dans le cadre de l'activité de surveillance de l'OFT.

Étant donné que les moyens et la démarche des cybercriminels évoluent et se professionnalisent, la présente directive sera perfectionnée au fil du temps.

3 Bases / référence

Le présent document se base sur les bases légales, normes et standards suivants :

[1] Loi fédérale du 20 décembre 1957 sur les chemins de fer (LCdF)[1]

[2] Ordonnance du 23 novembre 1983 sur les chemins de fer (OCF)[2] et ses dispositions d'exécution (DE-OCF)[3] (principalement la DE 5c.1)

[3] Règlement délégué (UE) 2018/762 de la Commission du 8 mars 2018 établissant des méthodes de sécurité communes relatives aux exigences en matière de système de gestion de la sécurité conformément à la directive (UE) 2016/798 du Parlement européen et du Conseil et abrogeant les règlements de la Commission (UE) n° 1158/2010 et (UE) n° 1169/2010 (des MSC [méthodes de sécurité communes] au SGS)[4]

[4] Ordonnance du 28 août 2019 sur les transports prioritaires dans des situations exceptionnelles (OTPE)[5]

[5] Loi fédérale du 25 septembre 2020 sur la protection des données (LPD)[6]

[6] Loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[7] – les articles concernant l'obligation de signaler les cyberattaques ne sont pas encore en vigueur.

[7] Ordonnance du 17 décembre 2014 sur les enquêtes de sécurité en cas d'incident dans le domaine des transports (OEIT)[8]

[8] SN ISO/IEC 27001:2022 (aperçu cf. annexe 2, chap. 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]

---

[1] RS **742.101**

[2] RS **742.144.1**

[3] RS **742.144.11**

[4] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R0762&qid=1691670279795

[5] RS **531.40**

[6] RS **235.1**

[7] RS **128** ; https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2022/vernehmlassung-meldepflicht.html

[8] RS **742.161**

[9] La norme ISO/IEC 27001 est exclusivement disponible sur la plate-forme de normes de l'UTP, pour les collaborateurs des entreprises ferroviaires suisses concernées (sans les CFF), ainsi que pour l'OFT et la ZVV : https://www.voev.ch/fr/Technik/Thmes-de-technique-ferroviaire-et-RTE/Plate-forme-de-normes-de-lUTP

[10] https://www.nist.gov/cyberframework (en anglais uniquement)

[11] La norme CLC/TS 50701 est exclusivement disponible sur la plate-forme de normes de l'UTP, pour les collaborateurs des entreprises ferroviaires suisses con-cernées (sans les CFF), ainsi que pour l'OFT et la ZVV : https://www.voev.ch/fr/Technik/Thmes-de-technique-ferroviaire-et-RTE/Plate-forme-de-normes-de-lUTP

[12] Des parties de cette norme sont exclusivement disponibles sur la plate-forme de normes de l'UTP, pour les collaborateurs des entreprises ferro-viaires suisses concernées (sans les CFF), ainsi que pour l'OFT et la ZVV : https://www.voev.ch/fr/Technik/Thmes-de-technique-ferroviaire-et-RTE/Plateforme-de-normes-de-lUTP

[13] Manuel sur la cybersécurité destiné aux entreprises de transports publics (Manuel de l'UTP de 2020[13]

[14] SN EN 50159:2010[14]

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

[16] Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (OVid-TP)[16]

[17] *Implementierungsleitfaden ISO/IEC 27001:2022 von ISACA*[17]

Quelles sont les normes à privilégier ?

La norme ISO/IEC 27001 s'est imposée comme la norme internationale reconnue pour la mise en place et le maintien d'un SGSI. L'ISO/IEC 27002 est le guide des mesures (contrôles) à mettre en œuvre, en fonction des risques, à partir des exigences de l'ISO/IEC 27001.

Les normes IEC 62443 se basent sur les normes ISO 27000 et étendent ces dernières aux différences et aux spécificités de l'automatisation industrielle. La spécification technique CLC/TS 50701 se base sur les normes IEC 62443 avec des spécificités propres aux systèmes et aux véhicules ferroviaires (cf. Illustration 1 en [11]).

Dans le domaine des installations électriques, le *whitepaper* référencé du BDEW [15] et la norme ISO/IEC 27019 sont largement utilisés.

Le manuel sur la cybersécurité destiné aux entreprises de transports publics [13] s'avère utile pour l'introduction à la cybersécurité dans le domaine des chemins de fer. Il contient également un outil d'autoévaluation.

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

[14] Cette norme est exclusivement disponible sur la plate-forme de normes de l'UTP, pour les collaborateurs des entreprises ferro-viaires suisses concernées (sans les CFF), ainsi que pour l'OFT et la ZVV : : https://www.voev.ch/fr/Technik/Thmes-de-technique-ferroviaire-et-RTE/Plateforme-de-normes-de-lUTP

[15] https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf (en allemand uniquement)

[16] RS **742.147.2**

[17] https://www.isaca.de/sites/default/files/isaca_implementierungsleitfaden_isms_2022.pdf (en allemand uniquement)

4 Structure

Le **chapitre 5** décrit le champ d'application de la présente directive et donne quelques indications concernant la délimitation des exigences minimales décrites.

Le **chapitre 6** souligne l'importance d'une intégration appropriée du SGSI dans les processus existants et dans la culture de la sécurité de l'entreprise. Il fait le lien avec d'autres systèmes de gestion ainsi qu'avec des normes et standards.

Les exigences minimales décrites sont structurées en deux parties :

- Le **chapitre 7** contient les exigences relatives au SGSI dans le but d'organiser et de gérer les aspects de la sécurité de l'information de manière systématique tout en tenant compte de l'ensemble des directives et des besoins. Le chap. 7 concrétise la DE 5*c*.1, ch. 1.2, des DE-OCF [2] et définit les exigences minimales d'un SGSI. Il met l'accent sur les exigences en matière de processus du système de gestion.

- **Le chapitre 8** comprend des mesures techniques et organisationnelles (appelées « contrôles ») visant à garantir un niveau de sécurité de l'information approprié pour le secteur ferroviaire, qui fait partie des infrastructures critiques de la Suisse. Il contient des mesures générales valables pour tous les systèmes et applications, des mesures spécifiques pour le domaine de la technologie opérationnelle (TO) et des mesures spécifiques pour les systèmes embarqués.

L'**annexe 1** offre un bref aperçu du rapport entre un SGSI et d'autres systèmes de gestion dans le cadre d'un système de gestion intégré (SGI).

L'**annexe 2** offre un bref aperçu des normes ISO/IEC 27001 et 27002, qui sont cruciales pour la mise en place et le perfectionnement d'un SGSI.

L'**annexe 3** renvoie à des auxiliaires en vue de l'implémentation d'un SGSI.

L'**annexe 4** contient le formulaire de demande d'exonération de l'obligation de mettre en place un SGSI pour les entreprises de transport ferroviaire (ETF) et les gestionnaires d'infrastructure (GI) selon le champ d'application du chap. 5.

5 Champ d'application

Les exigences minimales s'appliquent aux organisations et entreprises suivantes :

- **Gestionnaires de l'infrastructure ferroviaire (GI):** entreprises qui disposent d'une concession et d'un agrément de sécurité selon l'art. 5 LCdF pour construire et exploiter une infrastructure ferroviaire. L'infrastructure ferroviaire comprend les installations d'exploitation des chemins de fer, y compris les installations du courant de traction.

- **Entreprises de transport ferroviaire (ETF) :** entreprises qui disposent d'un certificat de sécurité conformément à l'art. 8*c* LCdF.

Les dispositions s'appliquent à tous les processus, systèmes de traitement des informations et réseaux de données utilisés dans le cadre des activités susmentionnées ou permettant indirectement ces activités. Elles sont également applicables lorsque certaines activités sont confiées à des tiers (par ex. fournisseurs, fabricants, entreprises de maintenance, détenteurs de véhicules ferroviaires, prestataires de services et services d'achat). Les GI ou les ETF restent responsables du respect des dispositions.

Les dispositions s'appliquent à tous les systèmes et réseaux de données traitant des informations *(hardware + software)* dans les domaines de la technologie de l'information (TI), de la technologie opérationnelle (TO) des installations fixes, ainsi qu'aux systèmes embarqués.

Les ETF et les GI qui ne présentent pas de vulnérabilité ou qu'une vulnérabilité négligeable aux attaques dans le domaine de la sécurité de l'information (par ex. chemins de fer historiques) peuvent demander à l'OFT d'être exemptées de l'obligation de mettre en place un SGSI. Pour ce faire, il convient de remplir la demande figurant à l'annexe 4 et de le transmettre à l'OFT via l'adresse électronique _BAV-WeiterentwicklungRegelwerke@bav.admin.ch ou le portail des requêtes électroniques (https://www.bav.admin.ch/bav/fr/home/contact/e-gesuche.html) [18].

5.1 Délimitations

Conformément au champ d'application, la responsabilité de la protection appropriée de leurs données et informations incombe au GI ou à l'ETF concerné. Le présent document définit les limites suivantes :

- Les dispositions contiennent des mesures visant à garantir un niveau de sécurité minimal de l'information.

- En fonction des conditions spécifiques à l'organisation et d'évaluations des risques, des mesures supplémentaires peuvent s'avérer nécessaires.

- La mise en œuvre des dispositions de la présente directive ne suffit pas pour obtenir une certification (par ex. ISO/IEC 27001).

[18] D'ici à l'entrée en vigueur de la présente directive, le nouveau formulaire de requête électronique est disponible sur bav.admin.ch. Jusqu'à nouvel ordre, il s'agit de transmettre la requête via l'adresse électronique : _BAV-WeiterentwicklungRegelwerke@bav.admin.ch

6 Rapport avec les autres systèmes de gestion

Lors de la conception et de la mise en œuvre du SGSI, il faut tenir compte du fait que les entreprises concernées disposent éventuellement déjà d'autres systèmes de gestion. Le SGSI doit être implémenté de manière à éviter tout conflit avec les systèmes de gestion existants. S'il s'avère impossible d'éviter des conflits avec des systèmes de gestion existants ou si l'on identifie des conflits potentiels, il convient de les documenter. Dans la mesure du possible et si cela s'avère pertinent, il convient d'utiliser les éléments existants et les synergies avec les systèmes de gestion déjà en place. Il s'agit de viser un système de gestion intégré (SGI) (cf. annexe 1).

7 Exigences minimales auxquelles doit répondre un SGSI

Le présent chapitre comprend les exigences relatives au SGSI dans le but d'ajuster et de piloter les aspects de la sécurité de l'information de manière systématique tout en tenant compte de l'ensemble des prescriptions et des besoins. **En outre, il concrétise la DE ad art. 5*c*, al. 1.2, DE-OCF** [2] **et définit les exigences minimales auxquelles doit répondre un SGSI**. L'accent est mis sur les exigences en matière de processus du système de gestion. Le **chapitre 8** décrit des mesures concrètes (contrôles) **qui contribuent au respect des exigences décrites dans le présent chapitre**.

La colonne « Renvoi » détaille les normes, standard et prescriptions régaliennes et indique les synergies potentielles avec les annexes I et II du règlement délégué 2018/762 [3][19]. La colonne « Contrôles » fait référence aux mesures liées l'exigence concernée.

Les entreprises ferroviaires sont tenues de tenir à jour un calendrier contraignant pour la mise en œuvre des exigences relatives au SGSI décrites ci-après et de le mettre à la disposition de l'OFT sur demande.

N°	Exigence	Renvoi	Contrôles chap. 8
A-01	**Stratégie en matière de sécurité de l'information** L'encadrement supérieur doit fixer les objectifs de la sécurité de l'information. Ceux-ci doivent être compatibles avec l'orientation stratégique de l'entreprise et avec les intérêts des parties concernées. L'encadrement supérieur doit veiller à ce que les ressources nécessaires à la réalisation des objectifs soient disponibles. En outre, il s'agit de définir les secteurs commerciaux couverts par le SGSI et ceux auxquels il ne s'applique pas. Le champ d'application minimal du SGSI est défini au chap. 5.	ISO/IEC 27001 ch. 5.1 NIST CSF 1.1 ID.BE-3 ID.GV-1 Manuel UTP ch. 3.2.1 et 3.2.3 RD 2018/762 ch. 1 et ch. 2.1	B-01 B-04 B-05 B-06 B-08 B-09 B-20
A-02	**Rôles et responsabilités** Les responsabilités et les compétences des rôles liés à la sécurité de l'information doivent être clairement définies et attribuées. Une personne chargée de la sécurité de l'information doit être désignée pour l'entreprise et communiquée à l'OFT.	ISO/IEC 27001 ch. 5.3 NIST CSF 1.1 ID.GV-2 Manuel UTP ch. 3.2.2 RD 2018/762 ch. 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] Les contenus des annexes I et II du règlement délégué 2018/762 étant identiques, aucune différentiation n'est faite entre eux.

N°	Exigence	Renvoi	Contrôles chap. 8
A-03	**Directives et organisation** **L'encadrement supérieur doit veiller à ce que le SGSI soit intégré dans les processus commerciaux de l'entreprise** (cf. exemple dans la Figure 1, annexe 1). Pour ce faire, il s'agit d'élaborer des directives en matière de sécurité de l'information qui doivent être approuvées par l'encadrement ou plus précisément par les personnes responsables, puis communiquées au sein de l'entreprise ainsi qu'auprès des services externes impliqués.	ISO/IEC 27001 ch. 5.2 NIST CSF 1.1 ID.GV-3 ID.GV-4 Manuel UTP ch. 3.2.3 RD 2018/762 ch. 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	**Vérification régulière de la sécurité de l'information / audits** La réalisation d'audits réguliers permet d'identifier les domaines dans lesquels la sécurité de l'information doit être améliorée. À cet égard, il s'agit également de prendre en compte les fournisseurs et les prestataires de. Les domaines thématiques à contrôler et la périodicité des audits doivent être consignés dans un programme d'audit. Les mesures qui en découlent doivent être mises en œuvre selon un ordre de priorité préétabli.	ISO/IEC 27001 ch. 9.1 ch. 9.2 NIST CSF 1.1 ID.SC-4 PR.PT-1 RD 2018/762 ch. 6.1 ch. 6.2	B-04 B-05 B-06 B-08 B-09 B-10 B-14 B-20
A-05	**Amélioration continue** L'entreprise doit améliorer constamment l'adéquation et l'efficacité de son SGSI. Cette vérification doit être effectuée au moins une fois par an.	ISO/IEC 27001 ch. 5.1 ch. 9.3 ch. 10 NIST CSF 1.1 RS.IM-1 RD 2018/762 ch. 6.3 ch. 7.2	B-04 B-08 B-14

N°	Exigence	Renvoi	Contrôles chap. 8
A-06	**Documentation** Toutes les activités et tous les résultats pertinents en rapport avec le SGSI doivent être documentés et consignés. À savoir en particulier : a) la description des processus et activités liés à la sécurité de l'information de l'entreprise ferroviaire, y compris les tâches déterminantes pour la sécurité et les responsabilités qui en découlent ; b) l'identification des mandataires, partenaires et fournisseurs, avec une description de la nature et de l'étendue des prestations fournies ; c) l'identification des conventions contractuelles et autres conventions commerciales entre l'entreprise et les autres parties citées à la let. b) qui sont nécessaires pour maîtriser les risques pour la sécurité générées par l'entreprise et le recours à des mandataires. La documentation et les journaux doivent être protégés contre toute consultation non autorisée et contre toute perte.	ISO/IEC 27001 ch. 4.1 ch. 2 ch. 7.5 NIST CSF 1.1 ID.GV-1 ID.GV-3 RD 2018/762 ch. 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	**Évaluation et traitement des risques** L'entreprise doit définir et appliquer un processus d'évaluation des risques liés à la sécurité de l'information. Des critères doivent être définis en matière d'acceptation des risques et de réalisation d'évaluations des risques. Ledit processus doit inclure les points suivants : **a) Identifier les risques** Les risques résultant d'une défaillance ou d'une perturbation des systèmes d'information doivent être identifiés en termes d'intégrité, de disponibilité et de confidentialité. Des personnes doivent être désignées comme propriétaires du risque. **b) Analyser les risques** Il s'agit d'évaluer les conséquences potentielles si les risques identifiés devaient se réaliser ainsi que la probabilité d'occurrence. **c) Évaluer les risques** Les conclusions de l'analyse des risques (évaluation des risques ou *risk assessment* en anglais) doivent être comparés aux critères de risque définis et il convient d'établir un classement par ordre de priorité en matière de traitement des risques. **d) Traiter les risques** Sur la base des conclusions de l'évaluation des risques, l'entreprise doit choisir des mesures appropriées pour traiter les risques ainsi que planifier et mettre en œuvre leur application. Le propriétaire du risque doit approuver ce plan, documenter les risques résiduels, les accepter le cas échéant et informer les collaborateurs et les parties externes. Il s'agit de s'assurer que ces étapes sont répétées en cas de changement significatif ou de détérioration du panorama des menaces. Les étapes a) à d) doivent être répétées au moins une fois par an afin d'identifier les nouveaux risques, de réévaluer les risques le cas échéant et d'évaluer l'efficacité des mesures mises en œuvre sur les risques.	DE-OCF 5*c*.1 ISO/IEC 27001 ch. 6.1.2 ch. 6.1.3 NIST CSF 1.1 ID.RM-1 ID.RM-2 ID.RM-3 Manuel UTP ch. 3.3 RD 2018/762 ch. 3.1 (Entrée dans les SGS des menaces pertinentes découlant de l'analyse des risques de la cybersécurité) Auxiliaires en matière de gestion des risques cf. Annexe 3	B-04 B-13 B-15 B-16 B-19 B-20 B-27

8 Contrôles (mesures de base)

Les mesures énumérées dans le présent chapitre contribuent à satisfaire aux exigences du chapitre 7 et à atteindre un niveau minimal de sécurité de l'information dans le secteur ferroviaire.

La mise en œuvre des mesures ou leur classement par ordre de priorité doivent être basés sur les risques. Cela signifie que des mesures supplémentaires peuvent s'imposer sur la base de l'analyse des risques et du besoin de protection des systèmes ou que certaines des mesures mentionnées ici ne sont pas opportunes.
Il est permis de réaliser d'autres mesures de compensation ou de réagir à des conflits d'objectifs, pour autant que l'objectif poursuivi par la loi et l'ordonnance soit ainsi atteint (cf. [11]). Les mesures de compensation doivent être consignées par écrit.

8.1 Contrôles organisationnels, personnels, physiques et technologie pour les TI et les TO, réseaux de données, y compris les véhicules ferroviaires

Le présent chapitre porte sur les mesures organisationnelles, personnelles, physiques et technologiques (contrôles) visant à garantir un niveau de sécurité de l'information adéquat pour le secteur ferroviaire, qui fait partie des infrastructures critiques de la Suisse.

Le ch. 8.1 présente les contrôles qui s'appliquent à tous les systèmes et applications. Le ch. 8.2 présente les contrôles spécifiques au domaine de la technologie opérationnelle (TO) et le ch. 8.3 les contrôles spécifiques aux systèmes embarqués.

La colonne « Contrôles » décrit des mesures concrètes qui s'orientent notamment sur les normes ISO/IEC 27001:2022 [8] ou ISO/IEC 27002:2022 [9]. La colonne « Renvoi » établit le rapport avec les normes, standards, auxiliaires et prescriptions régaliennes. La dernière colonne indique les synergies potentielles avec le SGSI [3].

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-01	**Détermination des rôles et responsabilités** Il faut définir les rôles et les responsabilités dans le domaine de la sécurité de l'information. Les différents groupes de tâches doivent être attribués à des personnes disposant des compétences nécessaires.	ISO/IEC 27002:2022 ch. 5.2 NIST CSF 1.1 ID.GV-2	ch. 2.3 ch. 4.1 ch. 4.2
B-02	**Gestion des accès et des identités** Les identités des personnes et des systèmes qui ont accès aux informations ou à d'autres actifs doivent être vérifiées et gérées. a) Une identité doit toujours être attribuée à une seule personne ou à un seul système. b) Il convient de définir quelles identités bénéficient de quelles autorisations et de quels accès. c) Les principes « du besoin de savoir » (*need-to-know*) et « de droit d'accès minimal » (*least-privilege*) doivent être appliqués. d) Les autorisations accordées doivent être régulièrement vérifiées et adaptées aux circonstances actuelles. e) Les identités qui ne sont plus actives doivent être désactivées.	ISO/IEC 27002:2022 ch. 5.3 ch. 5.15 ch. 5.16 ch. 5.17 ch. 5.18 NIST CSF 1.1 PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-6	

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-03	**Gestion des actifs (*asset management*)** a) Un inventaire des données, des informations et des systèmes de traitement de l'information doit être établi. b) Une personne responsable doit être désignée pour chaque actif ou catégorie. c) Une procédure doit être mise en place pour garantir que les nouveaux actifs sont inclus et que l'inventaire est mis à jour. d) Les actifs ou les catégories doivent être classés en fonction de leur besoin de protection en termes de confidentialité, d'intégrité et de disponibilité.	ISO/IEC 27002:2022 ch. 5.9 ch. 5.11 ch. 5.12 ch. 7.8 ch. 7.14 NIST CSF 1.1 ID.AM-1 ID.AM-2 ID.AM-5 Manuel UTP ch. 3.3.1 TS 50701:2023 ch. 4.2	ch. 5.2
B-04	**Gestion des fournisseurs** Conformément au champ d'application du chap. 5, il convient de s'assurer que la sécurité de l'information est prise en compte dans la collaboration avec les fournisseurs. a) Tous les fournisseurs et leur contribution à la sécurité de l'information doivent être recensés et évalués. b) En fonction du besoin de protection (criticité) des données traitées, les fournisseurs doivent être tenus, dans le cadre de la fourniture de leurs prestations, de respecter les directives pertinentes en matière de sécurité de l'information. Cette obligation doit également être transférée à leurs collaborateurs et à leurs éventuels sous-traitants. c) En outre, les collaborateurs des fournisseurs doivent être informés et formés par des formations régulières sur les prescriptions légales et internes relatives à la protection des informations et à l'utilisation sûre des systèmes de traitement des informations. d) Dès lors que les preuves ne sont pas suffisantes, il s'agit de prévoir un droit d'audit par contrat. e) Il convient de vérifier régulièrement si les dispositions contractuelles sont respectées.	ISO/IEC 27002:2022 ch. 5.18 ch. 5.19 ch. 5.20 ch. 5.21 LPD NIST CSF 1.1 ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 Manuel UTP Tableau 6 ch. 3.6 Cf. Annexe 3 Auxiliaires	ch. 2.4 ch. 5.3

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-05	**Sécurité de l'information dans des projet en rapport avec la TI et la TO** (y c. les acquisitions) ainsi que dans les développements de processus et d'organisation. a) Le projet doit suivre une méthode de gestion de projet définie. b) La sécurité de l'information fait partie intégrante de la méthode de gestion de projet. c) En début de projet, il convient de définir les besoins en matière de protection et les exigences pertinentes en matière de sécurité de l'information. d) En cours de projet, il faut vérifier et documenter le degré d'exécution des exigences susmentionnées. e) Il s'agit de communiquer au sein de l'entreprise les exigences non respectées en œuvre ou les risques connus. f) Les exigences en matière de sécurité de l'information doivent être intégrées dès le début des projets. Il convient de documenter leur respect et d'en informer les parties prenantes concernées.	ISO/IEC 27002:2022 ch. 5.2 ch. 5.8 NIST CSF 1.1 ID.RA-4 TS50701:2023 Figure 6	
B-06	**Mesure dans le domaine du *cloud*** Lors de l'acquisition de services *cloud*, il faut s'assurer que les exigences en matière de sécurité de l'information sont prises en compte et des mesures de protection mises en œuvre. Les services *cloud* qui concernent des processus essentiels pour l'entreprise ou des données personnelles doivent être examinés régulièrement dans le cadre d'un processus d'approbation interne afin de déterminer s'ils sont appropriés. a) Il s'agit de tenir une vue d'ensemble de tous les services *cloud* utilisés. Chaque service *cloud* doit être attribué à une personne responsable. b) Les responsabilités du fournisseur et de l'utilisateur du *cloud* doivent être clairement définies (modèle de responsabilité partagée). c) Avant d'utiliser des services *cloud*, il faut vérifier quelles données y sont stockées et traitées. Il convient de procéder à une analyse des risques et d'évaluer si les mesures de protection existantes ou celles proposées par le fournisseur de services *cloud* sont suffisantes.	LPD ISO/IEC 27002:2022 ch. 5.23 ch. 8.27 Manuel UTP ch. 3.6.3 Cf. Annexe 3 Auxiliaires	
B-07	**Surveillance (*security monitoring*)** Les systèmes et les réseaux doivent être conçus et configurés de manière que les attaques et les anomalies puissent être détectées et évaluées dans les meilleurs délais.	ISO/IEC 27002:2022 ch. 8.15 ch. 8.16 NIST CSF 1.1 DE.AE Manuel UTP ch. 3.6.4	

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-08	**Gestion d'incidents liés à la sécurité de l'information** Il s'agit d'établir des processus définissant la manière de traiter les incidents liés à la sécurité de l'information a) Le processus doit décrire la procédure à suivre en cas d'incident de sécurité et définir les responsabilités et les voies de communication. b) Le processus garantit que des mesures appropriées de réaction et de remise en état sont prises et mises en œuvre. c) Lors du traitement des incidents, il faut documenter les différentes étapes du traitement. d) Les obligations d'annoncer aux autorités et aux tiers (par ex. PFPDT[20], NCSC[21]) doivent être respectées. e) Des enseignements et des améliorations doivent être tirés des incidents liés à la sécurité de l'information	ISO/IEC 27002:2022 ch. 5.24 ch. 5.25 ch. 5.26 ch. 5.27 ch. 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 LPD LSI (future) OEIT	chap. 7 ch. 7.1. ch. 7.2.
B-09	**Gestion de la continuité des activités (*business continuity management*)** Il s'agit d'élaborer un processus garantissant la poursuite de l'activité en cas de défaillance de composants ou d'un système critique. Cela concerne non seulement les technologies de l'information et de la communication, mais aussi les TO et le domaine des véhicules. a) Les composants ou systèmes critiques sont identifiés et évalués. b) Un plan d'urgence et de remise en état doit être élaboré pour tous les composants et systèmes critiques. c) Ces plans sont testés et font l'objet d'exercices à intervalles réguliers ou après des modifications importantes.	art. 8 OTPE ISO/IEC 27002:2022 ch. 5.29 ch. 5.30 NIST CSF 1.1 ID.RA-4 RS.RP-1 Manuel UTP ch. 3.3.5	ch. 5.5

[20] www.edoeb.admin.ch

[21] www.ncsc.admin.ch

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-10	**Emploi de collaborateurs** Les mesures suivantes doivent être prises avant et pendant l'emploi d'une personne dans l'entreprise : a) En particulier pour les collaborateurs exerçant des activités sensibles en matière de sécurité : effectuer un contrôle de sécurité approprié en tenant compte des dispositions légales pertinentes et de la fonction prévue. b) Les collaborateurs sont informés par des formations régulières sur les prescriptions légales et internes relatives à la protection des informations et à l'utilisation sûre des systèmes de traitement des informations. c) Dans les conventions contractuelles, les collaborateurs sont tenus de respecter les prescriptions légales et internes en matière de sécurité de l'information. d) Les personnes qui travaillent avec des informations sensibles ou qui y ont accès doivent être tenues contractuellement au secret (obligation de maintien du secret). Modification et/ou résiliation de l'emploi : e) Les accès à l'infrastructure de l'entreprise doivent être rapidement désactivés pour les personnes qui quittent l'entreprise. f) Il convient d'établir un processus régissant la restitution ou la destruction des données, des informations et des appareils de traitement de l'information correspondants en cas de changement d'emploi (transfert et surtout départ).	ISO/IEC 27002:2022 ch. 6.1 ch. 6.2 ch. 6.3 ch. 6.4 ch. 6.5 ch. 6.6 NIST CSF 1.1 PR.AC-1 PR.AT-1 PR.AT-2 PR.AT-3 PR.IP-11 Manuel UTP ch. 3.7	ch. 4.2 ch. 4.3 ch. 4.4
B-11	**Exploitation de systèmes et de réseaux de données** Les systèmes et les réseaux de données doivent être configurés et protégés de manière à éviter les perturbations ou les pannes imprévues. a) Pour avoir une vue d'ensemble du réseau existant, il faut disposer de plans de réseau actualisés. b) Les réseaux doivent être séparés dans une mesure raisonnable et en tenant compte de leur taille. Pour ce faire, il convient d'établir un concept de réseau décrivant des mesures spécifiques en matière de protection de l'information. c) Si une mise en réseau de services TO et TI, par exemple à l'aide d'applications public-cloud, prend une telle ampleur que les passerelles ne peuvent plus être exploitées et gérées en toute sécurité au sens du concept classique des zones « *zones and conduits* », il faut mettre en place une architecture de sécurité appropriée, par exemple au sens du principe « à vérification systématique » (*zero-trust)* d) Les activités et les modifications des systèmes déterminantes pour la sécurité de l'information doivent être consignées conformément au processus de gestion des changements.	ISO/IEC 27002:2022 ch. 5.2 ch. 7.11 ch. 8.9 ch. 8.14 ch. 8.20 ch. 8.22 NIST CSF 1.1 PR.AC-5 PR.IP-1 PR.IP-3 PR.PT-4 Manuel UTP ch. 3.5	ch. 3.1.2

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-12	**Élaboration de directives (*policies*) en matière d'authentification pour les systèmes** a) Il convient d'établir des directives qui décrivent comment les utilisateurs s'inscrivent auprès des systèmes. b) Les directives décrivent les procédures d'authentification à utiliser (par ex. l'authentification à deux facteurs) et leur utilisation correcte. c) Les exigences de sécurité concernant les procédures d'authentification doivent, dans la mesure du possible, être appliquées techniquement (par ex. exigences minimales pour les mots de passe, modification des mots de passe initiaux). d) Si possible, il s'agit d'utiliser des procédures d'authentification fortes (par ex. authentification à deux facteurs, procédures à jetons ou biométriques, etc.).	ISO/IEC 27002:2022 ch. 5.17 NIST CSF 1.1 PR.AC-1 PR.AC-4 PR.AC-7 Manuel UTP ch. 3.5 Cf. Annexe 3 Auxiliaires	
B-13	**Mesures de protection des terminaux** Les terminaux utilisés dans le domaine des TI, des TO ou pour les véhicules doivent répondre aux exigences de sécurité suivantes : a) La configuration et l'utilisation se font conformément aux directives définies. b) Lors de l'utilisation de terminaux privés dans le contexte de l'entreprise, il faut veiller à ce qu'ils répondent au moins aux exigences de la directive établie en a). c) Les correctifs déterminants pour la sécurité doivent être installés en temps utile sur les systèmes et les terminaux. d) Si aucun correctif déterminant pour la sécurité ne peut être installé dans un délai raisonnable, il convient de prendre d'autres mesures en fonction des risques (par ex. restreindre les accès à distance, optimiser la surveillance de la sécurité afin de pouvoir identifier rapidement l'exploitation de points faibles). Cf. B-20 b)	ISO/IEC 27002:2022 ch. 8.1 NIST CSF 1.1 PR.DS-1 PR.DS-5 DE.AE-1 TS50701:2023 ch. 10.2 ch. 10.3 Manuel UTP ch. 3.5 Tabelle 6	
B-14	**Protection contre les maliciels (*malware*)** Des mesures de protection doivent être mises en œuvre en vue de la protection préventive et l'identification de maliciels sur les systèmes. Selon les technologies utilisées et l'objectif du système, l'implémentation peut se faire par l'utilisation de logiciels appropriés ou par un durcissement du système (par ex. protection du périmètre, défense en profondeur [*defence-in-depth*]). Pour TO : Cf. B-25	ISO/IEC 27002:2022 ch. 6.3 ch. 8.7 NIST CSF 1.1 DE.CM-1 DE.CM-4 DE.AE-2 TS50701:2023 B.4.4, C.3 Manuel UTP ch. 3.5	

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-15	**Gestion des configurations et des modifications** Les exigences en matière de sécurité de l'information doivent être respectées lors de la configuration du matériel informatique, des logiciels, des réseaux, ainsi que dans le domaine des TO et des véhicules. a) Les modifications doivent être autorisées et mises en œuvre selon un processus défini. b) Lors de la configuration, il convient de s'assurer que seules les personnes autorisées à exercer cette activité peuvent l'effectuer. c) Les mots de passe standards doivent être modifiés avant la mise en service.	ISO/IEC 27002:2022 ch. 5.22 ch. 8.9 ch. 8.32 NIST CSF 1.1 PR.IP-1 PR.IP-3 Manuel UTP ch. 3.5	ch. 5.2 ch. 5.4
B-16	**Travail à distance (*remote work*)** On parle de travail à distance lorsque des collaborateurs ou des prestataires de services externes travaillent depuis un lieu situé en dehors des locaux de l'entreprise tout en accédant à des informations via des appareils TIC. a) Lorsque des collaborateurs ou des prestataires de services externes accèdent à distance à des informations via des appareils TIC, il faut définir des directives sur la manière dont il convient d'articuler le travail à distance avec la sécurité de l'information. b) Il convient de définir les mécanismes d'authentification utilisés pour effectuer le travail à distance. c) Les collaborateurs doivent être sensibilisés au travail à distance et recevoir des informations appropriées (par ex. utilisation des comptes personnels). d) Il s'agit d'encourager des mesures garantissant que seules les personnes autorisées peuvent accéder aux informations via Internet (par ex. via VPN).	ISO/IEC 27002:2022 ch. 6.7 NIST CSF 1.1 PR.AC-3 PR.AT-1 PR-AT.3	
B-17	**Recours à des procédures cryptographique** Si des procédés cryptographiques sont utilisés dans des applications, ils doivent être basés sur des algorithmes reconnus et testés et sur une génération de clés sûre.	TS50701:2023 SR 4.2 SR 4.3 NIST CSF 1.1 PR.DS-1 Cf. Annexe 3 Auxiliaires	

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-18	**Protection des données et des informations** Les données et les informations doivent être protégées afin de répondre aux exigences de la loi, des autorités ou d'autres contrats. Il faut disposer d'une directive définissant les règles et les procédures de protection des données et des informations. a) Les données et les informations doivent être protégées lors de leur stockage et de leur transmission en fonction de leur besoin de protection. Il s'agit de documenter les mesures de protection et les procédures. b) Les données sensibles telles que les données personnelles ou les données d'accès doivent être protégées par des mesures techniques (par ex. par des procédés de chiffrage). c) Il faut mettre en œuvre des mesures de protection contre la perte de données au niveau des systèmes, des réseaux et autres appareils (par ex. la surveillance des accès aux données nécessitant une protection élevée). d) Il faut régulièrement effectuer et tester des copies de sauvegarde des données, des informations, des logiciels et des systèmes. e) Les données ou informations stockées sur des appareils ou des supports-mémoire qui ne sont plus utilisées doivent être effacées en fonction de leur besoin de protection. Pour la destruction des dispositifs de stockage, il est recommandé de faire appel à des fournisseurs agréés et certifiés de prestations d'élimination sécurisée.	ISO/IEC 27002:2022 ch. 5.24 ch. 5.31 ch. 8.10 ch. 8.11 ch. 8.12 ch. 8.13 ch. 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 LPD Manuel UTP ch. 3.5	ch. 4.5
B-19	**Protection des accès aux bâtiments et aux véhicules** Les bâtiments, les locaux et les zones contenant des systèmes déterminants pour la sécurité au niveau des installations, installations extérieures et des véhicules doivent être protégés, dans la mesure du possible et de manière proportionnée, contre tout accès non autorisé.	ISO/IEC 27002:2022 ch. 5.15 ch. 7.1 ch. 7.2 ch. 7.3 ch. 7.4 NIST CSF 1.1 PR.AC-2 Manuel UTP ch. 3.5.5	ch. 5.2
B-20	**Gestion des failles** Il faut mettre en place une gestion des failles qui prend en compte tous les systèmes et qui répond aux critères suivants : a) Les responsabilités en termes d'identification et de notification des failles doivent être clairement définies pour chaque système entre l'exploitant, l'intégrateur de systèmes, le fabricant et au niveau des accords de niveau de service (*service level agreements* [SLA]). b) Si une faille est identifiée, le risque qui en découle doit être évalué par le service compétent (il peut s'agir de plusieurs service), puis il s'agit de décider sur cette base si et quelles mesures immédiates peuvent être prises et quand ou dans quelles conditions un correctif de sécurité doit être appliqué. Cela peut générer un risque temporaire qui doit être assumé le cas échéant.	ISO/IEC 27002:2022 ch. 8.8 TS50701:2023 ch. 10.2 ch. 10.3 NIST CSF 1.1 PR.IP-12	

N°	Contrôle	Renvoi	Synergie avec RD 2018/762 [3]
B-21	**Séparation des environnements de développement, de test et de production** a) Les systèmes de développement, de test et de production doivent être séparés les uns des autres. b) Les modifications apportées aux systèmes de production doivent être effectuées dans un environnement de test avant d'être appliquées aux systèmes de production.	ISO/IEC 27002:2022 ch. 8.29 ch. 8.31 NIST CSF 1.1 PR.DS-7	

8.2 Contrôles spécifiques dans le domaine des TO

Dans le présent chapitre, les contrôles concernent aussi bien les systèmes TO des installations fixes que les systèmes TO embarqués.

Pour les systèmes TO, il faut partir du principe que l'accent est mis en particulier sur la disponibilité et l'intégrité des systèmes et que la confidentialité joue un rôle secondaire. Lorsque des mesures de cybersécurité sont mises en œuvre dans le domaine des TO, il faut donc toujours vérifier si celles-ci influencent la sécurité fonctionnelle (*safety*) ou l'exploitabilité du système concerné ou si elles ont des effets indirects en la matière. La mise en œuvre des mesures de cybersécurité doit toujours être décidée et réalisée en étroite collaboration et coordination avec la gestion de la sécurité, afin de tenir compte de manière appropriée des interactions possibles (absence de rétroaction) et de pouvoir identifier les risques.

Il s'agit de démonter l'absence d'effets rétroactifs, à savoir l'absence de répercussions, ce qui signifie que la fonction n'interfère pas avec d'autres fonctions liées à la sécurité. Des méthodes analytiques et des tests de régression doivent être utilisés au cas par cas pour apporter cette preuve.

Les modifications significatives ou importantes des systèmes existants sont soumises à autorisation conformément à l'art. 8 [2] OCF. En cas de doute, il convient de contacter l'OFT.

N°	Contrôle	Renvoi
B-22	**Installation de logiciels dans le domaine des TO** En raison de la criticité (besoin de protection) des systèmes TO, les installations de logiciels doivent être surveillées et contrôlées. a) L'installation de mises à jour sur les systèmes TO ne doivent être effectués que par du personnel qualifié. b) Il faut s'assurer que les mises à jour des logiciels des fabricants des systèmes TO sont mises à disposition dans une période définie préalablement avec ledit fabricant. c) L'installation de mises à jour doit passer par des procédures d'approbation qui impliquent également la gestion de la sécurité fonctionnelle. d) Avant d'installer des mises à jour sur des systèmes TO, le logiciel doit être testé de manière approfondie. Des protocoles de test doivent être établis pour documenter les fonctions testées et les éventuelles anomalies. En cas de problèmes, il ne faut pas procéder à l'installation ou à la mise à jour. e) Il s'agit de définir à l'avance une stratégie de *rollback*, permettant, en cas de non-fonctionnement, de ramener les systèmes TO à leur état initial de fonctionnement. f) Il convient de consigner qui installe des mises à jour ou des logiciels et pour quelle raison. g) Les anciennes versions du logiciel doivent être archivées avec les informations et les paramètres nécessaires.	TS50701:2023 ch. 9 ch. 10.2 ch. 10.3 NIST CSF 1.1 PR.DS-6 PR.MA-1

N°	Contrôle	Renvoi
B-23	**Identification et authentification** Par rapport aux systèmes informatiques classiques, les systèmes TO sont souvent très limités en matière de gestion des utilisateurs et de possibilités d'authentification, ou celles-ci ne s'avèrent pas réalisables conformément à l'état de la technique en raison d'exigences de disponibilité élevées. Il convient d'y remédier par des contre-mesures appropriées. a) Sur la base des risques, il s'agit de prendre des mesures compensant les possibilités d'authentification limitées de nombreux systèmes TO. Par exemple, une authentification forte à la limite de la zone réseau via un *policy enforcement point* tel qu'un proxy ou un point d'accès VPN, une surveillance accrue des accès au système par le biais de journaux d'accès, etc. b) Il s'agit de protéger les terminaux utilisés dans le cadre de systèmes TO en fonction de leur besoin de protection.	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	**Surveillance (*security monitoring*)** Les journaux déterminant pour la sécurité des systèmes en réseau doivent être transmis à un système central d'analyse et y être conservés conformément aux prescriptions internes de l'entreprise ou au concept de journalisation. Cf. 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	**Intégrité des systèmes** Souvent, il n'est pas possible d'installer un logiciel de détection sur les systèmes en vue d'une protection anti-maliciel. Il convient de mettre en place des mécanismes préventifs à titre de contre-mesures tels que des directives concernant l'utilisation de supports de données amovibles et de terminaux, associées à des mécanismes de détection en amont (par ex. IDS).	TS50701:2023 SR 3.2 NIST CSF 1.1 DE.CM-1 DE.CM-2 DE.CM-7 PR.PT-2
B-26	**Restriction du flux des données** En partant du niveau de protection des systèmes et de l'analyse des risques effectuée, les réseaux doivent être segmentés de manière judicieuse. Il faut veiller à ce que des zones du réseau puissent être séparées du reste du réseau en cas d'urgence afin de réduire les dommages à un minimum. Il convient donc de vérifier quels services centraux doivent être mis à disposition de manière redondante dans plusieurs zones (par ex. DHCP, DNS, etc.). Dans la mesure du possible et du raisonnable, il faudrait en particulier isoler les systèmes importants pour la sécurité fonctionnelle (*safety*) des autres réseaux afin de limiter les dommages.	TS50701:2023 SR 5.1 NIST CSF 1.1 PR.AC-5 RS.MI-1
B-27	**Disponibilité** a) Il faut établir une protection adéquate contre les attaques par déni de service. Les attaques ne doivent pas pouvoir se propager sur plusieurs systèmes ou zones de réseau. b) Il faut définir et mettre en œuvre une procédure de copies de sauvegarde (*backup*) appropriée pour les données et les fichiers pertinents. Il s'agit d'élaborer une stratégie de restauration des copies de sauvegarde. En outre, il convient de régulièrement tester la possibilité de restaurer les copies de sauvegarde afin de pouvoir garantir une restauration sûre et conforme des données. c) Les systèmes et les applications TO doivent être externalisés de manière qu'un système redondant assure la disponibilité en cas de panne. L'entreprise doit planifier et mettre en œuvre des procédures afin d'activer des composants et des équipements de traitement redondants.	TS50701:2023 SR 7.1 SR 7.2 SR 7.3 SR 7.4 SR 7.5 ISO/IEC 27002:2022 ch. 8.14 NIST CSF 1.1 PR.IP-4 PR.IP-7 PR.IP-9

8.3 Contrôles spécifiques pour des systèmes TIC embarqués

N°	Contrôle	Renvoi
B-28	**Identification et authentification** Dans les véhicules, les procédures d'authentification ne doivent pas empêcher l'accès rapide aux systèmes. Les systèmes dont le conducteur de locomotive a besoin pour faire fonctionner le véhicule ne doivent pas être bloqués automatiquement après l'identification initiale, par ex. par une clé ou un badge. La protection de l'accès doit en outre être assurée par des mesures physiques (par ex. portes de la cabine de conduite verrouillées). Pour les autres travaux qui ne sont pas effectués pendant l'exploitation commerciale ou normale, telles que les modifications de configurations logicielles ou de paramètres, il faut viser une gestion stricte des identifications et des authentifications.	TS50701:2023 SR 1.4 NIST CSF 1.1 PR.AC-1
B-29	**Protection physique** a) Il faut s'assurer par des mesures appropriées (par ex. armoire verrouillable) que les composants sensibles sont protégés contre les manipulations physiques. b) S'il n'est pas possible de mettre en œuvre une protection physique de manière à empêcher l'accès aux personnes ne disposant pas des autorisations suffisantes, il convient d'appliquer d'autres mesures, par exemple sous forme d'un système de surveillance des véhicules. c) Pour la surveillance, il faut configurer et protéger des systèmes d'alarme en conséquence (par ex. en installant une vidéosurveillance, en surveillant les couvertures de composants sensibles). (cf. point suivant) d) Les systèmes de surveillance doivent se situer dans une zone inaccessible à la personne qui déclenche l'alarme. e) Les systèmes de surveillance doivent être dotés de mécanismes inviolables et être testés régulièrement.	ISO/IEC 27002:2022 ch. 7.4 NIST CSF 1.1 PR.AC-2 Vidéosurveillance : OVid-TP [16]

9 Glossaire

Terme	Définition
Absence de rétroaction	Preuve que les adaptations effectuées n'ont d'effet que sur les systèmes, composants ou fonctions concernés, y compris les interfaces, conformément à la description des modifications, et plus précisément, que la fonction n'affecte pas d'autres fonctions liées à la sécurité.
Accès à distance	L'accès à distance doit permettre aux collaborateurs et à certains prestataires de services externes (par ex. à des fins de maintenance) d'accéder en toute sécurité au réseau d'une entreprise ou à un réseau TO, de sorte que certaines applications puissent également être utilisées de l'extérieur. À cet effet, il faut disposer d'un terminal équipé de sorte à être en mesure d'établir une relation de communication sécurisée avec le réseau de l'entreprise via un accès réseau (par ex. DSL, WLAN, téléphonie mobile) et un réseau de transfert (par ex. Internet).
Actif	Un actif (*asset*) est tout ce qui représente de la valeur pour l'organisation (également appelé bien informationnel et valeur informationnelle). Il existe de nombreux types d'actifs tels que les informations, les logiciels, le matériel, les services, les personnes et leurs qualifications, leurs compétences et leur expérience, ainsi que les actifs immatériels tels que la réputation et l'image. La norme ISO/IEC 27005:2022 fait la distinction entre les actifs primaires et secondaires. Les actifs primaires sont ceux qui doivent absolument être protégés. Ils constituent la valeur réelle d'une organisation ou d'une entreprise. Il s'agit par exemple des processus et des secrets professionnels, des données de base, de la réputation d'une entreprise, etc. Les actifs secondaires sont ceux qui sont nécessaires pour que les actifs primaires puissent développer leur valeur ajoutée. Il s'agit par exemple des moyens d'exploitation TIC (matériel, logiciels), des biens immobiliers, du personnel, des sites Web.
Agsec	L'**agrément de sécurité** comprend la confirmation que le système de gestion de la sécurité du gestionnaire d'infrastructure est opportun et l'acceptation des mesures préventives prises par le gestionnaire d'infrastructure pour assurer une exploitation sûre sur ses lignes.
Asset owner	L'*asset owner* (propriétaire des actifs) est la personne responsable de la gestion quotidienne des actifs. Cela englobe non seulement des informations numériques et imprimées, mais aussi du matériel, des logiciels, des services et des équipements.
Authentification / s'authentifier (de l'anglais « *authentication* »)	Le substantif « authentification » et le verbe « s'authentifier » décrivent des processus partiels différents, par exemple d'inscription. Un utilisateur s'authentifie sur un système via des informations d'inscription univoques (par ex. mot de passe ou carte à puce). Sur ce, le système vérifie la validité des données utilisées en procédant à l'authentification de l'utilisateur.
Autorisation	Dans le domaine des technologies de l'information, on entend par l'autorisation l'attribution initiale et le contrôle répété des droits d'accès aux données et aux services au moyen de méthodes spéciales. Les deux formes les plus courantes sont : • l'accès autorisé aux ressources (par ex. aux répertoires ou aux fichiers) stockés dans un réseau informatique. • l'autorisation d'installer ou d'utiliser des programmes informatiques.
Besoin de protection (classification d'un objet à protéger)	Le besoin de protection d'un objet s'oriente sur l'ampleur des dommages potentiels en cas de violation de la sécurité de l'information. Il peut s'agir de violations de la confidentialité, de la cohérence et de la disponibilité. Les catégories suivantes en matière de besoin de protection sont généralement courantes : • **Normal :** les conséquences des dommages restent limitées et maîtrisables.

	• **Élevé :** les conséquences des dommages peuvent être considérables. **Très élevé :** les conséquences des dommages peuvent menacer l'existence ou prendre une ampleur catastrophique.
BSI	***Bundesamt für Sicherheit in der Informationstechnik* (Office fédéral [allemand] de la sécurité des technologies de l'information)**
Cersec	Le **certificat de sécurité** dans le transport ferroviaire confirme que l'entreprise est organisée de manière à pouvoir effectuer des transports en toute sécurité sur une infrastructure étrangère avec le personnel et le matériel roulant appropriés.
CLC	**CENELEC** : Comité Européen de Normalisation Électrotechnique
Cohérence	Garantie de l'exactitude ou de l'intégrité des données ainsi que le bon fonctionnement des systèmes.
Confidentialité	La confidentialité signifie que les données ne peuvent être consultées ou transmises que par le personnel autorisé. Pour cela, il convient de définir clairement qui peut y accéder et comment. Cf. [5].
Contrôles	Les contrôles sont des mesures qui permettent de réaliser les objectifs des mesures et de réduire de manière significative les risques liés à la sécurité de l'information.
CSM-RA	***Common safety method for risk evaluation and assessment* (méthode de sécurité commune [MSC] relative à l'évaluation et à l'appréciation des risques)** de l'ERA (Agence de l'UE pour les chemins de fer)
Cyberattaque	Toute forme d'activité malveillante déclenchée intentionnellement par des personnes non autorisées et dirigée contre les technologies de l'information ou les personnes qui les utilisent.
Cybermenace	Toute circonstance ou tout événement susceptible d'engendrer un cyberincident.
Cybersécurité	Technologies, services, stratégies, pratiques et directives visant à protéger les systèmes ou les réseaux de technologie de l'information contre les attaques d'acteurs malveillants.
Cyberincident	Événement survenant lors de l'exploitation de moyens informatiques et susceptible de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations ou à la traçabilité de leur traitement.
Disponibilité	Il s'agit de la capacité d'un système à remplir une fonction requise dans des conditions données, à un moment donné ou pendant un intervalle de temps donné, pour autant que les moyens nécessaires soient mis à disposition [5].
ECE	**Entité chargée de l'entretien** Service chargé de la maintenance en matière de transport ferroviaire
ETF	**Entreprise de transport ferroviaire** (au bénéfice d'une concession)
GI	**Gestionnaires d'infrastructure** (des chemins de fer, à savoir les systèmes au sol)
IDS	***Intrusion detection system* (système de détection d'intrusion)**. Systèmes de détection d'accès non autorisés à des données ou à des ordinateurs.
ISACA	***Information Systems Audit and Control Association*** *:* association professionnelle internationale dont l'objectif est d'améliorer la gouvernance des systèmes d'information, notamment par l'amélioration des méthodes d'audit informatique
NCSC	**Centre national pour la cybersécurité**
OFT	**Office fédéral des transports**
OTPE	**Ordonnance sur les transports prioritaires dans des situations exceptionnelles** (RS 531.40).

Principe de droit d'accès minimal (*least-privilege*) Principe du besoin de savoir (*need-to- know*)	Un système ou une personne n'a accès qu'aux informations dont il a besoin pour accomplir ses tâches. Des tâches ou des rôles différents entraînent des informations de besoin de savoir différentes et donc des profils d'accès différents.
Principe « à vérification systématique » (*zero trust* en anglais)	Approche dans laquelle chaque accès aux ressources requiert une authentification. La fiabilité de chaque flux de données est ainsi vérifiée (cf. prise de position *zero trust* sur http://www.bsi.bund.de ou la publication spéciale NIST 800-207 sur https://nvlpubs.nist.gov/).
RS	**Recueil systématique** (droit suisse)
RTE	**Ouvrage de référence en matière de technique ferroviaire -** ouvrage de référence de l'UTP.
SCI	**Système de contrôle industriel** – (*industrial control system*) ; utilisé dans le présent document comme synonyme des abréviations « TO » et « SCADA ».
Sécurité de l'information	La sécurité de l'information vise à garantir l'authenticité, la confidentialité, l'intégrité et la disponibilité des données traitées par un système d'information et de communication ou enregistrées dans celui-ci.
Séparation des tâches (de l'anglais *segregation of duties* [SoD])	Aussi connu comme « principe de la séparation des fonctions ».
SGI	Le **système de gestion intégré** (de l'anglais, *integrated management system [IMS]*) regroupe dans une structure uniforme les méthodes et les instruments permettant de satisfaire aux exigences de différents domaines servant à la gouvernance d'entreprise (par ex. qualité, sécurité, sécurité de l'information, maintenance). L'exploitation des synergies et le regroupement des ressources offrent une gestion plus légère et plus efficiente que les systèmes de gestion individuels et isolés.
SGS	**Système de gestion de la sécurité** selon [3]
SGSI	**Système de gestion de la sécurité de l'information** (en anglais, *SGSI information security management system)* – partie du système de gestion transversal, basé sur une approche des risques commerciaux, pour établir, mettre en œuvre, exploiter, surveiller, vérifier, maintenir et améliorer la sécurité de l'information. Le système de gestion comprend la structure organisationnelle, les directives, les activités de planification, les responsabilités, les pratiques, les processus et les ressources.
SR	***System requirement*** (exigences système) selon CLC/TS50701, tableau 6 [11], resp. IEC 62443-3-3 [12]
Systèmes / applications traitant des informations	Systèmes et applications dans lesquels les informations sont traitées ou stockées.
TI	**Technologie de l'information** Toutes les techniques, le matériel et les logiciels utilisés en rapport avec le traitement électronique des données. Pour les comparaisons entre TI/TIC et TO, cf. manuel UTP, tableau 5 [13].
TIC	**Technologies de l'information et de la communication –** technologies utilisées pour gérer des processus de communication tels que les télécommunications, la radiodiffusion, les systèmes intelligents de gestion des bâtiments, les systèmes de traitement et de transmission audiovisuels et les fonctions de contrôle et de surveillance basées sur les réseaux.
TO	**Technologie opérationnelle** désigne le matériel et les logiciels qui surveillent et pilotent les performances des appareils physiques. Dans le passé, la TO concernait principalement les systèmes de pilotage et de surveillance dans les entreprises de fabrication, de transport et d'approvision-

	nement. Pour les comparaisons entre TI et TO, cf. manuel UTP, tableau 5 [13].
UTP	**Union des transports publics** (www.voev.ch)

D’autres cyber-termes sont disponibles sur https://www.ncsc.admin.ch/ncsc/fr/home/glossaire.html.

10 Annexe 1 – Système de gestion intégré et SGSI

Un système de gestion intégré (SGI) permet de regrouper les instruments existants prévus pour répondre aux exigences de différents domaines dans une structure uniforme et plus légère. Une présentation plus globale permet d'exploiter les synergies et de regrouper les ressources.

Les systèmes de gestion suivants disposent d'interfaces et donc d'un potentiel de synergie :

- Système de gestion de la sécurité (CSM SGS)
- Système de gestion de la qualité (QMS)
- Système de gestion de la maintenance ECE (CSM ECE)
- Système de gestion de la conformité (de l'anglais, *compliance management system* [CMS])
- Système de gestion des risques (GDR)
- Système de contrôle interne (SCI)

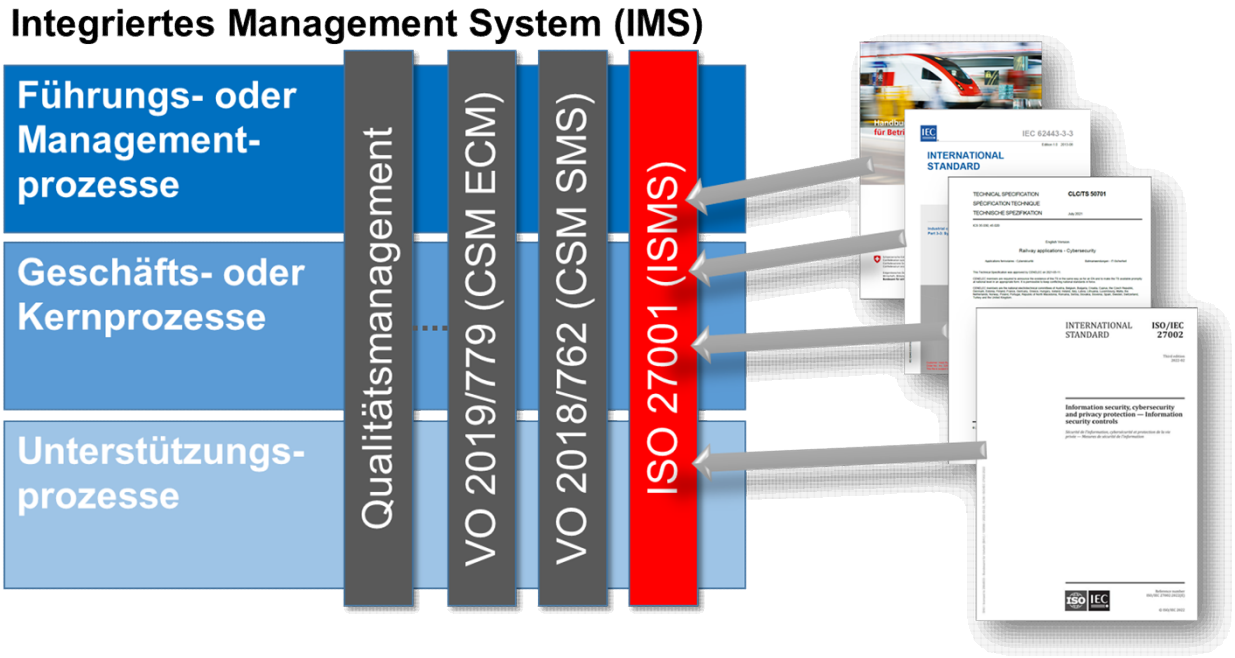
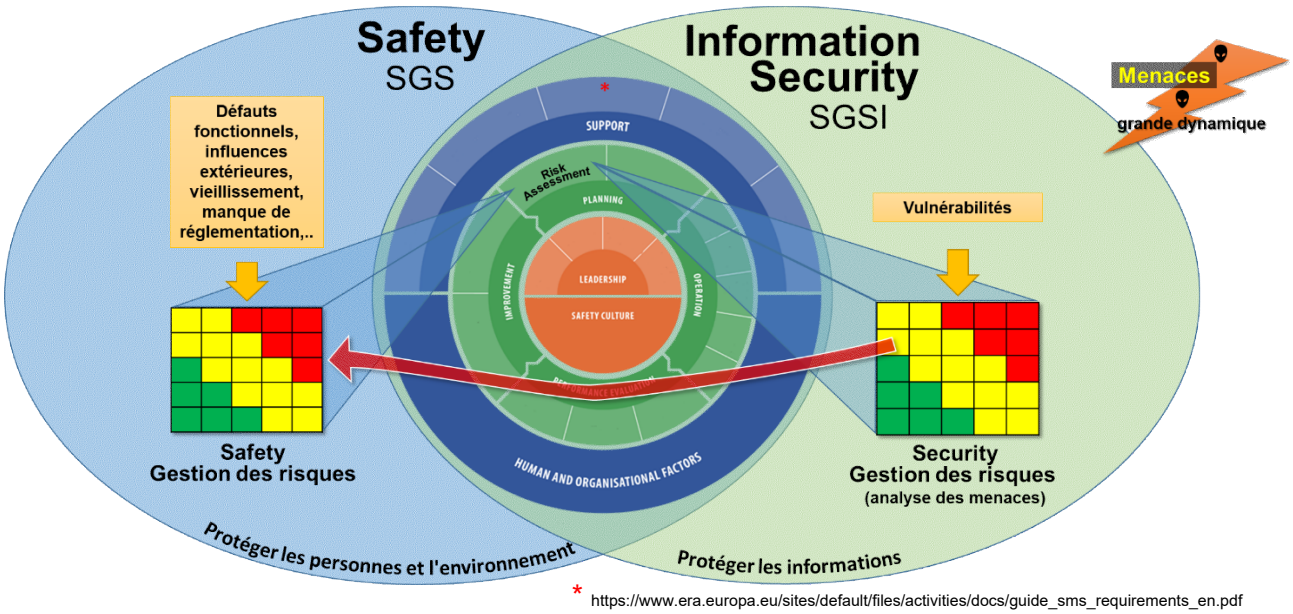


Figure 1 - SGI typique d'une moyenne ou grande entreprise de transport lié aux processus de l'entreprise, aux normes/standards avec exigences sécuritaires

Du point de vue de la sécurité, les SGSI et les systèmes de gestion de la sécurité (SGS) ont une interface commune. Les deux systèmes visent à réduire avant tout les risques afin d'améliorer continuellement le niveau de sécurité. Pour ce faire, il s'agit d'identifier les risques en amont et de les communiquer.

L'interface la plus importante entre un SGSI et un SGS est donc la gestion des risques. Les conclusions issues de l'analyse des menaces par un SGSI doivent être intégrées dans la gestion des risques du SGS, conformément à la Figure 2. Les risques jugés pertinents pour la sécurité doivent être consignés dans le journal des menaces (cf. *hazard-log* selon la norme SN EN 50126:2017).



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

Figure 2 – Rapports entre SGSI et SGS (illustration simplifiée avec la jonction la plus importante SGSI - SGS)

11 Annexe 2 – Aperçu de la norme ISO/IEC 27001 et ISO/IEC 27002

La série de normes ISO/IEC 27000 englobe plusieurs normes partielles sur le thème de la gestion de la sécurité de l'information.
La norme ISO/IEC 27001 est la norme centrale. Elle se compose d'une partie principale avec des exigences générales pour un SGSI et une vaste annexe A avec des objectifs de mesures spécifiques. Le champ d'application d'un SGSI porte généralement sur l'ensemble de l'entreprise. Les tâches importantes d'un SGSI sont :

- Formulation d'objectifs en matière de sécurité
- Détermination des actifs
- Évaluation des risques
- Traitement des risques
- Amélioration continue (par ex. selon le cycle PDCA – *plan-do-check-act*)

Selon la norme ISO/IEC 27001, toutes les informations, données et systèmes de traitement de données pertinents d'une entreprise doivent être saisis ou inventoriés. Les informations, données ou systèmes informatiques de même valeur et présentant des risques comparables peuvent être regroupés et considérés comme une seule valeur.

L'annexe A de la norme ISO/IEC 27001:2022 est un catalogue constitué de quatre thèmes sécuritaires (*control clauses*) de 93 *contrôles*. Les quatre thèmes sécuritaires sont :

- *Organizational controls* – mesures organisationnelles (5.1 à 5.37)
- *People controls* – mesures personnelles (6.1 à 6.8)
- *Physical controls* – mesures physiques (7.1 à 7.14)
- *Technological controls* – mesures technologiques (8.1 à 8.34)

Les explications concernant la mise en œuvre des 93 contrôles et des exemples de mesure se trouvent dans la norme ISO 27002.

L'annexe A de la norme ISO/IEC 27002:2022 présente les contrôles sous forme de matrice avec leurs valeurs d'attribut respectives. La matrice permet de regrouper et de filtrer les exigences de sécurité auxquelles une entreprise doit satisfaire.

Des informations complémentaires sur les normes et les standards sont disponibles dans le manuel sur la cybersécurité destiné aux entreprises de transports publics (ch. 6.2 [13]) et sur différents sites Web[22].

[22] Par exemple : https://en.wikipedia.org/wiki/IT_security_standards (en anglais)

12 Annexe 3 – Auxiliaires pour la mise en œuvre d'un SGSI

Auxiliaire	Remarque
Manuel sur la cybersécurité destiné aux entreprises de transports publics, manuel UTP de 2020) [13]	Le manuel UTP sert d'introduction à la sécurité de l'information dans le secteur des transports publics et permet aux entreprises de procéder à une auto-évaluation. Le manuel est basé sur la norme minimale TIC intersectorielle de l'Office fédéral pour l'approvisionnement économique du pays (OFAE[23]).
Implementierungsleitfaden ISO/IEC 27001:2022 de l'ISACA (cf[17] ; en allemand)	Sert d'auxiliaire en vue de l'implémentation d'un SGSI.
ICS Security Kompendium (en allemand et en anglais) : 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	L'*ICS Security Kompendium* de l'Office fédéral (allemand) de la sécurité des technologies de l'information (BSI) est un ouvrage de base pour la sécurité informatique dans les SCI.
Gestion des points faibles et des fournisseurs : ENISA : - *Good Practices for Supply Chain Cybersecurity* - *Threat Landscape for Supply Chain Attacks*	
Menaces actuelles : www.ncsc.admin.ch	Une fois inscrites, les entreprises peuvent se connecter au *Cyber Security Hub*. Le NCSC y fournit des informations sur les menaces actuelles. Les utilisateurs enregistrés ont la possibilité d'échanger activement des informations sur cette plate-forme. Les demandes d'enregistrement peuvent être transmises au NCSC via l'adresse électronique suivante : ncsc-useraccounts@gs-efd.admin.ch
Auxiliaires pour des analyses des risques (*risk assessments*) : - ISO/IEC 27005:2022 - IEC 62443-3-2 - CLC/TS 50701, chap. 6 et 7	Cf. également : http://www.enisa.europa.eu ➔ *risk management* et spécifiquement ferroviaire : https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management
Auxiliaires en matière de segmentation des réseaux : - IEC 62443-3-2 et IEC 62443-3-3 - CLC/TS 50701 - *Zoning and Conduits for Railways* (ENISA, ER-ISAC)	
NIST *Cryptography* : www.nist.gov/cryptography (en anglais)	Informations concernant les normes de chiffrement.
Recommandations du BSI concernant les procédures de chiffrement et les longueurs de clé : 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] https://www.bwl.admin.ch

https://standards.ieee.org/ (en anglais)	
Protection par mot de passe et informations complémentaires sur la sensibilisation des collaborateurs : http://www.s-u-p-e-r.ch/de/tipps/e-wie-einloggen/	Notamment des indications utiles concernant le choix des mots de passe.
Auxiliaire permettant de déterminer la maturité de la cybersécurité d'une organisation : Norme minimale pour les TIC	RAILplus propose son propre outil pour déterminer la maturité de la sécurité de l'information.
Auxiliaires sur le sujet du *cloud* : - Cloud Security Alliance (en anglais) - ENISA : Cloud Cybersecurity Market Analysis (en anglais) - BSI : Mindeststandard des BSI zur Nutzung externer Cloud-Dienste (en allemand et anglais uniquement) - BSI : Kriterienkatalog C5 (cloud computing compliance criteria catalogue) ; en anglais et en allemand	
Tableaux de mapping pour différentes normes : - Norme minimale pour les TIC – outil d'évaluation - *Mapping-Tabelle zwischen ISO/IEC 27019:2020 und ISO/IEC 27002:2022 der Bundesnetzagentur* (en allemand et en anglais) - *Mapping of OES security requirements to specific sectors,* de l'ENISA (en anglais)	Il n'est pas toujours garanti que les tableaux de mapping soient à jour.

Autres auxiliaires : cf. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen.html

13 Annexe 4 – liste de contrôle et demande d'exemption de l'obligation de devoir mettre en place un SGSI pour des ETF et des GI

Nom et numéro d'identification des entreprises (IDE) du requérant : ☐ ETF ☐ GI

Interlocuteur (Prénom, nom de famille, courriel, n° de téléphone, fonction) :

N°	Point de contrôle	Réponse	Commentaires / références
1	Nous utilisons les systèmes / véhicules suivants qui entrent dans le champ d'application des DE-OCF :		
2	Il existe des interfaces numériques avec les systèmes d'exploitation et techniques suivants (en particulier avec les systèmes d'arrêt automatique et de contrôle de la marche des trains)[24] : Remarque : veuillez également décrire le type d'interface (par ex. interface TCP/IP).		
3	Nous dépendons des prestataires de services suivants pour l'exploitation des systèmes mentionnés à la question 2[25] :		
4	Les prestataires de services (visés à la question 3) sont-ils tenus par contrat de respecter les exigences minimales de cybersécurité pour leur part de livraison ?	☐ Oui ☐ Non Si oui, quelles exigences minimales ? Remarques :	
5	Sans nos systèmes informatiques[26], nous pouvons maintenir nos activités pendant ... heures.	Nombre d'heures : Motif :	

[24] La figure 5 dans le manuel de l'UTP [13] peut servir d'aperçu.

[25] Les prestataires de services envisageables sont en premier lieu ceux des domaines des TI et des TO ainsi que les propriétaires d'installations et de matériel roulant loués.

[26] Les systèmes informatiques comprennent entre autres l'informatique d'entreprise et le stockage des données.

N°	Point de contrôle	Réponse	Commentaires / références
		Systèmes informatique pertinents pour l'exploitation (par ex. système de gestion du trafic) :	
6	Nous avons pris les mesures suivantes pour que les informations enregistrées numériquement et pertinentes pour notre exploitation et notre maintenance soient disponibles à tout moment[27] :		
7	Nous avons prévu les modifications/renouvellements suivants, qui sont / pourraient être pertinents en matière de cybersécurité.		
8	Bases existantes (par ex. analyses des risques, descriptions de systèmes) qui sont utiles pour l'évaluation de la présente demande (veuillez les joindre) :		
9	Le requérant doit justifier pourquoi la mise en place et la maintenance d'un SGSI ne sont pas pas jugées nécessaires pour son entreprise :		

Critères de dérogation à l'obligation de disposer d'un SGSI :

1. Le besoin de protection de l'information des systèmes TI et TO existants du requérant pour un fonctionnement sûr et fiable (criticité).

2. Importance du requérant (ETF ou GI) pour l'approvisionnement économique du pays et ses rapports avec les autres entreprises de transport.

3. Possibilités d'atteindre les objectifs de sécurité **sans SGSI avec les systèmes de gestion existants** tels que le SGS.

Remarques : la demande d'exemption de l'obligation de disposer d'un SGSI doit être renouvelée tous les cinq ans, et ce, en coordination avec les processus Cersec/Agsec (413/414). Si le requérant effectue des modifications pouvant avoir une incidence sur la cybersécurité, une demande actualisée doit être soumise à l'OFT au plus tard au moment de la mise en service de la modification.

Lieu, date :

Nom, Prénom et signature[28] :

[27] Par ex. copie de secours hors ligne, qui est régulièrement vérifiée

[28] Responsables au sens de l'art. 14, al. 4, OCF ; RS **742.141.1**