CYBERSÉCURITÉ

G15004 f Publication janvier 2025

INFORMATION

Guide

de mise en œuvre de la norme minimale pour la sécurité des technologies de l'information et de la communication dans l'approvisionnement en gaz (G1008)

axé sur le niveau de protection C

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de l'énergie OFEN

SVGW

gaz energie

Impressum

Date 24 janvier 2025

Lieu Zurich

Éditeur

Association pour l'eau, le gaz et la chaleur
SVGW
Grütlistrasse 44
8027 Zurich
Tél : +41 44 288 33 33
info@svgw.ch
www.svgw.ch

Association Suisse de l'Industrie Gazière
ASIG
Grütlistrasse 44
8027 Zurich
Tél : +41 44 288 31 31
vsg@gazenergie.ch
www.gazenergie.ch

Direction du projet

Daniela DECURTINS (ASIG)
Stéphane HENRY (OFEN)
Karsten REICHART (SVGW)

Auteurs principaux

Fabio BASTINE-NIEHÖRSTER (ASIG)
Marc BONVIN (OFEN)

Coauteur.e.s

Roger BÄCHTIGER (IFP)
Sandra BREITSCHMID (GVM AG)
Dominik CAVEGN (EGO AG)
Daniela DECURTINS (ASIG)
Stéphane HENRY (OFEN)
Hans-Peter KÄSER (OFCS)
Wolfgang KOROSEC (St.Galler Stadtwerke)
Marcel KÜHNI (Regionalwerke AG)
Christof NIEHÖRSTER (ASIG)
Sven PINTON (EZL AG)
Andreas WOLF (EGO AG)
Karsten REICHART (SVGW)

Traducteur

Marc BONVIN (OFEN)

Préface

La sécurité de l'approvisionnement en gaz suisse dépend entre autres de la résistance de la Suisse aux cyberattaques. Les menaces auxquelles le secteur énergétique est confronté ont augmenté drastiquement ces dernières années. Afin de se prémunir au mieux contre cette tendance, l'art. 39*a* de l'ordonnance sur la sécurité des installations de transport par conduites (OSITC ; RS 746.12) prévoit l'obligation de mesures de cybersécurité. Ces dernières sont fixées dans la norme minimale pour la sécurité des technologies de l'information et de la communication (TIC) dans l'approvisionnement en gaz (Norme minimale TIC G1008[1]) qui se base sur le *NIST Cybersecurity Framework V.1.1*[2] (NIST CSF V1.1) et définit par la même occasion des exigences[3] à atteindre pour chaque niveau de protection (A, B ou C).

Un outil d'autoévaluation (*Self-Assessment Tool*) est disponible[4] afin de faciliter la mise en œuvre de la norme minimale TIC G1008. En complément, la branche a élaboré ce guide. Il a pour objectif d'expliquer certains termes de la norme minimales TIC G1008 et de proposer une structure cohérente pour la mise en œuvre de la cybersécurité. Étant donné qu'il se concentre sur les 39 mesures obligatoires pour le niveau de protection C, le document s'adresse en premier lieu aux PME du secteur gazier. Bien évidemment, les recommandations peuvent également être suivies par d'autre entreprises.

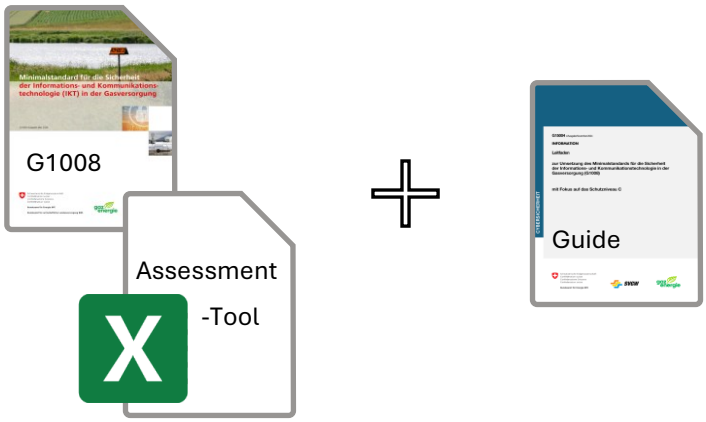

Figure 1 : Outils visant à renforcer la cybersécurité dans l'approvisionnement en gaz

Le guide se compose d'une première partie qui introduit les principes et notions de base de la cybersécurité. **La deuxième partie du document est consacrée aux 39 sous-catégories retenues pour le niveau de protection C**. Pour chaque sous-catégorie, les exigences ont été précisées, les attentes expliquées et une aide à la mise en œuvre formulée.

---

[1] La norme minimale TIC G1008 peut être téléchargé à l'adresse suivante : https://www.svgw.ch/fr/boutiquer%C3%A9glementation/produits/g1008-f-norme-minimale-pour-garantir-la-s%C3%A9curit%C3%A9-des-technologies-de-linformation-et-de-la-communication-tic-requises-pour-lapprovisionnement-en-gaz/.

[2] Le *NIST Cybersecurity Framework V.1.1* (NIST CSF V1.1) peut être téléchargé à l'adresse suivante : https://www.nist.gov/cyberframework.

[3] Les exigences se trouvent au chapitre 5.2 de la norme minimale TIC G1008.

[4] L'outil d'auto-évaluation peut être téléchargé à l'adresse suivante : https://www.bwl.admin.ch/bwl/fr/home/bereiche/ikt/ikt_minimalstandard.html.

Table des matières

Partie 1 – Introduction

Contexte et objectif

La sécurité des TIC implique un comportement basé sur les risques et l'utilisation de systèmes sûrs relevant de la responsabilité des acteurs concernés. La mise en œuvre de mesures recommandées, telles que présentées dans la norme minimale TIC G1008, permet déjà de se prémunir contre un grand nombre d'attaques contre les TIC moyennant un effort raisonnable. La norme minimale TIC G1008 a pour objectif de fournir aux entreprises et aux organisations un outil polyvalent leur permettant d'améliorer individuellement la résilience de leur infrastructure TIC.

Les exigences fixées dans la norme minimale TIC G1008 sont rendues obligatoires par l'art. 39*a* al. 4 OSITC[5]. Les entreprises sont donc tenues de mettre en œuvre les principes de cybersécurité prévus en fonction de leur catégorie (A, B ou C).

Ce guide sert d'aide à la mise en œuvre des exigences définies dans la norme minimale TIC G1008. Il se concentre sur les 39 sous-catégories sélectionnées pour le niveau de protection C. Les recommandations des 39 sous-catégories s'appliquent, bien entendu, également aux niveaux de protection A et B.

Le guide précise les exigences pour chacune des 39 sous-catégories. Il vise à faciliter la mise en œuvre des mesures avec des ressources limitées et à aider les entreprises à atteindre leurs objectifs de conformité.

Bien que ce guide ait été élaboré avec le plus grand soin, il ne garantit pas aux entreprises une protection infaillible contre les cyberattaques, ni le respect de toute les exigences fixées à l'art. 39*a* OSITC. Chaque entreprise reste responsable de sa cybersécurité. Bien que les mesures prévues par la norme minimale TIC G1008 visent à augmenter la résilience, la démarche de cybersécurité de chaque entreprise doit être basée sur un processus individuel de gestion des risques. Selon les objectifs, d'autres mesures peuvent ou doivent donc être prises en plus de celles mentionnées dans la norme minimale TIC G1008 et dans le présent document.

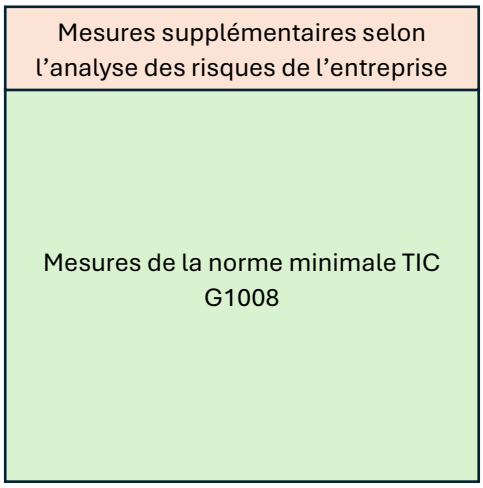

Figure 2 : Aperçu des mesures de cybersécurité

Certaines des 39 mesures retenues pour le niveau de protection C ne concernent que la mise en place organisationnelle et managériale de la cybersécurité, mais pas encore son exécution par

[5] Entrée en vigueur prévue le 01.07.2025.

des mesures techniques. La mise en place organisationnelle d'un processus ne suffit évidemment pas à garantir la sécurité de l'entreprise. Elle doit dans tous les cas être accompagnée de mesures techniques appropriées. Dans la mesure du possible, le présent guide recommande des outils qui doivent permettre ou faciliter la mise en œuvre technique de la cybersécurité.

La norme minimale TIC G1008 et le présent guide sont basés sur le NIST CSF V.1.1. Cette approche a fait ses preuves auprès des entreprises et au sein du secteur de l'énergie. Il existe toutefois d'autres moyens de mettre en œuvre un programme de cybersécurité et d'obtenir des résultats similaires. Chaque entreprise est libre de choisir la méthodologie qui lui permettra d'atteindre les exigences fixées. Pour faciliter l'implémentation, les correspondances avec d'autres normes reconnues (ISO, COBIT, NERC, BSI, ...) peuvent être consultées pour chaque mesure du standard minimal TIC sous l'onglet « *Assessment* » de l'outil d'auto-évaluation[6].

[6] L'outil d'autoévaluation peut être téléchargé à l'adresse suivante : https://www.bwl.admin.ch/bwl/fr/home/bereiche/ikt/ikt_minimalstandard.html.

Notions de base

Ce chapitre définit les notions et principes de base de la cybersécurité auxquels la norme minimale TIC G1008 fait référence, mais qui ne font pas partie des exigences. Ces différents concepts permettent une meilleure compréhension de la cybersécurité dans son ensemble.

Protection de l'information

La protection de l'information vise à protéger de manière adéquate les informations et l'infrastructure TIC en fonction des objectifs de protection définis, tels que la **confidentialité**, l'**intégrité** et la **disponibilité**. Il s'agit d'empêcher l'accès non autorisé aux systèmes ou la manipulation des informations et de réduire autant que possible les risques qui en résultent afin d'éviter les dommages économiques qui en découlent.

Dans le travail quotidien, les termes « protection de l'information », « protection des données » et « sécurité informatique » sont souvent confondus ou utilisés dans un contexte erroné.

Comme le montre le graphique ci-dessous, la protection des données et la sécurité informatique font partie de la protection de l'information, qui est elle-même une composante importante de la gestion des risques d'entreprise et de la gestion de la continuité des activités (GCA ou *Business Continuity Management BCM* en anglais).

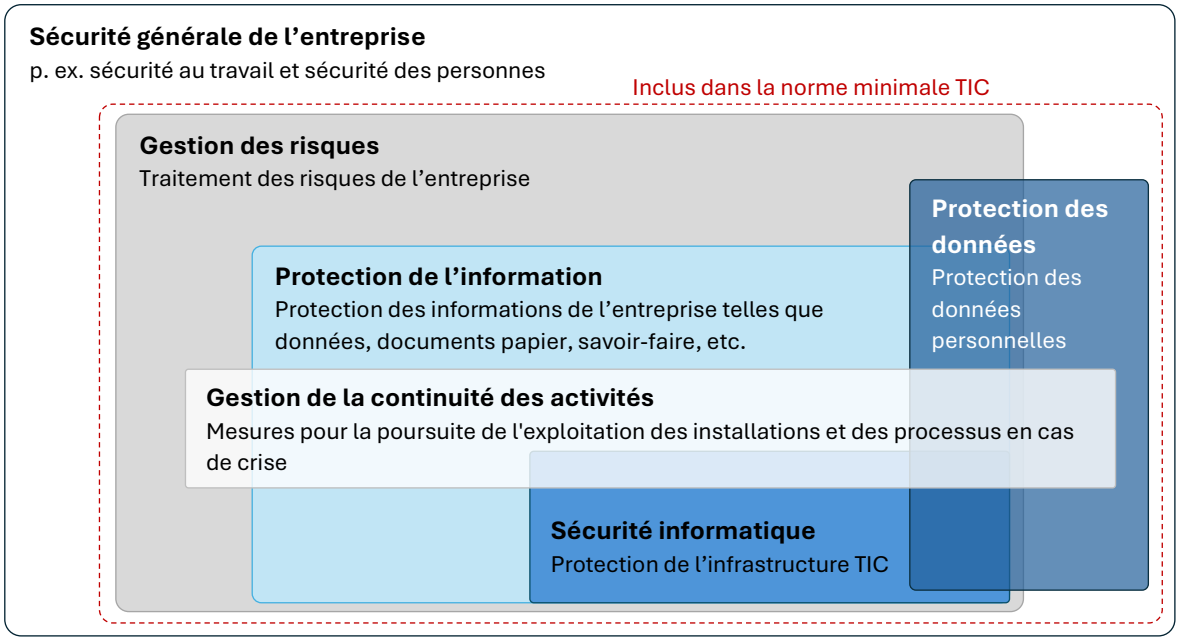

Figure 3 : Sécurité de l'entreprise

Stratégie de protection de l'information

Une stratégie de protection de l'information efficace protège les ressources d'une organisation qui sont nécessaires à l'exécution des processus commerciaux (critiques). Il n'existe pas de définition universelle des exigences ou des solutions.

Pour pouvoir identifier et traiter intégralement les risques de sécurité liés aux systèmes critiques d'information et de communication, il est indispensable d'adopter une stratégie de protection de l'information multicouche, qui suit le concept de défense en profondeur (*Defense-in-Depth*). Celui-ci repose sur le principe de l'utilisation de plusieurs couches de sécurité afin de contrer les attaques et de minimiser le risque d'une intrusion totale dans le système. Chaque couche – de la

sécurité physique aux contrôles d'accès, en passant par la protection du réseau – sert de barrière supplémentaire. Même si une couche est compromise, les autres continuent d'offrir une protection.

Outre les mesures techniques, cette stratégie devrait également comprendre les processus nécessaires, la formation et l'éducation des collaborateurs ainsi que la gouvernance de la sécurité requise. Cette dernière désigne la responsabilité de la direction de l'entreprise de concevoir l'organisation et les processus informatiques de manière à atteindre les objectifs fixés.

Les stratégies *Defense-in-Depth* sont individuelles et doivent s'orienter sur les besoins, les possibilités et les risques de l'organisation. L'approche basée sur les risques tient alors compte non seulement des processus ou des ressources internes, mais aussi des dépendances externes.

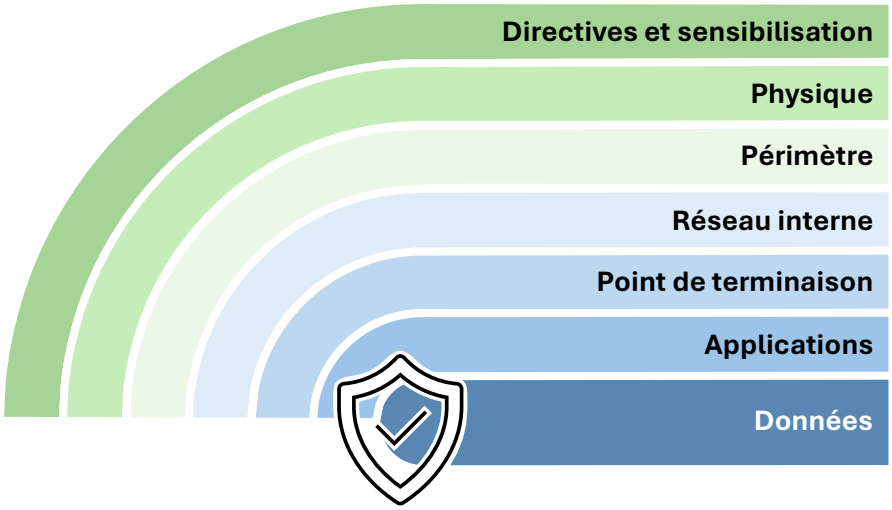

Figure 4 : Stratégie Defense-in-Depth

La stratégie ***Defense-in-Depth*** tient compte du fait qu'il ne peut pas y avoir de protection complète contre tous les types de cybermenaces. Au contraire, les propres vulnérabilités sont connues et des stratégies et mesures sont développées afin d'identifier l'exposition des TIC aux risques (IDENTIFIER), de se protéger au mieux (PROTÉGER), de détecter les atteintes à la cybersécurité (DÉTECTER) et de réagir (RÉAGIR) afin de revenir le plus rapidement possible à la situation normale (RÉCUPÉRER).

Protection des données

La protection des données décrit la protection des données personnelles et des données personnelles sensibles ainsi que la protection du droit à l'autodétermination en matière d'information. Elle comprend des mesures organisationnelles et techniques contre le traitement et l'utilisation abusifs de données personnelles.

La protection des données en Suisse est, en principe, régie par la loi fédérale sur la protection des données (LPD ; RS 235.1) et l'ordonnance sur la protection des données (OPDo ; RS 235.11). Toutefois, dès lors que des données de citoyens (clients, collaborateurs) de l'Union européenne sont traitées, il se peut que les prescriptions du Règlement général sur la protection des données de l'UE (Règlement (UE) 2016/679 du 27.04.2016, UE-RGPD) doivent également être observées en Suisse.

L'importance de la protection des données n'a cessé de croître depuis le début de la digitalisation, car la gestion, le traitement, la saisie, la transmission et l'analyse des données se simplifient

et sont de plus en plus complets. Les innovations numériques telles que l'Internet, la messagerie électronique, la téléphonie mobile, la vidéosurveillance ainsi que les moyens de paiement électroniques créent des possibilités toujours plus nombreuses et nouvelles de collecte de données personnelles.

Lors de l'enregistrement et du traitement de données personnelles, il convient notamment d'appliquer les principes suivants :

- Les données personnelles doivent être traitées conformément à ce qui est prévu par la loi.
- Leur traitement doit respecter les principes de bonne foi et de proportionnalité.

Les données personnelles ne doivent être traitées que dans la finalité déterminée lors de leur collecte, reconnaissable au vu des circonstances ou qui est prévu par la loi.

Sécurité informatique

La sécurité informatique, en tant que sous-domaine de la protection de l'information, sert à protéger les informations stockées électroniquement (données), leur traitement ainsi que les objectifs de protection que sont la **confidentialité**, la **disponibilité** et l'**intégrité**. Elle inclut également le fonctionnement sans faille ni interruption et la fiabilité des systèmes TIC.

Dans ce contexte, il faut également inclure les systèmes qui ne sont souvent pas directement identifiés comme des systèmes TIC, tels que les installations téléphoniques, les systèmes de commande (ICS) ou les systèmes IoT. Lors de l'utilisation de systèmes *Cloud* (en nuage), le champ d'action de la sécurité informatique classique s'étend au-delà du périmètre de l'entreprise dans le cyberespace.

Les fournisseurs de systèmes sont de plus en plus désireux de collecter et d'analyser les données d'exploitation des appareils et des systèmes. D'une part, pour améliorer leurs produits, d'autre part, pour suivre leur utilisation et leur déploiement. La publication intentionnelle de telles informations devrait faire l'objet d'un examen critique préalable, être clairement clarifiée et faire l'objet d'un contrat. Il convient également de définir par quelles connexions sécurisées et à quels intervalles (en temps réel, quotidien, hebdomadaire, etc.) les informations seront transmises aux fournisseurs.

Partie 2 – Précision des exigences

Dans ce chapitre, 39 des 108 sous-catégories sont décrites de manière plus détaillée afin de rendre la mise en œuvre de la norme minimale TIC G1008 plus compréhensible. Ces 39 mesures sont celles qui sont obligatoires pour le niveau de protection C.

En raison de la sélection des mesures les plus pertinentes pour le niveau de protection C, l'accent est mis sur les mesures de protection (PROTÉGER).

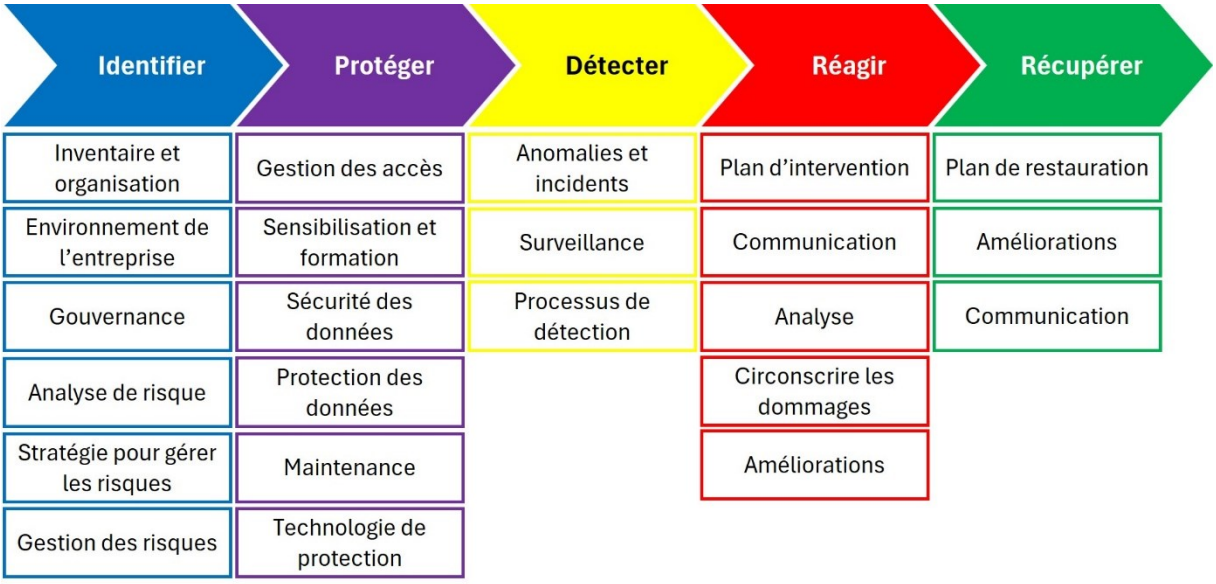

Figure 5 : Aperçu des catégories et sous-catégories du NIST CSF V1.1

Afin de faciliter la compréhension des attentes et la mise en œuvre des mesures de cybersécurité, la structure suivante a été suivie pour chacune des sous-catégories :

1. De quoi s'agit-il ?
2. Qu'est-ce qui doit être accompli ?
3. Comment satisfaire aux exigences ?
4. Quand les exigences sont-elles satisfaites ?
5. Lorsque cela s'avère utile : "Qu'est-ce qui est nécessaire pour la mise en œuvre ?"

Pour chaque sous-catégorie, le niveau de maturité correspondant au niveau de protection C est indiqué à droite sous « NM ». Vous trouverez de plus amples informations sur les niveaux de maturité au chapitre 4.5 de la norme minimale TIC G1008.

Sous-catégorie	NM
Tâche	...

Figure 6 : Exemple de sous-catégorie avec niveau de maturité

Le niveau de maturité indiqué correspond aux exigences légales minimales. Afin de se protéger efficacement, les recommandations contenues dans ce document vont parfois au-delà de ce qui est nécessaire pour respecter les exigences de conformité (notamment en ce qui concerne les indications temporelles). Il incombe à chaque entreprise de décider, en fonction de sa situation, de la fréquence à laquelle ses mesures de cybersécurité doivent être contrôlées, mises à jour et améliorées.

Identifier (ID)

La catégorie « identifier » aide à développer une compréhension organisationnelle de la gestion des risques de cybersécurité. La compréhension du contexte commercial, des ressources qui soutiennent les activités critiques et des risques de cybersécurité associés permet à une organisation de cibler et de prioriser ses efforts en fonction de sa stratégie de gestion des risques et des exigences opérationnelles.[7]

Inventaire et organisation (ID.AM)

Les informations, les personnes, les appareils, les systèmes et les installations d'une organisation sont identifiés, catalogués et évalués selon leur criticité par rapport aux processus opérationnels à réaliser, ainsi que selon la stratégie de gestion des risques de l'organisation.

Gouvernance (ID.GV)

La gouvernance constitue le cadre réglementaire pour la conduite et la surveillance de la cybersécurité. Elle définit les responsabilités, surveille et s'assure que les exigences réglementaires et juridiques de l'environnement commercial ainsi que les exigences opérationnelles sont correctement comprises et informe la direction en conséquence.

Gestion des risques liés à la chaîne d'approvisionnement (ID.SC)

Définissez les priorités, les contraintes et les risques maximaux que votre organisation est prête à assumer en lien avec les risques liés aux fournisseurs. Utilisez la définition des risques liés aux fournisseurs comme base pour évaluer les risques opérationnels.

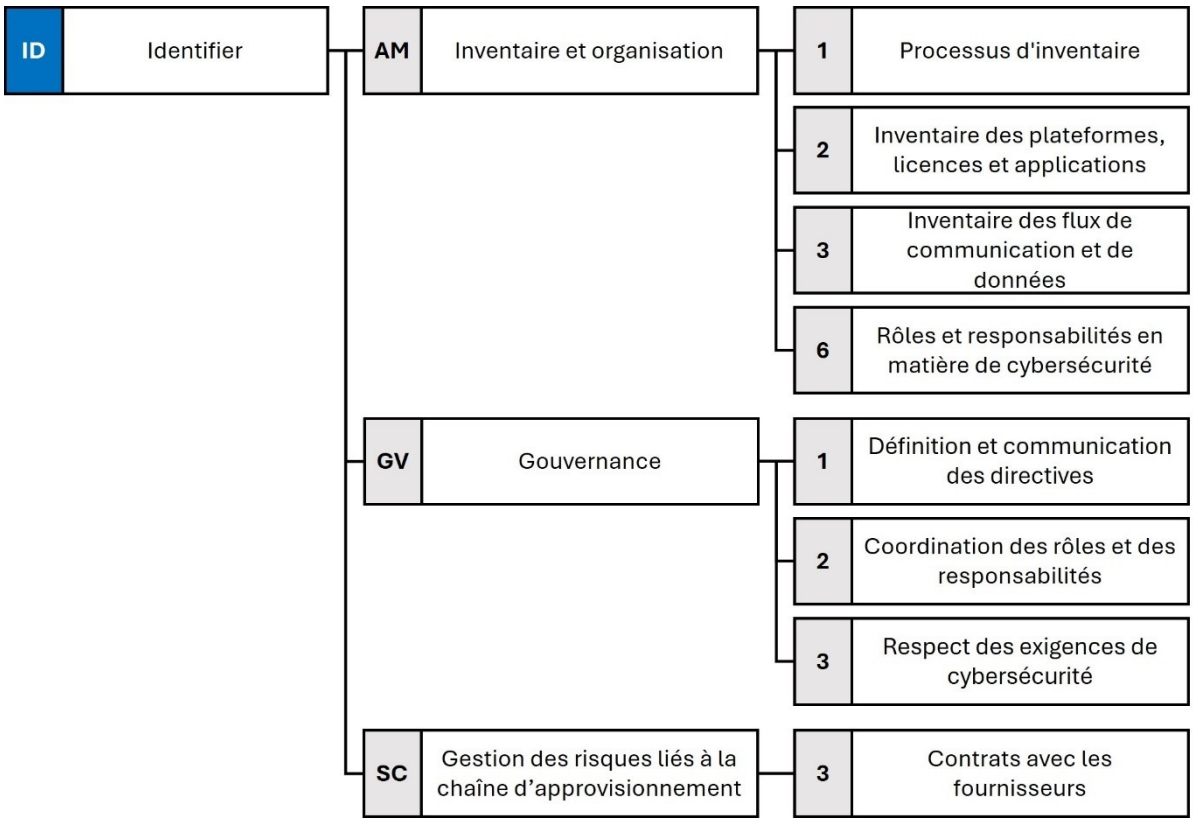

Figure 7 : Sous-catégories ID prescrites pour le niveau de protection C

[7] https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

Inventaire et organisation (ID.AM)

ID.AM-1 Processus d'inventaire	NM
Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC (Asset).	3

De quoi s'agit-il ?

ID.AM-1 exige la mise en place d'un processus garantissant la disponibilité continue d'un inventaire complet et actualisé de tous les équipements IT et OT. Un tel inventaire est essentiel pour une gestion efficace et la minimisation des risques de sécurité. Un inventaire manquant ou obsolète augmente le risque de failles de sécurité.

Qu'est-ce qui doit être accompli ?

Un processus d'inventaire efficace requiert les éléments suivants :

- Exhaustivité : tous les moyens d'exploitation (gérés de manière centrale, locale ou dans le cloud) doivent être répertoriés.
- Actualisation : l'inventaire doit être régulièrement mis à jour en cas de changements tels que des installations ou des mises à jour de systèmes.
- Unicité : chaque ressource doit être clairement identifiée afin d'éviter les doublons.
- Responsabilité : il est nécessaire de définir clairement les responsabilités en matière de gestion et d'entretien.

Comment satisfaire aux exigences ?

- Inventaire centralisé : tous les équipements sont enregistrés de manière centralisée avec des informations telles que les numéros de série et les détails du système.
- Identification univoque : les équipements sont saisis avec des identifiants individuels, les scanners de réseau aident à la saisie.
- Mise à jour automatisée : des processus de mise à jour automatique ou manuelle régulière sont nécessaires à chaque modification.
- Attribution des responsabilités : les responsabilités en matière de maintenance et de gestion doivent être définies et documentées.

Quand les exigences sont-elles satisfaites ?

Les exigences sont considérées comme satisfaites lorsque les éléments suivants sont mis en œuvre :

- Un inventaire complet et à jour de tous les équipements TIC est disponible.
- Tous les équipements sont clairement identifiés et sans doublons.
- Le processus d'inventaire est automatisé ou vérifié manuellement à intervalles définis.
- Les responsabilités sont clairement attribuées et documentées.

ID.AM-2 Inventaire des plateformes, licences et applications	NM
Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise.	2

De quoi s'agit-il ?

ID.AM-2 se concentre sur l'inventaire de toutes les plateformes logicielles (*software*), licences et applications utilisées au sein de l'organisation. Cela comprend aussi bien les solutions logicielles centralisées que les applications installées localement ou dans le *cloud*. Un inventaire complet et à jour des logiciels est essentiel pour assurer la conformité des licences, éviter les failles de sécurité et permettre une gestion efficace de l'environnement logiciel.

Qu'est-ce qui doit être accompli ?

Pour être efficace, le processus d'inventaire des logiciels nécessite les éléments suivants :

- Exhaustivité : toutes les plateformes logicielles, licences et applications utilisées doivent être répertoriées, y compris les informations sur leurs versions et leur utilisation.
- Actualité : l'inventaire doit être mis à jour régulièrement, en particulier lors de nouvelles installations ou désinstallations. Il est recommandé de procéder au moins à un contrôle annuel.
- Conformité des licences : les licences doivent être vérifiées régulièrement afin de s'assurer qu'il n'y a pas un excès ou une insuffisance de licences.
- Responsabilité : des responsabilités claires doivent être définies pour la gestion et la maintenance de l'inventaire des logiciels afin de garantir la conformité des licences et l'utilisation efficace des applications.

Comment satisfaire aux exigences ?

- Création d'un inventaire central des logiciels : enregistrez tous les produits logiciels, versions, licences et applications utilisés, y compris les contrats de licence et les utilisateurs qui leur sont assignés.
- Mise à jour automatisée ou manuelle : utilisez des processus automatisés pour enregistrer les nouveaux logiciels ou les mises à jour. Pour les logiciels installés manuellement, des vérifications régulières sont nécessaires.
- Gestion des licences : contrôle régulier des conditions/contrats afin de s'assurer que l'organisation respecte à la fois les exigences de conformité et qu'elle est couverte de manière rentable en termes de licences.
- Définir les responsabilités : les responsabilités en matière de gestion des logiciels et des licences doivent être clairement attribuées et documentées.

Quand les exigences sont-elles satisfaites ?

- Un inventaire centralisé de toutes les plateformes logicielles et licences utilisées est disponible et à jour.
- Les licences sont correctement attribuées et il est régulièrement vérifié qu'il n'y a pas de violation du contrat de licence.
- Les responsabilités pour la gestion et la maintenance de l'inventaire des logiciels sont documentées.

ID.AM-3 Inventaire des flux de communication et de données	NM
Listez tous les flux de communication et de transferts de données en interne.	2

De quoi s'agit-il ?

ID.AM-3 concerne le contrôle et la surveillance des flux d'informations au sein d'une organisation et entre les systèmes et les partenaires. L'objectif est de répertorier l'ensemble des flux d'informations afin de s'assurer que les bonnes informations sont transmises ou traitées par les systèmes autorisés, dans le respect de toutes les politiques de sécurité et de confidentialité.

Qu'est-ce qui doit être accompli ?

Pour répondre aux exigences d'ID.AM-3, tous les flux d'informations au sein de l'organisation doivent être cartographiés et documentés en indiquant les systèmes impliqués, les utilisateurs, les types de données échangées et les protocoles utilisés. Les règles et les mécanismes qui régissent les flux d'information doivent être clairement décrits et correctement mis en œuvre.

Comment satisfaire aux exigences ?

- Directives : mise en place de directives pour la gestion des flux d'information.
- Flux d'informations : identification, documentation et visualisation de tous les flux de données importants entre les systèmes et les utilisateurs, y compris les protocoles et les mécanismes de sécurité.
- Canaux de communication : cartographie de tous les canaux de communication internes et externes, y compris les scénarios tels que la télémaintenance.
- Classification : classez les informations en fonction de leur sensibilité et assurez-vous de respecter toutes les réglementations et les exigences de conformité.
- Architecture réseau : visualisation de l'ensemble du réseau, y compris les réseaux physiques, WLAN et virtuels, ainsi que les connexions entre les appareils.
- Surveillance : détectez les flux de données non autorisés à l'aide d'outils de gestion des événements de sécurité (SIEM). Pour sécuriser les informations, consultez la sous-catégorie
- Mise à jour régulière : adaptation de la documentation à chaque modification de l'architecture du réseau ou des flux d'information.

Quand les exigences sont-elles satisfaites ?

Tous les flux d'information des systèmes critiques sont cartographiés et contiennent les informations suivantes :

- Direction des flux.
- Types, sensibilité et stockage des données échangées et sensibilité.
- Processus (modification des données).
- Entités externes (source ou destination des informations).

Le diagramme peut être complété, par exemple, par les protocoles utilisés et les mécanismes de sécurité existants, mais devrait rester simple à interpréter.

ID.AM-6 Rôles et responsabilités en matière de cybersécurité	NM
Les rôles et responsabilités de l'ensemble du personnel et des parties prenantes externes (p.ex. fournisseurs, clients, partenaires) sont établies.	3

De quoi s'agit-il ?

ID.AM-6 définit des rôles et des responsabilités clairs en matière de cybersécurité, tant pour les collaborateurs que pour les partenaires externes, tels que les fournisseurs et les clients. L'objectif est de s'assurer que chacun sait qui est responsable de quels aspects de sécurité.

Qu'est-ce qui doit être accompli ?

- Rôles définis en matière de cybersécurité : qui assume quelles tâches dans le domaine de la cybersécurité (par ex. RSSI, responsable des risques informatiques, ...) ?
- Responsabilités claires : chacun doit connaître ses tâches, y compris les partenaires externes.

Comment satisfaire aux exigences ?

- Désignation des rôles clés : le RSSI assume la responsabilité principale de la cybersécurité. Dans les petites entreprises, le directeur informatique pourrait assumer des tâches supplémentaires telles que la gestion des risques.
- Documentation et communication : les responsabilités doivent être définies et communiquées par écrit, par exemple par le biais d'accords de non-divulgation, de directives de travail et de formations. Tous les collaborateurs, y compris les partenaires externes, doivent comprendre leur rôle.
- Collaboration : les acteurs de la cybersécurité doivent collaborer efficacement. Dans les petites entreprises, un petit nombre de personnes se partagent souvent ces tâches.
- Surveillance régulière : les responsabilités en matière de sécurité font l'objet de vérifications ou d'audits réguliers.

Quand les exigences sont-elles satisfaites ?

- Les rôles sont définis et attribués (par ex. le RSSI pour la coordination des mesures de sécurité).
- Les partenaires externes se soumettent aux exigences de sécurité et signalent tout changement ayant une incidence sur la sécurité (par exemple, changement de personnel).
- Des adaptations et des vérifications régulières sont effectuées.

Qu'est-ce qui est nécessaire pour la mise en œuvre ?

- Descriptions des rôles : définition claire des tâches de cybersécurité (internes et externes).
- Formations régulières pour les collaborateurs et les partenaires (voir PR.AT-2).
- Audits réguliers pour vérifier le respect des responsabilités en matière de sécurité.
- Soutien de la direction : la direction de l'entreprise doit souligner l'importance de la cybersécurité et veiller à ce que les rôles et les responsabilités définis soient assumés.
- Contrats avec les partenaires : les fournisseurs externes devraient être tenus de respecter les directives de sécurité par le biais d'un contrat (par ex. par un accord de non-divulgation).

Gouvernance (ID.GV)

ID.GV-1 Définition et communication des directives	NM
Des directives sur la sécurité de l'information sont établies et communiquées dans l'entreprise.	3

De quoi s'agit-il ?

Les entreprises doivent développer, approuver, communiquer et mettre à jour régulièrement des politiques de sécurité de l'information. Ces documents concrétisent les décisions stratégiques et les objectifs de l'entreprise. Elles se basent sur la gestion des risques et définissent les moyens pour atteindre les objectifs. Elles protègent les informations sensibles, les infrastructures ainsi que les activités critiques et veillent au respect des lois et des réglementations.

Qu'est-ce qui doit être accompli ?

Les politiques de sécurité de l'information être établies et connues de tous les employés. Des mises à jour régulières ne sont pas obligatoires, mais recommandées pour aborder les nouvelles menaces.

Comment satisfaire aux exigences ?

Il convient au minimum d'élaborer, d'adopter et de communiquer une stratégie de sécurité de l'information.

Les étapes suivantes doivent être prises en compte :

- Comprendre les objectifs et les risques : identifier les processus, les informations et les risques critiques.
- Respecter les lois, les prescriptions et les normes : une analyse doit être réalisée. La collaboration avec l'équipe juridique doit être privilégiée.
- Développer une politique de sécurité de l'information : définir des objectifs clairs, des responsabilités et des attentes.
- Communication et mise en œuvre : la politique doit être accessible à tous les collaborateurs (par ex. via l'Intranet) et communiquée clairement. Des formations sont recommandées.
- Mise à jour et amélioration : révision régulière de la politique, basée sur les nouvelles menaces et le cycle PDCA.
- Exemple de contenu d'une politique de sécurité :
  - Gestion des risques.
  - Conformité légale.
  - Contrôles de sécurité, gestion des accès.
  - Gestion des incidents, réaction aux incidents.
  - Sensibilisation et formation.
  - Protection des données, chiffrement, règles BYOD.
  - Utilisation de l'intelligence artificielle.

Quand les exigences sont-elles satisfaites ?

- Des politiques de sécurité de l'information sont en place et sont appliquées par les collaborateurs.
- Les exigences imposées à chaque collaborateur sont claires et documentées.

ID.GV-2 Coordination des rôles et des responsabilités	NM
Convenez entre les responsables internes (gestion des risques par ex.) et les partenaires externes des rôles et des responsabilités en matière de sécurité informatique.	3

De quoi s'agit-il ?

Cette exigence vise à coordonner efficacement les rôles de sécurité déjà définis. Tous les acteurs concernés doivent savoir comment collaborer dans le domaine de la sécurité de l'information afin de garantir une réponse rapide et efficace aux incidents.

Qu'est-ce qui doit être accompli ?

Les entreprises doivent coordonner clairement les rôles déjà définis, afin que chaque acteur connaisse ses tâches et collabore sur les questions liées à la sécurité.

Comment satisfaire aux exigences ?

Les exigences peuvent être satisfaites au moyen des mesures suivantes :

- Coordination centrale : le RSSI (s'il existe) coordonne toutes les équipes de cybersécurité et veille à une communication claire. Il échange des informations avec les autres responsables de la sécurité (RM, BCM, ...).
- Concertations régulières : des réunions d'information régulières sur les risques et les mesures de sécurité permettent de s'assurer que toutes les personnes concernées sont informées et que leurs connaissances sont à jour.
- Réaction efficace aux incidents : des plans d'urgence définis et des responsabilités claires permettent de réagir rapidement et de manière coordonnée aux incidents.
- Processus d'escalade clairs : des plans d'escalade bien établis et structurés garantissent une transmission rapide et ordonnée des informations critiques.
- Intégration de partenaires externes : une bonne communication avec les prestataires de services externes permet de préparer et d'influencer positivement la réaction aux incidents.
- Contrôle régulier : un contrôle périodique de la coordination et des processus permet de les adapter en permanence aux nouveaux enjeux.

Quand les exigences sont-elles satisfaites ?

Les exigences sont considérées comme satisfaites lorsque tous les rôles au sein de l'entreprise, mais aussi avec les prestataires de services externes, sont efficacement coordonnés et qu'une capacité de réaction rapide est garantie en cas d'incident de sécurité.

ID.GV-3 Respect des exigences de cybersécurité	NM
Vérifiez que votre entreprise respecte toutes les exigences légales et réglementaires en matière de cybersécurité, y compris au niveau de la protection des données.	3

De quoi s'agit-il ?

Le respect des exigences légales et réglementaires garantit un niveau minimum de cybersécurité, protège les infrastructures critiques et minimise les risques tels que les fuites de données et les intrusions dans les systèmes. En outre, la conformité réduit les coûts et dommages potentiels liés aux sanctions, aux cyberattaques ou aux interruptions d'activité et renforce la confiance des clients et des partenaires.

Qu'est-ce qui doit être accompli ?

Les entreprises devraient intégrer toutes les lois et réglementations applicables dans leurs procédures et être en mesure de prouver leur conformité. Cela concerne notamment la cybersécurité et la protection des données des infrastructures critiques.

Comment satisfaire aux exigences ?

La mise en œuvre d'ID.GV-3 nécessite une approche systématique visant à identifier et à respecter les obligations légales, réglementaires et contractuelles. Une étroite collaboration entre les équipes juridiques, de conformité et de sécurité est nécessaire pour adapter les politiques et les procédures aux développements externes. Les étapes suivantes doivent être respectées :

- Identification des obligations légales et réglementaires : analyser les lois, les normes et les obligations contractuelles en vigueur afin d'établir un inventaire complet.
- Définition de politiques et de procédures internes : développer des politiques de conformité et mettre en place des procédures de surveillance pour un contrôle continu.
- Formation et sensibilisation : organiser des formations pour les employés afin de garantir le respect des exigences (voir PR.AT-1).
- Surveillance et gestion des risques : mettre en place des mécanismes pour minimiser les risques de non-conformité.
- Mise à jour régulière : revoir régulièrement les directives et les adapter aux nouvelles prescriptions afin de garantir leur conformité.
- Documentation et communication : documenter toutes les mesures de conformité et rédiger des rapports réguliers pour la direction et les parties prenantes.

Quand les exigences sont-elles satisfaites ?

Les exigences sont remplies si l'entreprise connaît et applique toutes les dispositions réglementaires pertinentes et peut prouver à tout moment qu'elle les respecte.

Gestion des risques liés à la chaîne d'approvisionnement (ID.SC)

ID.SC-3 Contrats avec les fournisseurs	NM
Exigez de vos fournisseurs et prestataires de services qu'ils s'engagent contractuellement à développer et à mettre en œuvre des mesures appropriées pour atteindre les objectifs du processus de gestion des risques liés à la chaîne d'approvisionnement.	3

De quoi s'agit-il ?

De plus en plus d'attaques se concentrent sur la chaîne d'approvisionnement. Les conséquences peuvent être graves, car certains services critiques sont souvent fournis par des prestataires externes. La relation étroite entre l'opérateur et le fournisseur ne doit en aucun cas masquer le besoin de cybersécurité. Chacun doit œuvrer à la résistance aux cyberattaques. La transparence, la communication et la collaboration sont des éléments clés de la cybersécurité.

Qu'est-ce qui doit être accompli ?

Les exploitants et leurs partenaires/fournisseurs doivent conclure des accords contractuels afin de s'assurer qu'ils respectent les exigences en matière de cybersécurité. L'exploitant doit pouvoir prouver que toutes les mesures nécessaires sont prises pour se protéger contre les cyberattaques. Le fournisseur, quant à lui, doit démontrer le sérieux de sa démarche.

Comment satisfaire aux exigences ?

Afin de garantir la cybersécurité dans le cadre de la collaboration avec les fournisseurs, il convient d'envisager les mesures suivantes[8] :

- Identifier les risques de la chaîne d'approvisionnement : identifier les fournisseurs critiques, leurs produits et services et évaluer les risques et impacts potentiels.
- Évaluer les fournisseurs : avant de faire appel à un nouveau fournisseur, un examen doit être réalisé. Il convient de répondre à des questions spécifiques concernant les politiques de sécurité, les certifications, la gestion des vulnérabilités, l'hébergement des données et le chiffrement. Ces questions concernent notamment les normes de sécurité des systèmes, la gestion des données et les mécanismes de contrôle pour garantir la cybersécurité.
- Définir les exigences de cybersécurité dans les contrats : les clauses peuvent contenir des exigences telles que les normes de sécurité à respecter (NIST, ISO, ...), des instructions pour la notification des incidents ou des violations de la protection des données ou encore des audits de sécurité réguliers.
- Planification de la continuité des activités (BCM) : obligation de respecter les processus de gestion des incidents comprenant entre autres des délais de notification clairs et des mesures en cas de cyberattaque. En outre, les fournisseurs doivent disposer de plans de continuité des activités et de reprise après un incident afin de minimiser l'impact sur leurs services et leur organisation.

Quand les exigences sont-elles satisfaites ?

L'opérateur a rempli ses objectifs s'il a exigé de ses fournisseurs qu'ils lui fournissent les informations requises et s'il a vérifié que les systèmes et les applications permettent de satisfaire aux critères mentionnés.

---

[8] De plus amples informations sont disponibles à l'adresse suivante : https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html

Protéger (PR)

La catégorie « protéger » décrit les mesures de protection appropriées afin d'assurer la fourniture de services d'infrastructures critiques et de limiter ou de minimiser l'impact d'un incident de cybersécurité éventuel.

Gestion des accès (PR.AC)

Veiller à ce que l'accès physique et logique aux ressources et installations TIC ne soit possible que pour les personnes, processus et appareils autorisés et uniquement pour les activités qui ont été préalablement autorisées. Ceci doit être réglé en fonction de l'évaluation du risque d'accès non autorisé aux activités et transactions autorisées.

Sensibilisation et formation (PR.AT)

Veillez à ce que vos collaborateurs et partenaires externes soient régulièrement formés et instruits sur tous les aspects de la cybersécurité. Veillez à ce que vos collaborateurs et partenaires externes exécutent leurs tâches liées à la sécurité conformément aux directives, accords et processus correspondants.

Sécurité des données (PR.DS)

Les informations, les données et les supports de données sont gérés de sorte que la confidentialité, l'intégrité et la disponibilité des données puissent être protégées conformément à la stratégie de l'organisation en matière de risques.

Règles de protection des données (PR.IP)

Des directives pour la protection des systèmes d'information et des moyens d'exploitation sont établies. Ces directives comprennent au minimum l'objectif, la portée, les rôles et les responsabilités ainsi que la coordination au sein de l'organisation. Ces directives sont utilisées pour protéger les systèmes d'information et les ressources.

Maintenance (PR.MA)

Les travaux d'entretien et de réparation des composants des systèmes informatiques et des ICS sont effectués conformément aux directives et aux processus en vigueur.

Technologies de protection (PR.PT)

Des solutions techniques de sécurité sont installées afin de garantir la sécurité et la résilience des systèmes et des données conformément aux prescriptions et aux processus.

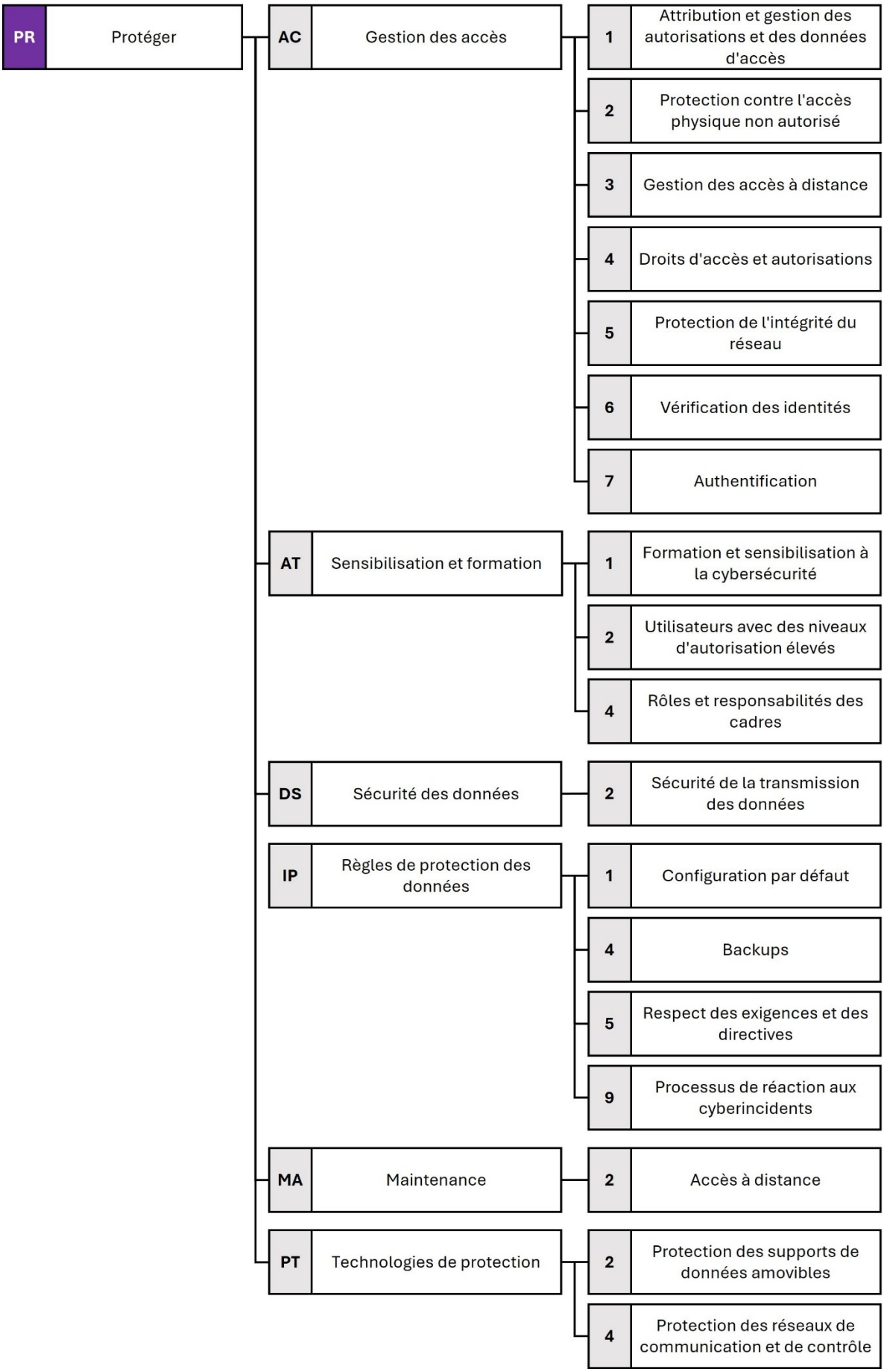

Figure 8 : Sous-catégories PR prescrites pour le niveau de protection C

Gestion des accès (PR.AC)

PR.AC-1 Attribution et gestion des autorisations et des données d'accès	NM
Définissez un processus clair pour octroyer et gérer les autorisations et les données d'identification pour utilisateurs, appareils/machines et processus.	2

De quoi s'agit-il ?

Cette mesure garantit que seuls les utilisateurs, appareils et processus autorisés ont accès aux ressources. Les identités et les autorisations sont gérées, contrôlées, révoquées et auditées. Les objectifs sont la mise en place de procédures de gestion des comptes utilisateurs, l'attribution univoque des identités ainsi que la révocation des autorisations en temps voulu.

Qu'est-ce qui doit être accompli ?

Les entreprises devraient implémenter les mesures suivantes :

- Matrice des utilisateurs et de leurs autorisations.
- Processus de gestion du cycle de vie des autorisations.
- Mécanismes de vérification de l'identité et d'attribution des autorisations.
- Authentification à deux ou plusieurs facteurs (2FA/MFA).
- Procédures de désactivation des comptes et de retrait des autorisations.
- Révocation à temps des autorisations afin d'éviter tout accès non-autorisé.

Comment satisfaire aux exigences ?

Les étapes suivantes devraient être entreprises :

- Directives : développer et appliquer des directives pour la gestion des identités et des autorisations, y compris les règles 2FA/MFA et les mots de passe.
- Changement de personnel : adapter les autorisations en cas de départ ou de changement interne. Les feuilles de suivi peuvent être très utiles à cet égard.
- Administration : utilisation de comptes administrateurs spéciaux à différents niveaux (par ex. domaine, serveur, terminaux).
- Audits : contrôle et audits réguliers des autorisations, par exemple selon la norme PS-CH 890[9].

Quand les exigences sont-elles satisfaites ?

Les exigences sont considérées comme satisfaites si :

- Les directives et les procédures sont documentées et appliquées.
- Les processus de gestion des comptes et des autorisations sont documentés par écrit et appliqués de manière vérifiable.
- Des formations avec attestation de participation sont organisées.
- Recommandation : réaliser des audits sur l'application des directives et des procédures.

[9] La norme peut être téléchargée dans la boutique en ligne d'EXPERTSuisse : https://www.expertsuisse.ch/fr-ch/boutique-en-ligne (payant).

PR.AC-2 Protection contre l'accès physique non autorisé	NM
Assurez-vous que seules les personnes autorisées ont physiquement accès aux équipements TIC. Prenez des mesures (architecturales) concrètes pour garantir que les ressources TIC sont protégées contre tout accès physique non autorisé.	2

De quoi s'agit-il ?

PR.AC-2 vise à contrôler et à protéger l'accès physique aux ressources critiques de l'entreprise. Cela permet de minimiser les risques liés aux menaces physiques et aux manipulations non autorisées.

Qu'est-ce qui doit être accompli ?

Pour atteindre les exigences de PR.AC-2, les entreprises devraient implémenter les mesures suivantes :

- Développer des directives et des procédures pour l'accès physique aux infrastructures critiques.
- S'assurer que seules les personnes autorisées ont accès aux zones sensibles.
- Enregistrer les accès afin de pouvoir retracer les incidents de sécurité.
- Examiner régulièrement les contrôles d'accès physique pour s'assurer qu'ils restent efficaces et répondent aux exigences de sécurité actuelles.

Comment satisfaire aux exigences ?

- Créer des directives et des procédures pour l'accès physique aux infrastructures critiques, y compris les autorisations d'accès, les mesures de protection et les procédures d'accès d'urgence.
- Implémenter des systèmes de fermeture et d'accès électroniques (p. ex. puces/clés RFID, lecteurs biométriques, codes d'accès).
- Mettre en place de mesures physiques (architecturales) de sécurité (p. ex. portes renforcées, sécurisation des fenêtres, etc.).
- Vérifier régulièrement les protocoles d'accès pour détecter les accès et activités non autorisés.
- Réaliser des audits annuels sur l'attribution, l'utilisation et la révocation des accès physiques. L'audit peut par exemple être effectué selon la norme PS-CH 890[10], comme cela est parfois exigé lors de la révision comptable.

Quand les exigences sont-elles satisfaites ?

- Les directives et les procédures sont documentées, mises en œuvre et appliquées.
- Selon la taille de l'entreprise, les protocoles d'accès sont vérifiés et les résultats sont documentés.
- Recommandation : au moins une fois par an, l'application des directives et procédures concernant l'octroi, l'utilisation et la révocation de l'accès physique aux infrastructures critiques est auditée, documentée et validée.

[10] La norme peut être téléchargée dans la boutique en ligne d'EXPERTSuisse : https://www.expertsuisse.ch/fr-ch/boutique-en-ligne (payant).

PR.AC-3 Gestion des accès à distance	NM
Définissez les processus pour gérer les accès à distance.	3

De quoi s'agit-il ?

PR.AC-3 a pour objectif la gestion sécurisée de l'accès à distance aux systèmes et aux données afin de protéger l'intégrité, la confidentialité et la disponibilité des informations. Cette mesure garantit que les utilisateurs distants peuvent accéder aux ressources en toute sécurité, tout en minimisant le risque de menaces de sécurité.

Qu'est-ce qui doit être accompli ?

- Créer des directives et des procédures pour l'accès à distance aux systèmes et aux données.
- Implémenter des procédures et des technologies sécurisées pour autoriser l'accès à distance.
- Surveiller et enregistrer les accès à distance afin d'identifier les activités non autorisées et suspectes.
- Enregistrer les accès à distance pour assurer la traçabilité en cas d'incident de sécurité.
- Sensibiliser et former les utilisateurs.

Comment satisfaire aux exigences ?

- Développer des directives et des procédures pour un accès à distance sécurisé. Les éléments suivants doivent être pris en compte :
  - Les accès à distance doivent être inventoriés, décrits et leur criticité évaluée.
  - L'accès à distance doit être limité au strict nécessaire (*need-to-know*).
  - Accès uniquement après authentification et autorisation, par ex. 2FA/MFA avec utilisation préférentielle d'une application d'authentification pour téléphones mobiles.
- Chiffrer les connexions d'accès à distance et les faire aboutir sur un composant d'accès à distance fiable, par exemple sur un proxy inverse et non directement sur le système cible.
- Installer régulièrement des mises à jour de sécurité pour les logiciels et les appareils d'accès à distance.
- Obliger contractuellement les prestataires de services à la gestion des correctifs, au chiffrement, à la protection des accès et à la protection des terminaux. L'entreprise se réserve le droit de vérifier à tout moment le respect de ces prescriptions, par elle-même ou par des tiers.
- Enregistrer de manière centralisée tous les accès à distance et contrôler les activités suspectes.
- Former aux pratiques sécurisées d'accès à distance, y compris à la détection des tentatives de phishing et autres attaques d'ingénierie sociale (voir PR.AT-1).

Quand les exigences sont-elles satisfaites ?

- Les directives et les procédures sont documentées, mises en œuvre et appliquées.
- Des directives écrites contraignantes sur les exigences techniques sont convenues avec les prestataires de services.
- Les accès à distance sont surveillés, enregistrés et les activités suspectes sont contrôlées.
- Recommandation : les accès à distance sont audités, documentés et validés au moins une fois par an.
- Les utilisateurs sont sensibilisés et formés à l'utilisation sûre des accès à distance.

PR.AC-4 Droits d'accès et autorisations	NM
Définissez les droits d'accès et les autorisations en tenant compte des principes du moindre privilège et de séparation des tâches.	2

De quoi s'agit-il ?

L'objectif de PR.AC-4 est de minimiser les risques de sécurité en ne donnant aux utilisateurs que le minimum d'autorisations nécessaires pour effectuer leurs tâches. Grâce aux principes du moindre privilège (*least-privilege*) et de la séparation des rôles (*seperation of duties*), le risque d'abus de données, de modifications involontaires et d'autres problèmes liés à la sécurité est considérablement réduit.

Qu'est-ce qui doit être accompli ?

Les entreprises peuvent répondre aux exigences de cette sous-catégorie en :

- Développant des directives et des procédures qui attribuent les autorisations (notamment les droits d'administrateur) selon le principe du moindre privilège et de connaissance sélective (*need-to-know*).
- Introduisant une séparation des rôles de sorte que les tâches critiques soient exécutées par différentes personnes. Exemple : détermination et attribution des autorisations par différentes personnes.

Comment satisfaire aux exigences ?

Les thèmes suivants doivent être pris en compte :

- Saisir les autorisations, par exemple dans une matrice, et évaluer leur criticité.
- N'accorder des autorisations temporaires que dans des cas exceptionnels et les retirer automatiquement.
- Contrôler et adapter régulièrement les autorisations.
- Supprimer les autorisations excessives après tout changement d'attribution des tâches.

L'introduction des instruments suivants est recommandée :

- Gestion des identités et des accès (IAM) : utiliser des systèmes de gestion des identités pour créer, modifier et supprimer l'accès des utilisateurs de manière centralisée.
- Accès basé sur les rôles (RBAC) : configurez des niveaux d'accès basés sur des rôles spécifiques, plutôt que d'accorder des droits d'accès individuels à chaque utilisateur, afin de simplifier la gestion des autorisations.
- Authentification multi-facteurs (MFA) : utilisez l'authentification à facteurs multiples pour renforcer la sécurité d'accès aux systèmes sensibles.

Quand les exigences sont-elles satisfaites ?

- Les directives et les procédures sont documentées, mises en œuvre et appliquées.
- Recommandation : les droits d'accès et les droits des utilisateurs sont audités, documentés et validés au moins une fois par an.

PR.AC-5 Protection de l'intégrité du réseau	NM
Vérifiez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, si cela s'avère nécessaire et judicieux.	2

De quoi s'agit-il ?

Une architecture réseau sûre et robuste constitue l'une des principales conditions préalables à une protection efficace contre les attaques. Il est possible, lorsque cela est nécessaire et pertinent, de réduire le risque de mouvements latéraux d'un attaquant en cas d'incident de sécurité en segmentant les réseaux.

Qu'est-ce qui doit être accompli ?

Les entreprises doivent mettre en œuvre des mesures de séparation logique et physique du réseau afin de le protéger contre les menaces internes et externes. Une segmentation et une ségrégation appropriée sont nécessaire afin d'en garantir l'intégrité.

Comment satisfaire aux exigences ?

- Inventaire et évaluation des risques : une analyse complète de tous les composants et connexions du réseau est nécessaire. Cette analyse doit permettre d'identifier les points faibles potentiels ou les zones critiques et de les classer par ordre de priorité.
- Segmentation du réseau :
  - Segmentation logique (logicielle) : des VLAN (*Virtual Local Area Networks*) devraient être utilisés pour diviser le réseau et séparer le trafic de données en fonction des différents niveaux de sécurité. Le *subnetting* peut être utilisé pour diviser le réseau en sous-réseaux plus petits et plus faciles à gérer.
  - Segmentation physique (matérielle) : le matériel dédié, comme les routeurs et les pare-feux, assure une séparation physique entre les réseaux. Les composants critiques devraient être placés dans des pièces ou des centres de données sécurisés afin de limiter l'accès physique.
- Contrôles d'accès : le contrôle d'accès réseau (*Network Access Control, NAC*) garantit que seuls les appareils autorisés ont accès au réseau.
- Surveillance et détection : les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) permettent de détecter et d'empêcher en temps réel les activités inhabituelles et les attaques potentielles. Une surveillance continue et des audits réguliers garantissent l'intégrité du réseau sur le long terme.

Quand les exigences sont-elles satisfaites ?

- Directives : des directives de sécurité documentées définissent la manière dont les réseaux sont segmentés, régulièrement contrôlés et mis à jour.
- Aspects techniques : en fonction de la stratégie de l'entreprise, l'architecture réseau la plus appropriée est choisie. Les outils nécessaires sont utilisés en fonction des risques afin de garantir la sécurité du réseau.

PR.AC-6 Vérification des identités	NM
N’attribuez des identités numériques qu’à des personnes ou à des processus que vous avez clairement identifiés.	2

De quoi s’agit-il ?

PR.AC-6 se réfère à l'attribution et à la vérification minutieuses des identités numériques afin de garantir la confidentialité et l'intégrité des systèmes numériques. Les identités numériques comprennent tous les identifiants numériques (nom, date de naissance, nom d'utilisateur, adresse e-mail, adresses IP, comportement de l'utilisateur, position, ...) qui peuvent être associés à une entité (personne physique ou morale) ou à un processus. Ces identités sont essentielles pour l'authentification des utilisateurs et l'accès sécurisé aux ressources internes.

Qu’est-ce qui doit être accompli ?

Les identités numériques ne devraient être attribuées qu'à des personnes et des processus qui ont été contrôlés au préalable et dont l'identité a été vérifiée. Cela permet d'éviter les accès non autorisés, de réduire le risque de vol d'identité, de garantir la conformité et de protéger les ressources sensibles contre les menaces externes et internes.

Comment satisfaire aux exigences ?

- Vérification préalable : les personnes et les processus qui doivent recevoir une identité numérique doivent être vérifiés. Dans certains cas, un contrôle de sécurité de la personne peut s’avérer utile.
- Principe « *zero trust* » : suivez le principe de ne jamais faire confiance et de toujours vérifier. Toute identité doit toujours être vérifiée.
- Système de gestion des identités (IDM) : déployez un IDM robuste qui crée, gère et surveille les identités numériques. Il devrait y avoir des directives pour l'attribution et la vérification des identités.
- Vérifier la sécurité des processus : examinez les processus et les systèmes à la recherche de failles de sécurité potentielles afin de minimiser les risques d'accès non autorisé.

Quand les exigences sont-elles satisfaites ?

- Vérification des personnes et des processus : assurez-vous que les personnes et les processus répondent à vos exigences de sécurité et sont conformes aux déclarations.
- Attribution d'identités numériques : assurez-vous que l'attribution d'identités numériques est effectuée avec soin et correctement.

Recommandation : une surveillance continue et des audits réguliers permettent de s'assurer que toutes les identités sont correctement attribuées et actives. Les droits d'accès devraient être régulièrement vérifiés afin de s'assurer qu'ils correspondent aux tâches et responsabilités actuelles.

Les plans d'urgence doivent inclure des mesures visant à bloquer immédiatement les identités compromises et à rétablir la sécurité.

PR.AC-7 Authentification	NM
L‘authentification d‘utilisateurs, appareils et autres *assets* (p. ex. authentification à un ou plusieurs facteurs) est effectuée en fonction du risque de la transaction (p. ex. risques de sécurité ou protection des données pour des personnes et autres risques d‘entreprise).	2

De quoi s’agit-il ?

L'authentification des utilisateurs, des appareils et d'autres actifs est essentielle pour la sécurité d'une entreprise. Ce processus permet à un système informatique de s'assurer de l'identité du requérant.

Qu’est-ce qui doit être accompli ?

Le choix de la méthode d'authentification, qu'il s'agisse d'un facteur unique ou d'une authentification multi-facteurs (MFA), doit être basé sur une évaluation minutieuse des risques. Un risque plus élevé nécessite des mécanismes d'authentification plus forts.

Comment satisfaire aux exigences ?

Le niveau d'authentification doit être défini en fonction des risques. Pour les opérations moins critiques, une méthode d'authentification simple (notamment par mots de passe) est suffisante, tandis que pour les transactions sensibles, la 2FA/MFA est nécessaire. Il s'agit de combiner deux ou plusieurs informations d'identification indépendantes, telles que des mots de passe, des données biométriques ou des jetons (*token*) de sécurité. Cela permet de garantir à la fois la sécurité et la protection des données.

En plus des utilisateurs, les appareils qui accèdent au réseau doivent également être authentifiés. Cela soutient le principe *zero trust* et protège le système contre les accès non autorisés. Des mécanismes adaptatifs qui intègrent des facteurs tels que l'adresse IP ou la géolocalisation augmentent encore la sécurité.

Quand les exigences sont-elles satisfaites ?

Pour répondre aux exigences, les mesures suivantes doivent être mises en œuvre :

- Évaluation des risques pour chaque transaction.
- Adaptation du niveau d'authentification aux risques.

De cette manière, il est possible de garantir que l'authentification répond aux exigences de sécurité spécifiques et offre un haut niveau de protection pour toutes les ressources de l'entreprise.

Recommandation : un contrôle et une adaptation continus des procédures d'authentification doivent être mis en œuvre afin de tenir compte des menaces actuelles et des évolutions technologiques.

Sensibilisation et formation (PR.AT)

PR.AT-1 Formation et sensibilisation à la cybersécurité	NM
Veillez à ce que tous vos collaborateurs soient sensibilisés et formés en matière de cybersécurité.	3

De quoi s'agit-il ?

Les mesures techniques de sécurité ne suffisent plus pour contrer les cyberattaques sophistiquées. Il est donc nécessaire de former régulièrement tous les collaborateurs, y compris les partenaires externes, à la sécurité de l'information afin de renforcer la conscience de la sécurité et d'améliorer la situation globale de l'entreprise en matière de sécurité.

Qu'est-ce qui doit être accompli ?

- Gérer les risques de cybersécurité : des évaluations régulières des menaces et des risques sont effectuées.
- Documentation/directives : les pratiques de sécurité doivent être documentées et standardisées.
- Processus de formation formalisés : les programmes de formation doivent être régulièrement revus et mis à jour.

Comment satisfaire aux exigences ?

- Élaborer un programme de formation : créer un programme de formation détaillé couvrant toutes les directives et procédures de cybersécurité pertinentes.
- Formation régulière : tous les collaborateurs, y compris les nouveaux employés et les partenaires externes, doivent être formés régulièrement.
- Campagnes de sensibilisation : menez continuellement des campagnes de sensibilisation.[11]
- Feedback et amélioration : utilisez les retours des participants pour améliorer le programme de formation. Vérifiez régulièrement que le programme est à jour et utile.

Quand les exigences sont-elles satisfaites ?

- La documentation est disponible.
- Des formations régulières sont organisées et font l'objet d'un suivi.
- Des campagnes de sensibilisation sont en place.
- Les retours des participants sont utilisés pour améliorer les mesures.

Qu'est-ce qui est nécessaire pour la mise en œuvre ?

Afin de mettre en œuvre les formations de manière efficace, les entreprises devraient commencer par des formations de sensibilisation adaptées aux groupes cibles et aux thèmes importants. Les progrès sont documentés et améliorés grâce à des retours réguliers et à des attestations de formation.

[11] Vous trouverez des informations sur les dernières campagnes de sensibilisation sur le site web de l'OFCS : https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sensibilisierung.html.

PR.AT-2 Utilisateurs avec des niveaux d'autorisation élevés	NM
Veillez à ce que les utilisateurs ayant des niveaux d'autorisation élevés soient conscients de leur rôle et de leurs responsabilités.	3

De quoi s'agit-il ?

Cette sous-catégorie garantit que les utilisateurs privilégiés, tels que les administrateurs et les utilisateurs disposant de droits d'accès étendus, connaissent et comprennent leurs responsabilités spécifiques en matière de sécurité. Étant donné que ces utilisateurs ont accès à des systèmes et des données critiques, ils sont souvent la cible de cyberattaques. Des formations régulières et spécialisées les aident à identifier les risques, à réagir aux incidents de sécurité et à réduire le risque global pour l'entreprise.

Qu'est-ce qui doit être accompli ?

- Définir et documenter les rôles et responsabilités spécifiques.
- Définir, documenter et mettre à jour régulièrement les pratiques de sécurité pour les utilisateurs privilégiés.
- Développer, appliquer et mettre à jour des programmes de formation formalisés. Ils doivent garantir que les utilisateurs privilégiés sont formés régulièrement.

Comment satisfaire aux exigences ?

- Définir clairement les rôles et les responsabilités : établir une description des rôles avec des exigences et des attentes claires en matière de cybersécurité, y compris l'attribution des droits d'accès.
- Développer des programmes de formation spécialisés : fournir du contenu permettant d'acquérir des connaissances plus approfondies (par rapport à PR.AT-1) sur la détection des menaces et la réaction aux incidents de sécurité.
- Organiser des formations régulières : établir un calendrier annuel de formation (voir PR.AT-1) et assurer ainsi des formations et des révisions régulières.
- Organiser des campagnes de sensibilisation : concevoir des campagnes spéciales pour les utilisateurs privilégiés.
- Obtenir des retours et améliorer les programmes : recueillir régulièrement les avis des participants à la formation et les utiliser pour améliorer continuellement vos programmes.

Quand les exigences sont-elles satisfaites ?

- La documentation est disponible et accessible à tout moment.
- Des formations régulières sont organisées pour les utilisateurs privilégiés selon des règles définies.
- Des processus standardisés existent et sont régulièrement mis à jour.
- Des campagnes de sensibilisation sont mises en place et menées en continu.
- Des processus de feedback sont mis en place afin d'assurer une amélioration continue.

PR.AT-4 Rôles et responsabilités des cadres	NM
Veillez à ce que tous les cadres soient conscients de leurs rôles spécifiques et de leurs responsabilités.	3

De quoi s'agit-il ?

PR.AT-4 veille à ce que toutes les personnes clés soient informées de leurs rôles et responsabilités en matière de cybersécurité. Cette mesure permet une meilleure mise en œuvre des mesures de cybersécurité en définissant clairement les tâches de chacun. Elle vise également à créer une culture de la cybersécurité portée par les échelons supérieurs et les cadres dirigeants.

Qu'est-ce qui doit être accompli ?

- Compréhension des rôles : les cadres doivent connaître leur rôle en matière de cybersécurité et être conscients de leur responsabilité.
- Sensibilisation : la cybersécurité est l'affaire de tous et doit être portée par la direction et le conseil d'administration. Ceux-ci doivent absolument être sensibilisés à la problématique. Ce n'est qu'avec leur soutien que des mesures proactives peuvent être prises pour réduire les risques.

Comment satisfaire aux exigences ?

- Documentation : définir et coordonner les rôles et les responsabilités conformément à ID.AM-6 et ID.GV-2.
- Communication : les rôles et les responsabilités doivent être communiqués de manière claire et lors de chaque changement.
- Sensibilisation et formation : les cadres sont sensibilisés aux cybermenaces et aux cyber-risques et sont formés en fonction de leur rôle (responsabilité légale, réglementation, ...).

Quand les exigences sont-elles satisfaites ?

- Documentation : les responsabilités en matière de cybersécurité sont ancrées dans l'organigramme.
- Communication : les rôles et les responsabilités des cadres sont clairement communiqués.
- Sensibilisation et formation : les cadres connaissent les défis de la cybersécurité et ont suivi une formation en cybersécurité.
- Contrôle : les rôles en matière de cybersécurité sont régulièrement contrôlés et adaptés si nécessaire.

Sécurité des données (PR.DS)

PR.DS-2 Sécurité de la transmission des données	NM
Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).	2

De quoi s'agit-il ?

La protection des informations pendant leur transmission est un élément crucial de la stratégie de sécurité d'une entreprise. Cette exigence vise à garantir la confidentialité, l'intégrité et la disponibilité des informations pendant leur transmission afin d'éviter toute atteinte à la sécurité.

Qu'est-ce qui doit être accompli ?

Pour répondre à cette exigence, il est indispensable de recourir à des méthodes de chiffrement robustes. Le chiffrement garantit que les informations ne peuvent être lues que par les destinataires autorisés lors de leur transmission. Pour ce faire, il convient d'utiliser des protocoles de chiffrement actuels et sûrs tels que TLS 1.3 (*Transport Layer Security*) afin de protéger les informations contre les tentatives d'interception et de manipulation.

Comment satisfaire aux exigences ?

- Chiffrement : le chiffrement entre les points de terminaison protège la confidentialité et l'intégrité des informations. Utilisez des protocoles tels que TLS 1.3.
- Réseaux privés virtuels (VPN) : les VPN peuvent contribuer à sécuriser la transmission de données sur les réseaux publics. Cette technologie crée une connexion sécurisée et chiffrée (IPsec) entre les terminaux et protège les informations contre tout accès non autorisé.
- Authentification : avant de transmettre des informations, les identités des parties impliquées doivent être vérifiées de manière univoque conformément à PR.AC-7.
- Intégrité des données : utiliser des fonctions de hachage et des signatures numériques pour garantir l'intégrité des informations pendant la transmission.
- Sécurité physique : l'infrastructure doit être protégée contre les attaques physiques conformément à PR.AC-2. La disponibilité peut être garantie à l'aide de la redondance des services et de l'infrastructure.
- Protection du réseau : s'assurer que les réseaux sont protégés conformément à PR.AC-5 et PR.PT-4.

Quand les exigences sont-elles satisfaites ?

Les exigences sont remplies si des moyens sont mis en œuvre pour protéger les informations pendant leur transmission.

Par ailleurs, la surveillance et la journalisation des transmissions de données sont essentielles pour détecter à temps les activités suspectes ou les anomalies et y remédier rapidement. La journalisation permet également d'assurer un suivi complet de toutes les transmissions et constitue un outil important pour les audits et l'amélioration des mesures de sécurité.

Il est important de s'assurer que le prestataire de services de transmission utilise toujours des protocoles à jour et recommandés.

Règles de protection des données (PR.IP)

PR.IP-1 Configuration par défaut	NM
Générez une configuration par défaut (standard) pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriel. Assurez-vous que cette configuration par défaut obéit aux règles usuelles de sécurité (par ex. redondance N-1, configuration minimale, etc.).	2

De quoi s'agit-il ?

L'établissement d'une configuration par défaut pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriels, est une étape fondamentale pour garantir la sécurité et l'efficacité des technologies de l'information. Ce point exige que la configuration standard respecte des principes de sécurité typiques, tels que la redondance N-1 et la configuration minimale.

Qu'est-ce qui doit être accompli ?

Une configuration par défaut garantit que tous les systèmes et appareils au sein de l'infrastructure sont configurés de manière uniforme et sécurisée. Cela permet non seulement de réduire la surface d'attaque, mais aussi de simplifier la gestion et la maintenance des systèmes.

Pour créer une configuration par défaut efficace, il faut d'abord identifier et documenter tous les composants de l'infrastructure d'information et de communication ainsi que les systèmes de contrôle industriels.

Comment satisfaire aux exigences ?

- Définir les objectifs : la performance, la sécurité, la fiabilité et l'évolutivité doivent être prises en compte.
- Redondance N-1 : ce principe garantit qu'il y a toujours un composant de réserve qui peut prendre le relais en cas de panne. Cela augmente la disponibilité et la fiabilité des systèmes et minimise le risque de temps d'arrêt.
- Configuration minimale : les systèmes et les appareils ne sont configurés qu'avec les fonctions et les services absolument nécessaires. Cela permet de réduire la surface d'attaque et de minimiser les points faibles potentiels. Les logiciels et services inutiles doivent être supprimés et l'accès aux fonctions nécessaires doit être limité.
- Configuration du réseau : l'adressage IP, la configuration DNS, le routage, ... font partie des paramètres et des réglages de base du réseau.
- Paramètres de sécurité : intégrez les mesures de sécurité directement dans votre configuration standard.

Quand les exigences sont-elles satisfaites ?

Les exigences sont satisfaites lorsque les systèmes sont identifiés, que la configuration par défaut a été définie pour chaque système et que les éléments de sécurité de base sont inclus.

Recommandation : des vérifications et des mises à jour régulières de la configuration par défaut doivent être effectuées. Les mises à jour de sécurité et les correctifs devraient être appliqués dans les meilleurs délais et des mécanismes de surveillance et d'application de la configuration par défaut devraient être mis en place. Cela peut être réalisé à l'aide d'outils automatisés et d'audits réguliers.

PR.IP-4 Backups	NM
Assurez-vous que des sauvegardes informatiques (*backups*) sont effectuées, gérées et testées régulièrement. Vérifiez que les données sauvegardées puissent être restaurées.	3

De quoi s'agit-il ?

La réalisation régulière de sauvegardes (*backups)*, leur gestion et leur vérification constituent un aspect essentiel de la sécurité informatique et de la continuité des activités. Les sauvegardes sont un élément indispensable de la cybersécurité permettant d'assurer la disponibilité des informations et des systèmes, la continuité des activités et de se prémunir contre un large éventail de menaces (p. ex. les *ransomwares*) en facilitant la restauration.

Qu'est-ce qui doit être accompli ?

Des sauvegardes des informations et des systèmes critiques doivent être régulièrement réalisées, gérées et testées. Cela garantit une réduction des pertes de données et des restaurations rapides et complètes.

Comment satisfaire aux exigences ?

- Informations et systèmes : il s'agit d'identifier et de classer par ordre de priorité les informations, processus et systèmes importants et critiques. L'efficacité des sauvegardes n'est garantie que par une utilisation réfléchie.
- Documentation : la réalisation de sauvegardes et leur gestion (responsabilités) doivent être documentées.
- Réalisation des sauvegardes en tenant compte des aspects suivants :
  - Type de sauvegarde : complète (sauvegarde complète), différentielle (uniquement les données qui ont changé depuis la dernière sauvegarde complète), incrémentielle (uniquement les données qui ont changé depuis la dernière sauvegarde complète ou différentielle, chaque nouvelle sauvegarde est enregistrée en tant que volume incrémentiel).
  - Support : des critères tels que le coût, la fiabilité, la disponibilité, la vitesse et la facilité d'utilisation doivent être pris en compte lors du choix d'un support (disque dur, lecteurs flash, cloud, hybride, ...). Les sauvegardes doivent être stockées dans des endroits sûrs et redondants.
  - Chiffrement : les données sensibles doivent être chiffrées. Le mot de passe principal ne doit pas être stocké au même endroit que les données chiffrées.
  - 3-2-1 : trois copies différentes doivent être conservées, sur deux types de stockage différents et une copie séparée (pas au même emplacement physique).
  - Dimension temporelle : les sauvegardes doivent être effectuées selon un calendrier défini, en fonction de la criticité des données et des exigences opérationnelles.
  - Documentation : les sauvegardes doivent être dûment répertoriées et facilement accessibles.
- Tests : la restauration des sauvegardes doit être testée régulièrement.

Quand les exigences sont-elles satisfaites ?

Les exigences sont satisfaites si les sauvegardes sont réalisées régulièrement, gérées et si leur capacité de restauration est vérifiée par des tests. Ces tests doivent être effectués suivant différents scénarios afin de s'assurer que la restauration fonctionne en toutes circonstances.

PR.IP-5 Respect des exigences et des directives	NM
Veillez à ce que toutes les exigences (réglementaires) et les directives concernant les équipements physiques soient respectées.	3

De quoi s'agit-il ?

Les exigences légales et réglementaires relatives aux équipements physiques sont généralement conçues pour garantir un niveau de sécurité minimal. La sécurité physique joue également un rôle important dans la cybersécurité, par exemple pour éviter d'endommager les serveurs utilisés pour les sauvegardes. La mesure PR.IP-5 garantit le respect de ces exigences, ce qui permet d'éviter des sanctions ou des amendes tout en garantissant un niveau de sécurité de base.

Qu'est-ce qui doit être accompli ?

Un processus de conformité doit être défini, adopté et mis en œuvre. Celui-ci doit servir à s'informer sur les normes, les réglementations et les lois en vigueur et à mettre en œuvre les exigences auxquelles l'entreprise est soumise. Pour aller au-delà des exigences, une veille juridique et réglementaire pourrait être envisagée.

Comment satisfaire aux exigences ?

Afin de se conformer aux directives et réglementations existantes, chaque entreprise doit réaliser un inventaire des exigences applicables. Celles-ci comprennent entre autres :

- Les normes et réglementations spécifiques au secteur.
- Les lois fédérales.
- Les lois cantonales.

Cette liste n'est pas exhaustive. Il est de la responsabilité de chaque entreprise de prendre les mesures nécessaires pour garantir le respect des prescriptions.

Les mesures techniques visant à augmenter la résilience des systèmes physiques sont par exemple :

- La prévention des accès non autorisés.
- La protection des moyens/appareils critiques.
- La prévention du vol de données (données stockées physiquement).
- La protection contre les attaques internes.
- La protection contre les catastrophes naturelles ou les incidents physiques.

Quand les exigences sont-elles satisfaites ?

La mesure PR.IP-5 est considérée comme atteinte lorsque toutes les exigences (réglementaires) existantes concernant les ressources/moyens physiques sont entièrement satisfaites.

PR.IP-9 Processus de réaction aux cyberincidents	NM
Instaurez des processus pour réagir aux cyberincidents (*Incident Response Planning*, *Business Continuity Management*, *Incident Recovery, Disaster Recovery*).	2

De quoi s'agit-il ?

PR.IP-9 décrit le développement et l'implémentation de plans de réponse aux incidents de sécurité qui couvrent l'ensemble du cycle de vie d'un incident, de l'identification jusqu'à la récupération. Il s'agit en particulier de la réponse aux incidents, de la continuité des activités et de la reprise des activités après un sinistre. Cela permet de garantir qu'une entreprise réagit efficacement aux incidents, qu'elle maintient ses activités et qu'elle les rétablit rapidement après un incident de sécurité.

Qu'est-ce qui doit être accompli ?

- Réponse aux incidents : les entreprises doivent avoir des politiques et des procédures documentées pour répondre aux incidents, mettre en place des systèmes de surveillance et de détection et former régulièrement les collaborateurs. Des plans de communication et des processus de suivi pour une amélioration continue sont essentiels.
- Continuité des activités : des évaluations des risques doivent être effectuées et des plans de continuité développés afin de maintenir les processus opérationnels critiques malgré un incident. Toutes les ressources nécessaires doivent être disponibles et des formations ainsi que des exercices réguliers doivent être organisés.
- Reprise des activités après un sinistre : les entreprises ont besoin de plans d'urgence pour la restauration des systèmes informatiques et des données. Des sauvegardes régulières, des tests et des exercices pour vérifier les plans ainsi que la préparation des collaborateurs sont des éléments indispensables.

Comment satisfaire aux exigences ?

- Réponse aux incidents : établir des directives et des procédures détaillées, mettre en œuvre des technologies de détection des incidents, organiser des formations et des simulations régulières et développer des stratégies de communication efficaces.
- Continuité des activités : effectuer des analyses des menaces, développer des plans de continuité et s'assurer que toutes les ressources nécessaires sont disponibles. Organiser des formations et des tests pour vérifier les plans.
- Récupération des activités après un sinistre : élaborer des plans d'urgence, effectuer des sauvegardes régulières et définir des procédures de récupération claires. Effectuer des tests réguliers pour vérifier les plans.

Quand les exigences sont-elles satisfaites ?

- Plans de réponse aux incidents : documentés, systèmes de surveillance testés mis en place et collaborateurs formés. Des stratégies de communication et de suivi efficaces sont mises en place.
- Plans de continuité des activités : documentés, testés et toutes les ressources nécessaires garanties. Les collaborateurs sont régulièrement formés.
- Plans de reprise des activités et sauvegardes : documentés, créés et testés. Les procédures de récupération sont efficaces.

Maintenance (PR.MA)

PR.MA-2 Accès à distance	NM
Veillez à ce que les travaux de maintenance effectués à distance sur vos systèmes soient enregistrés et documentés. Assurez-vous qu'aucun accès non autorisé n'est possible.	2

De quoi s'agit-il ?

L'accès à distance aux systèmes représente un risque de sécurité important, car il peut être exploité par des attaquants pour accéder à des systèmes critiques sans être physiquement présents. Cela rend possible des cyberattaques telles que le vol de données ou la prise de contrôle d'infrastructures sensibles. Sans mesures de sécurité adéquates, les systèmes sont exposés à des menaces considérables.

Qu'est-ce qui doit être accompli ?

Tous les travaux de maintenance effectués à distance sur des systèmes TIC doivent être enregistrés et documentés (journalisation). De plus, des mesures doivent être introduites pour empêcher tout accès non autorisé.

Comment satisfaire aux exigences ?

Les mesures suivantes peuvent être prises pour minimiser les risques liés à un accès non autorisé :

- Connexions sécurisées : utilisation de VPN avec chiffrement fort.
- Authentification à facteurs multiples (MFA) : garantir la vérification de l'identité.
- Contrôle d'accès : limiter les droits au minimum et utiliser des mots de passe à usage unique.
- Surveillance et journalisation : journaliser les activités et surveiller les actions suspectes (pare-feu, IPS, IDS, SIEM, etc.).
- Alertes et notifications : avertir les administrateurs des connexions inhabituelles ou des tentatives d'accès non autorisées.
- Gestion des fournisseurs : s'assurer que les fournisseurs tiers respectent les politiques de sécurité.
- Mises à jour régulières : mettre à jour régulièrement les systèmes et les logiciels.
- Formation du personnel : sensibiliser les équipes aux pratiques de cybersécurité.
- Directives claires : procédures définies et communiquées pour l'accès à distance.
- Sécurité des terminaux : protection des terminaux par des logiciels antivirus et des pares-feux.
- Segmentation du réseau : isoler les systèmes critiques.
- Chiffrement des données : chiffrer les données sensibles afin d'empêcher tout accès non autorisé.
- Plan d'intervention en cas d'incident : créer un plan d'action pour réagir rapidement et efficacement en cas d'incident lié à la sécurité lors de la maintenance à distance.

Quand les exigences sont-elles satisfaites ?

L'entreprise a entièrement défini et adopté des procédures de maintenance et d'accès à distance. Elle dispose d'une stratégie claire visant à empêcher les accès non autorisés. Les mesures techniques et les outils permettant d'enregistrer et de journaliser les activités sur les systèmes devraient être au moins partiellement mis en œuvre.

Technologies de protection (PR.PT)

PR.PT-2 Protection des supports de données amovibles	NM
Assurez-vous que les supports amovibles sont protégés et que leur utilisation se fait dans le strict respect des directives.	3

De quoi s'agit-il ?

Les supports de données amovibles sont un aspect essentiel de la stratégie de sécurité d'une entreprise. Cela exige que les supports amovibles et les informations qu'ils contiennent soient protégés.

Qu'est-ce qui doit être accompli ?

Les supports de données amovibles tels que les clés USB, les disques durs externes ou les supports optiques doivent être protégés physiquement et numériquement afin de garantir qu'ils ne puissent pas être utilisés ou manipulés de manière non autorisée. Cela peut se faire en utilisant des technologies de chiffrement afin de garantir que les informations stockées sur ces supports ne puissent être lues que par des personnes autorisées.

Comment satisfaire aux exigences ?

Les mesures suivantes sont nécessaires pour répondre aux exigences :

- Directives : il convient d'établir des directives et des procédures claires pour l'utilisation des supports de données amovibles (utilisation, exploitation, restitution, élimination, ...) et de s'assurer que tous les collaborateurs sont sensibilisés et informés à ce sujet.
- Chiffrement : pour éviter tout accès non autorisé, les données doivent être chiffrées.
- Authentification : protégez les supports de données amovibles par des mots de passe (ou MFA).
- *AutoRun/AutoPlay* : empêchez l'exécution automatique des fichiers.
- Prévention des pertes de données (DLP) : surveillez et contrôlez le transfert de données sensibles sur les supports de données amovibles.
- Sécurité physique : conservez les supports de données amovibles dans des endroits sûrs.
- Outils *anti-malware* : analysez régulièrement les appareils à la recherche de logiciels malveillants.
- Gestion des appareils : contrôlez l'accès aux ports USB et n'autorisez que les appareils autorisés.

Quand les exigences sont-elles satisfaites ?

Les exigences sont remplies lorsque :

- Les directives sont définies et appliquées conformément à ID.GV-1.
- L'utilisation se fait dans le respect des directives.
- Les supports de données amovibles sont protégés en fonction de leur utilisation et des risques auxquels ils sont exposés.

Recommandation : la surveillance et le contrôle de l'utilisation des supports de données amovibles sont essentiels pour garantir le respect des directives et pour détecter les incidents de sécurité potentiels. Cela peut être réalisé grâce à des technologies de surveillance de l'accès aux données et à des audits de l'utilisation des supports de données.

PR.PT-4 Protection des réseaux de communication et de contrôle	NM
Assurez la protection de vos réseaux de communication et de contrôle.	3

De quoi s'agit-il ?

Pour un exploitant, il est essentiel de maîtriser son réseau. Cela comprend les aspects informatiques de commande et de contrôle ainsi que les télécommunications qui soutiennent ces réseaux.

Qu'est-ce qui doit être accompli ?

La topologie globale du réseau devrait être connue (ID.AM-3). Des mesures de protection des réseaux de communication et de contrôle doivent être mises en œuvre.

Comment satisfaire aux exigences ?

Les principes de base suivants sont nécessaires pour garder le contrôle du réseau :

- Segmentation : voir PR.AC-5.
- Technologies de communication : les services non sécurisés, comme Telnet, Remote Shell ou rlogin, doivent être remplacés par des alternatives sécurisées comme SSH.
- Pare-feu :
  - Surveiller et contrôler les communications aux frontières extérieures et aux interfaces internes importantes.
  - Toutes les règles qui autorisent les communications informatiques à travers le pare-feu doivent être approuvées.
  - Les services non autorisés ou vulnérables doivent être désactivés ou bloqués.
  - Les règles du pare-feu doivent être régulièrement mises à jour, par exemple en supprimant les services inutilisés.
- Mots de passe : les mots de passe par défaut doivent être modifiés et les comptes génériques doivent être remplacés par des comptes utilisateurs individuels.
- L'interface d'administration doit être sécurisée par une authentification forte ou des mots de passe forts et les utilisateurs doivent être bloqués après plusieurs tentatives d'accès infructueuses.
- Accès à distance :
  - Définir et documenter les restrictions d'utilisation, les exigences de configuration/connexion et les directives de mise en œuvre pour chaque type d'accès à distance autorisé.
  - Autoriser chaque type d'accès à distance au système avant de permettre de telles connexions.
  - Utiliser des mécanismes automatisés pour surveiller et contrôler les méthodes d'accès à distance.

Quand les exigences sont-elles satisfaites ?

Les réseaux de communication et de contrôle sont protégés. Un test d'intrusion peut être effectué pour vérifier les mesures de sécurité. Par ailleurs, il ne devrait pas être possible de contrôler le système de gestion du réseau à partir d'un poste ou de contrôler un poste à distance à partir d'un autre poste.

Si l'accès à distance ne peut pas être suffisamment sécurisé, il est recommandé de renoncer à ce service.

Détecter (DE)

La catégorie « détecter » définit les mesures appropriées pour identifier la survenance d'un événement de cybersécurité et permet de détecter les anomalies à temps.

Surveillance (DE.CM)

Les systèmes TIC, y compris tous les moyens d'exploitation, sont surveillés à intervalles réguliers afin, d'une part, de détecter les incidents de cybersécurité et, d'autre part, de pouvoir garantir l'efficacité des contre-mesures.

Processus de détection (DE.DP)

Les processus et les instructions pour la détection des incidents de cybersécurité sont gérés, testés et maintenus de manière à détecter les incidents de cybersécurité.

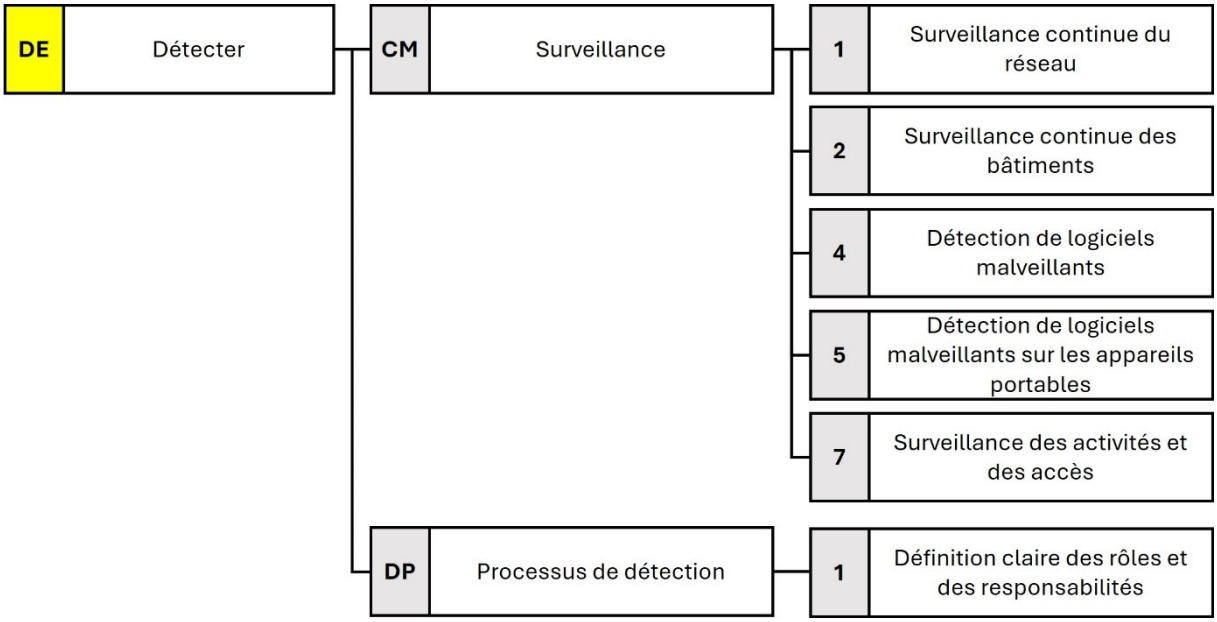

Figure 9 : Sous-catégories DE prescrites pour le niveau de protection C

Surveillance (DE.CM)

DE.CM-1 Surveillance continue du réseau	NM
Mettez en place une surveillance continue du réseau pour détecter les incidents de cybersécurité potentiels.	2

De quoi s'agit-il ?

La mise en œuvre d'une surveillance continue du réseau est essentielle pour la détection précoce des incidents de cybersécurité potentiels.

Qu'est-ce qui doit être accompli ?

Les éventuelles cyberattaques, anomalies ou activités suspectes doivent être détectées à temps afin de réduire l'ampleur des dommages. Des procédures adéquates doivent être mises en place et testées régulièrement. Les travaux de maintenance déclenchent souvent des alarmes identiques à celles d'une cyberattaque. Pour pouvoir effectuer une analyse rapide, les plans de maintenance doivent être définis et connus des spécialistes en cybersécurité.

Comment satisfaire aux exigences ?

La surveillance continue du réseau nécessite un contrôle permanent du trafic réseau, des activités des systèmes et des événements de sécurité. L'utilisation de technologies avancées telles que IDS, IPS et SIEM permet de détecter les anomalies et les activités suspectes.

La capacité de réaction aux incidents de sécurité détectés est un élément central de la surveillance. Les entreprises doivent disposer de plans de réponse aux incidents bien définis, avec des procédures claires d'analyse, de résolution et de récupération après un incident.

Quand les exigences sont-elles satisfaites ?

Toutes les personnes concernées doivent comprendre l'importance de la surveillance du réseau et savoir comment réagir aux menaces identifiées. Des formations régulières permettent de maintenir à jour les connaissances sur les menaces actuelles et les bonnes pratiques.

Recommandation : en évaluant et en améliorant continuellement leurs stratégies de surveillance, les entreprises peuvent optimiser en permanence la sécurité de leur réseau et réagir aux nouvelles menaces. Un système de surveillance du réseau bien établi contribue à protéger l'intégrité, la confidentialité et la disponibilité de l'infrastructure informatique et à minimiser l'impact des incidents de sécurité.

DE.CM-2 Surveillance continue des bâtiments	NM
Mettez en place une surveillance continue (*monitoring*) de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.	2

De quoi s'agit-il ?

Une surveillance continue des ressources physiques et des bâtiments est essentielle pour détecter à temps les incidents de cybersécurité potentiels.

Qu'est-ce qui doit être accompli ?

La surveillance continue des bâtiments est assurée, entre autres, par des mesures de sécurité physique telles que le contrôle d'accès, les caméras de surveillance et les systèmes d'alarme. L'objectif est d'identifier les activités inhabituelles ou suspectes qui pourraient indiquer des risques pour la sécurité. Il peut s'agir de menaces physiques directes, telles que des effractions ou des tentatives de sabotage, ou de menaces indirectes susceptibles de porter atteinte à l'infrastructure TIC.

Comment satisfaire aux exigences ?

La mise en œuvre d'un système de surveillance efficace nécessite l'utilisation de technologies de pointe et l'intégration de systèmes de surveillance dans un système de gestion de la sécurité centralisé. Cela permet une surveillance complète et continue des événements de sécurité physique.

Pour réagir rapidement aux incidents de sécurité identifiés, il est essentiel de disposer de plans de réponse aux incidents clairs. Ces plans doivent garantir que les incidents de sécurité peuvent être rapidement examinés, résolus et que les systèmes concernés peuvent être restaurés. Une étroite collaboration entre le responsable de sécurité physique et le responsable de sécurité informatique est essentielle à cet égard.

Quand les exigences sont-elles satisfaites ?

Les exigences sont remplies lorsque les accès non autorisés aux ressources physiques sont identifiés, signalés et traités en conséquence.

La formation et la sensibilisation des collaborateurs revêtent une grande importance. Toutes les personnes concernées devraient comprendre l'importance du contrôle continu et savoir comment réagir aux menaces identifiées. Des formations et des exercices réguliers peuvent aider à sensibiliser et à améliorer la capacité de réaction (voir PR.AT-1).

DE.CM-4 Détection de logiciels malveillants	NM
Veillez à pouvoir détecter les maliciels (*malwares*).	2

De quoi s'agit-il ?

La protection contre les logiciels malveillants est une composante critique de la stratégie de sécurité. Il convient de mettre en œuvre un processus permettant de détecter et d'identifier efficacement les logiciels malveillants.

Qu'est-ce qui doit être accompli ?

La détection des logiciels malveillants est essentielle pour identifier rapidement les atteintes potentielles à la sécurité et réagir de manière appropriée. Les logiciels malveillants peuvent se présenter sous différentes formes, allant des virus et des chevaux de Troie (*trojan*) aux *ransomwares* et aux logiciels espions (*spyware*), qui représentent des risques importants pour l'infrastructure TIC et l'intégrité des données.

Comment satisfaire aux exigences ?

Pour garantir une détection efficace des logiciels malveillants, les entreprises utilisent des technologies avancées, notamment des logiciels antivirus, des solutions EDR, des outils d'analyse des logiciels malveillants ou des IDS. Ces systèmes surveillent en permanence le trafic réseau, les activités des systèmes et l'intégrité des fichiers afin d'identifier toute activité inhabituelle susceptible d'indiquer une infection.

Il est essentiel de réagir rapidement aux logiciels malveillants détectés afin d'en minimiser l'impact. Les entreprises doivent disposer de plans de réponse aux incidents bien conçus qui définissent des procédures claires pour examiner, isoler et supprimer les logiciels malveillants et pour restaurer les systèmes affectés.

La formation et la sensibilisation des employés sont essentielles pour améliorer la détection des logiciels malveillants. Les employés doivent être informés des signes et des symptômes liés aux logiciels malveillants et savoir comment signaler toute activité suspecte. Des formations régulières permettent de sensibiliser aux menaces actuelles et d'encourager un comportement sensible à la sécurité.

Quand les exigences sont-elles satisfaites ?

Recommandation : il est important de contrôler et d'améliorer régulièrement les systèmes de détection afin de pouvoir réagir aux nouveaux types de logiciels malveillants et à l'évolution du spectre des menaces. Des tests, des audits et des mises à jour réguliers des logiciels de sécurité permettent d'identifier et de corriger les points faibles et d'améliorer l'efficacité de la détection des logiciels malveillants.

La mise en œuvre d'un système efficace de détection des logiciels malveillants est essentielle pour garantir la sécurité de l'infrastructure TIC. En prenant des mesures proactives et en réagissant rapidement, les entreprises peuvent minimiser les dommages potentiels et protéger l'intégrité de leurs données.

DE.CM-5 Détection de logiciels malveillants sur les appareils portables	NM
Veillez à pouvoir détecter les maliciels (*malwares*) sur les appareils portables.	2

De quoi s'agit-il ?

Garantir la détection des logiciels malveillants sur les appareils mobiles est important pour la stratégie de sécurité d'une entreprise.

Qu'est-ce qui doit être accompli ?

La détection des logiciels malveillants sur les appareils mobiles est essentielle pour identifier rapidement les atteintes potentielles à la sécurité et y répondre de manière appropriée. Les logiciels nuisibles peuvent se présenter sous différentes formes, notamment sous forme de logiciels malveillants, de logiciels espions et d'applications indésirables qui peuvent dérober des données sensibles ou nuire à la capacité de fonctionnement des appareils.

Comment satisfaire aux exigences ?

Pour s'assurer que les logiciels malveillants sont détectés efficacement, les entreprises utilisent des technologies avancées telles que la gestion des appareils mobiles (MDM), des logiciels de détection des menaces pour appareils mobiles et des programmes antivirus pour appareils mobiles. Ces systèmes surveillent en permanence l'état des appareils mobiles, analysent les applications et les données à la recherche d'anomalies et effectuent des contrôles de sécurité réguliers.

Outre les possibilités techniques, une directive doit être établie sur la manière dont les collaborateurs doivent utiliser les appareils mobiles. La directive doit également préciser quelles applications peuvent être utilisées et si le collaborateur peut/a le droit d'installer lui-même des applications.

Quand les exigences sont-elles satisfaites ?

Une réaction rapide aux logiciels malveillants détectés est essentielle pour minimiser les dommages potentiels. Les entreprises devraient disposer de plans de réponse aux incidents bien conçus, comprenant des procédures claires pour examiner, isoler et supprimer les logiciels malveillants sur les appareils mobiles, ainsi que pour restaurer les appareils et les données.

La formation et la sensibilisation des collaborateurs sont essentielles pour améliorer la détection des logiciels malveillants sur les appareils mobiles. Les collaborateurs doivent être informés des signes et des symptômes associés aux logiciels malveillants et savoir comment signaler toute activité suspecte. Des formations régulières et des campagnes de sensibilisation permettent de mieux faire connaître les menaces actuelles et d'encourager un comportement sensible à la sécurité (voir PR.AT-1).

DE.CM-7 Surveillance des activités et des accès	NM
Surveillez vos systèmes en permanence pour être certain que des activités ou accès liés à des personnes, équipements ou logiciels non autorisés seront détectés.	2

De quoi s'agit-il ?

La surveillance continue des systèmes est essentielle pour garantir que toutes les activités et tous les accès de personnes, d'appareils et de logiciels non autorisés sont détectés à temps.

Qu'est-ce qui doit être accompli ?

Les systèmes sont surveillés en permanence afin d'identifier les activités suspectes ou inhabituelles qui pourraient indiquer des atteintes potentielles à la sécurité. Cela comprend la surveillance du trafic réseau, des fichiers de journalisation des systèmes, de l'activité des utilisateurs et des schémas d'accès.

Comment satisfaire aux exigences ?

En utilisant des technologies avancées telles que les outils IDS, SIEM et de gestion des fichiers de journalisation, les entreprises peuvent effectuer cette surveillance de manière efficace.

Quand les exigences sont-elles satisfaites ?

Des réactions rapides aux incidents de sécurité identifiés sont essentielles pour minimiser les dommages potentiels. Des plans de réponse aux incidents bien conçus doivent inclure des procédures claires pour analyser, isoler et résoudre les incidents de sécurité et pour rétablir l'intégrité des systèmes.

La formation et la sensibilisation des collaborateurs jouent un rôle important dans l'amélioration de l'efficacité de la surveillance. Les collaborateurs doivent être informés de l'importance de la surveillance des systèmes et savoir comment signaler toute activité suspecte.

Processus de détection (DE.DP)

DE.DP-1 Définition claire des rôles et des responsabilités	NM
Définissez des rôles et des responsabilités clairs, de sorte que chacun sache clairement qui est responsable de quoi et qui dispose de quelles compétences.	2

De quoi s'agit-il ?

La détection des événements de cybersécurité doit être organisée de manière structurée. Les appareils doivent être configurés de manière à transmettre leurs informations à un système central (SIEM, syslog, ...). Ces systèmes doivent être analysés afin d'identifier les comportements suspects. Un collaborateur interne ou externe surveille les alarmes, filtre les fausses alarmes et décide des mesures à prendre (par exemple, isoler un système en cas d'alarme). Le collaborateur doit être informé des travaux de maintenance afin de pouvoir faire le tri entre les alarmes liées aux activités et les alarmes suspectes.

Tous les rôles pertinents dans le processus de détection (responsable informatique, administrateur système, responsable de la sécurité informatique) doivent être clairement définis et dotés de tâches et de pouvoirs de décision spécifiques.

En plus des personnes qui ont une responsabilité définie, tous les employés de l'entreprise ont un rôle à jouer dans la détection des cyberattaques. Toute activité suspecte devrait être signalée. Des moyens simples pour signaler les incidents devraient être mis à disposition.

Qu'est-ce qui doit être accompli ?

Un document sur les rôles et les responsabilités doit être rédigé et communiqué à tout le personnel concerné afin de s'assurer que tous comprennent leurs rôles et responsabilités dans la détection des événements de cybersécurité.

Comment satisfaire aux exigences ?

Formation : formations régulières à la détection des événements de cybersécurité, complétées par des cours de mise à jour des connaissances.

Surveillance : mécanismes de contrôle et rapports réguliers sur le respect des responsabilités et l'état des mesures de détection. Ces rapports doivent être transmis régulièrement à la direction et aux cadres concernés.

Quand les exigences sont-elles satisfaites ?

Les rôles et responsabilités définis doivent être régulièrement réexaminés afin de s'assurer qu'ils correspondent aux menaces actuelles et aux exigences organisationnelles. Si nécessaire, les descriptions des rôles et des responsabilités doivent être adaptées pour tenir compte des changements dans l'infrastructure informatique, des nouvelles menaces ou des changements organisationnels.

Réagir (RS)

La catégorie « réagir » comprend les mesures appropriées à prendre en cas de détection d'un incident de cybersécurité. Celles-ci sont essentielles pour limiter rapidement les dommages, endiguer les conséquences d'une attaque et renforcer la résilience de l'organisation en général.

Plan d'intervention (RS.RP)

Les processus et procédures de réponse sont exécutés et maintenus en permanence afin de garantir la réponse aux incidents de cybersécurité détectés.

Communication (RS.CO)

En cas d'incident de cybersécurité, une communication coordonnée entre toutes les parties prenantes internes et externes est de la plus haute importance. D'une part, pour résoudre l'incident le plus efficacement possible et, d'autre part, pour informer en permanence toutes les parties prenantes concernées.

Circonscrire les dommages (RS.MI)

Des mesures sont prises pour empêcher la propagation d'un événement, atténuer ses conséquences et remédier à l'incident.

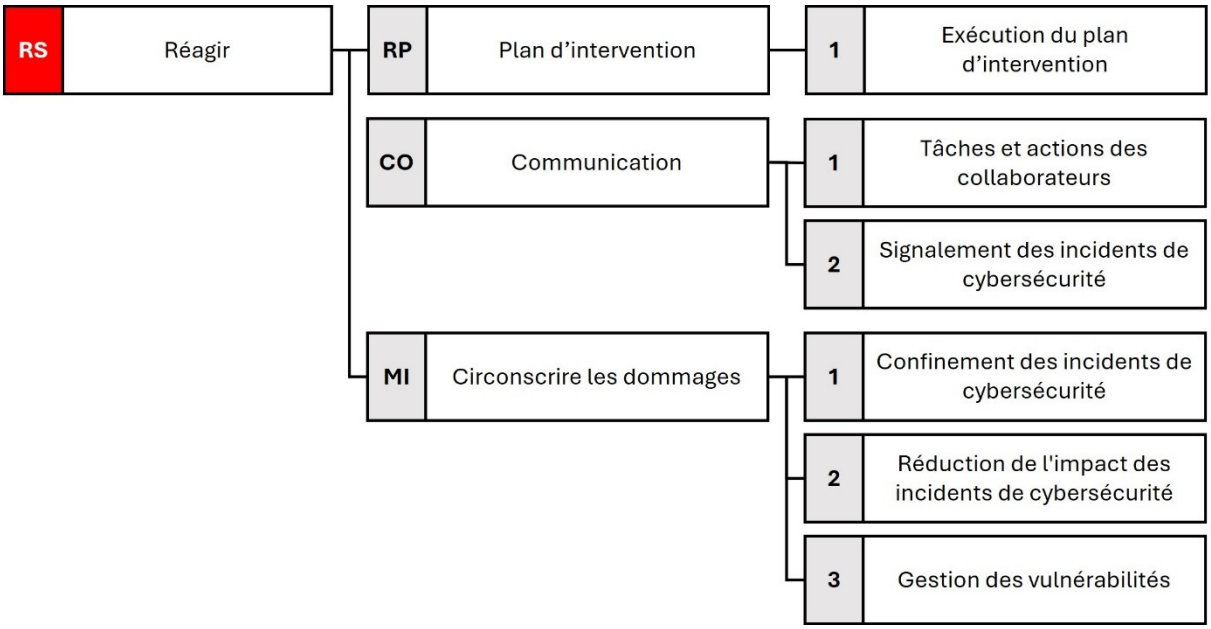

Figure 10 : Sous-catégories RS prescrites pour le niveau de protection C

Plan d’intervention (RS.RP)

RS.RP-1 Exécution du plan d’intervention	NM
Assurez-vous que le plan d’intervention est correctement suivi et rapidement exécuté si un incident de cybersécurité est détecté.	2

De quoi s’agit-il ?

Le plan de réponse aux incidents définit les mesures à mettre en œuvre rapidement et correctement pendant ou après un incident de cybersécurité détecté.

Qu’est-ce qui doit être accompli ?

Un plan de réponse aux incidents efficace définit des procédures et des responsabilités claires pour la gestion des incidents de sécurité. Il doit garantir que les équipes de sécurité puissent réagir rapidement pour analyser, isoler et résoudre l'incident afin de minimiser son impact sur l'organisation.

Comment satisfaire aux exigences ?

Le plan d'intervention en cas d 'incident doit être régulièrement revu, mis à jour et exécuté afin de s'assurer que toutes les personnes concernées connaissent les procédures et sont en mesure d'agir efficacement en cas d'urgence. Ce plan doit comporter les points suivants :

- Comment reconnaître l'ampleur et la portée de l'incident.
- Comment confiner et isoler les appareils compromis.
- Comment éliminer la menace.
- Comment restaurer les services et les rétablir d'abord à un niveau minimal, puis à un niveau normal.

La formation et les exercices sont essentiels pour améliorer la capacité de réaction et s'assurer que tous les collaborateurs savent comment agir de manière coordonnée en cas d'incident.

Créez des listes de contrôle et suivez-les scrupuleusement en cas de cyberincident.

Quand les exigences sont-elles satisfaites ?

La mise en œuvre d'un plan de réponse aux incidents robuste contribue à renforcer la résilience de l'organisation face aux cyberattaques et à minimiser les dommages potentiels. Les exigences attendues sont satisfaites si le plan de reprise d'activité est mis en œuvre conformément aux processus, rôles, responsabilités et objectifs définis. En cas de cyberattaque, il est important de se référer aux processus préalablement définis et de les suivre afin de ne pas se laisser gagner par le stress. Une action rapide et coordonnée en cas d'urgence est essentielle pour garantir la sécurité de l'infrastructure TIC et conserver la confiance des parties prenantes.

Communication (RS.CO)

RS.CO-1 Tâches et actions des collaborateurs	NM
Assurez-vous que toutes les personnes connaissent leurs tâches et la marche à suivre lorsqu'elles doivent réagir à un incident de cybersécurité.	2

De quoi s'agit-il ?

En cas d'attaque, le niveau de stress peut rapidement monter. Pour pouvoir réagir au mieux, une préparation en amont est nécessaire.

Qu'est-ce qui doit être accompli ?

Définissez des scénarios d'attaque et déterminez les contre-mesures les plus appropriées pour combattre l'incident. Par exemple, si un serveur est endommagé, il est préférable de l'isoler en supprimant toutes les connexions réseau plutôt que de simplement l'éteindre. Ainsi, les experts en cybersécurité pourront analyser le système afin d'identifier le problème.

Un plan de réponse aux incidents (RS.RP-1) contient des indications concrètes sur la manière dont les parties du réseau doivent être isolées afin d'éviter qu'un logiciel malveillant ne se propage.

Comment satisfaire aux exigences ?

Les points suivants doivent être préparés :

Technique :

- Déterminer les vecteurs d'attaque possibles et les contre-mesures techniques à prendre.
- Déterminer les critères qui permettent de suspecter une cyberattaque.

Organisation :

- Identifiez les différents rôles nécessaires pour gérer la cybersécurité dans votre organisation. Il s'agit notamment des responsables de la sécurité, des équipes de réponse aux incidents, des responsables des sauvegardes, etc.
- Décrivez clairement les responsabilités de chaque rôle lié à la cybersécurité.
- Vérifiez que tous les rôles et responsabilités sont clairement documentés et que les documents sont accessibles.

Communication :

- Assurez-vous que les informations sur les rôles et les responsabilités ont été correctement communiquées à toutes les personnes concernées.

Formation :

- Confirmez que la formation sur les rôles et responsabilités a été effectuée et que les collaborateurs comprennent leurs responsabilités.

Quand les exigences sont-elles satisfaites ?

La réaction aux incidents doit être testée et vérifiée régulièrement. Formez vos collaborateurs à la manière de réagir à d'éventuels incidents et mettez en place un canal de signalement (téléphone, canal Teams, etc.).

RS.CO-2 Signalement des incidents de cybersécurité	NM
Définissez des critères pour le signalement des incidents de cybersécurité et assurez-vous qu'ils sont signalés et traités conformément à ces critères.	2

De quoi s'agit-il ?

Il faut s'assurer que la communication avec les parties prenantes concernées, entre autres avec l'OFCS (Office fédéral de la cybersécurité) et avec le PFPDT (Préposé fédéral à la protection des données et à la transparence) est garantie. Les obligations de notification pour les infrastructures critiques et les délais correspondants doivent être pris en compte. Les entreprises doivent définir un processus à cet effet et tenir à disposition les plans et la documentation nécessaires. L'objectif de la notification est d'informer à temps les autres entreprises des nouvelles menaces et d'obtenir une vue d'ensemble des cyberattaques à l'échelle de la Suisse.

Les critères de l'obligation de notification sont définis dans l'ordonnance sur la cybersécurité (Ordonnance sur la cybersécurité, OCyS).[12]

Qu'est-ce qui doit être accompli ?

Les organisations devraient établir des directives et des procédures claires définissant ce qui est considéré comme un incident de cybersécurité[13] et la manière dont il devrait être signalé. Ces critères devraient prendre en compte les aspects techniques et opérationnels afin de garantir que tous les incidents importants sont répertoriés et traités de manière appropriée.

Comment satisfaire aux exigences ?

Les organisations doivent déterminer quels incidents doivent être signalés (par exemple, signaler le vol de données de clients au PFPDT et aux clients concernés).

Le personnel doit être formé pour savoir comment réagir en cas d'incident. La communication doit également être clairement définie :

- Qui doit être informé en cas d'incident ?
- Comment le prestataire de services ou le fournisseur doit-il être informé ?
- Inversement : quand et comment le prestataire de services ou le fournisseur doit-il informer l'entreprise ?

Quand les exigences sont-elles satisfaites ?

Les critères de signalement des incidents doivent être clairement communiqués et vérifiés afin de garantir qu'ils sont toujours d'actualité. Les employés doivent être formés pour identifier et signaler les cas suspects.

Après chaque incident, des mesures devraient être prises pour améliorer la défense, les procédures, la sensibilisation du personnel et la communication.

Des exercices réguliers de gestion de crise, adaptés à la taille de l'entreprise, permettent aux participants de se préparer à gérer les différents aspects.

[12] Projet, actuellement en consultation.
[13] L'ordonnance sur la cybersécurité doit définir une partie de ces mesures.

Circonscrire les dommages (RS.MI)

RS.MI-1 Confinement des incidents de cybersécurité	NM
Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que vous pouvez stopper leur propagation.	2

De quoi s'agit-il ?

La capacité à endiguer efficacement les incidents de cybersécurité et à interrompre leur propagation est essentielle. Le confinement des incidents de cybersécurité nécessite une action rapide et coordonnée afin de stopper la propagation des logiciels malveillants ou l'accès non autorisé aux systèmes. Pour ce faire, les entreprises doivent mettre en place des procédures et des processus clairs qui garantissent que les équipes de sécurité peuvent réagir rapidement aux alertes et prendre les mesures nécessaires.

Qu'est-ce qui doit être accompli ?

Les mesures comprennent l'isolation des systèmes ou des zones de réseau infectés (voir PR.AC-5), le blocage des connexions réseau indésirables et la restriction temporaire de l'accès aux données ou ressources sensibles. Ces mesures permettent d'éviter qu'un incident ne se propage et ne cause des dommages plus importants.

Pour la recherche d'un logiciel malveillant, il est recommandé de laisser le système actif mais complètement déconnecté du réseau. Pour ce faire, les câbles doivent être correctement étiquetés avant d'être débranchés afin de simplifier la mise en service une fois le problème résolu dans le système.

Une réaction efficace aux incidents nécessite une collaboration étroite entre les équipes informatiques et de sécurité ainsi que des voies de communication claires afin de pouvoir prendre des décisions et mettre en œuvre des mesures rapidement. Des formations et des exercices réguliers sont indispensables pour améliorer la capacité de réaction et s'assurer que toutes les personnes concernées sont familières avec les processus.

Comment satisfaire aux exigences ?

Il est également important de vérifier et d'optimiser en permanence les processus de réponse aux incidents afin de pouvoir réagir aux nouvelles menaces et technologies. En effectuant régulièrement des tests et des simulations, les entreprises peuvent continuer à améliorer leur capacité à circonscrire les incidents de cybersécurité et à renforcer leur résilience.

Quand les exigences sont-elles satisfaites ?

La mise en œuvre d'un système robuste permettant d'endiguer les incidents de cybersécurité contribue à minimiser les dommages potentiels et à garantir la continuité des opérations. Une intervention rapide et efficace peut faire la différence entre un incident de sécurité limité et un incident de sécurité grave.

RS.MI-2 Réduction de l'impact des incidents de cybersécurité	NM
Assurez-vous de pouvoir réduire l'impact des incidents de cybersécurité.	2

De quoi s'agit-il ?

Un aspect essentiel est de s'assurer que l'entreprise est en mesure de gérer efficacement les cyberincidents afin de minimiser les dommages potentiels.

Qu'est-ce qui doit être accompli ?

Un plan de réponse aux incidents bien structuré, comprenant une détection rapide, une réaction adéquate et des mesures de récupération efficaces, devrait être mis en œuvre. Ces mesures permettent de stopper la propagation des logiciels malveillants, de protéger les données sensibles et de rétablir rapidement la capacité opérationnelle.

En outre, la communication transparente avec les équipes internes, les parties prenantes et, au besoin, les partenaires externes joue un rôle décisif. Un flux d'informations clair pendant un incident contribue à maintenir la confiance et à garantir une collaboration efficace.

Comment satisfaire aux exigences ?

- Réaction rapide et intervention rapide de l'équipe de réponse/d'intervention.
- Processus d'escalade clairs pour que les décideurs soient rapidement informés.
- Endiguement de l'incident de cybersécurité conformément à RS.MI-1.
- Donner la priorité aux processus et activités critiques (OT).
- Récupération rapide (données + systèmes).
- Communiquer clairement à l'aide d'un plan de communication d'urgence pour informer à temps les collaborateurs, les partenaires et les clients.
- Chercher un soutien externe auprès d'experts (spécialistes) et/ou des autorités (OFCS, GovCERT, OFEN).
- Impliquer les forces de l'ordre si nécessaire.
- Cyber-assurance : évaluer les possibilités dont vous disposez.

L'amélioration continue des processus de réponse aux incidents par une analyse approfondie après chaque incident est également très importante. Cela permet à l'entreprise de tirer les leçons des expériences, d'identifier les points faibles et d'adapter en permanence la stratégie de sécurité afin de mieux gérer les incidents futurs.

Quand les exigences sont-elles satisfaites ?

En mettant en place une approche robuste pour réduire l'impact des cyberincidents, l'entreprise peut renforcer sa résilience face aux menaces de sécurité et protéger l'intégrité de ses systèmes et de ses données. Les mesures prises varient en fonction de l'incident. Il est toutefois important de les définir au préalable dans différents scénarios et de suivre méthodiquement leur mise en œuvre jusqu'au rétablissement complet.

RS.MI-3 Gestion des vulnérabilités	NM
Veillez à réduire au maximum les failles découvertes ou référencez-les comme des risques acceptables.	2

De quoi s'agit-il ?

L'identification et l'évaluation des vulnérabilités font partie intégrante d'une stratégie de sécurité globale. Sur la base d'une analyse continue des risques, l'entreprise doit décider de sa stratégie de gestion des vulnérabilités.

Qu'est-ce qui doit être accompli ?

Les organisations devraient effectuer régulièrement des analyses de vulnérabilité afin d'identifier les failles de sécurité avant qu'elles ne puissent être exploitées par des attaquants. Il est possible et recommandé d'obtenir des informations auprès de prestataires de services et de partenaires externes ou de la Confédération (Cyber Security Hub[14], MISP, ...).

Comment satisfaire aux exigences ?

Pour les vulnérabilités nouvellement identifiées, les entreprises doivent prendre des mesures appropriées afin de réduire le risque. Cela peut se faire par l'implémentation de correctifs de sécurité, de modifications de configuration ou d'autres contrôles qui éliminent la vulnérabilité ou réduisent son impact.

Dans les cas où il n'est pas possible de corriger ou d'éliminer immédiatement la vulnérabilité, il convient de procéder à une acceptation documentée des risques. Cela signifie que la direction a évalué les risques associés à la vulnérabilité et a délibérément décidé de les tolérer temporairement ou définitivement.

Quand les exigences sont-elles satisfaites ?

Il est essentiel de documenter ce processus afin de garantir la transparence et de s'assurer que l'évaluation des risques repose sur des informations solides. Cela facilite également le suivi et la gestion des vulnérabilités au fil du temps.

En mettant en œuvre une approche structurée, les organisations peuvent améliorer leur situation en matière de sécurité en abordant de manière proactive les vulnérabilités et en gérant efficacement les risques. Cela contribue à renforcer la résilience et à minimiser les risques de cyberattaques.

[14] Les questions relatives au CSH ou à d'autres services de l'OFCS doivent être adressées à info@ncsc.admin.ch.

Récupérer (RC)

La catégorie « récupérer » identifie les mesures appropriées pour créer et maintenir des plans de résilience et de récupération des fonctions ou des services qui ont été affectés par un incident de cybersécurité. Cela favorise le retour à un fonctionnement normal en temps voulu afin de réduire l'impact d'un incident de cybersécurité.

Plan de restauration (RC.RP)

Les processus et procédures de récupération sont exécutés et maintenus afin de garantir la récupération des systèmes ou des installations touchés par des incidents de cybersécurité.

Figure 11 : Sous-catégorie RC prescrite pour le niveau de protection C

Plan de restauration (RC.RP)

RC.RP-1 Exécution correcte du plan de récupération	NM
Assurez-vous que le plan de récupération est suivi à la lettre en cas d'incident de cybersécurité.	2

De quoi s'agit-il ?

Plusieurs étapes importantes sont nécessaires pour garantir la bonne exécution d'un plan de récupération après un incident de cybersécurité. Seules une préparation adéquate et une exécution minutieuse du plan de récupération permettent un retour rapide à la normale et une réduction de l'impact de l'incident.

Qu'est-ce qui doit être accompli ?

Le plan de récupération doit contenir des instructions claires sur la manière de traiter les différents types d'incidents de sécurité afin de permettre une réaction rapide. Des mises à jour régulières sont indispensables pour s'assurer que le plan tient compte des menaces et des technologies actuelles.

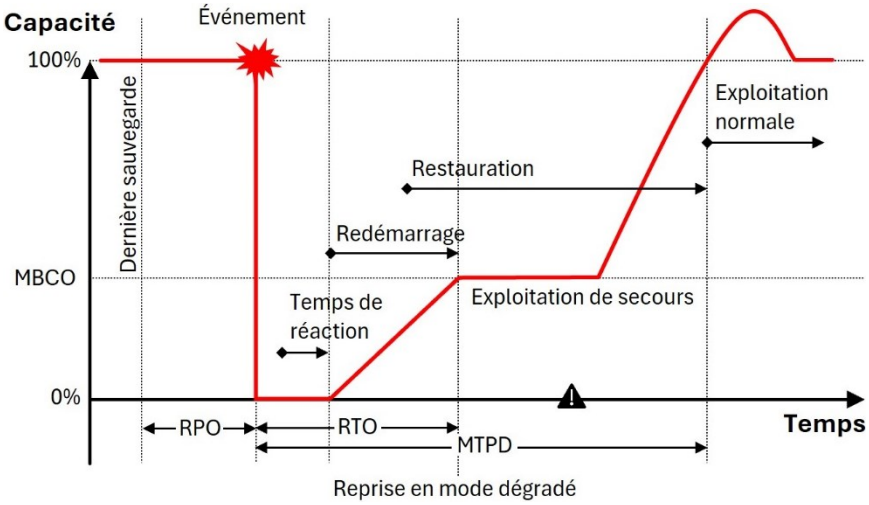

Figure 12 : Processus de restauration

RPO: *Recovery Point Objective*. À partir de ce moment, les données sont perdues.

RTO: *Recovery Time Objective*. Combien de temps faut-il pour que l'activité reprenne ? Du matériel de remplacement est-il disponible ? Y a-t-il suffisamment de ressources et de soutien de la part du prestataire de services ?

MBCO: *Minimum Business Continuity Objective*. Quels sont les systèmes nécessaires pour l'exploitation de secours (BCM) ?

MTPD: *Maximum Tolerable Period of Disruption*.

Comment satisfaire aux exigences ?

Une répartition claire des responsabilités, des procédures d'escalade définies et des canaux de communication clairs sont essentiels pour minimiser l'impact. L'utilisation de listes de contrôle (*checklists*) permet de suivre les étapes du plan de récupération de manière structurée et d'éviter les erreurs/oublis.

Quand les exigences sont-elles satisfaites ?

Les exigences sont remplies lorsque l'entreprise a défini le processus de récupération en étapes claires. La mise en œuvre doit être progressive et peut être soutenue par des outils (par exemple une liste de contrôle). Une documentation précise permet d'améliorer le plan après chaque incident. La cohérence dans ces mesures garantit la continuité des opérations et renforce la confiance.

Table des illustrations

Liste des abréviations

2FA	Authentification à deux facteurs
art.	Article
ASIG	Association suisse de l'industrie gazière
BCM	*Business Continuity Management* (Gestion de la continuité des activités)
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Office fédéral allemand de la sécurité des technologies de l'information)
BYOD	*Bring Your Own Device* (Apportez votre propre appareil)
COBIT	*Control Objectives for Information and Related Technology*
CSF	*Cybersecurity Framework* (Cadre de cybersécurité)
CSH	*Cybersecurity Hub*
DLP	*Data Loss Prevention* (Prévention de la perte de données)
DNS	*Domain Name System*
EDR	*Endpoint Detection and Response* (Détection et réponse des terminaux)
GCA	Gestion de la continuité des activités
GovCERT	*Government Computer Emergency Response Team* (Service national spécialisé dans la gestion technique des cyberincidents et dans l'analyse technique des cyberrisques)
IAM	*Identity and Access Management* (Gestion des identités et des accès)
IC	Infrastructure critique
ICS	*Industrial Control System* (Système de contrôle industriel)
IDM	*Identity Management* (Gestion des identités)
IDS	*Intrusion Detection System* (Système de détection d'intrusion)
IFP	Inspection fédérale des pipelines
IoT	*Internet of Things* (Internet des obets)
IP	*Internet Protocol*
IPS	*Intrusion Prevention System* (Système de prévention d'intrusion)
IPsec	*Internet Protocol Security*
ISO	*International Organization for Standardization* (Organisation internationale de normalisation)
IT	*Information Technology* (Technologie de l'information)
LPD	Loi sur la protection des données
MBCO	*Minimum Business Continuity Objective* (Objectif minimal de continuité des activités)

MDM	*Mobile Device Management* (Gestion d'appareils mobiles)
MFA	*Multi-factor authentication* (Authentification multifacteur)
MISP	*Malware Information Sharing Platform* (Plateforme de partage d'informations sur les logiciels malveillants)
MTPD	*Maximum Tolerable Period of Disruption (*Durée maximale d'interruption admissible)
NAC	*Network Access Control* (Contrôle d'accès au réseau)
NDA	*Non-Disclosure Agreement* (Accord de non-divulgation)
NERC	*North American Electric Reliability Corporation*
NIST	*National Institute of Standards and Technology*
NM	Niveau de maturité
OCyS	Ordonnance sur la cybersécurité (projet)
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCS	Office fédéral de la cybersécurité
OFEN	Office fédéral de l'énergie
OPDo	Ordonnance sur la protection des données
OSITC	Ordonnance sur la sécurité des installations de transport par conduites
OT	*Operational Technology* (Technologie opérationnelle)
PDCA	*Plan-Do-Check-Act* (Planifier – Mettre en oeuvre – Vérifier – Agir)
PFPDT	Préposé fédéral à la protection des données et à la transparence
PME	Petite ou moyenne entreprise
RBAC	*Role-Based Access Control* (Contrôle d'accès basé sur les rôles)
RFID	*Radio Frequency Identification*
RGPD	Règlement général sur la protection des données (UE)
Rlogin	*Remote Login*
RPO	*Recovery Point Objective* (Perte de données maximale admissible)
RS	Recueil systématique
RSSI	Responsable de la sécurité des systèmes d'information
RTO	*Recovery Time Objective* (Durée maximale d'interruption admissible)
SIEM	*Security Information and Event Management* (Système de gestion des informations et des événements de sécurité)
SSH	*Secure Shell*
SVGW	Association pour l'eau, le gaz et la chaleur
SYSLOG	*System Logging*
Telnet	*Teletype Network Protocol*
TIC	Technologies de l'information et de la communication
TLS	*Transport Layer Security*
UE	Union européenne
USB	*Universal Serial Bus*
VLAN	*Virtual Local Area Network* (Réseau local virtuel)
VPN	*Virtual Private Network* (Réseau privé virtuel)
WLAN	*Wireless Local Area Network*

Annexes

Annexe 1 : Glossaire

Les termes suivants ont une signification spécifique dans le cadre de ce document. Nous avons renoncé à lister les termes généralement utilisés dans le contexte des TIC (p. ex. hardware, software, backup, ...).

Terme	Signification
Cyberattaque	Les cyberattaques comprennent toutes les activités délibérées visant à porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité des données.
EDR	Un EDR (*Endpoint Detection and Response*) est un outil de cybersécurité qui surveille et analyse en permanence l'activité des terminaux (tels que les ordinateurs, les serveurs ou les appareils mobiles) afin de détecter et de prévenir les menaces et d'y répondre en fournissant un aperçu en temps réel et des mesures correctives.
Hardware Lifecycle Management	Le *Hardware Lifecycle Management* est une approche globale de la gestion du matériel TIC tout au long de sa durée d'utilisation.
Infrastructure TIC	Tous les éléments de l'équipement d'information et de télécommunication dont une organisation a besoin pour accomplir ses processus opérationnels. Par exemple, les ordinateurs de bureau, les téléphones portables, les centres de données, etc.
Systèmes de contrôle industriels	« Systèmes de contrôle industriels » est un terme générique qui désigne tous les éléments utilisés pour commander et surveiller des installations ou des processus industriels. Un système de contrôle industriel comprend typiquement des capteurs, des centres de calcul, des centres de contrôle, des lignes et des installations. Les termes anglais « Industrial Control System/ICS » et « Supervisory Control and Data Aqcuisition System/SCADA » sont utilisés comme synonymes.
IDS	Un IDS (*Intrusion Detection System*) est un système de détection des attaques dirigées contre un système informatique ou un réseau. L'IDS peut compléter un pare-feu ou fonctionner directement sur le système informatique à surveiller.
Compromission	Un système, une base de données ou même un simple enregistrement est considéré comme compromis si des données peuvent être manipulées et si le propriétaire (ou l'administrateur) du système ne peut plus contrôler son bon fonctionnement ou garantir que son contenu est correct.
Infrastructure critique	L'éventail des infrastructures critiques (IC) comprend neuf secteurs, subdivisés en 27 sous-secteurs (branches). L'aperçu complet est disponible en ligne, à l'adresse suivante : https://www.babs.admin.ch/fr/les-infrastructures-critiques
Least Privilege	Les collaborateurs ne disposent que des autorisations strictement nécessaires pour leurs activités, et d'aucune autorisation supplémentaire.
MDM	Un MDM (*Mobile Device Management*) est un outil de gestion qui harmonise la configuration et l'utilisation des appareils mobiles tout

Terme	Signification
	en garantissant un haut niveau de sécurité, par exemple grâce à des sauvegardes, au blocage à distance et à la gestion des mises à jour.
Need-to-know	Le principe du *« need-to-know »* veut que les utilisateurs n'aient accès qu'aux informations absolument nécessaires à leur travail.
Phishing	Le terme « *phishing* » désigne les tentatives d'obtenir des données personnelles d'un utilisateur via des pages web, des e-mails ou des messages courts falsifiés et de les utiliser à des fins d'usurpation d'identité.
Security Awareness Programm	Un programme de sensibilisation à la sécurité a pour objectif d'améliorer la prise de conscience des thèmes de sécurité et le comportement correspondant chez les collaborateurs, les partenaires, les fournisseurs, etc.
Security by Default	*Security by Default* signifie que les systèmes, applications ou appareils sont configurés par défaut de manière à offrir le niveau de sécurité le plus élevé possible sans que l'utilisateur n'ait à intervenir. Cela garantit que seules les fonctions nécessaires sont activées, réduisant ainsi le risque de menace.
Security by Design	*Security by Design* signifie que la sécurité est intégrée dès le début dans la conception d'un produit ou d'un système. Les aspects de sécurité sont pris en compte tout au long du processus de développement afin de garantir une architecture sûre et résistante aux attaques.
Security Monitoring	*Security Monitoring* décrit le processus permettant d'observer en permanence les flux de données et les activités réseau au sein de son propre réseau. L'objectif est de détecter à temps tout comportement suspect. Des systèmes de surveillance de sécurité (*Security Monitoring Systems*) sont utilisés à cette fin.
SIEM	Un SIEM (*Security Information and Event Management*) est un système qui collecte, analyse et met en corrélation en temps réel les données de sécurité provenant de différentes sources (telles que les logs des applications, des serveurs ou des équipements réseau) afin de détecter les menaces, d'alerter les équipes et d'aider à la gestion des incidents de sécurité.
Système	Un ensemble organisé de ressources et de procédures qui sont réunies et régies par l'interaction ou l'interdépendance afin de remplir une série de fonctions spécifiques. Elles peuvent par exemple permettre de mesurer, contrôler, traiter, transmettre, stocker, utiliser et sécuriser des données.
VPN	Un VPN (*Virtual Private Network*) est un réseau privé qui permet une connexion sécurisée via des réseaux publics. Une connexion VPN crée un tunnel à travers lequel des données chiffrées peuvent être communiquées.
Zero Trust	*Zero Trust* est un principe de sécurité selon lequel il ne faut jamais faire confiance par défaut à un utilisateur ou à un système, même s'ils se trouvent à l'intérieur du réseau, et qu'il faut toujours vérifier et valider chaque accès et chaque action par une authentification et des contrôles stricts.

Annexe 2 : Informations complémentaires

Les listes suivantes contiennent des exemples de ressources qui peuvent aider à mettre en œuvre des mesures de cybersécurité.

Ressources de l'OFCS

Thème	Lien
Cyberattaques contre les entreprises	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html
Cybersécurité de la chaîne logistique	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/lieferkette.html
Collaboration avec des prestataires de services informatiques	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html
Communication de crise en cas de cyberattaque	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/krisenkommunikation.html
Mesures en cas de cyberattaque	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/checkliste-ciso.html
Mesures en cas de fuite de données	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/datenabfluss.html
Mesures en cas d'attaque par rançongiciel (ransomware)	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html
Mesures de protection pour les systèmes de contrôle industriels (ICS)	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ics.html
Ransomware	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-bedrohungen/ransomware.html
Sécuriser l'accès à distance	https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/home-office.html

Documentation de l'UE

Thème	Lien
Awareness Campaign – Fuel for Cyber	https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/fuelforcyber
Cyber Insurance: Recent Advances, Good Practices and Challenges	https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges
Cyber Security Culture in Organisations	https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
Cybersecurity Guide for SMEs – 12 Steps to Securing your Business	https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
Cybersecurity Maturity Assessment for Small and Medium Enterprises	https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/

Good Practices for Supply Chain Cybersecurity	https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
Raising Awareness of Cybersecurity	https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

Autres ressources (UK/USA/AU)

Thème	Lien
Advice & Guidance (46 topics)	https://www.ncsc.gov.uk/section/advice-guidance/all-topics
Cyber-Physical Security Considerations for the Electricity Sub-Sector	https://www.cisa.gov/resources-tools/resources/sector-spotlight-cyber-physical-security-considerations-electricity-sub-sector
Cybersecurity Capability Maturity Model (C2M2)	https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
Cybersecurity Framework Profile for Liquefied Natural Gas	https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-liquefied-natural-gas
Device Security Guidance	https://www.ncsc.gov.uk/collection/device-security-guidance
Electricity Substation Physical Security	https://www.cisa.gov/resources-tools/resources/sector-spotlight-electricity-substation-physical-security
Energy Sector Cybersecurity Preparedness	https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness
Infographics of NCSC guidance	https://www.ncsc.gov.uk/section/infographics/home
Information for Small & Medium Sized Organisations	https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations
Operational Technology Guidance	https://www.ncsc.gov.uk/collection/operational-technology
Principles of Operational Technology Cyber security	https://www.cyber.gov.au/about-us/view-all-content/publications/principles-operational-technology-cyber-security?utm_source=international_partner&utm_medium=social&utm_campaign=critical_infrastructure
SCADA in the Cloud	https://www.ncsc.gov.uk/blog-post/scada-cloud-new-guidance-ot-organisations
Smartphone Security Checker	https://www.fcc.gov/smartphone-security

Publications NIST

Document	Lien
NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
NIST SP 800-82 Rev. 3, *Guide to Operational Technology (OT) Security*	https://csrc.nist.gov/pubs/sp/800/82/r3/final
NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*	https://csrc.nist.gov/pubs/sp/800/83/r1/final

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*	https://csrc.nist.gov/pubs/sp/800/84/final
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	https://csrc.nist.gov/pubs/sp/800/86/final
NIST SP 800-92, *Guide to Computer Security Log Management*	https://csrc.nist.gov/pubs/sp/800/92/final
NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	https://csrc.nist.gov/pubs/sp/800/94/final
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*	https://csrc.nist.gov/pubs/sp/800/115/final
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*	https://csrc.nist.gov/pubs/sp/800/128/upd1/final
NIST SP 1800-2, *Identity and Access Management for Electric Utilities*	https://csrc.nist.gov/pubs/sp/1800/2/final
NIST SP 1800-22, *Mobile Device Security: Bring Your Own Device (BYOD)*	https://csrc.nist.gov/pubs/sp/1800/22/final
NIST SP 1800-23, *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry*	https://csrc.nist.gov/pubs/sp/1800/23/final