Norme minimale pour améliorer la résilience informatique

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR
Office fédéral pour l'approvisionnement économique du pays OFAE

Avant-propos

Quand numérisation rime avec protection… impérative !

L'informatique et les réseaux numériques ayant envahi notre vie publique et privée, leur développement ouvre des perspectives économiques comme sociétales que la Suisse, pays développé et industrialisé, ne saurait ignorer. Cette croissance du numérique nous oblige à affronter de nouvelles menaces, requérant des réactions rapides et rigoureuses. Le risque de cyberattaques est une réalité tant pour les services étatiques que pour les exploitants d'infrastructures critiques, voire pour d'autres entreprises.

Il incombe fondamentalement à chaque entreprise de se protéger. Cependant, lorsque le fonctionnement des infrastructures critiques est en jeu, la responsabilité étatique émerge, fondée sur le mandat constitutionnel (donné à l'Approvisionnement économique du pays, AEP), explicité par la loi sur l'approvisionnement du pays. La présente norme minimale pour les TIC traduit concrètement la volonté étatique d'assumer la protection des citoyens, de l'économie du pays, des institutions et des administrations.

Cette norme concerne avant tout les secteurs clés de notre société moderne, là où les pannes ne sont pas tolérées, car ces secteurs sont liés à des infrastructures critiques. Les exploitants de ces systèmes sont invités à appliquer nos recommandations ou des spécifications garantissant un niveau de sécurité comparable (ISO, COBIT, etc.). Par ailleurs, notre norme offre des conseils pratiques aux entreprises ou établissements qui souhaitent améliorer leur propre résilience informatique.

Résumé

Cette norme minimale est une recommandation, voire une ligne directrice pour améliorer la résilience informatique. Elle s'adresse en premier lieu aux exploitants d'infrastructures critiques, mais toute entreprise[1] peut appliquer ces conseils gratuits.

Les responsables informatiques et les directeurs d'entreprises gérant des infrastructures critiques sont les premiers concernés par cette norme minimale.

Ce document comprend trois parties :

1) Les principes de base ou guide de référence fournissant des informations générales sur la sécurité informatique.

2) Le cadre *(Framework)* propose aux utilisateurs une série de mesures concrètes à mettre en œuvre, ventilées en cinq thèmes « identifier », « protéger », « détecter », « réagir » et « récupérer ». On compte 106 mesures en tout.

3) Grâce à l'outil d'auto-évaluation (sous Excel) et d'appréciation, les entreprises peuvent contrôler le degré d'application des mesures ou les faire contrôler par des externes (audit). Les résultats peuvent ensuite servir de base à une analyse comparative.

[1] *Pour alléger le texte et éviter les confusions, la traductrice n'a choisi que ce terme. Il est évident que la norme s'applique aussi à un établissement, un organisme, une institution, une association, etc.*

Sommaire

1 Introduction

1.1 Résumé

Cette partie fixe le cadre et les objectifs de la sécurité des TIC (technologies de l'information et de la communication), en précise la portée et détaille la manière d'utiliser ces standards minimaux.

1.2 Bases légales

Les textes de lois ci-dessous forment la base de l'action de l'Approvisionnement économique du pays (AEP).[2]

- Loi fédérale sur l'approvisionnement économique du pays (Loi sur l'approvisionnement du pays, LAP; RS 531)
- Ordonnance sur l'approvisionnement économique du pays (OAEP; RS 531.11)
- Ordonnance sur les préparatifs en matière d'approvisionnement économique du pays (RS 531.12)

1.3 Contexte et objectifs

La sécurité des TIC présuppose que chaque exploitant assume ses responsabilités en prenant conscience des risques et en recourant à des systèmes sûrs. L'application de mesures efficaces, comme celles présentées dans la présente norme, permet déjà de prévenir un grand nombre d'attaques informatiques, pour un investissement raisonnable. L'objectif de cette norme est de fournir un outil polyvalent aux entreprises pour qu'elles puissent améliorer la résilience de leur infrastructure informatique. Grâce à son approche basée sur le risque, cette norme permet d'introduire différents niveaux de protection, adaptés aux besoins de chaque entreprise.

1.4 Délimitation

L'AEP a mis au point la présente norme minimale pour les TIC avec des experts en sécurité informatique.

Il existe déjà nombre de normes, reconnues au niveau international, en matière de sécurité informatique. La plupart d'entre elles vont bien au-delà des préconisations du présent document (cf. point 1.4.1). La présente ne prétend pas concurrencer ces standards internationaux, mais elle est compatible avec eux, même si sa portée est réduite. Son but est de simplifier l'entrée en matière tout en garantissant un excellent niveau de sécurité.

En outre, l'AEP a élaboré d'autres normes sectorielles, (techniquement) plus détaillées.[3] Nous recommandons aux exploitants d'infrastructures critiques de prendre en considération non seulement cette norme minimale, mais aussi celles propres à leur secteur, dès lors qu'elles sont disponibles.

Lorsqu'une norme existe déjà pour un secteur, ou qu'un standard international est appliqué – comme ISO ou NIST – les entreprises peuvent utiliser la liste de vérification du chapitre 3 « Contrôle » pour vérifier si leur installation remplit les exigences de la norme minimale.

1.4.1 Documentation et normes

Les manières d'affronter les risques informatiques font l'objet de nombreuses normes et sont décrites dans quantité de documents. Certaines solutions, devenues des standards industriels, sont déjà appliquées. La présente norme minimale est basée sur *NIST Cybersecurity Framework Core*.[4] Si nécessaire, elle peut être complétée par d'autres standards reconnus, dont les principaux sont listés ci-dessous :

1) *NIST Guide to Industrial Control Systems (ICS) Security*
   Ce guide a été conçu et publié par le *National Institute of Standards and Technology (NIST)* qui le développe encore. Il complète le *NIST Cybersecurity Framework Core* par des exigences liées aux systèmes de contrôle industriels (SCI), notamment dans la *NIST Special Publication* 800-82, révision du 2 mai 2015.[5]

[2] Tous les textes de lois sont disponibles dans le recueil systématique du droit fédéral (RS). La recherche en ligne se trouve à l'adresse : https://www.admin.ch/gov/fr/accueil/droit-federal/recueil-systematique.html

[3] Disponibles (en allemand seulement) pour les secteurs : approvisionnement en électricité et en aliments. Les normes détaillées pour les autres secteurs, en cours d'élaboration, seront aussi publiées.

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

[5] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

2) ISO 2700x
   L'Organisation internationale de normalisation (ISO) publie une douzaine de normes de sécurité informatique complémentaires connues sous le nom de « famille 2700x ».
   La norme ISO 27001 est la plus connue. Elle détaille les exigences pour configurer, installer, assurer la maintenance et améliorer régulièrement un système documenté pour gérer la sécurité de l'information, en tenant compte des particularités de chaque entreprise.[6]

3) COBIT
   Control Objectives for Information and Related Technology (COBIT).[7]

4) *ENISA Good Practice Guide on National Cyber Security Strategies.*[8]

5) Bundesamt für Sicherheit in der Informationstechnik (Allemagne), BSI 100-2.[9]

1.4.2 Principes

1) responsabilité individuelle : les exploitants d'infrastructures critiques doivent veiller à sauvegarder leurs processus TIC cruciaux.

2) *Business Continuity Management :* tous les aspects de la sécurité informatique sont à intégrer dans un système, hiérarchiquement supérieur, gérant la continuité des affaires.

3) gestion des risques : il incombe aux utilisateurs de cette norme d'évaluer régulièrement les risques informatiques susceptibles d'entraver la disponibilité, l'intégrité ou la confidentialité des systèmes. Les entreprises déterminent elles-mêmes les risques supportables et ceux qui doivent absolument être circonscrits.

1.4.3 Mesures et renvois dans ce document

Nous nous sommes efforcés de ne pas dupliquer inutilement les informations. Nous vous renvoyons plutôt à d'autres normes. Nous conseillons aux utilisateurs de cette norme de consulter – si besoin est – les sources citées.

[6] *https://www.iso.org/standard/66435.html*

[7] *http://www.isaca.org/COBIT/Pages/default.aspx*

[8] *https://www.enisa.europa.eu/topics/national-cyber-security-strategies*

[9] *https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html (disponible en allemand uniquement).*

1.5 Introduction aux normes minimales pour les TIC

Les principaux thèmes de la norme minimale pour les TIC sont présentés dans cette section.

1.5.1 Principes de base pour la sécurité informatique

Une entreprise doit fixer ses principes en matière de TIC avant de mettre en œuvre sa stratégie concrète de sécurité informatique. Elle doit notamment se poser les questions suivantes :

- Que fait-on ?
- Comment le fait-on ?
- Qui est responsable ?
- Comment évaluera-t-on si les objectifs (de protection) sont atteints ?

Les principes de la sécurité informatique définissent les règles, les processus, les métriques et les structures organisationnelles requises pour une planification et un contrôle efficaces.

1.5.2 Organisation et responsabilités

Un organisme chargé de la sécurité informatique au sens large doit être créé dans l'entreprise. Il définira clairement les tâches, les responsabilités et les compétences de chacun. Il devra aussi définir et mettre en œuvre une stratégie de défense en profondeur. Les risques informatiques doivent être intégrés dans une politique globale de gestion des risques. Sinon, il sera difficile d'identifier les menaces potentielles liées aux TIC et de définir les mesures de protection adéquates. L'organisme de sécurité doit livrer toutes les informations utiles pour que la direction puisse décider des ressources à engager. La direction doit accorder à cet organisme les compétences nécessaires pour exécuter pleinement ses tâches principales en étroite collaboration avec les autres services.

1.5.3 Stratégie, consignes et lignes directrices

Il convient de définir les orientations, les processus et les consignes de travail d'une entreprise – ou au moins de les identifier – avant de mettre en œuvre une politique de sécurité informatique (par ex. une stratégie de défense en profondeur).

Les besoins opérationnels des différents services d'une entreprise doivent être documentés et communiqués aux responsables de la cybersécurité. Il peut s'agir d'exigences juridiques ou financières, de contraintes stratégiques ou opérationnelles par exemple.

1.5.4 Gestion des risques

Une gestion active des risques est indispensable pour améliorer la résilience informatique en mettant en place une stratégie de défense en profondeur. La propension au risque de l'entreprise doit être prise en compte. Il est donc vital que l'unité responsable de l'exploitation et de la maintenance des systèmes informatiques connaisse les méthodes et processus de gestion des risques choisis par l'organisme chargé de la sécurité et qu'elle les applique aux risques liés aux TIC. Le processus de gestion des risques informatiques vise à identifier, évaluer et gérer les dangers potentiels qui menacent les systèmes, les applications et les données TIC protégés, et à déterminer la façon de gérer les risques identifiés. Le processus de gestion des risques comprend trois phases : l'analyse des risques, l'évaluation des risques et la maîtrise des risques, impliquant de mettre en œuvre des mesures appropriées. Les risques sont régulièrement réévalués afin de vérifier l'efficacité de ces mesures, et tout changement doit être signalé. Les mesures sont alors ajustées, si nécessaire.

Il n'y aura jamais de sécurité absolue. La direction de l'entreprise doit donc déterminer sa propension au risque.

1.6 Éléments d'une stratégie de défense en profondeur

1.6.1 Aperçu de la « défense en profondeur »

Une entreprise doit axer sa stratégie de sécurité informatique sur la protection des équipements TIC indispensables aux processus opérationnels. Une approche à plusieurs niveaux est nécessaire : au plan international, on l'appelle *Defense-in-Depth,* soit défense en profondeur. En combinant plusieurs mesures de sécurité, on peut protéger les équipements TIC d'une entreprise. Le principe militaire qui veut qu'un ennemi aura plus de difficultés à surmonter un système de défense multicouche complexe qu'à franchir une simple barrière est à la base de cette stratégie. En parallèle, il faut étudier les méthodes et les modes opératoires des agresseurs potentiels pour préparer des systèmes de défense adaptés. Dans le secteur de la sécurité informatique, le principe (plan) de défense en profondeur vise à détecter les atteintes à la sécurité des TIC pour réagir à ces atteintes et en réduire les effets, ou du moins en atténuer l'impact. La défense en profondeur poursuit une approche holistique qui vise à protéger toutes les ressources (TIC) contre n'importe quel risque. Une entreprise devrait consacrer ses ressources à se protéger des risques connus et à cerner les risques potentiels. Des mesures appropriées doivent protéger l'intégralité des systèmes TIC. Cela comprend les personnes, les processus, les bâtiments, les données et les appareils. Un agresseur ne constitue une menace pour un système TIC que s'il parvient à détecter et exploiter une faille dans l'un de ces éléments. Les entreprises doivent régulièrement contrôler l'efficacité des mesures de protection et les adapter aux nouvelles menaces, si nécessaire.

1.6.2 Systèmes de contrôle industriels *(Industrial Control Systems)* ou SCI

Vu l'architecture complexe des SCI, certaines failles critiques peuvent rester longtemps non détectées alors que les attaques (« *exploits* ») correspondantes (de type *Advanced Persistent Threat*) sont une véritable menace.

Voici quelques méthodes d'attaque typiques visant les SCI :

- attaques via Internet d'un SCI accessible en ligne pour établir un accès à distance permanent,
- accès à distance à un SCI en utilisant des données d'accès volées,
- attaques d'un SCI en profitant des failles d'interfaces Web,
- contamination d'un SCI par des logiciels malveillants sur des supports de données corrompus (clés USB, smartphone, etc.),
- attaques de la bureautique (par ex. via des courriels d'hameçonnage, infections par téléchargement furtif, etc.) visant à pénétrer dans un SCI par n'importe quelle interface.

Fondamentalement, il existe des différences importantes entre la bureautique et un SCI lorsqu'on met en œuvre des plans de défense en profondeur. Le tableau 1 liste les sujets liés à la sécurité et les implications différentes pour les TIC et les SCI.

Thématique sécuritaire	TIC (bureautique par ex.)	SCI (centrale nucléaire par ex.)
Antivirus	Largement répandu. Facile à distribuer et à mettre à jour. Les utilisateurs ont la possibilité de le personnaliser. Une protection par antivirus peut être configurée au niveau de l'équipement ou d'une entreprise.	La mémoire requise et le ralentissement des échanges de données pour cause d'analyse par l'antivirus peuvent affecter le fonctionnement d'un SCI. Pour protéger leurs SCI les plus anciens, les sociétés n'ont souvent pas d'autre choix que d'acheter des produits issus du marché secondaire. Les solutions antivirus recourent souvent à des dossiers « d'exception » dans les environnements SCI pour éviter la mise en quarantaine de fichiers stratégiques.
Mises à jour de sécurité *(Update Management)*	Doivent être précisément définies, appliquées à toute l'entreprise et automatisées grâce à des accès à distance.	Délais et planification prennent du temps jusqu'à ce que les correctifs soient correctement installés ; toujours tributaires du fournisseur ; peuvent (temporairement) stopper le SCI ; d'où l'obligation de définir un « risque acceptable ».
Cycles de vie de la technologie *(Technology Support Lifecycle)*	2 à 3 ans, plusieurs fournisseurs, développement et mises à niveau constants.	10 à 20 ans, souvent un seul fournisseur ou prestataire de service sur tout le cycle de vie, sa fin générant de nouveaux risques pour la sécurité.
Méthodes de tests et d'audits *(Testing and Audit Methods)*	Utilisation de méthodes modernes (si possible automatisées). Les systèmes sont normalement suffisamment résilients et fiables pour supporter des évaluations *(assessments)* sans interrompre l'exploitation.	Les méthodes d'évaluation automatisées ne conviennent pas forcément, vu le haut degré de personnalisation par ex. Les risques qu'une erreur se produise pendant une évaluation sont élevés. De fait, les évaluations en cours de production sont généralement plus délicates.
Gestion des modifications *(Change Management)*	Planifiées et périodiques. Respectant les exigences de l'entreprise : durées minimale + maximale de fonctionnement d'un appareil.	Processus complexe avec un impact possible sur les activités de l'entreprise. Une planification stratégique et individuelle est indispensable.
Classification des actifs *(Asset Classification)*	Se fait normalement chaque année. Les dépenses + investissements sont planifiés en fonction des résultats.	Faite seulement si nécessaire ou sur demande. Faute d'inventaire, les contre-mesures ne sont souvent pas adaptées à l'importance de l'élément système.
Réaction + analyse en cas d'incidents *(Incident Response and Forensics)*	Facile à développer et à mettre en œuvre. Au besoin, se conformer aux prescriptions réglementaires (protection des données).	Se concentre principalement sur le redémarrage du système. Processus d'analyse peu réglementés.
Sécurité physique *(Physical Security)*	Variable : faible pour la bureautique et forte pour les centres de calculs protégés.	Normalement, la sécurité physique est bonne.
Développement de logiciels sécurisés *(Secure Software Development)*	Partie intégrante du processus de développement.	Historiquement, les SCI étaient conçus comme des systèmes distincts. Il n'était pas prévu d'intégrer la sécurité dans leur développement. Les fournisseurs de SCI ont fait des progrès, mais moins que dans le domaine des TIC. Il n'existe guère de solutions pour sécuriser a postériori les éléments centraux des SCI.
Règles de sécurité	Prescriptions réglementaires générales, selon le secteur (pas pour tous les secteurs).	Normes réglementaires propres au secteur (mais pas pour tous les secteurs).

Tableau 1 : différences selon TIC et SCI

Lorsqu'on établit un plan de défense en profondeur pour un SCI, il faut prendre en compte les éléments suivants :

- coûts pour sécuriser les anciens systèmes selon les normes actuelles
- tendance croissante à connecter les SCI aux réseaux de l'entreprise
- possibilité de fournir un accès à distance aux utilisateurs des environnements TIC et SCI
- obligation de faire confiance à sa propre chaîne d'approvisionnement
- surveillance et protection des protocoles propres aux SCI, avec des outils modernes
- capacité à rester constamment informé des nouvelles menaces planant sur les SCI

L'approche « défense en profondeur » complique les attaques directes des systèmes TIC et augmente la probabilité de détecter rapidement des comportements suspects ou inhabituels dans le système. Cette approche permet également de créer des zones distinctes pour mettre en œuvre des technologies permettant de détecter les intrusions dans le système *(Intrusion-Detection-Technology)*. Les éléments représentatifs d'une stratégie de défense en profondeur sont présentés au tableau 2.

Éléments d'une stratégie de défense en profondeur	
Programme de gestion des risques	• reconnaissance des risques pour la sécurité • profil de risques • gestion minutieuse (inventaire) des équipements TIC
Architecture de cybersécurité	• normes/recommandations • lignes directrices • mode opératoire
Sécurité physique	• protection des terminaux • surveillance des accès au centre de contrôle • vidéosurveillance, contrôle des accès et barrières
Architecture de réseau	• zones de sécurité standards • « zones démilitarisées » (DMZ) • réseaux locaux virtuels (LAN)
Périmètre de sécurité réseau	• pare-feu • accès à distance et authentification • serveurs hôtes/intermédiaires (*jump servers/hosts*)
Sécurité de l'hôte	• gestion des correctifs et des points faibles • terminaux • machines virtuelles
Surveillance de sécurité	• systèmes de détection d'intrusion • journaux *(logs)* des audits de sécurité • incidents de sécurité et contrôle des évènements
Gestion des fournisseurs	• gestion et contrôle de la chaîne fournisseurs • services d'infogérance *(managed services)* et externalisation • utilisation d'informatique en nuage *(cloud)*
Facteurs humains	• lignes directrices • mode opératoire • formation et sensibilisation

Tableau 2 : éléments d'une stratégie de défense en profondeur

1.6.3 Gestion des risques

1.6.3.1 Programme de gestion des risques

Il faut comprendre les risques auxquels une entreprise est exposée (menaces informatiques) pour mettre en œuvre une stratégie de défense en profondeur. Ils doivent être gérés en fonction de la propension au risque dans l'entreprise. Les responsables de l'exploitation et de la maintenance des systèmes TIC doivent pouvoir identifier, évaluer et traiter les cyber-risques. Ils doivent savoir comment appliquer ces méthodes dans leurs environnements respectifs. Cela exige une bonne connaissance des scénarios de menace, des processus opérationnels et techniques, ainsi que des technologies en jeu. On ne peut intégrer dans les tâches quotidiennes une stratégie de défense en profondeur qu'après avoir analysé ces paramètres. La direction de l'entreprise doit définir la sécurité comme prérequis à toutes ses activités informatiques.

Les règles énoncées ci-dessus ne sont que des principes généraux. Certaines applications TIC sont particulièrement importantes, voire critiques, notamment dans les systèmes de contrôle industriels ou SCI *(Industrial Control Systems).* Pour concevoir une architecture de sécurité SCI efficace, il faut que les risques d'entreprise soient rapportés aux exigences fonctionnelles (opérationnelles) du SCI. Cela peut avoir des incidences dans le monde réel (par ex. un périmètre de sécurité autour d'un centre de calcul). Les décideurs, à tous les niveaux de l'entreprise, doivent comprendre l'importance des cyber-risques et être activement impliqués dans leur processus de gestion. Il faut faire régulièrement des analyses de risques pour les systèmes, applications et processus cruciaux, y compris pour les réseaux associés. Elles doivent être effectuées selon des règles strictes, suivant une approche structurée et systématique.

1.6.3.2 Cadre pour gérer les risques *(framework)*

Les analyses des risques informatiques devraient être intégrées dans la gestion globale des risques et être effectuées régulièrement sur des objets de recherche clairement définis : systèmes, processus et applications stratégiques (même en cours de développement) ainsi que d'autres systèmes, réseaux et services dont ils dépendent.

Ce cadre pour gérer les risques permet d'affecter aux risques identifiés des responsables qui vont surveiller (monitorage), évaluer et mettre en œuvre des mesures permettant de circonscrire les risques dans des limites préalablement définies comme acceptables (= propension au risque).

1.6.3.3 Analyse des risques

Il faut clairement définir la portée de l'analyse des risques informatiques, décrire les processus opérationnels et les éléments techniques pertinents (et d'éventuels facteurs externes), puis pondérer ces facteurs et éléments. Ainsi on aura défini le contenu et les limites de l'analyse.

1.6.4 Analyse d'impact sur les affaires

Cette analyse permet d'évaluer quel serait l'impact (réaliste voire dans le pire des cas) d'une composante TIC corrompue (y compris les personnes, les données, les processus, les services ou les réseaux) sur les activités d'une entreprise, et ce, à divers titres (financier, opérationnel, juridique, réputationnel, sanitaire).

Enfin, il faut déterminer l'impact sur ses activités que l'entreprise est prête à assumer si ses ressources informatiques ne sont pas disponibles contrairement à ce qui était prévu. Par conséquent, il convient de définir les exigences et les niveaux de protection nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des ressources TIC choisies en fonction d'un risque jugé acceptable.

1.6.5 Mesures

Il faut identifier, examiner et avaliser les mesures à prendre pour se prémunir contre les risques décrits dans l'analyse d'impact. La direction de l'entreprise doit les avaliser en même temps que les plans précisant la marche à suivre.

On doit aussi penser à évaluer le risque résiduel pour tous les équipements dans l'environnement considéré et à le gérer de manière adéquate (l'atténuer, le contourner, le transférer ou l'accepter), selon la propension au risque de l'entreprise.

Il faut déterminer le risque maximal acceptable pour chaque équipement *(asset),* ce qui permet de calculer les risques informatiques (cumulés).

1.6.6 Architecture de la cybersécurité

Une architecture de cybersécurité comprend des mesures spécifiques et leur place stratégique dans le réseau afin d'instaurer une couche de sécurité requise pour une défense en profondeur. Elle facilite également la collecte d'informations sur les flux de données entre tous les systèmes et sur leurs connexions. L'architecture de cybersécurité devrait être en phase avec l'inventaire des installations et des ressources TIC pour garantir que les flux informatiques sont globalement identifiés dans l'entreprise.

Une architecture de cybersécurité devrait être en adéquation avec le *NIST Framework Core* et prendre en compte la protection de la confidentialité, de l'intégrité et de la disponibilité des données, des services et des systèmes. Pour ce faire, il faut élaborer un plan de mise en œuvre respectant la culture d'entreprise et les objectifs stratégiques, tenant adéquatement compte des besoins de sécurité et indiquant les ressources requises. En général, une architecture de cybersécurité est complétée par une liste de tâches qui détaille les résultats espérés (signalant des problèmes et l'urgence de poursuivre l'analyse en profondeur pour établir des plans plus précis), établit les agendas des projets, évalue les besoins en ressources et cerne les principaux facteurs de dépendance du projet.

1.6.7 Sécurité physique

Les mesures de sécurité (physique) réduisent le risque de pertes accidentelles ou intentionnelles, ou de dommages causés aux équipements informatiques de l'entreprise ou dans le voisinage. Les équipements à protéger comprennent le matériel comme les outils et les installations, l'environnement (au sens écologique) et le voisinage ainsi que ce qui relève de la propriété intellectuelle, notamment les données propriétaires (paramètres de configuration ou fichiers clients). Les contrôles de sécurité doivent fréquemment répondre à des exigences spécifiques – question environnement, sécurité, réglementation, droit, etc. Les entreprises doivent adapter les contrôles de sécurité et les contrôles techniques à leurs besoins de protection. Pour garantir une protection globale, la sécurité physique comprend également la protection des composantes informatiques *(= security)* et des données liées à ces composantes. La sécurité de nombreuses infrastructures TIC est étroitement liée à la sécurité des installations *(= safety).* L'objectif est de mettre les employés à l'abri du danger sans entraver leur travail ou à cause de procédures d'urgence. Les contrôles de sécurité sont des mesures actives ou passives qui limitent l'accès à toutes les composantes de l'infrastructure TIC. Ces mesures de protection doivent notamment empêcher les cas suivants :

- visiteurs indésirables aux endroits critiques
- modifications physiques, manipulations, vols ou autres disparitions voire destructions de systèmes, d'infrastructures, d'interfaces de communication, voire de sites
- observations inopportunes d'installations critiques, émanant de curieux, de photographes ou de personnes faisant d'autres sortes de relevés
- introduction ou installation non autorisée de nouveaux systèmes, infrastructures, interfaces de communication ou autre équipement informatique
- introduction subreptice d'appareils (clés USB, point d'accès sans fil, *Bluetooth* ou mobiles), destinés à endommager des équipements, intercepter des communications ou nuire d'une autre manière.

Pour répondre aux besoins de sécurité informatique, il faut protéger les équipements, y compris les systèmes et le matériel réseau, la bureautique (imprimantes en réseau et appareils multifonctions) et les équipements spéciaux (par ex. les SCI) tout au long de leur cycle de vie, de l'acquisition (achat ou location) à leur élimination, en passant par la maintenance.

Les appareils mobiles (ordinateurs portables, tablettes et smartphones) et leurs données doivent également être protégés contre le piratage, la perte et le vol en configurant les paramètres de sécurité, en limitant les accès, en installant des logiciels de sécurité et en gérant les appareils de manière centralisée.

1.6.8 Gestion des cycles de vie du matériel *(hardware)*

L'achat ou la location de matériel robuste et fiable doit toujours se faire en respectant les exigences de sécurité. Les éventuels points faibles du matériel doivent toujours être identifiés.

L'objectif est de garantir que les équipements offrent les fonctionnalités désirées et ne compromettent pas la sécurité des informations et des systèmes critiques ou sensibles et ce, tout au long de leur cycle de vie.

1.6.9 Configuration des appareils mobiles

Pour protéger les données contre les accès non autorisés, la perte et le vol, les appareils mobiles (ordinateurs portables, tablettes et smartphones) doivent toujours avoir une configuration standardisée qui réponde aux exigences de sécurité.

Le but de cette configuration standardisée est de garantir, même en cas de perte ou de vol, la sécurité informatique des données stockées ou envoyées sur l'appareil mobile.

1.6.10 Systèmes de contrôle industriels

Les systèmes de contrôle industriels (SCI) doivent être surveillés et contrôlés conformément aux exigences de sécurité. Il faut notamment les protéger techniquement et physiquement afin de garantir les processus cruciaux pour l'approvisionnement.

1.6.11 Architecture réseau SCI

Lorsqu'on conçoit une architecture réseau, il est généralement recommandé de séparer les réseaux SCI du réseau de l'entreprise. Le type de données est différent sur ces deux réseaux : accès Internet, FTP, courrier électronique et accès à distance sont généralement autorisés dans un réseau d'entreprise, mais pas dans un réseau SCI. Les données SCI transmises au réseau de l'entreprise peuvent être interceptées ou exposées à des attaques par déni de service distribué (DDoS) ou de l'intercepteur. On peut considérablement réduire les problèmes de sécurité et de performances dans le réseau SCI en limitant la connectivité entre le réseau d'entreprise et le réseau SCI, voire en les séparant carrément.

1.6.12 Périmètre de sécurité des réseaux SCI

Le coût d'une installation SCI et la maintenance d'une infrastructure de réseau homogène exigent souvent une connexion entre le SCI et le réseau d'entreprise. Cette connexion représente un important risque pour la sécurité, elle devrait être techniquement protégée. Si les réseaux doivent absolument être interconnectés, il est fortement recommandé de n'autoriser qu'un minimum de connexions (voire des connexions uniques) via un pare-feu et une DMZ (segment de réseau séparé). Les serveurs SCI contenant des données du réseau d'entreprise doivent être placés dans une de ces zones « démilitarisées ». Les connexions avec l'extérieur doivent être recensées et limitées le plus possible via le pare-feu. En outre, des systèmes de détection d'anomalies permettent de surveiller les échanges de données et de les valider.

1.6.13 Sécurité des hôtes

Une couche de sécurité supplémentaire doit être apportée au niveau du poste de travail (hôte). Les pare-feu protègent la plupart des appareils contre les intrusions extérieures. Un bon système de sécurité exige cependant des défenses à plusieurs niveaux. Une sécurisation complète du réseau implique de sécuriser tous les ordinateurs hôtes. Cette couche de sécurité doit permettre à un opérateur d'utiliser divers systèmes d'exploitation et différentes applications tout en assurant une protection correcte des équipements.

Les directives sur les mots de passe doivent être identiques pour tous les utilisateurs d'un système. Les noms de comptes classiques (administrateur par ex.) doivent être modifiés. Les utilisateurs auront tendance à contourner des pratiques trop restrictives, en notant leur mot de passe (sur des post-it par ex.) ou en utilisant systématiquement des chaînes de caractères semblables. La complexité des règles relatives aux mots de passe devrait être adaptée au niveau d'autorisation des utilisateurs. On peut aussi exiger des changements de mots de passe à intervalles réguliers.

Les recommandations générales suivantes devraient être mises en œuvre par les entreprises pour chaque hôte SCI et chaque appareil doté d'un accès au réseau de l'entreprise (quel que soit le système d'exploitation) :

- installer et configurer un pare-feu basé sur l'hôte
- régler si possible les écrans de veille à intervalles très courts, obligeant de redonner le mot de passe
- installer régulièrement les correctifs des systèmes d'exploitation et mettre à jour les micrologiciels
- configurer les *logs* (journaux) et les activer sur tous les appareils
- désactiver les services et les comptes non utilisés
- remplacer les services non sécurisés (Telnet, *remote shell* ou rlogin) par des solutions plus sûres (*secure shell* ou « coque de sécurité »)
- ne pas autoriser les utilisateurs à désactiver des services
- effectuer et contrôler les sauvegardes des systèmes, surtout si elles ne sont pas gérées de manière centralisée
- activer ou remplacer les modules de sécurité fournis avec le système d'exploitation (scanners de sécurité) par des logiciels plus performants

Appliquer les mêmes stratégies aux ordinateurs portables et autres appareils mobiles non connectés en permanence au réseau de l'entreprise. Il est aussi recommandé de crypter les disques durs des équipements mobiles.

1.6.14 Surveillance de la sécurité

L'utilisation de systèmes de monitorage et de composants réseau qui détectent les comportements anormaux et les « signatures d'attaque » ajoute de la complexité à un environnement informatique ou à un SCI. Les fonctions de surveillance et de détection, selon le plan de défense en profondeur, sont toutefois indispensables pour protéger les équipements critiques. Une barrière électronique autour du réseau SCI ne suffit pas à protéger les ressources critiques contre une intrusion. Le plan de défense en profondeur prévoit qu'une entreprise soit alertée, dès que possible, par son système de surveillance en cas de problème de sécurité. La plupart des entreprises ont une surveillance standard dans leur environnement informatique. Elles oublient souvent de le faire pour leurs réseaux SCI.

Il est indispensable :

- d'effectuer des audits de sécurité exhaustifs, indépendants et réguliers (secteurs critiques dans l'entreprise, processus, applications et systèmes/réseaux supportés)
- de surveiller les risques informatiques, de respecter les éléments des exigences légales, réglementaires et contractuelles importants pour la sécurité et d'informer régulièrement la direction de l'entreprise sur la sécurité informatique

1.6.15 Politique de sécurité informatique

Une fois qu'on a défini, maintenu et contrôlé la stratégie globale de sécurité informatique, la direction d'une entreprise peut fixer des lignes directrices claires, les défendre tant dans l'application des exigences que dans la gestion des risques.

1.6.16 Gestion des fournisseurs

La gestion des fournisseurs concerne l'identification et la gestion des risques liés aux technologies de l'information pour les fournisseurs externes (matériel + logiciels, services d'externalisation, services en nuage, etc.). Respecter les exigences en matière de sécurité informatique par le biais de contrats formels permet de minimiser les risques.

1.6.17 Les facteurs humains

Les erreurs humaines posent de nombreux défis aux entreprises. Les mesures techniques de protection ne peuvent jamais garantir qu'aucune erreur ne se produira, que ce soit par malveillance ou par négligence. Dans une entreprise, le risque d'erreur est directement lié au taux d'employés inexpérimentés ou peu qualifiés. Lutter contre d'éventuels actes malveillants commis par ses propres collaborateurs confronte une entreprise à un autre genre de défi. Elle doit, pour ce faire, résoudre divers problèmes :

1.6.17.1 Les cycles de la vie professionnelle

La sécurité informatique doit être un souci permanent, dans toute la période d'occupation (de l'embauche à la retraite). Cela implique de nombreuses mesures de sécurité, par exemple lors du transfert de ressources (matériel, accès aux systèmes), ou l'obligation de protéger les accès aux locaux et bâtiments. Un programme de formation pertinent doit sensibiliser les employés à la sécurité et définir leurs comportements en matière de sécurité. L'entreprise doit retenir par écrit l'avancement et le déroulement de ces formations.

L'objectif est de s'assurer que les employés ont les compétences, connaissances et outils nécessaires pour défendre les valeurs de l'entreprise tout en respectant les consignes de sécurité informatique en vigueur.

1.6.17.2 Les règles et directives

Des règles et des directives claires et réalistes définissent le comportement des employés en matière de sécurité. Elles donnent un cadre et prévoient des contrôles pour protéger les systèmes en appliquant ces règles. Elles décrivent également les modes opératoires et définissent les attentes de l'entreprise envers ses collaborateurs. Les consignes et les instructions déterminent ce qui doit être respecté ainsi que la manière de sanctionner les infractions.

1.6.17.3 Les processus

L'organisme responsable de la sécurité informatique est chargé de gérer la sécurité et les spécificités de ses processus. Sa fonction première est de protéger les informations et les données de l'entreprise. Les processus de gestion de la sécurité doivent être appliqués aux systèmes de contrôle industriels. Pour ce faire, il faut définir les processus précisant la manière d'opérer ou de configurer certains systèmes. Ces processus doivent être normalisés et reproductibles. L'entreprise formera toujours ses nouveaux collaborateurs afin de maintenir un niveau de sécurité constant, ce qui garantit qu'ils connaissent toutes les réglementations et normes requises. Le processus de détection d'un cyberaccident *(Intrusion Detection)* est extrêmement important. Les procédures de sécurité liées au réseau sont cruciales pour les protocoles propriétaires et les systèmes patrimoniaux.

1.6.17.4 Tâches et responsabilités dans les secteurs critiques de l'entreprise

Il faut clairement définir et attribuer à des personnes compétentes les tâches et les responsabilités dans les environnements critiques, les processus, les applications (y compris les systèmes et réseaux supportés) et les informations.

L'objectif est de susciter chez les employés un sentiment de responsabilité individuelle. Un tel climat dans une entreprise aide les employés à effectuer leurs tâches en respectant les prescriptions de sécurité informatique.

1.6.17.5 Communication et programme de sensibilisation à la sécurité

Un programme de sensibilisation à la sécurité et une politique de communication en découlant responsabilisent les employés et favorisent les comportements adaptés, à tous les niveaux hiérarchiques de l'entreprise.

L'objectif est d'obtenir, dans une entreprise, un climat qui favorise les comportements de sécurité individuels. Chacun devrait pouvoir prendre des décisions en fonction du risque dans sa sphère de compétences.

1.7 NIST Framework

L'objectif du cadre NIST et de ses recommandations est de mettre à la disposition des opérateurs d'infrastructures critiques et d'autres entreprises liées à des TIC un outil leur permettant d'accroître, de manière autonome et responsable, leur résilience face aux risques de sécurité. Le cadre NIST se fonde sur un choix de normes, de directives et de règles de bonnes pratiques ; il est technologiquement neutre.

1.7.1 NIST Framework Core

Le *NIST Framework Core* est basé sur le risque. Il a cinq fonctions :

1) identifier (Identify)
2) protéger (Protect)
3) reconnaître/détecter (Detect)
4) réagir (Respond)
5) restaurer/récupérer (Recover)

1.7.2 Implementation Tiers

Le *NIST Framework* comprend 4 niveaux, appelés *Implementation Tiers.* Ils décrivent le niveau de protection qu'une entreprise a mis en place. Ces niveaux vont de partiel (*Tier* 1) à dynamique (*Tier* 4). Pour déterminer son niveau de protection, une entreprise doit parfaitement connaître ses pratiques de gestion des risques, le genre de menaces plausibles, les exigences légales et réglementaires, ses objectifs commerciaux et ses besoins organisationnels.

2 Implementation

2.1 Résumé

Ce chapitre décrit les tâches à effectuer pour appliquer la norme minimale pour les TIC. Elles sont ventilées selon les cinq fonctions du *NIST Core Framework* (voir point 1.7.1), à savoir : identifier, protéger, détecter, réagir et récupérer. Les désignations anglaises sont indiquées chaque fois entre parathèses. La classification des tâches se fait grâce aux abréviations suivantes :

Les deux premières lettres (par ex. « ID » pour identifier) se rapportent à la fonction. La deuxième paire de lettres se réfère à la catégorie (par ex. « AM » pour *Asset Management*). Enfin, le chiffre accolé désigne le numéro de la tâche. Elles sont numérotées dans l'ordre pour chaque catégorie. Voici un exemple concret : « ID.AM-1 » correspond à la première tâche de la catégorie *Asset Management* de la fonction *Identify.*

Chaque tableau qui décrit des tâches du *NIST Framework Core* est suivi d'un second qui répertorie d'autres normes internationales pour les TIC. Ils sont classés par catégories, *Asset Management* par ex. Le but est de faciliter le travail des utilisateurs qui gèrent leurs tâches de sécurité TIC selon d'autres normes.

2.2 Identifier *(Identify)*

2.2.1 Inventaire et organisation *(Asset Management)*

Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation se fait en fonction de leur criticité pour les processus opérationnels à mettre en place et de la stratégie de l'entreprise en matière de risque.

Désignation	tâche
ID.AM-1	Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC *(Asset)*.
ID.AM-2	Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise.
ID.AM-3	Listez tous les flux de communication et de transferts de données en interne.
ID.AM-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.AM-5	Etablissez des priorités pour les ressources inventoriées (équipements, applications, données) selon leur criticité.
ID.AM-6	Définissez clairement les rôles et les responsabilités en matière de cybersécurité.

Tableau 3 : tâches ID.AM

Norme	référence
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193

Tableau 4 : références ID.AM

2.2.2 Environnement de l'entreprise *(Business Environment)*

Les objectifs, les tâches et les activités de l'entreprise sont hiérarchisés et évalués.
Cette information sert à répartir les responsabilités.

Désignation	tâche
ID.BE-1	Définissez, documentez et communiquez le rôle exact de votre entreprise dans la chaîne d'approvisionnement (critique).
ID.BE-2	Identifiez et communiquez l'importance de votre entreprise en tant qu'infrastructure vitale et sa position dans le secteur critique.
ID.BE-3	Evaluez et hiérarchisez les objectifs, les tâches et les activités dans l'entreprise.
ID.BE-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.BE-5	Priorisez les ressources inventoriées (équipements, applications, données) selon leur criticité.

Tableau 5 : tâches ID.BE

Norme	référence
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11
BSI 100-2	B 1.11, M 2.256, B 2.2, B 2.12, M 2.214

Tableau 6 : références ID.BE

2.2.3 Règles *(Governance)*

Une bonne gouvernance fixe les responsabilités, surveille et s'assure que les exigences réglementaires, juridiques et opérationnelles soient respectées dans la sphère d'activité.

Désignation	tâche
ID.GV-1	Édictez des directives sur les besoins en sécurité informatique dans votre entreprise.
ID.GV-2	Convenir entre les responsables internes (gestion des risques par ex.) et des partenaires externes, des rôles et des responsabilités en matière de sécurité informatique.
ID.GV-3	Vérifiez que votre entreprise respecte toutes les exigences légales et réglementaires en matière de cybersécurité, y compris au niveau de la protection des données.
ID.GV-4	Assurez-vous que les cyber-risques sont bien intégrés dans la gestion des risques pour toute l'entreprise.

Tableau 7 : tâches ID.GV

Norme	référence
COBIT 5	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, DSS04.02
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.18.1
NIST-SP-800-53 Rev. 4	PM-1, PS-7, PM-9, PM-11
BSI 100-2	M 2.192, M 2.193, M 2.336, B 1.16

Tableau 8 : références ID.GV

2.2.4 Analyse de risque *(Risk Assessment)*

L'entreprise analyse l'impact des cyber-risques sur ses activités, ses équipements et son personnel, y compris les risques réputationnels.

Désignation	tâche
ID.RA-1	Identifiez les faiblesses (techniques) de vos équipements et documentez-les.
ID.RA-2	Participez à des forums et à des réunions d'experts pour échanger des informations et être au courant des cybermenaces.
ID.RA-3	Identifiez et documentez les cybermenaces, aussi bien internes qu'externes.
ID.RA-4	Identifiez l'impact potentiel des cybermenaces sur vos activités et évaluez leur probabilité d'occurrence.
ID.RA-5	Évaluez les risques pour votre entreprise en fonction des menaces, des vulnérabilités, de l'impact (sur ses activités) et de leur probabilité d'occurrence.
ID.RA-6	Définissez les mesures à prendre immédiatement lorsqu'un risque se concrétise et fixez des priorités.

Tableau 9 : tâches ID.RA

Norme	référence
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14
BSI 100-2	M 2.35, M 2.199, M 2.546

Tableau 10 : références ID.RA

2.2.5 Stratégie pour gérer les risques *(Risk Management Strategy)*

Définissez les priorités, les restrictions et les risques maximaux supportables pour votre entreprise.
Évaluez vos risques opérationnels sur cette base.

Désignation	tâche
ID.RM-1	Définissez les processus de gestion des risques, gérez-les activement et faites-les confirmer par les personnes impliquées ou les parties prenantes.
ID.RM-2	Définissez et communiquez les risques supportables pour votre entreprise.
ID.RM-3	Assurez-vous que les risques supportables sont évalués en prenant en compte l'importance de votre entreprise du fait qu'elle exploite une infrastructure critique. Prenez également en considération, dans votre analyse, les risques propres au secteur.

Tableau 11 : tâches ID.RM

Norme	référence
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tableau 12 : références ID.RM

2.2.6 Gestion des risques liés à la chaîne d'approvisionnement *(Supply Chain Riskmanagement)*

Définissez les priorités, les restrictions et les risques maximaux que votre entreprise peut accepter par rapport à ses fournisseurs.

Désignation	tâche
ID.SC-1	Définissez des processus clairs pour gérer les risques liés à une perturbation dans la chaîne d'approvisionnement. Faites contrôler et valider ces processus par toutes les parties prenantes.
ID.SC-2	Identifiez les fournisseurs et les prestataires de services cruciaux pour vos systèmes, composants et services critiques à partir des processus définis ci-dessus et fixez les priorités.
ID.SC-3	Exigez de vos fournisseurs et prestataires de services qu'ils s'engagent contractuellement à développer et mettre en œuvre des mesures appropriées pour atteindre les objectifs du processus pour gérer les risques liés à la chaîne d'approvisionnement.
ID.SC-4	Faites un suivi systématique pour vous assurer que tous vos fournisseurs et prestataires de services remplissent leurs obligations conformément aux exigences. Faites-le vérifier régulièrement par des rapports d'audit ou par les résultats des tests techniques.
ID.SC-5	Définissez avec vos fournisseurs et prestataires les processus pour réagir et récupérer après des problèmes de cybersécurité. Validez ces processus par des simulations.

Tableau 13 : tâches ID.SC

Norme	référence
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11 7
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-12, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BSI	B 1.11, B 1.17, M 2.256, B 1.3

Tableau 14 : références ID.SC

2.3 Protéger *(Protect)*

2.3.1 Gestion des accès *(Access management)*

Veiller à ce que les accès physique et logique aux équipements et installations TIC ne soient possibles que pour les personnes, processus et appareils autorisés et à ce que seules les activités prévues soient permises.

Désignation	tâche
PR.AC-1	Définissez un processus clair pour octroyer et gérer les autorisations et les données d'identification pour utilisateurs, appareils/machines et processus.
PR.AC-2	Assurez-vous que seules les personnes autorisées ont physiquement accès aux équipements TIC. Prenez des mesures concrètes pour garantir que les ressources TIC sont protégées contre tout accès physique non autorisé.
PR.AC-3	Définissez les processus pour gérer les accès à distance.
PR.AC-4	Définissez les niveaux d'autorisation en étant le plus restrictif possible et séparez les fonctions.
PR.AC-5	Vérifiez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, si c'est nécessaire et judicieux.
PR.AC-6	N'attribuez des identités numériques qu'à des personnes ou à des processus que vous avez clairement identifiés.

Tableau 15 : tâches PR.AC

Norme	référence
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, AC-17, AC-19, AC-20, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24, IA-2, IA-4, IA-5, IA-8
BSI	M 2.30, M 2.220, M 2.11, M 4.15, M 1.79, M 2.17, B 2.2, B 2.12, B 5.8, B 4.1, M 2.393, M 2.5, B 1.18, M 2.220, M 2.8, M 4.135, B 4.1, M 5.77, M 2.393, M 2.5, M 3.33, M 2.31, M 2.586, M 4.135

Tableau 16 : références PR.AC

2.3.2 Sensibilisation et formation

Assurez-vous que vos employés et vos partenaires externes sont correctement formés et conscients de tous les aspects de la cybersécurité. Veillez à ce qu'ils exécutent les tâches impactant la sécurité conformément aux exigences et aux processus définis.

Désignation	tâche
PR.AT-1	Veillez à ce que tous vos collaborateurs soient sensibilisés et formés en matière de cybersécurité.
PR.AT-2	Veillez à ce que les utilisateurs ayant des niveaux d'autorisation élevés soient conscients de leur rôle et de leurs responsabilités.
PR.AT-3	Veillez à ce que tous les acteurs extérieurs à votre entreprise (fournisseurs, clients, partenaires) soient conscients de leur rôle et de leurs responsabilités.
PR.AT-4	Veillez à ce que tous les cadres soient conscients de leurs rôles spécifiques et de leurs responsabilités.
PR.AT-5	Veillez à ce que les responsables de la sécurité physique et de la sécurité informatique soient conscients de leurs rôles spécifiques et de leurs responsabilités.

Tableau 17 : tâches PR.AT

Norme	référence
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS06.03, APO07.03, APO10.04, APO10.05
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.6.1.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, AT-3, PM-7
BSI	M 2.193, B 1.13

Tableau 18 : références PR.AT

2.3.3 Sécurité des données *(Data Security)*

Assurez-vous que les informations, les données et leurs supports sont gérés de manière à protéger la confidentialité, l'intégrité et la disponibilité des données, conformément à la stratégie de votre entreprise pour gérer les risques.

Désignation	tâche
PR.DS-1	Assurez-vous que les données stockées sont protégées (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-2	Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-3	Veillez à ce qu'un processus formel soit défini pour votre matériel TIC afin de protéger les données lorsque des équipements sont supprimés, déplacés ou remplacés.
PR.DS-4	Veillez à ce que vos équipements TIC aient une réserve de capacité suffisante afin que vos données soient toujours disponibles.
PR.DS-5	Assurez-vous que des mesures appropriées sont mises en œuvre contre les fuites de données.
PR.DS-6	Définissez un processus pour vérifier l'intégrité du micrologiciel, des systèmes d'exploitation, des logiciels d'application et des données.
PR.DS-7	Pour le développement et les tests, ayez un environnement informatique totalement indépendant des systèmes de production.
PR.DS-8	Définissez un processus pour vérifier l'intégrité du matériel utilisé.

Tableau 19 : tâches PR.DS

Norme	référence
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
NIST-SP-800-53 Rev. 4	SC-28, SC-8, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, SI-7, CM-2, SA-10
BSI	M 2.217, B 4.1, M 2.393, B 5.3, B 5.4, B 5.21, B 5.24, B 1.7, M 2.3, B 1.15, M 5.23, M 3.33, M 2.226, M 3.2, M 3.6, B 1.18, M 2.220, M 2.8, M 4.135, M 4.494, M 5.77, M 2.393, B 5.3, M 3.55, B 5.4, B 5.21, B 5.24, B 1.7, B 1.6, B 1.9, B 5.4, B 5.21, B 5.24, M 2.62, M 2.4

Tableau 20 : références PR.DS

2.3.4 Protection des données *(Information Protection Processes and Procedures)*

Etablissez des directives pour protéger vos systèmes informatiques et vos équipements de production. Et appliquez-les strictement pour garantir cette protection.

Désignation	tâche
PR.IP-1	Générez une configuration standard pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriels. Assurez-vous que cette configuration par défaut obéit aux règles usuelles de sécurité (par ex. redondance N-1, configuration minimale, etc.).
PR.IP-2	Définissez un processus « cycle de vie » pour l'utilisation des équipements TIC.
PR.IP-3	Définissez un processus pour contrôler les changements de configuration.
PR.IP-4	Assurez-vous que des sauvegardes informatiques *(backups)* sont effectuées, gérées et testées régulièrement (+ qu'on peut restaurer les données sauvegardées).
PR.IP-5	Veillez à ce que toutes les exigences (réglementaires) et les directives concernant les équipements « physiques » soient respectées.
PR.IP-6	Veillez à ce que les données soient toujours détruites selon les prescriptions.
PR.IP-7	Développez et améliorez régulièrement vos processus de sécurité informatique.
PR.IP-8	Discutez de l'efficacité des différentes technologies de protection avec vos partenaires.
PR.IP-9	Instaurez des processus pour réagir aux cyberincidents. *(Incident Response-Planing, Business Continuity Management, Incident Recovery, Disaster Recovery).*
PR.IP-10	Testez les plans de réaction et de récupération.
PR.IP-11	Tenez compte de la cybersécurité dès le processus de recrutement (en vérifiant les antécédents ou par des contrôles de sécurité personnels, par ex.).
PR.IP-12	Développez et mettez en œuvre un processus pour traiter les failles repérées.

Tableau 21 : tâches PR.IP

Norme	référence
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, DSS01.04, DSS05.05, BAI09.03, APO11.06, DSS04.05, DSS04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISA 62443-3:2013	SR 7.6
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.12.6.1, A.18.2.2
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, A-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, CA-7, SI-4, CP-2, IR-8, IR-3, PM-14, RA-3, RA-5, SI-2
BSI	B 1.4, B 1.3, M 2.217, B 1.14, B 1.9, M 2.62, B 5.27, M 4.78, M 2.9, B 1.0, M 2.80, M 2.546, B 5.27, B 5.21, B 5.24

Tableau 22 : références PR.IP

2.3.5 Maintenance

Veillez à ce que la maintenance et la réparation des composantes des systèmes TIC et du SCI soient effectuées conformément aux directives et méthodes en vigueur.

Désignation	tâche
PR.MA-1	Veillez à ce que le fonctionnement, la maintenance et les éventuelles réparations des équipements soient enregistrés et documentés (journalisation). Assurez-vous qu'elles sont effectuées rapidement et en ne recourant qu'à des moyens testés et approuvés.
PR.MA-2	Enregistrez et documentez également les travaux de maintenance de vos systèmes distants. Assurez-vous qu'aucun accès non autorisé n'est possible.

Tableau 23 : tâches PR.MA

Norme	référence
COBIT 5	BAI09.03, DSS05.04, APO11.04, DSS05.02, APO13.01
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5
BSI	M 2.17, M 2.4, M 2.218, M 2.4, B 1.11, B 1.17, M 2.256

Tableau 24 : références PR.MA

2.3.6 Technologie de protection *(Protective Technology)*

Installez des solutions techniques pour assurer la sécurité et la résilience de vos systèmes ICT et de leurs données selon les exigences et processus.

Désignation	tâche
PR.PT-1	Définissez les exigences pour les audits et les enregistrements des fichiers journaux (*logs*). Générez et vérifiez ces fichiers régulièrement, selon les exigences et les directives.
PR.PT-2	Assurez-vous que les supports amovibles sont protégés et que leur utilisation se fait dans le strict respect des directives.
PR.PT-3	Veillez à ce que votre système soit configuré pour toujours fonctionner, même en mode dégradé.
PR.PT-4	Assurez la protection de vos réseaux de communication et de contrôle.
PR.PT-5	Définissez des scénarios pour les différents modes de fonctionnement de vos systèmes. Par ex. : fonctionnalités en cas d'attaque, fonctionnalités pendant la phase de récupération, fonctionnalités normales pendant l'exploitation.

Tableau 25 : tâches PR.PT

Norme	référence
COBIT 5	APO11.04, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.3, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-4, MP-5, MP-7, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
BSI	B 5.22, M 2.500, M 2.220, M 2.64, M 4.227, M 2.64, B 1.18, B 4.1, M 2.393, B 1.3, B 2.4, B 2.9

Tableau 26 : références PR.PT

2.4 Détecter

2.4.1 Anomalies et incidents *(Anomalies and Events)*

Veillez à ce que les anomalies et autres incidents de sécurité soient détectés à temps et que le personnel soit conscient de l'impact potentiel de ces évènements.

Désignation	tâche
DE.AE-1	Définissez des valeurs par défaut pour les opérations réseau licites et les flux de données prévus pour les utilisateurs et les systèmes. Surveillez ces valeurs en permanence.
DE.AE-2	Assurez-vous que les incidents de cybersécurité détectés sont analysés quant à leurs objectifs et méthodes.
DE.AE-3	Assurez-vous que les informations sur les incidents de cybersécurité provenant de différentes sources et capteurs sont compilées et exploitées.
DE.AE-4	Déterminez les conséquences probables des incidents.
DE.AE-5	Définissez les valeurs limites au-delà desquelles les incidents de cybersécurité doivent générer des alertes.

Tableau 27 : tâches DE.AE

Norme	référence
COBIT 5	DSS03.01, APO12.06
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
BSI	B 1.8

Tableau 28 : références DE.AE

2.4.2 Surveillance *(Security Continous Monitoring)*

Veillez à ce que le système TIC, équipements compris, soit régulièrement contrôlé pour pouvoir détecter les incidents de cybersécurité et vérifier l'efficacité des mesures de protection.

Désignation	tâche
DE.CM-1	Mettez en place une surveillance permanente du réseau pour détecter les incidents de cybersécurité potentiels.
DE.CM-2	Mettez en place une surveillance continue (monitorage) de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.
DE.CM-3	Mettez en place un monitorage de l'utilisation des TIC par les employés pour détecter les incidents de cybersécurité potentiels.
DE.CM-4	Veillez à pouvoir détecter les maliciels.
DE.CM-5	Veillez à pouvoir détecter les maliciels sur les appareils mobiles.
DE.CM-6	Assurez-vous que les activités des prestataires de services externes sont surveillées (monitorées) pour détecter d'éventuels incidents de cybersécurité.
DE.CM-7	Surveillez votre système en permanence pour être certain que des activités ou accès liés à des personnes, équipements ou logiciels non autorisés seront détectés.
DE.CM-8	Procédez à des tests de vulnérabilité.

Tableau 29 : tâches DE.CM

Norme	référence
COBIT 5	DSS05.01, DSS05.07, APO07.06, BAI03.10
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.12.4.1, A.12.2.1, A.12.5.1, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SC-18, SI-4, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, SI-4, AU-12, RA-5
BSI	B 5.22, M 2.500, B 1.6, B 2.9, B 1.9, B 5.25, B 1.11, M 2.256, M 2.35

Tableau 30 : références DE.CM

2.4.3 Processus de détection *(Detection Processes)*

Maintenez, testez et entretenez les processus et les instructions pour détecter les incidents de cybersécurité.

Désignation	tâche
DE.DP-1	Définissez clairement les rôles et les responsabilités pour que tous sachent bien qui est responsable de quoi et qui a telles ou telles compétences.
DE.DP-2	Assurez-vous que les processus de détection correspondent aux exigences et conditions fixées.
DE.DP-3	Testez vos processus de détection.
DE.DP-4	Communiquez aux personnes concernées (par ex. fournisseurs, clients, partenaires, autorités) les incidents que vous avez détectés.
DE.DP-5	Améliorez en permanence vos processus de détection.

Tableau 31 : tâches DE.DP

Norme	référence
COBIT 5	DSS05.01, APO13.02, APO12.06, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.18.1.4, A.14.2.8, A.16.1.2, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, SI-3, SI-4, AU-6, CA-2, CA-7, RA-5
BSI	M 2.193, M 2.568, B 1.8

Tableau 32 : références DE.DP

2.5 Réagir *(Respond)*

2.5.1 Plan d'intervention *(Response Planning)*

Élaborez un plan d'intervention pour traiter les incidents de cybersécurité détectés. Assurez-vous qu'en cas d'incident ce plan d'intervention est exécuté correctement et en temps utile.

Désignation	tâche
RS.RP-1	Assurez-vous que le plan d'intervention est correctement suivi et rapidement exécuté si un incident de cybersécurité est détecté.

Tableau 33 : tâches RS.RP

Norme	référence
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Tableau 34 : références RS.RP

2.5.2 Communication

Contrôlez que vos processus de réaction sont coordonnés avec ceux des parties prenantes, internes et externes. Selon le type d'incident, veillez à pouvoir bénéficier du soutien des autorités si la situation l'exige.

Désignation	tâche
RS.CO-1	Assurez-vous que toutes les personnes connaissent leurs tâches et la marche à suivre lorsqu'elles doivent réagir à un incident de cybersécurité.
RS.CO-2	Définissez des critères pour les communications et assurez-vous que les incidents de cybersécurité sont signalés et traités conformément à ces critères.
RS.CO-3	Partagez les informations sur les incidents de cybersécurité relevés – ainsi que les enseignements qui en découlent – selon ces critères prédéfinis.
RS.CO-4	Coordonnez-vous avec les parties prenantes selon ces critères.
RS.CO-5	Améliorez la sensibilisation aux incidents de cybersécurité grâce à des échanges réguliers avec vos partenaires.

Tableau 35 : tâches RS.CO

Norme	référence
COBIT 5	
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.3, A.16.1.2
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, CA-2, CA-7, IR-4, IR-8, PE-6, RA-5, SI-4, PM-15, SI-5
BSI	B 1.3, B 1.8, M 2.193

Tableau 36 : références RS.CO

2.5.3 Analyses

Effectuez régulièrement des analyses afin de réagir correctement en cas d'incidents de cybersécurité.

Désignation	tâche
RS.AN-1	Assurez-vous que les alertes émanant de systèmes de détection sont prises en compte et déclenchent des enquêtes.
RS.AN-2	Veillez à pouvoir évaluer correctement l'impact d'un incident de cybersécurité.
RS.AN-3	Effectuez une analyse technique après chaque incident.
RS.AN-4	Classez les incidents selon les exigences du plan de réaction.

Tableau 37 : tâches RS.AN

Norme	référence
COBIT 5	DSS02.07
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, CP-2, IR-4, AU-7, CP-2, IR-5, IR-8
BSI	B 5.22, M 2.500, M 2.64, B 1.8

Tableau 38 : références RS.AN

2.5.4 Circonscrire les dommages *(Mitigation)*

Faites tout pour éviter qu'un incident de cybersécurité se propage afin de limiter les éventuels dommages.

Désignation	tâche
RS.MI-1	Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que vous pouvez stopper leur propagation.
RS.MI-2	Assurez-vous de pouvoir réduire l'impact des incidents de cybersécurité.
RS.MI-3	Veillez à réduire au maximum les failles récemment découvertes ou référencez-les comme des risques acceptables.

Tableau 39 : tâches RS.MI

Norme	référence
COBIT 5	
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4, A.12.2.1, A.16.1.5
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5
BSI	B 1.6, B 1.8, M 2.35

Tableau 40 : références RS.MI

2.5.5 Améliorations *(Improvements)*

Améliorez régulièrement la réactivité de votre entreprise face aux incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	tâche
RS.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans d'intervention.
RS.IM-2	Actualisez vos stratégies de réaction.

Tableau 41 : tâches RS.IM

Norme	référence
COBIT 5	BAI01.13
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8
BSI	B 1.8

Tableau 42 : références RS.IM

2.6 Récupérer *(Recover)*

2.6.1 Plan de restauration *(Recovery Planning)*

Contrôlez que les processus de récupération sont tenus à jour pour être exécutés en tout temps, permettant ainsi une récupération rapide des systèmes.

Désignation	tâche
RC.RP-1	Assurez-vous que le plan de récupération est suivi à la lettre en cas d'incident de cybersécurité.

Tableau 43 : tâches RC.RP

Norme	référence
COBIT 5	DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tableau 44 : références RC.RP

2.6.2 Améliorations *(Improvements)*

Améliorez constamment vos processus de récupération après les incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	tâche
RC.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de récupération.
RC.IM-2	Actualisez vos stratégies de récupération.

Tableau 45 : tâches RC.IM

Norme	référence
COBIT 5	BAI05.07
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tableau 46 : références RC.IM

2.6.3 Communication

Veillez à coordonner vos actions de récupération avec vos partenaires internes et externes (fournisseurs de services Internet, CERT, autorités, intégrateurs de systèmes, etc.).

Désignation	tâche
RC.CO-1	Anticipez les réactions du public pour ne pas dégrader la réputation de votre entreprise.
RC.CO-2	Veillez à ce que votre entreprise retrouve vite une image positive après un incident de cybersécurité.
RC.CO-3	Communiquez à l'interne aux parties prenantes tout ce que vous avez entrepris en matière de récupération, sans oublier les cadres et la direction.

Tableau 47 : tâches RC.CO

Norme	référence
COBIT 5	EDM03.02
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tableau 48 : références RC.CO

3 Contrôle

3.1 Introduction

Ce chapitre décrit la façon de procéder pour vérifier régulièrement l'exhaustivité et l'efficacité des mesures prévues. Cet examen devrait déboucher sur une appréciation quant au degré de préparation de votre cybersécurité. Il devrait aussi permettre d'effectuer des comparaisons, sectorielles ou intersectorielles.

Les mesures pour améliorer la résilience informatique qui sont présentées ici (voir chapitre 2) restent purement théoriques tant que les entreprises ne jugent pas utile de les appliquer. Il est crucial que les responsables comprennent l'importance des questions de cybersécurité. Il faut sensibiliser les employés et les partenaires et prévoir des ressources suffisantes à dégager. Il est recommandé d'effectuer un audit de cette norme minimale au moins une fois par an, d'en tirer des conclusions et d'appliquer au plus vite les mesures préconisées pour améliorer la résilience.

La sécurité n'est pas un état idéal à atteindre. La sécurité est un processus qui doit être régulièrement exécuté, testé, modifié et amélioré. La cybersécurité ne peut plus être simplement ignorée. Vous devez appliquer sans tarder les mesures adéquates pour améliorer la résilience de vos ressources informatiques critiques.

Chacune des tâches présentées au chapitre 2 doit faire l'objet d'une évaluation et recevoir une note comprise entre 0 et 4, selon le barème ci-dessous. Ces notes permettent ensuite d'évaluer le niveau *Tier* d'une entreprise (cf. point 3.3).

3.1.1 Barème établi pour les tâches

0 = pas mis en œuvre
1 = partiellement mis en œuvre, pas entièrement défini ni validé
2 = partiellement mis en œuvre, entièrement défini et accepté
3 = entièrement ou très largement mis en œuvre, définitif (« statique »)
4 = mis en œuvre dynamiquement, contrôlé et amélioré en permanence

3.2 Description des niveaux *Tier* d'une entreprise

Ces niveaux vont de partiel (*Tier* 1) à dynamique (*Tier* 4). Ils indiquent le degré – par ordre croissant – de préparation (« maturité »). Les entreprises devraient déterminer le niveau qu'elles souhaitent atteindre et vérifier que le niveau choisi répond à leurs objectifs organisationnels.

Voici les descriptions détaillées des quatre niveaux *Tier*.

3.2.1 *Tier* 1 : partiel

Le niveau 1 signifie que les processus de gestion des risques ainsi que les exigences organisationnelles pour la sécurité des TIC ne sont pas formalisés (pas de règles fixées). Les risques informatiques sont généralement gérés au jour le jour, en mode réactif. Il existe un programme intégré pour gérer les risques au niveau organisationnel, mais on n'a pas instauré une véritable prise de conscience des risques informatiques ou une approche globale pour y faire face dans l'entreprise. Cette dernière ne dispose généralement pas de processus pour relayer en son sein les informations sur la cybersécurité. Il en va de même en cas d'incident de sécurité, l'entreprise n'a le plus souvent pas prévu de processus standardisés pour communiquer ou coordonner ses activités avec ses partenaires externes.

3.2.2 *Tier* 2 : conscient des risques

Les entreprises qui optent pour un classement au niveau 2 disposent généralement de processus pour gérer leurs risques informatiques. Cependant, ces programmes ne sont pas concrètement appliqués ni obligatoires. Au niveau organisationnel, les risques informatiques sont intégrés dans un système de gestion global et tous les niveaux de l'entreprise ont été sensibilisés aux risques informatiques. Toutefois on enregistre souvent dans l'entreprise un manque de volonté pour gérer et améliorer la sensibilisation aux risques informatiques, actuels et futurs. Les processus et méthodes approuvés sont définis et mis en œuvre. Les collaborateurs disposent de ressources suffisantes pour effectuer leurs tâches de cybersécurité. Les informations sur la cybersécurité sont partagées de manière informelle au sein de l'entreprise. Cette dernière est consciente de son rôle et n'hésite pas à communiquer avec ses partenaires externes (clients, fournisseurs, prestataires de services, etc.) sur les questions de cybersécurité. Il n'existe cependant aucun processus standardisé pour collaborer ou échanger des informations avec ces partenaires.

3.2.3 *Tier* 3 : reproductible

Les entreprises de niveau 3 ont formellement validé leurs plans pour gérer les risques et leurs instructions pour les faire appliquer en leur sein. La gestion des risques informatiques est définie dans les directives de l'entreprise. Les risques informatiques sont répertoriés de manière standardisée et les directives pour y remédier font l'objet de mises à jour régulières. Cette pratique tient compte des nouveaux besoins de l'entreprise, des progrès technologiques et d'un environnement où les menaces sont mouvantes, que ce soit à cause de nouveaux acteurs ou d'une nouvelle législation.

La documentation interne décrit les processus et procédures pour gérer les nouveaux risques. Des méthodes standardisées sont définies pour répondre à l'évolution des menaces. Les collaborateurs ont les connaissances et les compétences nécessaires pour accomplir leurs tâches.

L'entreprise sait qu'elle est tributaire de ses partenaires externes. Elle partage les informations qui lui permettent, face à des incidents, de prendre elle-même des décisions.

3.2.4 *Tier* 4 : dynamique

Le niveau 4 signifie qu'une entreprise répond entièrement aux exigences des niveaux 1 à 3, et qu'en plus, elle analyse en permanence ses propres processus, méthodes et capacités pour les adapter, le cas échéant. Il est indispensable de bien documenter tous les incidents de cybersécurité pour pouvoir continuellement s'améliorer. L'entreprise tire les leçons nécessaires de l'analyse des incidents passés et adapte, de manière dynamique, ses processus et techniques de sécurité aux technologies de pointe et à l'évolution des menaces. La gestion des risques informatiques fait intégralement partie de la culture d'entreprise. Les enseignements tirés des incidents passés, les informations provenant de sources externes et la surveillance constante des systèmes et réseaux internes sont constamment intégrés dans le processus de gestion des risques. L'entreprise partage en permanence ses informations avec ses partenaires en recourant à des processus standardisés.

3.3 Exemple d'évaluation

La figure ci-dessous montre un exemple fictif d'évaluation qui prend en compte toutes les tâches décrites plus haut. Ce type d'évaluation peut être effectué grâce au fichier Excel, à télécharger du site de l'Office fédéral pour l'approvisionnement économique du pays.[9]

Les graphiques ci-dessous renseignent l'utilisateur sur le niveau de cybersécurité atteint par son entreprise dans chacune des cinq catégories. Pour chaque catégorie, les tâches ont été notées entre 0 et 4 (ligne colorée). La ligne grise en traitillé indique la valeur moyenne pour chaque catégorie. Le graphique en haut à gauche (degré de préparation en matière de cybersécurité) indique le score global, calculé à partir des moyennes dans chaque catégorie.

Ces diagrammes ne sont que des exemples et non des recommandations ou des valeurs minimales à respecter. Chaque entreprise doit elle-même définir sa propension au risque et fixer, pour chaque catégorie, le niveau de protection qu'elle juge approprié.

[9] *https://www.bwl.admin.ch*

Exemple de présentation d'une évaluation

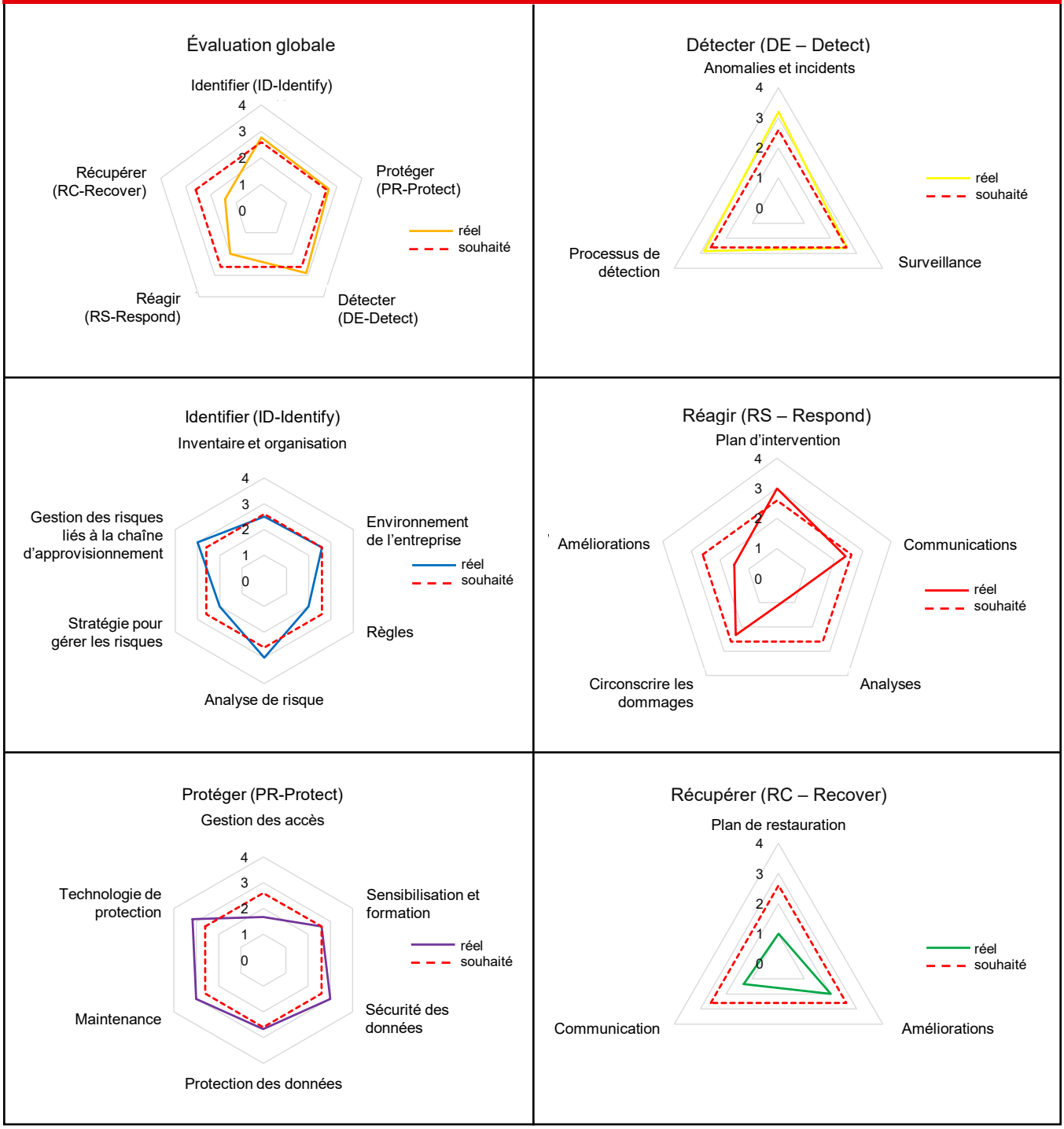

Illustration 1 : exemple de présentation d'une évaluation

4 Annexes

4.1 Table des illustrations

4.2 Liste des tableaux

4.3 Glossaire

La liste suivante comporte des termes (souvent en anglais) qui ont un sens spécifique dans le présent document. Nous avons omis les termes couramment utilisés en informatique.

Terme	signification
Benchmarking	Un *benchmark* est un indice de référence. Le *Benchmarking* est une analyse comparative des processus ou des résultats. Ce document fait volontairement référence à une comparaison avec des entreprises qui recherchent un niveau de protection similaire.
Cyberattaques	Les cyberattaques englobent tous les actes délibérément conçus pour entraver la disponibilité, l'intégrité ou la confidentialité de certaines données.
Drive-By (Infection)	Une infection *Drive-by* se produit lorsqu'un ordinateur est infecté par des logiciels malveillants (virus, chevaux de Troie, etc.) lorsque l'utilisateur ne fait que consulter un site internet. Il suffit d'afficher une page Web piégée pour infecter l'ordinateur.
Hardware Lifecycle Management	Le *Hardware Lifecycle Management* est une méthode exhaustive pour gérer le matériel informatique tout au long de son cycle de vie.
Host security	La sécurité de l'hôte englobe tous les systèmes de sécurité installés sur l'équipement (pare-feu ou programmes antivirus par ex.).
ICS Network Perimeter Security	La sécurité du périmètre concerne la transition entre un réseau d'entreprise et un réseau public comme Internet. La sécurité du périmètre est assurée par des pare-feu de périmètre qui assurent une première protection stratégique contre les attaques.
Infrastructure TIC	L'infrastructure TIC regroupe tous les équipements d'information et de télécommunications dont une entreprise a besoin pour ses activités (ordinateurs, téléphones mobiles, centres de calculs par ex.)
systèmes de contrôle industriels	Systèmes de contrôle industriels est une expression générique pour tous les éléments servant à contrôler et surveiller des installations et des processus industriels. Un système de contrôle industriel comprend généralement des capteurs, des centres de calculs, des centres de contrôle, des câbles et des installations. Les termes *ICS (Industrial Control System)* et *SCADA (Supervisory Control and Data Aqcuisition System)* sont ici synonymes.
Information Security Management System (ISMS)	Un système de gestion de la sécurité de l'information (SGSI) est un système de gestion dans toute l'entreprise qui assure, de manière durable et efficace, le respect des exigences en matière de sécurité et de continuité de l'information.
Intrusion Detection System	Un système de détection d'intrusion est un système qui permet de repérer les attaques dirigées contre un système informatique ou un réseau. L'IDS peut s'installer en complément d'un pare-feu ou directement sur le système informatique à surveiller.

Terme	signification
Compromission (piratage)	Un système, une base de données ou même un seul enregistrement sont considérés comme compromis si des données ont été altérées et si le propriétaire (ou l'administrateur) du système n'en contrôle plus précisément le fonctionnement ou le contenu.
Infrastructure critique	L'éventail des infrastructures critiques englobe neuf secteurs, subdivisés en 27 branches. Une vue d'ensemble est disponible sous : https://www.babs.admin.ch/fr/aufgabenbabs/ski/kritisch.html
système patrimonial	Ce terme désigne des systèmes anciens ou obsolètes qui, pour une raison ou une autre, ne peuvent pas être remplacés. Ils peuvent présenter un risque particulier et nécessiter des mesures de protection spécifiques.
Man-In-The-Middle (Attack)	Une attaque de l'intercepteur est propre au monde des réseaux informatiques. L'attaquant agit physiquement ou – le plus souvent – logiquement entre deux équipements qui communiquent. Son système lui permet d'avoir un contrôle total sur les transmissions entre deux ou plusieurs membres du réseau, il peut visualiser toutes les informations qu'il souhaite, voire les manipuler.
Mobile Device Configuration	La configuration des appareils mobiles englobe toutes les mesures techniques et les paramètres pour mieux protéger les données sur les appareils mobiles (smartphones, ordinateurs portables, etc.) même en cas de perte ou de vol de l'appareil.
Phishing-Mail	Le terme *phishing* (hameçonnage) désigne les tentatives pour obtenir des informations personnelles d'un utilisateur au travers de faux sites Internet, courriels ou messages privés en vue d'usurper son identité.
Security Awarness Programm	Un programme de sensibilisation à la sécurité vise à responsabiliser les collaborateurs, les partenaires, les fournisseurs, etc. face aux problèmes de sécurité et à les rendre attentifs à leurs comportements.
Security Monitoring	Le système de contrôle de la sécurité décrit les processus qui contrôlent en permanence les flux de données et les activités sur le réseau interne d'une entreprise. L'objectif est de détecter sans délai tous les comportements inhabituels. On utilise pour ce faire des systèmes de *Security-Monitoring* dédiés.

Organisation du projet

Donneur d'ordre pour le projet
Werner Meier, Office fédéral pour l'approvisionnement économique du pays
délégué AEP

Chef de projet
Daniel Caduff, Office fédéral pour l'approvisionnement économique du pays
suppléant du chef du domaine TIC

Gestion stratégique
Marcel von Vivis, chef du domaine TIC de l'AEP

Auteurs

Gestion opérationnelle
- Reto Häni, l'approvisionnement économique du pays chef de la section prestataires d'infrastructures, PwC

Comité d'experts
- Urs Küderli, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, PwC
- Christian Weigele, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, SAP
- Candid Wüest, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, Symantec
- Marc Holitscher, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, Microsoft
- Markus Pfyffer, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, IBM
- Hansruedi Münger, l'approvisionnement économique du pays expert de la section prestataires d'infrastructures, ATOS

Adresse de contact

Département fédéral de l'économie
de la formation et de la recherche DEFR
Office fédéral pour l'approvisionnement économique du pays

Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Téléphone +41 58 462 21 71

Licence