CyFun®

ESSENTIEL

# CyberFondamentaux 2023

Version 2023-03-01

# TABLE DES MATIÈRES

# INTRODUCTION

Le **cadre des cyberfondamentaux du CCB** est un ensemble de mesures concrètes pour :

- protéger les données,
- réduire considérablement le risque des cyberattaques les plus courantes,
- accroître la cyber-résilience d'une organisation.

Les exigences et les lignes directrices sont complétées par les idées pertinentes incluses dans le cadre NIST/CSF, l'ISO 27001/ISO 27002, la CEI 62443 et les contrôles de sécurité critiques CIS (ETSI TR 103 305-1).

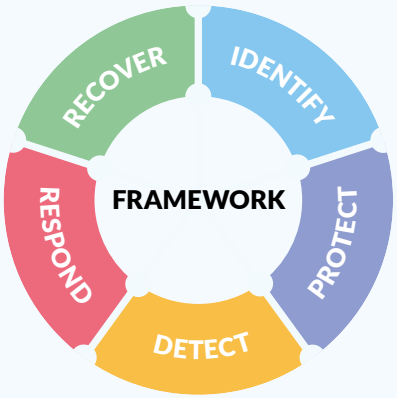
Le codage des exigences correspond aux codes utilisés dans le cadre NIST CSF. Comme toutes les exigences du NIST CSF ne sont pas applicables, certains codes qui existent dans le cadre NIST CSF peuvent manquer.

Le cadre et l'approche proportionnelle des niveaux d'assurance sont validés par des praticiens sur le terrain et à l'aide d'informations anonymes sur les cyberattaques du monde réel fournies par la Cyber Emergency Response Team fédérale (CERT.be - le service opérationnel du Centre pour la cybersécurité en Belgique).

Le **cadre des cyberfondamentaux du CCB** s'articule autour de cinq fonctions essentielles : identifier, protéger, détecter, répondre et rétablir. Ces fonctions permettent, quels que soient l'organisation et le secteur d'activité, de promouvoir la communication autour de la cybersécurité entre les praticiens techniques et les parties prenantes afin que les risques liés à la cybernétique puissent être intégrés dans la stratégie globale de gestion des risques de l'organisation.

### Identifier (Identify)

Connaître les principales cybermenaces qui pèsent sur vos actifs les plus précieux. Essentiellement, vous ne pouvez pas protéger ce dont vous ignorez l'existence. Cette fonction aide à développer une compréhension organisationnelle de la manière de gérer les risques de cybersécurité liés aux systèmes, aux personnes, aux actifs, aux données et aux capacités.




### Protéger (Protect)

La fonction de protection se concentre sur l'élaboration et la mise en œuvre des mesures de protection nécessaires pour atténuer ou contenir un cyberrisque.

### Détecter (Detect)

L'objectif de la fonction Détecter est d'assurer la détection en temps utile des événements de cybersécurité.

### Répondre (Respond)

La fonction de réponse concerne les contrôles qui permettent de répondre aux incidents de cybersécurité. La fonction de réponse soutient la capacité à contenir l'impact d'un incident de cybersécurité potentiel.

### Rétablir (Recover)

La fonction de rétablissement se concentre sur les mesures de protection qui contribuent à maintenir la résilience et à restaurer les services qui ont été affectés par un incident de cybersécurité.

---

Pour répondre à la gravité de la menace à laquelle une organisation est exposée, en plus du niveau de départ ***Small***, 3 niveaux d'assurance sont proposés : ***Basique, Important et Essentiel***.

Le **niveau de départ Small** permet à une organisation de faire une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées.

Le **niveau d'assurance Basic** contient les mesures de sécurité de l'information standard pour toutes les entreprises. Celles-ci fournissent une valeur de sécurité efficace avec des technologies et des processus qui sont généralement déjà disponibles. Lorsque cela est justifié, les mesures sont adaptées et affinées.

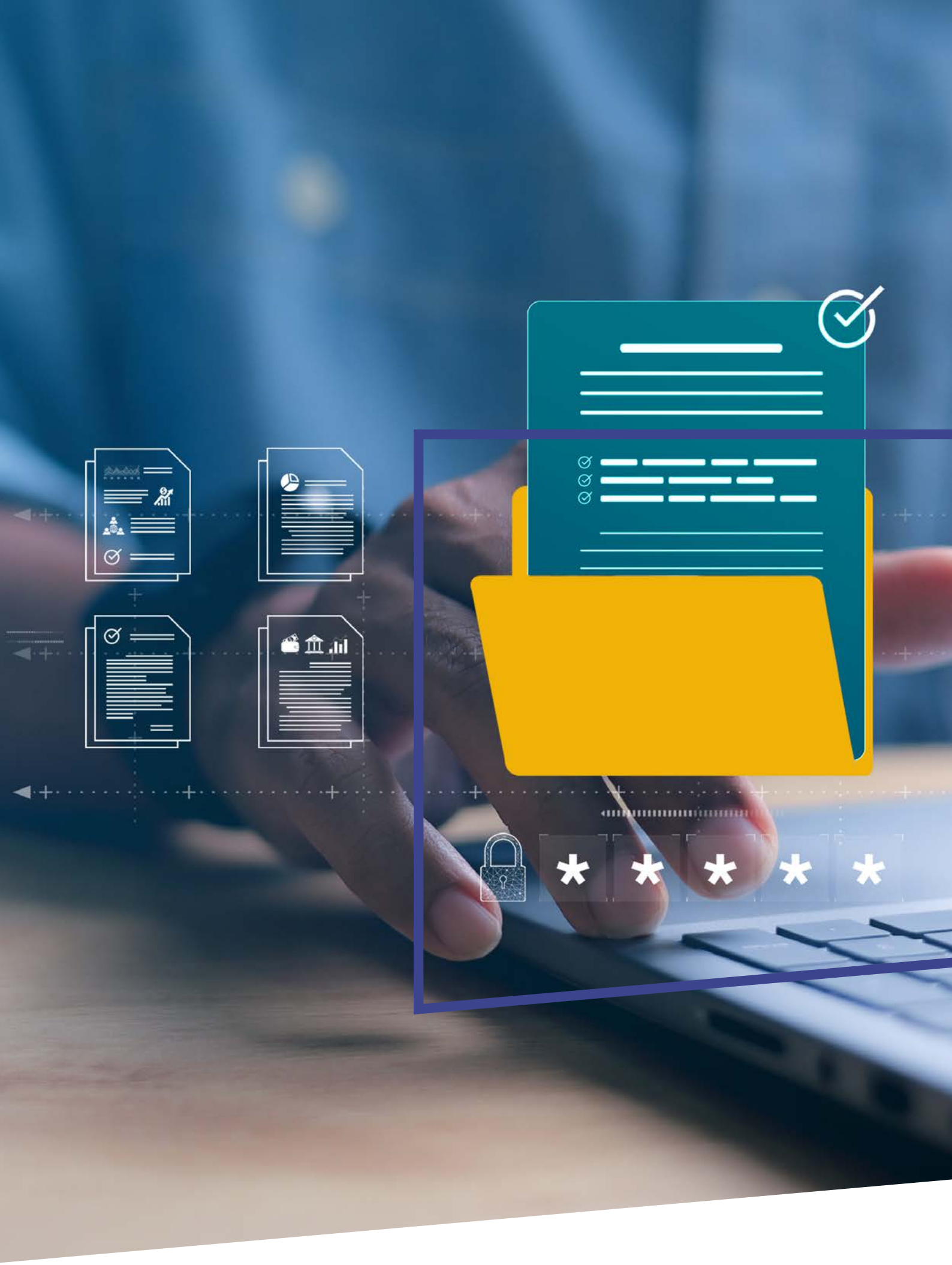
Sur la base du niveau de base, les mesures de sécurité sont complétées pour protéger les organisations contre les cyberrisques accrus afin d'atteindre un niveau d'assurance plus élevé.

Le **niveau d'assurance Important** est conçu pour minimiser les risques de cyber-attaques ciblées par des acteurs disposant de compétences et de ressources communes, en plus des risques de cybersécurité connus.

Le **niveau d'assurance Essentiel** va plus loin pour répondre également au risque de cyber-attaques avancées par des acteurs disposant de compétences et de ressources étendues.

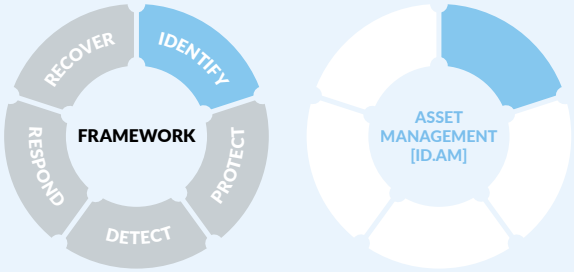
Plusieurs contrôles requièrent une attention particulière ; ces mesures sont étiquetées comme **mesure clé** .

Le cadre est un document vivant et continuera d'être mis à jour et amélioré en tenant compte des commentaires reçus des parties prenantes, de l'évolution du risque de menaces spécifiques de cybersécurité, de la disponibilité des solutions techniques et de la perspicacité progressive.



# IDENTIFIER

# Identify




Les données, le personnel, les dispositifs, les systèmes et les installations qui permettent à l'organisation d'atteindre ses objectifs opérationnels sont identifiés et gérés en fonction de leur importance relative par rapport aux objectifs de l'organisation et à sa stratégie en matière de risques.

## ID.AM-1 Les dispositifs et systèmes physiques utilisés dans l'organisation sont inventoriés.

Un inventaire des actifs associés aux informations et aux installations de traitement de l'information au sein de l'organisation doit être documenté, examiné et mis à jour lorsque des changements surviennent.

### Orientation

- Cet inventaire comprend des ordinateurs fixes et portables, des tablettes, des téléphones mobiles, des contrôleurs logiques programmables (PLC), des capteurs, des actionneurs, des robots, des machines-outils, des micrologiciels, des switchs, des routeurs, des alimentations et d'autres composants ou dispositifs en réseau.
- Cet inventaire doit inclure tous les actifs, qu'ils soient ou non connectés au réseau de l'organisation.
- L'utilisation d'un outil de gestion des actifs informatiques pourrait être envisagée.

L'inventaire des actifs associés aux informations et aux installations de traitement de l'information doit refléter les changements intervenus dans le contexte de l'organisation et inclure toutes les informations nécessaires à une responsabilisation efficace.

### Orientation

- Les spécifications de l'inventaire comprennent par exemple le fabricant, le type de dispositif, le modèle, le numéro de série, les noms de machine et les adresses de réseau, l'emplacement physique...
- La responsabilisation est l'obligation de rendre compte, d'expliquer, de justifier et d'assumer la responsabilité de ses actions, elle implique la responsabilité du résultat de la tâche ou du processus.
- Les changements incluent le déclassement de matériel.

**Lorsque du matériel non autorisé est détecté, il est mis en quarantaine pour un éventuel traitement d'exception, retiré ou remplacé, et l'inventaire est mis à jour en conséquence.**

### Orientation

- Tout matériel non pris en charge, sans documentation d'exception, est désigné comme non autorisé.
- Le matériel non autorisé peut être détecté lors de l'inventaire, des demandes d'assistance de l'utilisateur ou par d'autres moyens.

**Les mécanismes permettant de détecter la présence de composants matériels et micrologiciels non autorisés dans le réseau de l'organisation doivent être identifiés.**

### Orientation

- Lorsque cela est possible et sûr, il convient d'automatiser ces mécanismes.
- Il convient d'avoir un process pour traiter les actifs non autorisés sur une base fréquente ; L'organisation peut choisir de retirer l'actif du réseau, de l'empêcher de se connecter à distance au réseau ou de le mettre en quarantaine.

## ID.AM-2 Les plateformes et applications logicielles utilisées au sein de l'organisation sont inventoriées.

**Un inventaire reflétant les plateformes et les applications logicielles utilisées dans l'organisation doit être documenté, révisé et mis à jour lorsque des changements surviennent.**

### Orientation

- Cet inventaire comprend les programmes logiciels, les plateformes logicielles et les bases de données, même s'ils sont externalisés (SaaS).
- Il convient que les accords d'externalisation fassent partie des accords contractuels avec le fournisseur.
- Il convient que les informations de l'inventaire comprennent par exemple : le nom, la description, la version, le nombre d'utilisateurs, les données traitées, etc.
- Il convient de faire la distinction entre les logiciels non pris en charge et les logiciels non autorisés.
- L'utilisation d'un outil de gestion des actifs informatiques pourrait être envisagée.

**L'inventaire des plates-formes logicielles et des applications associées à l'information et au traitement de l'information doit refléter l'évolution du contexte de l'organisation et inclure toutes les informations nécessaires à une responsabilisation efficace.**

### Orientation

Il convient que l'inventaire des plateformes logicielles et des applications comprenne le titre, l'éditeur, la date d'installation/utilisation initiale et l'objectif de l'organisation pour chaque entrée ; le cas échéant, il convient d'inclure l'adresse web (URL), le ou les magasins d'applications, la ou les versions, le mécanisme de déploiement et la date de mise hors service.

**Les personnes qui sont responsables de l'administration des plates-formes et des applications logicielles au sein de l'organisation et qui doivent en rendre compte doivent être identifiées.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**Lorsqu'un logiciel non autorisé est détecté, il est mis en quarantaine en vue d'un éventuel traitement d'exception, supprimé ou remplacé, et l'inventaire est mis à jour en conséquence.**

### Orientation

- Tout logiciel non pris en charge sans documentation d'exception, est désigné comme non autorisé.
- Les logiciels non autorisés peuvent être détectés lors de l'inventaire, des demandes d'assistance de l'utilisateur ou par d'autres moyens.

**Les mécanismes permettant de détecter la présence de logiciels non autorisés dans l'environnement TIC/OT de l'organisation doivent être identifiés.**

### Orientation

- Lorsque cela est possible et sûr, il convient d'automatiser ces mécanismes.
- Il convient d'avoir un process pour traiter les actifs non autorisés sur une base fréquente ; L'organisation peut choisir de retirer l'actif du réseau, de l'empêcher de se connecter à distance au réseau ou de le mettre en quarantaine.

## ID.AM-3 La communication organisationnelle et les flux de données sont schématisés.

**Les informations que l'organisation stocke et utilise doivent être identifiées.**

### Orientation

- Commencez par énumérer tous les types d'informations que votre organisation stocke ou utilise. Définissez le "type d'information" de toute manière utile et logique pour votre organisation. Vous pouvez demander à vos employés de dresser une liste de toutes les informations qu'ils utilisent dans le cadre de leurs activités habituelles. Dressez une liste de tout ce à quoi vous pouvez penser, mais il n'est pas nécessaire d'être trop précis. Par exemple, vous pouvez conserver les noms et adresses électroniques de vos clients, les reçus de matières premières, vos informations bancaires ou d'autres informations exclusives.
- Envisagez de mettre en correspondance ces informations avec les actifs associés identifiés dans les inventaires des dispositifs physiques, des systèmes, des plateformes logicielles et des applications utilisés au sein de l'organisation (voir ID.AM-1 & ID.AM-2).

**Toutes les connexions au sein de l'environnement TIC/OT de l'organisation, ainsi qu'à d'autres plateformes internes à l'organisation, doivent être schématisées, documentées, approuvées et mises à jour le cas échéant.**

### Orientation

- Les informations relatives à la connexion comprennent, par exemple, les caractéristiques de l'interface, les caractéristiques des données, les ports, les protocoles, les adresses, la description des données, les exigences de sécurité et la nature de la connexion.
- La gestion de la configuration peut être utilisée comme soutien.
- Il convient que cette documentation ne soit pas stockée uniquement sur le réseau qu'elle représente.
- Envisagez de conserver une copie de cette documentation dans un environnement hors ligne sûr (par exemple, disque dur hors ligne, copie papier,...).

**Les flux d'informations/de données dans l'environnement TIC/OT de l'organisation, ainsi que vers d'autres systèmes internes à l'organisation, doivent être schématisés, documentés, autorisés et mis à jour lorsque des changements surviennent.**

### Orientation

- En connaissant les flux d'informations et de données au sein d'un système et entre les systèmes, il est possible de déterminer où les informations peuvent et ne peuvent pas aller.
- Envisagez de :
  - Appliquer des contrôles restreignant les connexions aux seules interfaces autorisées.
  - Renforcer l'activité de surveillance du système chaque fois qu'il y a une indication d'un risque accru pour les opérations et les actifs critiques de l'organisation.
  - Protéger le système contre les fuites d'informations dues aux émanations de signaux électromagnétiques.

## ID.AM-4 Les systèmes d'information externes sont catalogués.

**L'organisation doit schématiser, documenter, autoriser et, lorsque des changements surviennent, mettre à jour, tous les services externes et les connexions établies avec eux.**

### Orientation

- L'externalisation des systèmes, des plates-formes logicielles et des applications utilisées au sein de l'organisation est traitée dans ID.AM-1 & ID.AM-2
- Les systèmes d'information externes sont des systèmes ou des composants de systèmes pour lesquels les organisations n'ont généralement pas de supervision et d'autorité directes sur l'application des exigences et des contrôles de sécurité, ou la détermination de l'efficacité des contrôles mis en œuvre sur ces systèmes, c'est-à-dire les services qui sont exécutés dans le nuage, le SaaS, l'hébergement ou d'autres environnements externes, les API (Application Programming Interface)...
- Schématiser les services externes et les connexions qui leur sont destinées et les autoriser à l'avance évite de gaspiller des ressources inutiles en enquêtant sur une connexion supposée non authentifiée à des systèmes externes.

**Le flux d'informations vers/depuis les systèmes externes doit être schématisé, documenté, autorisé et mis à jour lorsque des changements surviennent.**

### Orientation

Envisagez d'exiger des fournisseurs de services externes qu'ils identifient et documentent les fonctions, ports, protocoles et services nécessaires aux services de connexion.

## ID.AM-5 Les ressources sont organisées par ordre de priorité en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.

**Les ressources de l'organisation (matériel, dispositifs, données, temps, personnel, informations et logiciels) doivent être organisées par ordre de priorité en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.**

### Orientation

- Déterminer les ressources de l'organisation (par exemple, le matériel, les dispositifs, les données, le temps, le personnel, les informations et les logiciels) :
  - Qu'arriverait-il à mon organisation si ces ressources étaient rendues publiques, endommagées, perdues... ?
  - Qu'arriverait-il à mon organisation lorsque l'intégrité des ressources ne serait plus garantie ?
  - Que se passerait-il pour mon organisation si mes clients ou moi-même ne pouvions pas accéder à ces ressources ? Et organisez ces ressources en fonction de leur classification, de leur criticité et de leur valeur opérationnelle.
- Il convient que les ressources incluent les actifs de l'organisation.

- Créez une classification pour les informations sensibles en déterminant d'abord les catégories, par ex.
  - Public - librement accessible à tous, même à l'extérieur.
  - Interne - accessible uniquement aux membres de votre organisation
  - Confidentiel - accessible uniquement aux personnes dont les fonctions l'exigent.
- Communiquer ces catégories et identifier les types de données qui en font partie (données RH, données financières, données juridiques, données personnelles, etc.)
- Envisager l'utilisation du protocole de feux de circulation (TLP).
- Il convient que la classification des données s'applique aux trois aspects : C-I-A
- Envisagez de mettre en place un outil automatisé, tel qu'un outil de prévention des pertes de données (DLP) basé sur l'hôte, pour identifier toutes les données sensibles stockées, traitées ou transmises par le biais des actifs de l'organisation, y compris ceux situés sur place ou chez un fournisseur de services distant.

## ID.AM-6 Les rôles, responsabilités et pouvoirs en matière de cybersécurité pour l'ensemble du personnel et les parties prenantes tierces (par exemple, les fournisseurs, les clients, les partenaires) sont établis.

**Les rôles, les responsabilités et les pouvoirs en matière de sécurité de l'information et de cybersécurité au sein de l'organisation sont documentés, examinés, autorisés et mis à jour et alignés sur les rôles internes de l'organisation et les partenaires externes.**

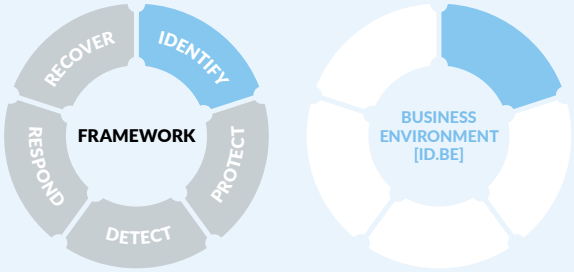
### Orientation

Il convient d'envisager :
- Décrire les rôles, les responsabilités et les autorités en matière de sécurité : qui, dans votre organisation, il convient de consulter, informer et tenir responsable de tout ou partie de vos actifs.
- Fournir les rôles, les responsabilités et l'autorité en matière de sécurité pour toutes les fonctions clés de la sécurité de l'information/cyber (juridique, activités de détection...).
- Inclure les rôles et responsabilités en matière de sécurité de l'information/cybersécurité pour les fournisseurs tiers ayant un accès physique ou logique à l'environnement TIC/OT de l'organisation.

**L'organisation doit nommer un responsable de la sécurité des informations.**

### Orientation

Il convient que le responsable de la sécurité de l'information soit chargé de surveiller la mise en œuvre de la stratégie de sécurité de l'information/cyber et des mesures de protection de l'organisation.




La mission, les objectifs, les parties prenantes et les activités de l'organisation sont compris et classés par ordre de priorité ; ces informations sont utilisées pour définir les rôles, les responsabilités et les décisions en matière de gestion des risques liés à la cybersécurité.

## ID.BE-1 Le rôle de l'organisation dans la chaîne d'approvisionnement est identifié et communiqué.

Le rôle de l'organisation dans la chaîne d'approvisionnement doit être identifié, documenté et communiqué.

### Orientation

- Il convient que l'organisation soit en mesure d'identifier clairement qui se trouve en amont et en aval de l'organisation et quels fournisseurs lui apportent des services, des capacités, des produits et des articles.
- Il convient que l'organisation communique sa position à ses partenaires en amont et en aval afin de comprendre où ils se situent en termes d'importance critique pour les opérations de l'organisation.

L'organisation doit protéger son environnement TIC/OT des menaces pesant sur la chaîne d'approvisionnement en appliquant des mesures de sécurité dans le cadre d'une stratégie de sécurité globale documentée.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## ID.BE-2 La place de l'organisation dans les infrastructures critiques et son secteur d'activité est identifiée et communiquée.

La place de l'organisation dans les infrastructures critiques et dans son secteur d'activité doit être identifiée et communiquée.

### Orientation

L'organisation couverte par la législation NIS a la responsabilité de connaître les autres organisations du même secteur afin de travailler avec elles pour atteindre les objectifs fixés par NIS pour ce secteur particulier.

## ID.BE-3 Les priorités de la mission, des objectifs et des activités de l'organisation sont établies et communiquées.

Les priorités pour les opérations, les objectifs et les activités de l'organisation doivent être établies et communiquées.

### Orientation

- Il convient que la mission, les objectifs et les activités de l'organisation soient déterminés et classés par ordre de priorité.
- Il convient que les besoins en matière de protection de l'information soient déterminés, et les processus connexes révisés si nécessaire, jusqu'à l'obtention d'un ensemble réalisable.

## ID.BE-4 Les dépendances et les fonctions critiques pour la prestation des services critiques sont établies.

Les dépendances et les fonctions essentielles à la fourniture de services critiques doivent être identifiées, documentées et classées par ordre de priorité en fonction de leur criticité dans le cadre du processus d'évaluation des risques.

### Orientation

Il convient que les dépendances et les fonctions essentielles à l'organisation incluent les services de soutien.

## ID.BE-5 Les exigences en matière de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états de fonctionnement (par exemple, en cas de contrainte/attaque, pendant le rétablissement, les opérations normales).

**Pour soutenir la cyber-résilience et sécuriser la prestation de services essentiels, les exigences nécessaires sont identifiées, documentées et leur mise en œuvre testée et approuvée.**

### Orientation

- Envisagez de mettre en œuvre des mécanismes de résilience pour prendre en charge les situations opérationnelles normales et défavorables (par exemple, failsafe, équilibrage de charge, hot swap).
- Examiner les aspects de la gestion de la continuité des activités, par exemple l'analyse de l'impact sur les activités (BIA), le plan de reprise d'activités (PRA) et le plan de continuité des activités (PCA).

**Les installations de traitement de l'information et de soutien doivent mettre en œuvre la redondance pour répondre aux exigences de disponibilité, telles que définies par l'organisation et/ou les cadres réglementaires.**

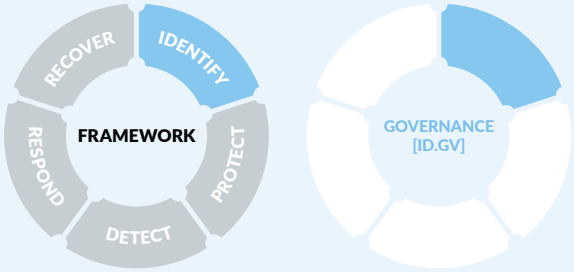
### Orientation

- Envisagez de prévoir une redondance adéquate des données et du réseau (par exemple, des dispositifs de réseau redondants, des serveurs avec répartition de la charge, des matrices Raid, des services de sauvegarde, deux centres de données distincts, des connexions réseau à basculement, deux fournisseurs d'accès Internet...).
- Envisagez de protéger les équipements/services critiques contre les pannes de courant et autres défaillances dues aux interruptions de service (par exemple, onduleurs et systèmes sans coupure, tests fréquents, contrats de service incluant une maintenance régulière, câblage électrique redondant, 2 fournisseurs de services d'alimentation différents...).

**Des objectifs de temps et de points de rétablissement pour le rétablissement des processus essentiels des systèmes TIC/OT sont définis.**

### Orientation

- Envisagez d'appliquer la règle de sauvegarde 3-2-1 pour améliorer le RPO et le RTO (conservez au moins 3 copies de vos données, dont 2 à des endroits différents et il convient de stocker une copie hors site).
- Envisagez de mettre en œuvre des mécanismes tels que le hot swap, l'équilibrage des charges et le failsafe pour accroître la résilience.




Les politiques, procédures et processus de gestion et de suivi des exigences réglementaires, juridiques, environnementales et opérationnelles de l'organisation sont compris et contribuent à la gestion du risque de cybersécurité.

## ID.GV-1 La politique de cybersécurité de l'organisation est établie et communiquée.

**Les politiques et procédures en matière de sécurité de l'information et de cybersécurité doivent être créées, documentées, examinées, approuvées et mises à jour lorsque des changements interviennent.**

### Orientation

- Les politiques et les procédures qui servent à identifier les pratiques et les attentes acceptables pour les opérations, peuvent être utilisées pour former les nouveaux employés sur vos attentes en matière de sécurité de l'information et peuvent faciliter une enquête en cas d'incident. Il convient que ces politiques et procédures soient facilement accessibles aux employés.
- Il convient que les politiques et procédures en matière de sécurité de l'information et de cybersécurité décrivent clairement vos attentes en matière de protection des informations et des systèmes de l'organisation, ainsi que la manière dont la direction s'attend à ce que les ressources de l'organisation soient utilisées et protégées par tous les employés.
- Il convient que les politiques et procédures soient revues et mises à jour au moins une fois par an et à chaque fois que des changements interviennent dans l'organisation ou la technologie. Chaque fois que les politiques sont modifiées, il convient d'informer les employés des changements.

**Une politique de sécurité des informations et de cybersécurité à l'échelle de l'organisation doit être établie, documentée, mise à jour en cas de changement, diffusée et approuvée par la direction générale.**

### Orientation

Il convient que la politique inclue, par exemple, les éléments suivants :

- L'identification et l'attribution des rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et la conformité. Des conseils sur les profils de rôle ainsi que leurs titres, missions, tâches, aptitudes, connaissances et compétences sont disponibles dans le "European Cybersecurity Skills Framework Role Profiles" de ENISA. (https ://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)

- La coordination entre les entités organisationnelles responsables des différents aspects de la sécurité (c'est-à-dire technique, physique, personnel, cyber-physique, information, contrôle d'accès, protection des médias, gestion des vulnérabilités, maintenance, surveillance).
- La couverture du cycle de vie complet des systèmes TIC/OT.

## ID.GV-3 Les exigences légales et réglementaires concernant la cybersécurité, y compris les obligations en matière de vie privée et de libertés civiles, sont comprises et gérées.

**Les exigences légales et réglementaires en matière de sécurité de l'information/cybersécurité, y compris les obligations en matière de respect de la vie privée, doivent être comprises, mises en œuvre et gérées.**

### Orientation

- Il convient de procéder à des examens réguliers afin de garantir le respect permanent des exigences légales et réglementaires en matière de sécurité de l'information/cybersécurité, y compris les obligations en matière de protection de la vie privée.
- Cette exigence s'applique également aux entrepreneurs et aux prestataires de services.

## ID.GV-4 Les processus de gouvernance et de gestion des risques traitent les risques de cybersécurité.

**Dans le cadre de la gestion globale des risques de l'organisation, une stratégie complète de gestion des risques liés à la sécurité de l'information et à la cybersécurité doit être élaborée et mise à jour lorsque des changements surviennent.**

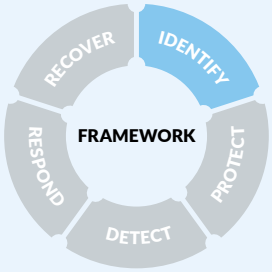
### Orientation

Il convient d'inclure dans cette stratégie la détermination et l'affectation des ressources nécessaires à la protection des actifs critiques de l'organisation.

**Les risques liés à la sécurité de l'information et à la cybersécurité doivent être documentés, approuvés formellement et mis à jour lorsque des changements surviennent.**

### Orientation

Envisagez d'utiliser des outils de gestion des risques.





L'organisation comprend le risque de cybersécurité pour les opérations de l'organisation (y compris la mission, les fonctions, l'image ou la réputation), ses actifs et les individus.

## ID.RA-1 Les vulnérabilités des actifs sont identifiées et documentées.

**Les menaces et les vulnérabilités doivent être identifiées.**

### Orientation

- Une vulnérabilité fait référence à une faiblesse dans le matériel, les logiciels ou les procédures de l'organisation. Il s'agit d'une faille par laquelle un acteur malveillant peut accéder aux actifs de l'organisation. Une vulnérabilité expose une organisation à des menaces.
- Une menace est un événement malveillant ou négatif qui tire parti d'une vulnérabilité.
- Le risque est la possibilité de perte et de dommage lorsque la menace se concrétise.

**Un processus doit être établi pour surveiller, identifier et documenter en permanence les vulnérabilités des systèmes critiques de l'organisation.**

### Orientation

- Lorsque cela est sûr et possible, il convient d'envisager l'utilisation d'une analyse de vulnérabilité.
- Il convient que l'organisation établisse et maintienne un programme de tests adapté à sa taille, sa complexité et sa maturité.

**Pour s'assurer que les opérations de l'organisation ne sont pas affectées par le processus de test, les tests de performance/charge et les tests de pénétration sur les systèmes de l'organisation doivent être menés avec soin.**

### Orientation

Envisager de valider les mesures de sécurité après chaque test de pénétration

## ID.RA-2 Les renseignements sur les cybermenaces sont reçus de forums de partage d'informations et de sources.

**Un programme de sensibilisation aux menaces et aux vulnérabilités, comprenant une capacité de partage d'informations entre les organisations, doit être mis en œuvre.**

### Orientation

Il convient qu'un programme de sensibilisation aux menaces et aux vulnérabilités inclue un contact permanent avec les groupes et associations de sécurité afin de recevoir les alertes et les conseils de sécurité. (Les groupes et associations de sécurité comprennent, par exemple, des groupes d'intérêt spéciaux, des forums, des associations professionnelles, des groupes de presse et/ou des groupes de pairs composés de professionnels de la sécurité appartenant à des organisations similaires). Il convient que cette capacité de partage aie une capacité de partage d'informations classifiées et non classifiées.

**Il se doit d'identifier les endroits où des mécanismes automatisés peuvent être mis en œuvre pour mettre les informations relatives aux alertes et aux avis de sécurité à la disposition des parties prenantes pertinentes de l'organisation.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## ID.RA-5 Les menaces, les vulnérabilités, les probabilités et les impacts sont utilisés pour déterminer les risques.

**L'organisation doit effectuer des évaluations des risques dans lesquelles le risque est déterminé par les menaces, les vulnérabilités et l'impact sur les processus et les actifs de l'organisation.**

### Orientation

- N'oubliez pas que les menaces exploitent les vulnérabilités.
- Identifier les conséquences que les pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs et les processus opérationnels connexes.

**L'organisation doit effectuer et documenter des évaluations des risques dans lesquelles le risque est déterminé par les menaces, les vulnérabilités, l'impact sur les processus et les actifs de l'organisation, et la probabilité qu'ils se produisent.**

### Orientation

- Il convient que l'évaluation des risques inclue les menaces provenant de personnes internes et externes.
- Les méthodes d'analyse de risque qualitatives et/ou quantitatives(MAPGOOD, ISO27005, CIS RAM,...) peuvent être utilisées avec des outils logiciels.

**Les résultats de l'évaluation des risques sont diffusés aux parties prenantes concernées.**

### Orientation

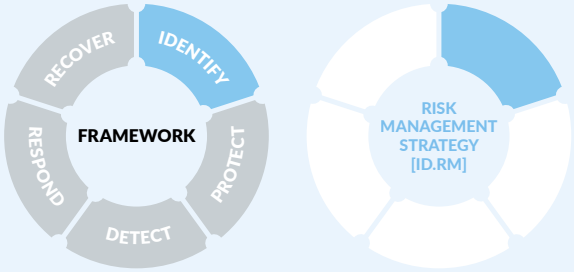
Aucune Orientation supplémentaire sur ce sujet.

## ID.RA-6 Les réponses aux risques sont identifiées et classées par ordre de priorité.

**Une stratégie globale doit être élaborée et mise en œuvre pour gérer les risques auxquels sont exposés les systèmes critiques de l'organisation, qui comprend l'identification et la hiérarchisation des réponses aux risques.**

### Orientation

- Il convient que la direction et les employés soient impliqués dans la sécurité de l'information et la cybersécurité.
- Il convient de déterminer quels sont les actifs les plus importants et comment ils sont protégés.
- Il convient que l'impact d'une compromission de ces actifs soit clair.
- Il convient d'établir comment la mise en œuvre de mesures d'atténuation adéquates sera organisée.




Les priorités, contraintes, tolérances au risque et hypothèses de l'organisation sont établies et utilisées pour soutenir les décisions relatives au risque opérationnel.

## ID.RM-1 Les processus de gestion des risques sont établis, gérés et acceptés par les parties prenantes de l'organisation.

Un processus de gestion des cyber-risques qui identifie les principales parties prenantes internes et externes et facilite le traitement des questions et des informations liées aux risques doit être créé, documenté, examiné, approuvé et mis à jour lorsque des changements surviennent.

### Orientation

Les parties prenantes externes comprennent les clients, les investisseurs et les actionnaires, les fournisseurs, les agences gouvernementales et la communauté au sens large.

## ID.RM-2 La tolérance de l'organisation au risque est déterminée et clairement exprimée.

L'organisation doit déterminer clairement son appétit pour le risque.

### Orientation

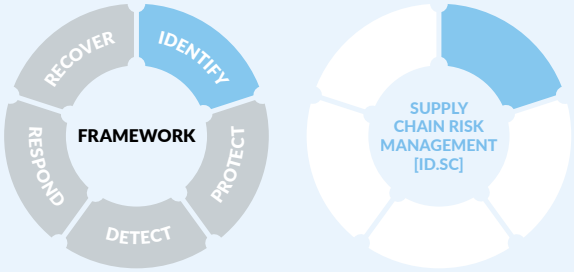
Il convient que la détermination et l'expression de la tolérance au risque (appétit pour le risque) soient conformes aux politiques de sécurité de l'information et de cybersécurité, afin de faciliter la démonstration de la cohérence entre les politiques, la tolérance au risque et les mesures.

## ID.RM-3 La détermination de la tolérance au risque de l'organisation est éclairée par son rôle dans l'infrastructure critique et l'analyse des risques spécifiques au secteur.

Le rôle de l'organisation dans les infrastructures critiques et son secteur déterminent l'appétit de l'organisation pour le risque.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Les priorités, les contraintes, les tolérances au risque et les hypothèses de l'organisation sont établies et utilisées pour soutenir les décisions liées à la gestion des risques de la chaîne d'approvisionnement. L'organisation a établi et mis en œuvre les processus pour identifier, évaluer et gérer les risques liés à la chaîne d'approvisionnement.

## ID.SC-1 Les processus de gestion des risques liés à la chaîne d'approvisionnement sont identifiés, établis, évalués, gérés et acceptés par les parties prenantes de l'organisation.

L'organisation doit documenter, examiner, approuver, mettre à jour lorsque des changements surviennent et mettre en œuvre un processus de gestion des risques liés à la chaîne d'approvisionnement cybernétique qui soutient l'identification, l'évaluation et l'atténuation des risques associés à la nature distribuée et interconnectée des chaînes d'approvisionnement en produits et services TIC/OT.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## ID.SC-2 Les fournisseurs et les partenaires tiers de systèmes d'information, de composants et de services sont identifiés, classés par ordre de priorité et évalués à l'aide d'un processus d'évaluation des risques de la cyberchaîne d'approvisionnement.

L'organisation doit effectuer des évaluations des risques liés à la chaîne d'approvisionnement cybernétique au moins une fois par an ou lorsqu'un changement intervient dans les systèmes critiques, l'environnement opérationnel ou la chaîne d'approvisionnement de l'organisation ; ces évaluations doivent être documentées et les résultats diffusés aux parties prenantes concernées, y compris les responsables des systèmes TIC/OT.

### Orientation

Il convient que cette évaluation permette d'identifier et de hiérarchiser les impacts négatifs potentiels pour l'organisation des risques associés à la nature distribuée et interconnectée des chaînes d'approvisionnement en produits et services TIC/OT.

Une liste documentée de tous les fournisseurs, vendeurs et partenaires de l'organisation susceptibles d'être impliqués dans un incident majeur doit être établie, tenue à jour et mise à disposition en ligne et hors ligne.

### Orientation

Il convient d'inclure dans cette liste les coordonnées des fournisseurs, des vendeurs et des partenaires, ainsi que les services qu'ils fournissent, afin qu'ils puissent être contactés pour une assistance en cas de panne ou de dégradation du service.

## ID.SC-3 Les contrats avec les fournisseurs et les partenaires tiers sont utilisés pour mettre en œuvre des mesures appropriées conçues pour atteindre les objectifs du programme de cybersécurité et du plan de gestion des risques de la chaîne d'approvisionnement de l'organisation.

Sur la base des résultats de l'évaluation des risques liés à la cyberchaîne d'approvisionnement, un cadre contractuel est établi pour les fournisseurs et les partenaires externes afin de traiter le partage d'informations sensibles et de produits et services TIC/OT distribués et interconnectés.

### Orientation

- Il convient que les entités qui ne sont pas soumises à la législation NIS ne considèrent que les fournisseurs et les partenaires tiers essentiels à leur activité.
- N'oubliez pas que les exigences du GDPR doivent être respectées lorsque les informations opérationnelles contiennent des données à caractère personnel (applicable à tous les niveaux), c'est-à-dire que les mesures de sécurité doivent être abordées dans le cadre contractuel.

Des exigences contractuelles en matière de "sécurité de l'information et de cybersécurité" pour les fournisseurs et les partenaires tiers sont mises en œuvre pour garantir un processus vérifiable de correction des failles et pour garantir la correction des failles identifiées lors des tests et des évaluations de "sécurité de l'information et de cybersécurité".

### Orientation

- Il convient que les systèmes d'information contenant des logiciels (ou micrologiciels) affectés par des failles logicielles récemment annoncées (et les vulnérabilités potentielles résultant de ces failles) soient identifiés.
- Les correctifs de sécurité récemment publiés, les Service Packs et hot fixes doivent être installés, et leur efficacité ainsi que les effets secondaires potentiels sur les systèmes d'information de l'organisation sont testés avant leur installation. Les failles découvertes lors des évaluations de sécurité, de la surveillance continue, des activités de réponse aux incidents ou du traitement des erreurs du système d'information sont également traitées rapidement. Il convient que la correction des failles soit intégrée à la gestion de la configuration en tant que changement d'urgence.

L'organisation doit établir des exigences contractuelles lui permettant d'examiner les programmes de "sécurité des informations et de cybersécurité" mis en œuvre par les fournisseurs et les partenaires tiers.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## ID.SC-4 Les fournisseurs et les partenaires tiers sont régulièrement évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluation pour confirmer qu'ils respectent leurs obligations contractuelles.

L'organisation doit examiner les évaluations de la conformité des fournisseurs et des partenaires tiers aux obligations contractuelles en examinant régulièrement les audits, les résultats des tests et autres évaluations.

### Orientation

Les entités non soumises à la législation NIS pourraient se limiter aux seuls fournisseurs et partenaires tiers critiques pour l'organisation.

L'organisation doit examiner les évaluations de la conformité des fournisseurs et des partenaires tiers aux obligations contractuelles en examinant régulièrement les audits indépendants de tiers, les résultats des tests et autres évaluations.

### Orientation

Il convient que la profondeur de l'examen dépende de la criticité des produits et services fournis.

## ID.SC-5 La planification et les tests de réponse et de rétablissement sont effectués avec les fournisseurs et les prestataires tiers.

**L'organisation doit identifier et documenter le personnel clé des fournisseurs et des partenaires tiers afin de les inclure en tant que parties prenantes dans les activités de planification de la réponse et du rétablissement.**

### Orientation

Les entités non soumises à la législation NIS pourraient se limiter aux seuls fournisseurs et partenaires tiers critiques pour l'organisation.

**L'organisation doit identifier et documenter le personnel clé des fournisseurs et des partenaires tiers afin de les inclure en tant que parties prenantes dans les tests et l'exécution des plans de réponse et de rétablissement.**

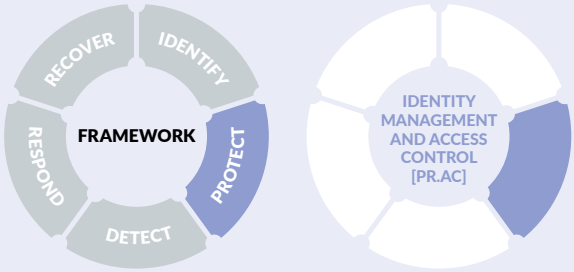
### Orientation

Aucune Orientation supplémentaire sur ce sujet.


Username
Password
Remember me
Protected
Balance:
5.367.50 $

# PROTÉGER

# Protect




L'accès aux actifs physiques et logiques et aux installations associées est limité aux utilisateurs, processus et dispositifs autorisés, et est géré en fonction du risque évalué d'accès non autorisé aux activités et transactions autorisées.

## PR.AC-1 Les identités et les identifiants sont émis, gérés, vérifiés, révoqués et audités pour les dispositifs, utilisateurs et processus autorisés.

**Les identités et les identifiants des dispositifs et des utilisateurs autorisés doivent être gérés.**

### Orientation

Les identités et les identifiants des dispositifs et des utilisateurs autorisés peuvent être gérées par une politique de mot de passe. Une politique de mot de passe est un ensemble de règles destinées à renforcer la sécurité des TIC/OT en encourageant l'organisation à (liste non limitative et mesures à envisager le cas échéant) :

- Changez tous les mots de passe par défaut.
- Veillez à ce que personne ne travaille avec des privilèges d'administrateur pour les tâches quotidiennes.
- Conservez une liste limitée et mise à jour des comptes d'administrateur système.
- Appliquer les règles relatives aux mots de passe, par exemple, les mots de passe doivent être plus longs qu'un nombre de caractères adéquat avec une combinaison de types de caractères et être changés périodiquement ou lorsqu'il y a un soupçon de compromission.
- N'utilisez que des comptes individuels et ne partagez jamais vos mots de passe.
- Désactiver immédiatement les comptes inutilisés.
- Les droits et les privilèges sont gérés par des groupes d'utilisateurs.

**Les identités et les identifiants des dispositifs et des utilisateurs autorisés sont gérés, si possible par des mécanismes automatisés.**

### Orientation

- Des mécanismes automatisés peuvent contribuer à la gestion et à l'audit des informations d'identification des systèmes d'information.
- Considérons l'authentification forte des utilisateurs, c'est-à-dire une authentification basée sur l'utilisation d'au moins deux facteurs d'authentification appartenant à des catégories différentes de connaissance (quelque chose que seul l'utilisateur sait), de possession (quelque chose que seul l'utilisateur possède) ou d'inhérence (quelque chose que l'utilisateur est) qui sont indépendantes, en ce sens que la violation de l'une d'entre elles ne compromet pas la fiabilité des autres, et qui sont conçues de manière à protéger la confidentialité des données d'authentification.


**Les identifiants du système doivent être désactivés après une période d'inactivité déterminée, à moins que cela ne compromette le fonctionnement sûr des processus (critiques).**

### Orientation

- Pour garantir un fonctionnement sûr, Il convient d'utiliser des comptes de service pour les processus et les services en cours d'exécution.
- Envisagez l'utilisation d'une procédure d'accès formelle pour les parties externes.

**Pour les transactions au sein des systèmes critiques de l'organisation, l'organisation doit mettre en œuvre :**

- **l'authentification multifactorielle de l'utilisateur final (MFA ou "authentification forte").**
- **authentification basée sur des certificats pour les communications système à système**

### Orientation

Envisagez l'utilisation du SSO (Single Sign On) en combinaison avec le MFA pour les systèmes critiques internes et externes de l'organisation.

**Les systèmes critiques de l'organisation doivent être surveillés pour détecter toute utilisation atypique des informations d'identification du système. Les identifiants associés à un risque important doivent être désactivés.**

### Orientation

- Envisagez de limiter le nombre de tentatives de connexion infructueuses en mettant en place un verrouillage automatique.
- Le compte verrouillé ne sera pas accessible tant qu'il n'aura pas été réinitialisé ou que la durée de verrouillage du compte ne sera pas écoulée.

## PR.AC-2 L’accès physique aux actifs est géré et protégé.

**L'accès physique à l'installation, aux serveurs et aux composants du réseau doit être géré.**

### Orientation

- Envisagez de gérer strictement les clés d'accès aux locaux et les codes d'alarme. Il convient de prendre en compte les règles suivantes :
  - Récupérez toujours les clés ou les badges d'un employé lorsqu'il quitte définitivement l’organisation.
  - Changez fréquemment les codes d'alarme de l’organisation.
  - Ne jamais donner de clés ou de codes d'alarme à des prestataires extérieurs (agents de nettoyage, etc.), sauf s'il est possible de tracer ces accès et de les limiter techniquement à des plages horaires données.
- Envisagez de ne pas laisser les prises d'accès au réseau interne accessibles dans les lieux publics. Ces lieux publics peuvent être des salles d'attente, des couloirs...

**L'accès physique doit être géré, y compris les mesures relatives à l'accès dans les situations d'urgence.**

### Orientation

- Les contrôles d'accès physiques peuvent inclure, par exemple, des listes de personnes autorisées, des pièces d'identité, des exigences d'escorte, des gardes, des clôtures, des tourniquets, des serrures, la surveillance de l'accès aux installations, la surveillance par caméra.
- Il convient d’envisager les mesures suivantes :
  - Mettez en place un système de badges et créez différentes zones de sécurité.
  - Limitez l'accès physique aux serveurs et aux composants du réseau au personnel autorisé.
  - Consigner tous les accès aux serveurs et aux composants du réseau.
- Il convient que les enregistrements d'accès des visiteurs soient conservés, examinés et traités selon les besoins.

**L'accès physique aux zones critiques doit être contrôlé en plus de l'accès physique à l'installation.**

### Orientation

Par exemple, la production, la R&D, les équipements des systèmes critiques de l'organisation (salles de serveurs, etc.).

**Les actifs liés aux zones critiques doivent être protégés physiquement.**

### Orientation

- Pensez à protéger les équipements d'alimentation, le câblage d'alimentation, le câblage réseau et les interfaces d'accès au réseau contre les dommages accidentels, les perturbations et les manipulations physiques.
- Envisagez de mettre en place des systèmes d'alimentation redondants et physiquement séparés pour les opérations critiques de l'organisation.

## PR.AC-3 L'accès à distance est géré.

**Les points d'accès sans fil de l'organisation doivent être sécurisés.**

### Orientation

Tenez compte des éléments suivants lorsque vous utilisez un réseau sans fil :

- Changez le mot de passe administratif lors de l'installation d'un point d'accès sans fil.
- Configurez le point d'accès sans fil de manière à ce qu'il ne diffuse pas son identifiant (SSID).
- Configurez votre routeur pour qu'il utilise au moins le WiFi Protected Access (WPA-2 ou WPA-3 si possible), avec la norme de cryptage avancée (AES) pour le cryptage.
- Veillez à ce que l'accès Internet sans fil des clients soit séparé du réseau de votre organisation.
- Il convient d'éviter de se connecter à des points d'accès sans fil inconnus ou non sécurisés, et si cela est inévitable, il faut le faire par le biais d'un réseau privé virtuel (VPN) crypté.
- Gérer tous les dispositifs d'extrémité (fixes et mobiles) conformément aux politiques de sécurité de l'organisation.

**Les restrictions d'utilisation, les exigences de connexion, les conseils de mise en œuvre et les autorisations d'accès à distance à l'environnement des systèmes critiques de l'organisation doivent être identifiés, documentés et mis en œuvre.**

### Orientation

Considérez ce qui suit :

- Les méthodes d'accès à distance comprennent, par exemple, des connexions sans fil, à large bande, à un réseau privé virtuel (VPN), des connexions de dispositifs mobiles et des communications par des réseaux externes.
- Il convient que les identifiants de connexion soient conformes aux politiques d'authentification des utilisateurs de l'organisation.
- Il convient que l'accès à distance pour les activités de soutien ou la maintenance des actifs de l'organisation soit approuvé, enregistré et effectué de manière à empêcher tout accès non autorisé.
- Il convient d'informer l'utilisateur de toute connexion à distance à son appareil par une indication visuelle.

**L'accès à distance aux systèmes critiques de l'organisation doit être surveillé et des mécanismes cryptographiques doivent être mis en œuvre lorsque cela est jugé nécessaire.**

### Orientation

Il convient d'inclure que seule l'utilisation autorisée des fonctions privilégiées à partir d'un accès à distance est permise.

**Les réseaux de l'organisation auxquels on accède à distance doivent être sécurisés, notamment par une authentification multifactorielle (MFA).**

### Orientation

Appliquer le MFA (par exemple 2FA) sur les systèmes en contact avec l'Internet, tels que le courrier électronique, le bureau à distance et le réseau privé virtuel (VPN).

**La sécurité des connexions avec les systèmes externes doit être vérifiée et encadrée par des accords documentés.**

### Orientation

L'accès à partir d'adresses IP prédéfinies pourrait être envisagé.

## PR.AC-4 Les permissions et autorisations d'accès sont gérées en intégrant les principes du moindre privilège et de la séparation des tâches.

**Les autorisations d'accès des utilisateurs aux systèmes de l'organisation doivent être définies et gérées.**

### Orientation

Il convient de considérer les éléments suivants :

- Établir et réviser régulièrement les listes d'accès par système (fichiers, serveurs, logiciels, bases de données, etc.), éventuellement par l'analyse de l'Active Directory dans les systèmes basés sur Windows, dans le but de déterminer qui a besoin de quel type d'accès (privilégié ou non), à quoi, pour exercer ses fonctions dans l'organisation.
- Créez un compte distinct pour chaque utilisateur (y compris pour les sous-traitants ayant besoin d'un accès) et exigez que des mots de passe forts et uniques soient utilisés pour chaque compte.
- Veillez à ce que tous les employés utilisent des comptes informatiques sans privilèges administratifs pour effectuer des fonctions de travail typiques. Cela inclut la séparation des comptes personnels et des comptes administratifs.
- Pour les comptes d'invités, envisagez d'utiliser les privilèges minimaux (par exemple, l'accès à l'Internet uniquement) requis pour vos besoins opérationnels.
- Il convient que la gestion des autorisations soit documentée dans une procédure et mise à jour le cas échéant.
- Utilisez l'authentification unique (SSO) si nécessaire.

**Dans la mesure du possible, des mécanismes automatisés doivent être mis en œuvre pour prendre en charge la gestion des comptes d'utilisateurs sur les systèmes critiques de l'organisation, y compris la désactivation, la surveillance, l'établissement de rapports et la suppression des comptes d'utilisateurs.**

### Orientation

Envisagez d'identifier séparément chaque personne ayant accès aux systèmes critiques de l'organisation avec un nom d'utilisateur afin de supprimer les comptes et les accès génériques et anonymes.

**Les restrictions d'utilisation des comptes pour des périodes et des lieux spécifiques doivent être prises en compte dans la politique d'accès sécurisé de l'organisation et appliquées en conséquence.**

### Orientation

Les restrictions spécifiques peuvent inclure, par exemple, la limitation de l'utilisation à certains jours de la semaine, à certaines heures de la journée ou à des durées spécifiques.

**L'organisation doit identifier qui devrait avoir accès aux informations et aux technologies critiques de l'organisation et les moyens d'y accéder.**

### Orientation

Les moyens d'accès peuvent inclure : une clé, un mot de passe, un code ou un privilège administratif.

**L'accès des employés aux données et aux informations doit être limité aux systèmes et aux informations spécifiques dont ils ont besoin pour faire leur travail (principe du moindre privilège).**

### Orientation

- Il convient que le principe du moindre privilège soit compris comme le principe selon lequel une architecture de sécurité doit être conçue de manière à ce que chaque employé se voie accorder les ressources système et les autorisations minimales dont il a besoin pour exercer sa fonction.
- À considérer :
  - Ne pas permettre à un employé d'avoir accès à toutes les informations de l'organisation.
  - Limiter le nombre d'accès Internet et d'interconnexions avec les réseaux partenaires au strict nécessaire pour pouvoir centraliser et homogénéiser plus facilement le suivi des échanges.
  - Assurez-vous que lorsqu'un employé quitte l'organisation, tout accès aux informations ou aux systèmes de l'organisation est bloqué instantanément.

**La séparation des tâches est assurée dans la gestion des droits d'accès.**

### Orientation

La séparation des tâches comprend, par exemple :

- la répartition des fonctions opérationnelles et des fonctions de soutien du système entre différents rôles.
- mener des fonctions de soutien du système avec différentes personnes.
- ne pas permettre à une seule personne d'initier et d'approuver une transaction (financière ou autre).
- s'assurer que le personnel de sécurité qui gère les fonctions de contrôle d'accès ne gère pas également les fonctions d'audit.

**Personne ne doit avoir de privilèges d'administrateur pour les tâches quotidiennes.**

### Orientation

Considérez ce qui suit :

- Séparez les comptes d'administrateur des comptes d'utilisateur.
- Ne pas privilégier les comptes d'utilisateurs pour effectuer les tâches d'administration.
- Créez des mots de passe uniques pour les administrateurs locaux et désactivez les comptes inutilisés.
- Envisagez d'interdire la navigation sur Internet aux comptes administratifs.

**Les utilisateurs privilégiés doivent être gérés, surveillés et audités.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.AC-5 L'intégrité du réseau (séparation du réseau, segmentation du réseau...) est protégée.

**Des pare-feu doivent être installés et activés sur tous les réseaux de l'organisation.**

### Orientation

Considérez ce qui suit :

- Installez et faites fonctionner un pare-feu entre votre réseau interne et l'Internet. Il peut s'agir d'une fonction d'un point d'accès/routeur (sans fil) ou d'un routeur fourni par le fournisseur d'accès Internet (FAI).
- Assurez-vous qu'un logiciel antivirus est installé sur les solutions de pare-feu achetées et veillez à ce que le mot de passe de connexion et d'administration de l'administrateur soit modifié lors de l'installation et régulièrement par la suite.
- Installez, utilisez et mettez à jour un pare-feu logiciel sur chaque système informatique (y compris les téléphones intelligents et autres appareils en réseau).
- Installez des pare-feu sur chacun de vos ordinateurs et réseaux, même si vous utilisez un fournisseur de services en nuage ou un réseau privé virtuel (VPN). Assurez-vous que le réseau et les systèmes de votre domicile de télétravail sont équipés de pare-feu matériels et logiciels installés, opérationnels et régulièrement mis à jour.
- Envisagez d'installer un système de détection et de prévention des intrusions (IDPS). Ces dispositifs analysent le trafic réseau à un niveau plus détaillé et peuvent fournir un plus grand niveau de protection.

**Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par l'intégration de la segmentation et de la ségrégation du réseau.**

### Orientation

- Envisagez de créer différentes zones de sécurité dans le réseau (par exemple, segmentation de base du réseau par des VLAN ou d'autres mécanismes de contrôle d'accès au réseau) et contrôlez/surveillez le trafic entre ces zones.
- Lorsque le réseau est «plat», la compromission d'un composant vital du réseau peut entraîner la compromission de l'ensemble du réseau.

**Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par :**
**(1) Identifier, documenter et contrôler les connexions entre les composants du système.**
**(2) Limiter les connexions externes aux systèmes critiques de l'organisation.**

### Orientation

Les mécanismes de protection des limites comprennent, par exemple, les routeurs, les gateways, les gateways unidirectionnelles, les data diodes et les pare-feu qui séparent les composants du système en réseaux ou sous-réseaux logiquement distincts.

**L'organisation doit mettre en œuvre, dans la mesure du possible, des serveurs proxy authentifiés pour le trafic de communication défini entre les systèmes critiques de l'organisation et les réseaux externes.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit surveiller et contrôler les connexions et les communications à la frontière externe et aux principales frontières internes des systèmes critiques de l'organisation en mettant en œuvre des dispositifs de protection des frontières, le cas échéant.**

### Orientation

Envisagez de mettre en œuvre les recommandations suivantes :

- Séparez votre réseau WIFI public de votre réseau professionnel.
- Protégez votre WIFI professionnel grâce à un cryptage de pointe.
- Mettre en œuvre une solution de contrôle d'accès au réseau (NAC).
- Cryptez les connexions à votre réseau d'organisation.
- Divisez votre réseau en fonction des niveaux de sécurité et appliquez des règles de pare-feu. Isolez vos réseaux pour l'administration des serveurs.
- Forcer le VPN sur les réseaux publics.
- Mettez en œuvre une politique de fermeture des gateways de sécurité (politique de refus de tout : n'autorisez/ouvrez que les connexions qui ont été explicitement préautorisées).

**L'organisation doit s'assurer que les systèmes critiques de l'organisation tombent en panne en toute sécurité lorsqu'un dispositif de protection des frontières tombe en panne opérationnelle.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.AC-6 Les identités sont prouvées et liées aux identifiants et présentées dans les interactions.

L'organisation doit mettre en œuvre des procédures documentées pour vérifier l'identité des personnes avant de délivrer des identifiants donnant accès aux systèmes de l'organisation.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit garantir l'utilisation d'identifiants uniques liés à chaque utilisateur, dispositif et processus vérifié interagissant avec les systèmes critiques de l'organisation ; s'assurer qu'ils sont authentifiés et que les identifiants uniques sont capturés lors des interactions avec le système.

### Orientation

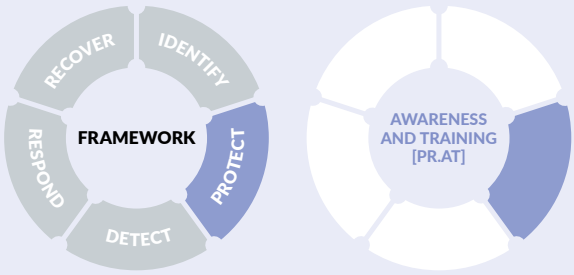
Aucune Orientation supplémentaire sur ce sujet.

## PR.AC-7 Les identités sont prouvées et liées aux identifiants et présentées dans les interactions.

L'organisation doit effectuer une évaluation des risques documentée sur les transactions des systèmes critiques de l'organisation et authentifier les utilisateurs, les dispositifs et les autres actifs (par exemple, à un ou plusieurs facteurs) en fonction du risque de la transaction (par exemple, les risques pour la sécurité et la vie privée des individus et les autres risques pour l'organisation).

### Orientation

Envisagez une approche de sécurité par la conception pour les nouveaux systèmes ; pour les systèmes existants, il convient d'utiliser une évaluation des risques distincte.




Le personnel et les partenaires de l'organisation reçoivent une formation de sensibilisation à la cybersécurité et sont formés à l'exécution de leurs tâches et responsabilités liées à la cybersécurité, conformément aux politiques, procédures et accords connexes.

## PR.AT-1 Tous les utilisateurs sont informés et entrainés.

**Les employés doivent être formés de manière appropriée.**

### Orientation

- Les employés comprennent tous les utilisateurs et les gestionnaires des systèmes TIC/OT, et il convient qu'ils soient formés dès leur embauche, puis régulièrement, aux politiques de sécurité de l'information de l'organisation et à ce qu'on attend d'eux pour protéger les informations et les technologies de l'organisation.
- Il convient que la formation soit continuellement mise à jour et renforcée par des campagnes de sensibilisation.

**L'organisation doit intégrer la reconnaissance et le signalement des menaces internes dans la formation à la sécurité.**

### Orientation

À considérer :

- Communiquez et discutez régulièrement afin de vous assurer que chacun est conscient de ses responsabilités.
- Développez un programme de sensibilisation en rassemblant dans un document les messages que vous souhaitez transmettre à votre personnel (sujets, publics, objectifs, etc.) et votre rythme de communication sur un calendrier (hebdomadaire, mensuel, ponctuel, etc.). Communiquez de manière continue et engageante, en impliquant la direction, les collègues informaticiens, le fournisseur de services TIC et les responsables des RH et de la communication.
- Les sujets abordés sont les suivants : reconnaissance des tentatives de fraude, hameçonnage, gestion des informations sensibles, incidents, etc. L'objectif est que tous les employés comprennent les moyens de protéger les informations de l'organisation.
- Discutez avec votre direction, vos collègues des TIC ou votre fournisseur de services TIC de certains scénarios pratiques (par exemple, que faire en cas d'alerte au virus, de coupure de courant due à un orage, de blocage des données, de piratage d'un compte, etc.), déterminez les comportements à adopter, documentez-les et communiquez-les à l'ensemble de votre personnel. Il convient que le point de contact central en cas d'incident soit connu de tous.
- Organisez une simulation d'un scénario pour tester vos connaissances. Envisagez de réaliser cet exercice, par exemple, au moins une fois par an.

L'organisation doit mettre en œuvre une méthode d'évaluation pour mesurer l'efficacité des formations de sensibilisation.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.AT-2 Les utilisateurs privilégiés comprennent leurs rôles et leurs responsabilités.

Les utilisateurs privilégiés doivent être qualifiés avant que les privilèges ne leurs soient accordés, et ces utilisateurs doivent pouvoir démontrer qu'ils comprennent leurs rôles, leurs responsabilités et leurs pouvoirs.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.AT-3 Les parties prenantes tierces (par exemple, les fournisseurs, les clients, les partenaires) comprennent leurs rôles et responsabilités.

L'organisation doit établir et appliquer des exigences de sécurité pour les fournisseurs et les utilisateurs tiers essentiels à l'organisation.

### Orientation

Il convient que la mise en application inclue le fait que les utilisateurs des "parties prenantes tierces" (par exemple, les fournisseurs, les clients, les partenaires) puissent démontrer qu'ils comprennent leurs rôles et leurs responsabilités.

Les fournisseurs tiers sont tenus de notifier tout transfert, licenciement ou transition de personnel ayant un accès physique ou logique aux composants des systèmes critiques de l'organisation.

### Orientation

Les fournisseurs tiers comprennent, par exemple, des prestataires de services, des entrepreneurs et d'autres organisations fournissant le développement de systèmes, des services technologiques, des applications externalisées ou la gestion du réseau et de la sécurité.

L'organisation doit contrôler les fournisseurs de services et les utilisateurs critiques pour l'organisation en matière de conformité à la sécurité.

### Orientation

Les résultats d'audits réalisés par des tiers peuvent être utilisés comme preuves d'audit.

L'organisation doit auditer les fournisseurs de services externes critiques pour l'organisation afin de vérifier leur conformité en matière de sécurité.

### Orientation

Les résultats d'audits réalisés par des tiers peuvent être utilisés comme preuves d'audit.

## PR.AT-4 Les cadres supérieurs comprennent leurs rôles et responsabilités.

Les cadres supérieurs doivent démontrer qu'ils comprennent leurs rôles, leurs responsabilités et leurs pouvoirs.

### Orientation

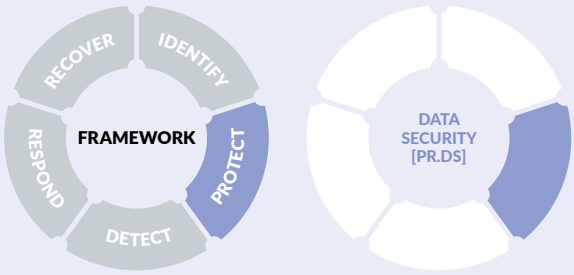
Des conseils sur les profils de rôle ainsi que leurs titres, missions, tâches, aptitudes, connaissances et compétences sont disponibles dans le document "European Cybersecurity Skills Framework Role Profiles" de ENISA. (https ://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles )

## PR.AT-5 Le personnel de la sécurité physique et de la cybersécurité comprend ses rôles et responsabilités.

L'organisation doit s'assurer que le personnel responsable de la protection physique et de la sécurité des systèmes et installations critiques de l'organisation est qualifié par une formation avant que des privilèges ne soient accordés, et qu'il comprend ses responsabilités.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Les informations et les enregistrements (données) sont gérés conformément à la stratégie de l'organisation en matière de risques afin de protéger la confidentialité, l'intégrité et la disponibilité des informations.

## PR.DS-1 Les données au repos sont protégées.

**L'organisme doit protéger ses informations critiques du système déterminées comme étant critiques/sensibles lorsqu'elles sont au repos.**

### Orientation

- Envisagez d'utiliser des techniques de cryptage pour le stockage des données, la transmission des données ou le transport des données (par exemple, ordinateur portable, USB).
- Envisagez de crypter les appareils des utilisateurs finaux et les supports amovibles contenant des données sensibles (disques durs, ordinateurs portables, appareils mobiles, périphériques de stockage USB, etc.) Cela peut être fait par exemple avec Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,...
- Envisagez de crypter les données sensibles stockées dans le nuage.
- Mettre en œuvre des mesures de protection spécifiques pour empêcher l'accès non autorisé, la déformation ou la modification des données du système et des enregistrements d'audit (par exemple, droits d'accès restreints, sauvegardes quotidiennes, cryptage des données, installation de pare-feu).
- Chiffrez les disques durs, les supports externes, les fichiers stockés, les fichiers de configuration et les données stockées dans le nuage.

## PR.DS-2 Les données en transit sont protégées.

**Comme ce contrôle est inclus dans d'autres éléments du cadre, aucune exigence n'est identifiée ici pour le niveau d'assurance "Basic". Des directives spécifiques sont fournies pour renforcer la sécurité de l'information.**

### Orientation

Lorsque l'organisation envoie souvent des documents ou des courriels sensibles, il est recommandé de chiffrer ces documents et/ou courriels à l'aide d'outils logiciels appropriés, pris en charge et autorisés.

**L'organisation doit protéger les informations de ses systèmes jugées critiques lorsqu'elles sont en transit.**

### Orientation

Si vous envoyez des documents ou des courriels sensibles, vous pouvez envisager de les crypter.

## PR.DS-3 Les actifs sont gérés de manière formelle tout au long de leur retrait, de leur transfert et de leur mise à disposition.

**Les actifs et les supports doivent être éliminés de manière sûre.**

### Orientation

- Lors de l'élimination d'actifs tangibles tels que les ordinateurs professionnels/portables, les serveurs, le(s) disque(s) dur(s) et autres supports de stockage (clés USB, papier...), assurez-vous que toutes les données professionnelles ou personnelles sensibles sont supprimées de manière sécurisée (c'est-à-dire "effacées" électroniquement) avant d'être retirées et ensuite physiquement détruites (ou remises en service). Cette opération est également connue sous le nom de "assainissement" et est donc liée à l'exigence et aux conseils de PR.IP-6.
- Envisager d'installer une application d'effacement à distance sur les ordinateurs portables, les tablettes, les téléphones portables et autres appareils mobiles de l'organisation.

**L'organisation doit faire respecter l'obligation de rendre compte de tous ses actifs essentiels à l'organisation tout au long du cycle de vie du système, y compris lors du retrait, du transfert et de leur mise à disposition.**

### Orientation

Il convient que la responsabilité inclue :

- L'autorisation pour les actifs critiques d'entrer et de sortir de l'installation.
- Le suivi et maintien de la documentation relative aux mouvements des actifs critiques pour l'organisation.

**L'organisation doit s'assurer que les actions d'élimination sont approuvées, suivies, documentées et vérifiées.**

### Orientation

Les actions d'élimination comprennent des actions de assainissement des médias (voir PR.IP-6).

L'organisation doit veiller à ce que les mesures nécessaires soient prises pour faire face à la perte, à l'utilisation abusive, à la détérioration ou au vol des actifs.

### Orientation

Cela peut se faire par des politiques, des processus et des procédures (reporting), des moyens techniques et organisationnels (cryptage, contrôle d'accès (AC), gestion des appareils mobiles (MDM), surveillance, effacement sécurisé, sensibilisation, accord d'utilisation signé, directives et manuels, sauvegardes, mise à jour de l'inventaire...).

## PR.DS-4 Une capacité adéquate pour assurer la disponibilité est maintenue.

La planification des capacités doit garantir des ressources adéquates pour le traitement de l'information, la mise en réseau, les télécommunications et le stockage des données des systèmes critiques de l'organisation.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

Les systèmes critiques de l'organisation doivent être protégés contre les attaques par déni de service ou, du moins, l'effet de ces attaques sera limité.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

Les données d'audit des systèmes critiques de l'organisation doivent être déplacées vers un système alternatif.

### Orientation

Sachez que les services de log peuvent devenir un goulot d'étranglement et entraver le bon fonctionnement des systèmes sources.

## PR.DS-5 Les protections contre les fuites de données sont mises en œuvre.

**L'organisation doit prendre des mesures appropriées qui se traduisent par la surveillance de ses systèmes critiques aux frontières extérieures et aux points internes critiques lorsqu'un accès et des activités non autorisés, y compris une fuite de données, sont détectés.**

### Orientation

- Pensez à mettre en place des mesures de protection dédiées (droits d'accès restreints, sauvegardes quotidiennes, cryptage des données, installation de pare-feu, etc.) pour les données les plus sensibles.
- Envisager un audit fréquent de la configuration de l'annuaire central (Active Directory dans l'environnement Windows), en se concentrant spécifiquement sur l'accès aux données des personnes clés de l'organisation.

## PR.DS-6 Des mécanismes de vérification de l'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations.

**L'organisation doit mettre en œuvre des contrôles d'intégrité des logiciels, des microprogrammes et des informations pour détecter les modifications non autorisées apportées aux composants de ses systèmes critiques pendant le stockage, le transport, le démarrage et lorsque cela est jugé nécessaire.**

### Orientation

Les mécanismes de vérification de l'intégrité conformes à l'état de l'art (par exemple, les contrôles de parité, les contrôles de redondance cyclique, les hachages cryptographiques) et les outils associés peuvent surveiller automatiquement l'intégrité des systèmes d'information et des applications hébergées.

**L'organisation doit mettre en œuvre des outils automatisés, dans la mesure du possible, afin de fournir une notification lors de la découverte de divergences pendant la vérification de l'intégrité.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit mettre en œuvre une capacité de réponse automatique avec des garanties de sécurité prédéfinies lorsque des violations de l'intégrité sont découvertes.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.DS-7 L’environnement ou les environnements de développement et de test sont séparés de l’environnement de production.

**Les environnements de développement et de test doivent être isolés de l'environnement de production.**

### Orientation

- Il convient que tout changement que l'on souhaite apporter à l'environnement ICT/OT soit d'abord testé dans un environnement différent et distinct de l'environnement de production (environnement opérationnel) avant que ce changement ne soit effectivement mis en œuvre. De cette façon, l'effet de ces changements peut être analysé et des ajustements peuvent être effectués sans perturber les activités opérationnelles.
- Envisagez d'ajouter et de tester des fonctions de cybersécurité dès le début du développement (principes du cycle de développement sécurisé).

## PR.DS-8 Les mécanismes de contrôle d’intégrité sont utilisés pour vérifier l’intégrité du matériel.

**L'organisation doit mettre en œuvre des contrôles d'intégrité du matériel pour détecter les altérations non autorisées du matériel de ses systèmes critiques.**

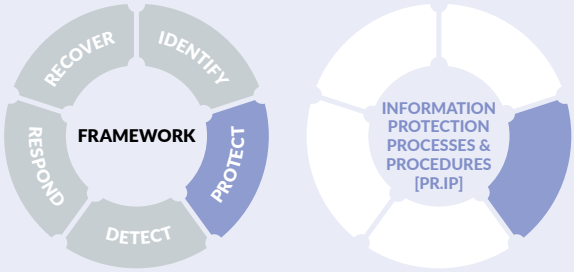
### Orientation

Les mécanismes de vérification de l'intégrité conformes à l'état de l'art (par exemple, les contrôles de parité, les contrôles de redondance cyclique, les hachages cryptographiques) et les outils associés peuvent surveiller automatiquement l'intégrité des systèmes d'information et des applications hébergées.

**L'organisation doit intégrer la détection de l'altération non autorisée du matériel de ses systèmes critiques dans sa capacité de réponse aux incidents.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Les politiques de sécurité (qui traitent de l'objectif, de la portée, des rôles, des responsabilités, de l'engagement de la direction et de la coordination entre les entités organisationnelles), les processus et les procédures sont maintenus et utilisés pour gérer la protection des systèmes d'information et des actifs.

## PR.IP-1 Une configuration de base des systèmes de contrôle des technologies de l'information/de l'industrie est créée et maintenue en intégrant les principes de sécurité.

**L'organisation doit développer, documenter et maintenir une configuration de base pour ses systèmes critiques.**

### Orientation

- Ce contrôle inclut le concept de la moindre fonctionnalité.
- Les configurations de base comprennent, par exemple, des informations sur les systèmes critiques de l'organisation, les numéros de version actuels et les informations sur les correctifs des systèmes d'exploitation et des applications, les paramètres de configuration, la topologie du réseau et l'emplacement logique de ces composants dans l'architecture du système.
- Il convient que la topologie du réseau inclue les points névralgiques de l'environnement IT/OT (connexions externes, serveurs hébergeant des données et/ou des fonctions sensibles, sécurité des services DNS, etc.)

**L'organisation doit configurer ses systèmes critiques pour fournir uniquement les capacités essentielles. Par conséquent, la configuration de base doit être revue et les capacités inutiles doivent être désactivées.**

### Orientation

- La configuration d'un système pour fournir uniquement les capacités essentielles à la mission définies par l'organisation est connue sous le nom de "concept de moindre fonctionnalité".
- Les capacités comprennent les fonctions, les ports, les protocoles, les logiciels et/ou les services.

## PR.IP-2 Un cycle de vie du développement des systèmes pour gérer les systèmes est mis en œuvre.

**Le cycle de vie du développement des systèmes et des applications doit inclure des considérations de sécurité.**

### Orientation

- Il convient que le cycle de vie du développement des systèmes et des applications inclue le processus d'acquisition des systèmes critiques de l'organisation et de ses composants.
- Il convient d'envisager une formation à la sensibilisation aux vulnérabilités et à la prévention pour les développeurs (d'applications web), ainsi qu'une formation avancée à la sensibilisation à l'ingénierie sociale pour les rôles importants.
- Lorsque l'on héberge des applications tournées vers l'internet, il convient d'envisager la mise en place d'un pare-feu pour applications web (WAF).

**Le processus de développement des systèmes critiques et de leurs composants doit couvrir l'ensemble du cycle de conception et fournir une description des propriétés fonctionnelles des contrôles de sécurité, ainsi que des informations sur la conception et la mise en œuvre des interfaces du système relatives à la sécurité.**

### Orientation

Le cycle de développement comprend :

- Toutes les phases de développement : spécification, conception, développement, mise en œuvre.
- Gestion de la configuration pour les changements planifiés et non planifiés et contrôle des changements pendant le développement.
- Suivi et résolution des failles.
- Test de sécurité.

## PR.IP-3 Des processus de contrôle des changements de configuration sont en place.

**Les modifications doivent être testées et validées avant d'être mises en œuvre dans les systèmes opérationnels.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**Pour les modifications prévues des systèmes critiques de l'organisation, une analyse d'impact sur la sécurité doit être effectuée dans un environnement de test distinct avant la mise en œuvre dans un environnement opérationnel.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.IP-4 Des sauvegardes des informations sont effectuées, maintenues et testées.

**Les sauvegardes des données critiques de l'organisation doivent être effectuées et stockées sur un système différent du dispositif sur lequel se trouvent les données originales.**

### Orientation

- Les données des systèmes critiques de l'organisation comprennent par exemple les logiciels, les configurations et les paramètres, la documentation, les données de configuration du système, y compris les sauvegardes de la configuration de l'ordinateur, les sauvegardes de la configuration des applications, etc.
- Envisagez une sauvegarde régulière et mettez-la hors ligne périodiquement.
- Il convient que les objectifs de temps et de point de rétablissement soient pris en compte.
- Envisagez de ne pas stocker la sauvegarde des données de l'organisation sur le même réseau que le système sur lequel résident les données originales et fournissez une copie hors ligne. Cela permet notamment d'éviter le cryptage des fichiers par les pirates (risque de ransomware).

**La fiabilité et l'intégrité des sauvegardes doivent être vérifiées et testées régulièrement.**

### Orientation

Il convient d'inclure des tests réguliers des procédures de restauration des sauvegardes.

**La vérification des sauvegardes doit être coordonnée avec les fonctions de l'organisation qui sont responsables des plans connexes.**

### Orientation

- Les plans connexes comprennent, par exemple, les plans de continuité des activités, les plans de reprise après sinistre, les plans de continuité des opérations, les plans de communication de crise, les plans d'infrastructure critique et les plans de réponse aux cyberincidents.
- Il convient que la restauration des données de sauvegarde pendant les tests du plan d'urgence soit prévue.

**Un site de stockage alternatif distinct pour les sauvegardes du système doit être exploité et les mêmes mesures de sécurité que le site de stockage principal doivent être utilisées.**

### Orientation

Une sauvegarde hors ligne de vos données est idéalement stockée dans un endroit physique distinct de la source de données originale et, si possible, hors site pour une protection et une sécurité supplémentaire.

La sauvegarde des systèmes critiques doit être séparée de la sauvegarde des informations critiques.

### Orientation

Il convient que la séparation de la sauvegarde des systèmes critiques et de la sauvegarde des informations critiques devrait permette de réduire le temps de rétablissement.

## PR.IP-5 La politique et les règlements concernant l'environnement physique d'exploitation des actifs de l'organisation sont respectés.

L'organisation doit définir, mettre en œuvre et appliquer une politique et des procédures concernant les systèmes d'urgence et de sécurité, les systèmes de protection contre l'incendie et les contrôles de l'environnement pour ses systèmes critiques.

### Orientation

Il convient de considérer les mesures ci-dessous :

- Protégez les équipements informatiques non surveillés avec des cadenas ou un système de casiers et de clés.
- Il convient que les mécanismes d'extinction des incendies tiennent compte de l'environnement des systèmes critiques de l'organisation (par exemple, les systèmes d'extincteurs automatiques à eau peuvent être dangereux dans certains environnements).

L'organisation doit mettre en place des dispositifs de détection d'incendie qui se déclenchent et avertissent automatiquement le personnel clé en cas d'incendie.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.IP-6 Les données sont détruites conformément à la politique.

**L'organisation doit s'assurer que les données de son système critique sont détruites conformément à la politique.**

### Orientation

- Les actions d'élimination comprennent des actions d'assainissement des médias (voir PR.DS-3).
- Il existe deux principaux types de supports utilisés couramment :
  - Supports papier (représentations physiques de l'information)
  - Les supports électroniques ou informatiques (les bits et les octets contenus dans les disques durs, les mémoires vives (RAM), les mémoires mortes (ROM), les disques, les dispositifs de mémoire, les téléphones, les dispositifs informatiques mobiles, les équipements de réseau...).

**Les processus d'assainissement doivent être documentés et testés.**

### Orientation

- Les processus d'assainissement comprennent les procédures et les équipements.
- Envisagez d'appliquer des techniques d'assainissement non destructives aux dispositifs de stockage portables.
- Considérez les procédures d'assainissement en fonction des exigences de confidentialité.

## PR.IP-7 Les processus de protection sont améliorés.

**L'organisation doit intégrer les améliorations découlant de la surveillance, des mesures, des évaluations et des enseignements tirés dans les mises à jour du processus de protection (amélioration continue).**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit mettre en place des équipes indépendantes pour évaluer le(s) processus de protection.**

### Orientation

- Les équipes indépendantes peuvent comprendre du personnel impartial interne ou externe.
- L'impartialité implique que les évaluateurs soient libres de tout conflit d'intérêt perçu ou réel concernant le développement, l'exploitation ou la gestion du système critique de l'organisation soumis à l'évaluation ou la détermination de l'efficacité du contrôle de sécurité.

L'organisation doit s'assurer que le plan de sécurité de ses systèmes critiques facilite l'examen, le test et l'amélioration continue des processus de protection de la sécurité.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.IP-8 L'efficacité des technologies de protection est partagée.

L'organisation doit collaborer et partager avec les partenaires désignés les informations relatives aux incidents de sécurité liés à son système critique et aux mesures d'atténuation.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

La communication de l'efficacité des technologies de protection est partagée avec les parties appropriées.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit mettre en œuvre, dans la mesure du possible, des mécanismes automatisés pour faciliter la collaboration en matière d'information.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.IP-9 Des plans de réponse (réponse aux incidents et continuité des activités) et des plans de rétablissement (reprise après incident et reprise après sinistre) sont en place et gérés.

**Des plans de réponse en cas d'incident (réponse aux incidents et continuité des activités) et des plans de rétablissement (rétablissement en cas d'incident et reprise après sinistre) doivent être établis, maintenus, approuvés et testés afin de déterminer l'efficacité des plans et l'état de préparation à l'exécution des plans.**

### Orientation

- Le plan de réponse aux incidents est la documentation d'un ensemble prédéterminé d'instructions ou de procédures pour détecter, répondre et limiter les conséquences d'une cyber-attaque malveillante.
- Il convient d'intégrer dans les plans les objectifs de rétablissement, les priorités de rétablissement, les mesures, les rôles d'urgence, les affectations du personnel et les informations de contact.
- Il convient que le maintien des fonctions essentielles malgré la perturbation du système et la restauration éventuelle des systèmes de l'organisation soient abordés.
- Envisagez de définir les types d'incidents, les ressources et le soutien de gestion nécessaires pour maintenir et développer efficacement les capacités de réponse aux incidents et de contingence.

**L'organisation doit coordonner l'élaboration et le test des plans de réponse aux incidents et des plans de rétablissement avec les parties prenantes responsables des plans connexes.**

### Orientation

Les plans connexes comprennent, par exemple, les plans de continuité des activités, les plans de reprise après sinistre, les plans de continuité des opérations, les plans de communication de crise, les plans d'infrastructure critique, les plans de réponse aux cyberincidents et les plans d'urgence pour les occupants.

## PR.IP-11 La cybersécurité est incluse dans les pratiques de ressources humaines (déprovisionnement, sélection du personnel...).

**Le personnel ayant accès aux informations ou aux technologies les plus critiques de l'organisation doit être vérifié.**

### Orientation

- Il convient que l'accès aux informations ou aux technologies critiques soit pris en compte lors du recrutement, pendant l'emploi et lors de la cessation d'activité.
- Il convient que les vérifications des antécédents tiennent compte des lois, des règlements et de l'éthique applicables, proportionnellement aux besoins de l'organisation, à la classification des informations auxquelles il faut accéder et aux risques perçus.

Élaborer et maintenir un processus de sécurité de l'information/cyber des ressources humaines applicable lors du recrutement, pendant l'emploi et à la fin de l'emploi.

### Orientation

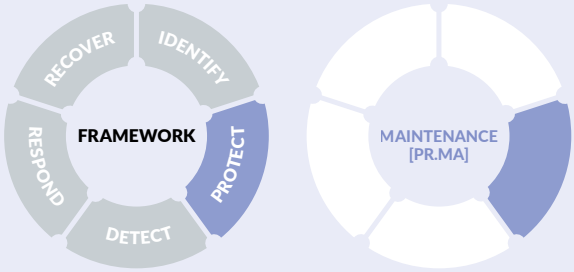
Il convient que le processus de sécurité des ressources humaines en matière d'information et de cybercriminalité comprenne l'accès aux informations ou aux technologies essentielles, la vérification des antécédents, le code de conduite, les rôles, les pouvoirs et les responsabilités...

## PR.IP-12 Un plan de gestion des vulnérabilités est élaboré et mis en œuvre.

L'organisation doit établir et maintenir un processus documenté qui permet un examen continu des vulnérabilités et des stratégies pour les atténuer.

### Orientation

- Envisager de recenser les sources susceptibles de signaler les vulnérabilités des composants identifiés et de diffuser les mises à jour (sites web des éditeurs de logiciels, site web du CERT, site web de ENISA).
- Il convient que l'organisation identifie où les vulnérabilités de son système critique peuvent être exposées à des adversaires.




La maintenance et la réparation des composants des systèmes de contrôle et d'information industriels sont effectuées conformément aux politiques et procédures.

## PR.MA-1 L'entretien et la réparation des actifs de l'organisation sont effectués et consignés, avec des outils approuvés et contrôlés.

**Les correctifs et les mises à jour de sécurité pour les systèmes d'exploitation et les composants critiques du système doivent être installés.**

### Orientation

Il convient de considérer les éléments suivants :

- Limitez-vous à l'installation des applications (systèmes d'exploitation, microprogrammes ou plugins) dont vous avez besoin pour gérer votre organisation et mettez-les à jour régulièrement.
- Il convient de n'installer que la version actuelle et prise en charge par le fournisseur du logiciel que vous choisissez d'utiliser. Il peut être utile d'attribuer un jour par mois à la vérification des correctifs.
- Il existe des produits qui peuvent analyser votre système et vous avertir lorsqu'il existe une mise à jour pour une application que vous avez installée. Si vous utilisez l'un de ces produits, assurez-vous qu'il vérifie les mises à jour pour chaque application que vous utilisez.
- Installer les correctifs et les mises à jour de sécurité en temps voulu.

**L'organisation doit planifier, réaliser et documenter la maintenance préventive et les réparations des composants critiques de son système selon des processus et des outils approuvés.**

### Orientation

Il convient de considérer les éléments suivants :

- Effectuer les mises à jour de sécurité sur tous les logiciels en temps voulu.
- Automatisez le processus de mise à jour et contrôlez son efficacité.
- Introduire une culture interne de l'application de correctifs sur les ordinateurs de bureau, les appareils mobiles, les serveurs, les composants de réseau, etc. pour assurer le suivi des mises à jour.

L'organisation doit empêcher le retrait non autorisé des équipements de maintenance contenant des informations critiques sur les systèmes de l'organisation.

### Orientation

Cette exigence concerne principalement les environnements OT/ICS.

L'organisation doit appliquer les exigences d'approbation, de contrôle et de surveillance des outils de maintenance destinés à être utilisés sur ses systèmes critiques.

### Orientation

Les outils de maintenance peuvent inclure des équipements de test de diagnostic matériel/logiciel, des renifleurs de paquets matériel/logiciel et des ordinateurs portables.

Les outils de maintenance et les dispositifs de stockage portables doivent être inspectés lorsqu'ils sont introduits dans l'établissement et doivent être protégés par des solutions anti-malware afin qu'ils soient analysés pour détecter les codes malveillants avant d'être utilisés sur les systèmes de l'organisation.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit vérifier les contrôles de sécurité après la maintenance ou la réparation du matériel et prendre les mesures qui s'imposent.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit vérifier les contrôles de sécurité à la suite de la maintenance ou de la réparation/du correctif du matériel et des logiciels et prendre les mesures qui s'imposent.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.MA-2 La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé.

La télémaintenance ne doit avoir lieu qu'après approbation préalable, surveillance pour éviter tout accès non autorisé, et approbation du résultat des activités de maintenance telles que décrites dans les processus ou procédures approuvés.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit exiger que les services de diagnostic relatifs à la télémaintenance soient effectués à partir d'un système qui met en œuvre une capacité de sécurité comparable à celle mise en œuvre sur le système critique de l'organisation équivalent.

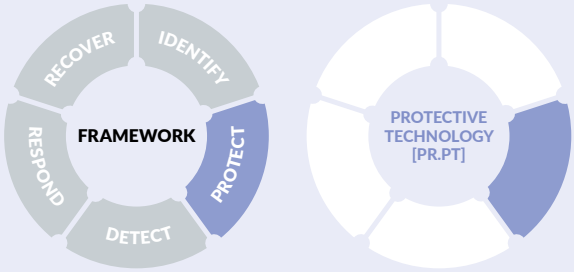
### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit s'assurer de la mise en œuvre d'authentificateurs forts, de la prise d'enregistrements et de la fermeture de session pour la maintenance à distance.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Les solutions de sécurité technique sont gérées de manière à garantir la sécurité et la résilience des systèmes et des actifs, conformément aux politiques, procédures et accords connexes.

## PR.PT-1 Les enregistrements d'audit/logs sont déterminés, documentés, mis en œuvre et révisés conformément à la politique.

**Les logs doivent être maintenus, documentés et examinés.**

### Orientation

- Assurez-vous que la fonctionnalité d'enregistrement des activités du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les antivirus) est activée.
- Il convient que les logs soient sauvegardés et conservés pendant une période prédéfinie.
- Il convient que les logs soient examinés pour déceler toute tendance inhabituelle ou indésirable, telle qu'une utilisation importante des sites Web de médias sociaux ou un nombre inhabituel de virus trouvés régulièrement sur un ordinateur particulier. Ces tendances peuvent indiquer un problème plus grave ou signaler la nécessité de renforcer les protections dans un domaine particulier.

**L'organisation doit s'assurer que les enregistrements de log comprennent une source de temps faisant autorité ou un horodateur d'horloge interne qui sont comparés et synchronisés avec une source de temps faisant autorité.**

### Orientation

Les sources de temps faisant autorité comprennent, par exemple, un serveur interne NTP (Network Time Protocol), une horloge radio, une horloge atomique, une source de temps GPS.

**L'organisation doit s'assurer que les échecs de traitement des audits sur les systèmes de l'organisation génèrent des alertes et déclenchent des réponses définies.**

### Orientation

L'utilisation de serveurs System Logging Protocol (Syslog) peut être envisagée.

L'organisation doit permettre aux personnes autorisées d'étendre les capacités d'audit lorsque les événements l'exigent.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.PT-2 Les supports amovibles sont protégés et leur utilisation est limitée conformément à la politique.

La restriction de l'utilisation des dispositifs de stockage portables doit être assurée par une politique documentée appropriée et des mesures de protection complémentaires.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

Les dispositifs de stockage portables contenant des données système doivent être contrôlés et protégés pendant leur transport et leur stockage.

### Orientation

Il convient que la protection et le contrôle incluent le scannage de tous les dispositifs de stockage portables pour détecter les codes malveillants avant qu'ils ne soient utilisés sur les systèmes de l'organisation.

Il convient que l'organisation interdisse techniquement la connexion de supports amovibles, sauf si cela est strictement nécessaire ; dans les autres cas, il convient de désactiver l'exécution de programmes automatiques à partir de ces supports.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.PT-3 Le principe de la moindre fonctionnalité est incorporé en configurant les systèmes de manière à ne fournir que les capacités essentielles.

L'organisation doit configurer les systèmes critiques pour l'organisation afin de ne fournir que les capacités essentielles.

### Orientation

Envisagez d'appliquer le principe de la moindre fonctionnalité aux systèmes d'accès et aux actifs (voir également PR.AC-4).

L'organisation doit désactiver les fonctions, ports, protocoles et services définis au sein de ses systèmes critiques qu'il juge inutiles.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit mettre en œuvre des mesures de protection techniques pour appliquer une politique de refus de tout, d'autorisation par exception, afin de n'autoriser que l'exécution des programmes logiciels autorisés.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## PR.PT-4 Les réseaux de communication et de contrôle sont protégés.

Des filtres web et e-mail doivent être installés et utilisés.

### Orientation

- Il convient que les filtres de messagerie détectent les courriers électroniques malveillants et il convient que le filtrage soit configuré en fonction du type de pièces jointes des messages afin que les fichiers des types spécifiés soient automatiquement traités (par exemple, supprimés).
- Il convient que les filtres Web avertissent l'utilisateur si un site Web est susceptible de contenir des logiciels malveillants et empêcher potentiellement les utilisateurs d'accéder à ce site.

**L'organisation doit maîtriser les flux d'informations/de données au sein de ses systèmes critiques et entre les systèmes interconnectés.**

### Orientation

Considérez ce qui suit :

- Le flux d'informations peut être facilité, par exemple, par l'étiquetage ou la coloration des connecteurs physiques pour faciliter le branchement manuel.
- L'inspection du contenu des messages peut permettre d'appliquer la politique de circulation des informations. Par exemple, un message contenant une commande à un actionneur peut ne pas être autorisé à circuler entre le réseau de contrôle et tout autre réseau.
- Les adresses physiques (par exemple, un port série) peuvent être implicitement ou explicitement associées à des étiquettes ou à des attributs (par exemple, une adresse d'I/O hardware). Les méthodes manuelles sont généralement statiques. Les mécanismes de politique d'étiquettes ou d'attributs peuvent être mis en œuvre dans le matériel, les microprogrammes et les logiciels qui contrôlent ou ont accès aux dispositifs, tels que les drivers et les contrôleurs de communications.

**L'organisation doit gérer l'interface pour les services de communication externe en établissant une politique de flux de trafic, protégeant la confidentialité et l'intégrité des informations transmises ; cela inclut l'examen et la documentation de chaque exception à la politique de flux de trafic.**

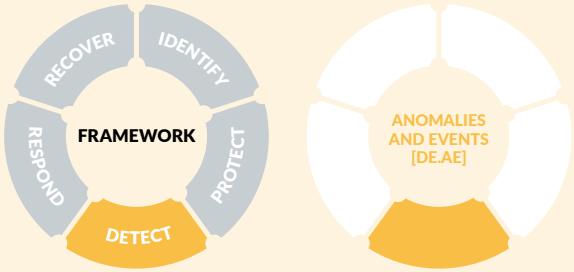
### Orientation

Aucune Orientation supplémentaire sur ce sujet.


WARNING!
SYSTEM WARNING

# DÉTECTER

# Detect




Les activités anormales sont détectées et l'impact potentiel des événements est compris.

## DE.AE-1 Une base de référence des opérations du réseau et des flux de données attendus pour les utilisateurs et les systèmes est établie et gérée.

L'organisation doit s'assurer qu'une base de référence des opérations du réseau et des flux de données attendus pour ses systèmes critiques est développée, documentée et maintenue pour suivre les événements.

### Orientation

- Envisagez d'activer l'enregistrement local sur tous vos systèmes et périphériques réseau et conservez-les pendant une certaine période, par exemple jusqu'à 6 mois.
- Assurez-vous que vos logs contiennent suffisamment d'informations (source, date, utilisateur, horodatage, etc.) et que vous disposez d'un espace de stockage suffisant pour leur génération.
- Envisagez de centraliser vos logs.
- Envisagez le déploiement d'un outil de gestion des informations et des événements de sécurité (SIEM) qui facilitera la corrélation et l'analyse de vos données.

## DE.AE-2 Les événements détectés sont analysés pour comprendre les cibles et les méthodes d'attaque.

L'organisation doit examiner et analyser les événements détectés pour comprendre les cibles et les méthodes d'attaque.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit mettre en œuvre des mécanismes automatisés, lorsque cela est possible, pour examiner et analyser les événements détectés.

### Orientation

Pensez à examiner régulièrement vos logs pour identifier les anomalies ou les événements anormaux.

## DE.AE-3 Les données d'événements sont collectées et corrélées à partir de sources et de capteurs multiples.

**La fonctionnalité d'enregistrement de l'activité du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les anti-virus) doit être activée, sauvegardée et examinée.**

### Orientation

- Il convient que les logs soient sauvegardés et conservés pendant une période prédéfinie.
- Il convient que les logs soient examinés pour déceler toute tendance inhabituelle ou indésirable, telle qu'une utilisation importante des sites Web de médias sociaux ou un nombre inhabituel de virus trouvés régulièrement sur un ordinateur particulier. Ces tendances peuvent indiquer un problème plus grave ou signaler la nécessité de renforcer les protections dans un domaine particulier.

**L'organisation doit s'assurer que les données relatives aux événements sont compilées et corrélées dans l'ensemble de ses systèmes critiques en utilisant diverses sources telles que les rapports d'événements, la surveillance des audits, la surveillance du réseau, la surveillance de l'accès physique et les rapports des utilisateurs/administrateurs.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit intégrer l'analyse des événements, lorsque cela est possible, à l'analyse des informations du scannage de vulnérabilité, aux données sur les performances, à la surveillance de ses systèmes critiques et à la surveillance des installations, afin d'améliorer encore la capacité à identifier les activités inappropriées ou inhabituelles.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.AE-4 L’impact des événements est déterminé.

Les impacts négatifs sur les opérations, les actifs et les individus de l'organisation résultant des événements détectés doivent être déterminés et mis en corrélation avec les résultats de l'évaluation des risques.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.AE-5 Les seuils d’alerte des incidents sont établis.

L'organisation doit mettre en œuvre des mécanismes automatisés et des alertes générées par le système pour faciliter la détection des événements et l'identification des seuils d'alerte de sécurité.

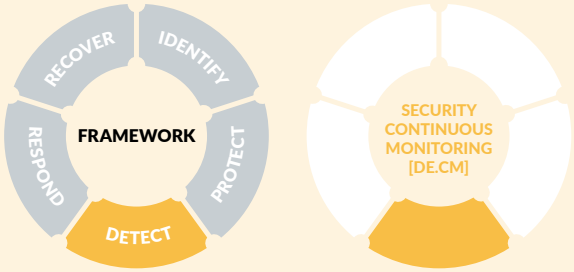
### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit définir des seuils d'alerte d'incidents.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Le système d'information et les actifs sont surveillés pour identifier les événements de cybersécurité et vérifier l'efficacité des mesures de protection.

## DE.CM-1 Le réseau est surveillé pour détecter les événements potentiels de cybersécurité.

**Des pare-feu doivent être installés et exploités aux limites du réseau et complétés par une protection pare-feu sur les terminaux.**

### Orientation

- Les terminaux comprennent les ordinateurs de bureau, les ordinateurs portables, les serveurs...
- Envisagez, dans la mesure du possible, d'inclure les téléphones intelligents et autres appareils en réseau dans l'installation et l'exploitation des pare-feu.
- Envisagez de limiter le nombre de gateways vers internet

**L'organisation doit surveiller et identifier l'utilisation non autorisée de ses systèmes critiques pour l'organisation en détectant les connexions locales, les connexions réseau et les connexions à distance non autorisées.**

### Orientation

- Il convient que la surveillance des communications réseau doit se fasse à la frontière externe des systèmes critiques de l'organisation et aux frontières internes clés des systèmes.
- Lors de l'hébergement d'applications tournées vers l'internet, il convient d'envisager la mise en place d'un pare-feu pour applications web (WAF).

**L'organisation doit effectuer une surveillance permanente de l'état de sécurité de son réseau afin de détecter les événements définis en matière d'information/cybersécurité et les indicateurs d'événements potentiels en matière d'information/cybersécurité.**

### Orientation

Il convient que la surveillance de l'état de la sécurité inclue :

- La génération d'alertes système en cas d'indications de compromission ou de compromission potentielle.
- Détection et signalement de l'utilisation atypique des systèmes critiques de l'organisation.
- L'établissement d'enregistrements d'audit pour des événements définis en matière d'information/cybersécurité.
- Renforcer l'activité de surveillance du système dès qu'il y a une indication d'un risque accru.
- Environnement physique, personnel et fournisseur de services.

**L'environnement physique de l'installation doit être surveillé pour détecter les événements potentiels liés à l'information et à la cybersécurité.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.CM-2 L'environnement physique est surveillé pour détecter les événements potentiels de cybersécurité.

**En plus de la surveillance de l'accès physique à l'installation, l'accès physique aux systèmes et dispositifs critiques de l'organisation doit être renforcé par des alarmes d'intrusion physique, des équipements de surveillance et des équipes de surveillance indépendantes.**

### Orientation

Il est recommandé d'enregistrer tous les visiteurs.

## DE.CM-3 L'activité du personnel est surveillée pour détecter les événements potentiels de cybersécurité.

**Des outils de protection des terminaux et des réseaux permettant de surveiller le comportement de l'utilisateur final pour détecter toute activité dangereuse doivent être mis en œuvre.**

### Orientation

Envisagez le déploiement d'un système de détection/prévention des intrusions (IDS/IPS).

**Les outils de protection des terminaux et des réseaux qui surveillent le comportement de l'utilisateur final pour détecter toute activité dangereuse doivent être gérés.**

### Orientation

- Envisagez l'utilisation d'une plateforme centralisée pour la consolidation et l'exploitation des fichiers de logs.
- Envisagez d'examiner activement les alertes générées par des activités suspectes et prenez les mesures appropriées pour remédier à la menace, par exemple en déployant un centre opérationnel de sécurité (SOC).

**Les restrictions d'utilisation et d'installation des logiciels sont appliqués.**

### Orientation

Il convient que seuls les logiciels autorisés soient utilisés, et que les droits d'accès des utilisateurs soient limités aux données, ressources et applications spécifiques nécessaires pour accomplir une tâche requise (principe du moindre privilège).

## DE.CM-4 Le code malveillant est détecté.

**Des programmes anti-virus, anti-spyware et autres programmes malveillants doivent être installés et mis à jour.**

### Orientation

- Les logiciels malveillants comprennent les virus, les logiciels espions et les ransomwares et il convient qu'ils soient combattus par l'installation, l'utilisation et la mise à jour régulière de logiciels antivirus et anti logiciels espions sur chaque appareil utilisé dans le cadre des activités de l'organisation (y compris les ordinateurs, les smartphones, les tablettes et les serveurs).
- Il convient que les logiciels antivirus et anti logiciels espions recherchent automatiquement les mises à jour en "temps réel" ou au moins quotidiennement, puis procèdent à une analyse du système, le cas échéant.
- Il convient de fournir les mêmes mécanismes de protection contre les codes malveillants pour les ordinateurs à domicile (télétravail, par exemple) ou les appareils personnels utilisés pour le travail professionnel (BYOD).

**L'organisation doit mettre en place un système de détection des faux positifs lors de la détection et de l'éradication des codes malveillants.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.CM-5 Un code mobile non autorisé est détecté.

**L'organisation doit définir le code mobile et les technologies de code mobile acceptables et inacceptables ; et autoriser, surveiller et contrôler l'utilisation du code mobile au sein du système.**

### Orientation

- Le code mobile comprend tout programme, application ou contenu qui peut être transmis sur un réseau (par exemple, intégré dans un courrier électronique, un document ou un site web) et exécuté sur un système distant. Les technologies de code mobile comprennent par exemple les applets Java, JavaScript, HTML5, WebGL et VBScript.
- Il convient que les décisions concernant l'utilisation du code mobile dans les systèmes organisationnels soient fondées sur le potentiel du code à causer des dommages aux systèmes en cas d'utilisation malveillante. Il convient que des restrictions d'utilisation et des conseils de mise en œuvre s'appliquent à la sélection et à l'utilisation du code mobile installé.

## DE.CM-6 L'activité des prestataires de services externes est surveillée pour détecter les événements potentiels de cybersécurité.

**Toutes les connexions externes des fournisseurs qui prennent en charge des applications ou des infrastructures IT/OT doivent être sécurisées et surveillées activement afin de garantir que seules des actions autorisées se produisent pendant la connexion.**

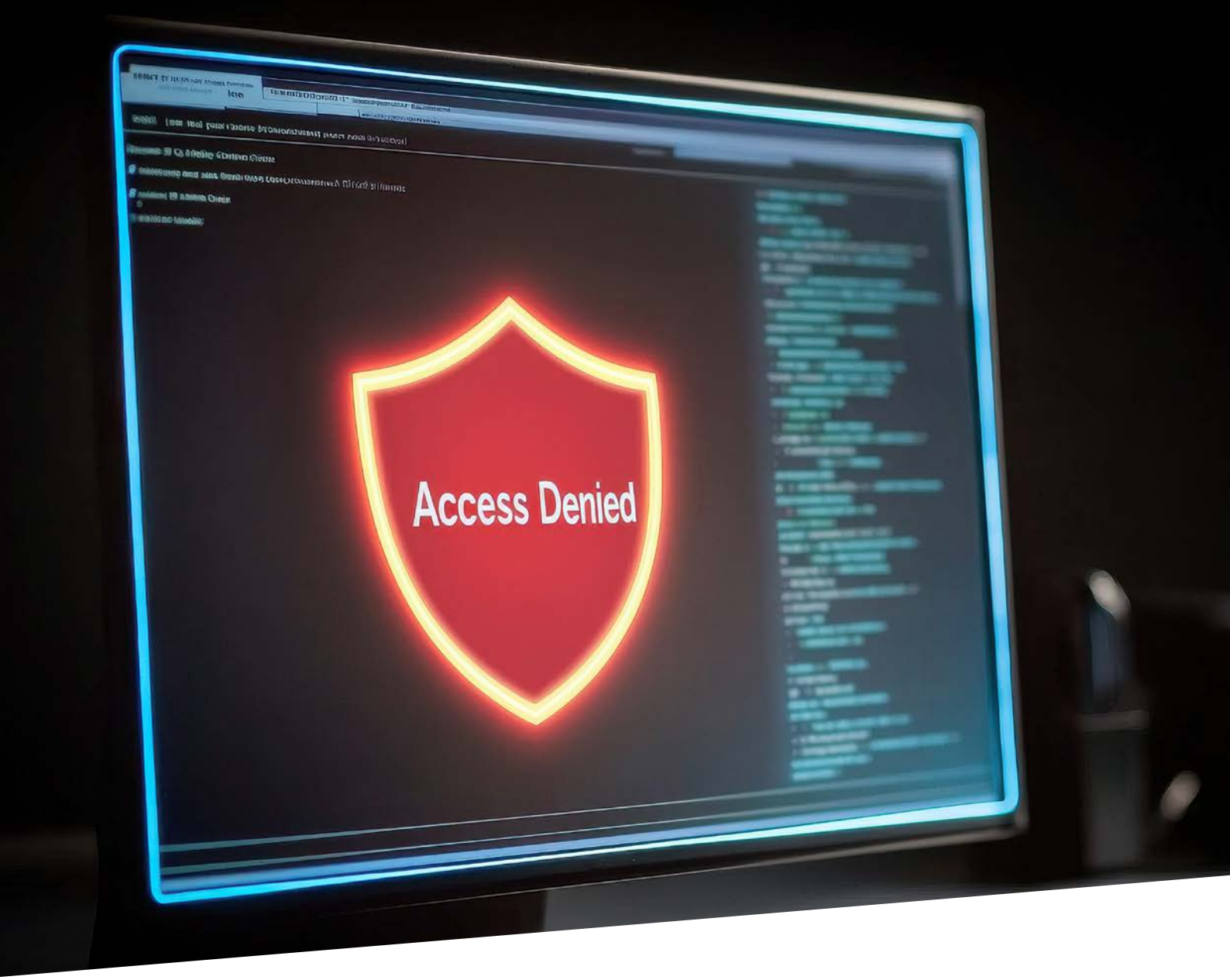
### Orientation

Cette surveillance comprend l'accès du personnel non autorisé, les connexions, les dispositifs et les logiciels.

**La conformité des prestataires de services externes aux politiques et procédures de sécurité du personnel et aux exigences de sécurité contractuelles est contrôlée par rapport aux risques de cybersécurité qu'ils présentent.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




## DE.CM-7 La surveillance du personnel, des connexions, des dispositifs et des logiciels non autorisés est effectuée.

Les systèmes essentiels aux opérations de l'organisation doivent être surveillés pour détecter les accès, les connexions, les dispositifs, les points d'accès et les logiciels non autorisés par le personnel.

### Orientation

- L'accès par du personnel non autorisé comprend l'accès par des prestataires de services externes.
- Il convient d'inclure dans le suivi les écarts d'inventaire du système.
- Il convient que les changements de configuration non autorisés des systèmes critiques de l'organisation soient inclus dans la surveillance.

Les modifications non autorisées de la configuration des systèmes de l'organisation doivent être surveillées et traitées par des mesures d'atténuation appropriées.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.CM-8 Les analyses de vulnérabilité sont effectuées.

L'organisation doit surveiller et analyser les vulnérabilités de ses systèmes critiques et de ses applications hébergées en veillant à ce que les fonctions du système ne soient pas affectées par le processus d'analyse.

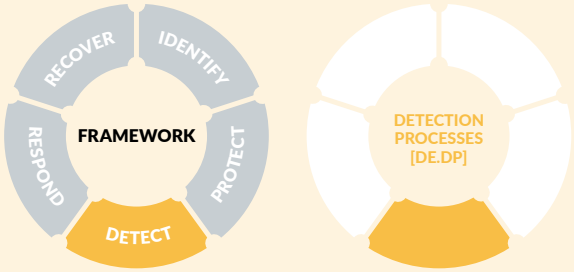
### Orientation

Envisagez la mise en œuvre d'un programme de scannage continu des vulnérabilités ; y compris les rapports et les plans d'atténuation.

Le processus d'analyse de la vulnérabilité comprend l'analyse, la correction et le partage des informations.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Les processus et procédures de détection sont maintenus et testés pour garantir la prise de conscience des événements anormaux.

## DE.DP-2 Les activités de détection sont conformes à toutes les exigences applicables.

L'organisation doit mener des activités de détection conformément aux lois fédérales et régionales, aux réglementations et normes industrielles, aux politiques et aux autres exigences applicables.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## DE.DP-3 Les processus de détection sont testés.

L'organisation doit valider que les processus de détection des événements fonctionnent comme prévu.

### Orientation

- La validation comprend des tests.
- Il convient de pouvoir démontrer la validation.

## DE.DP-4 Les informations relatives à la détection des événements sont communiquées.

**L'organisation doit communiquer les informations relatives à la détection des événements aux parties prédéfinies.**

### Orientation

Les informations de détection d'événements comprennent, par exemple, des alertes sur l'utilisation atypique d'un compte, l'accès à distance non autorisé, la connectivité sans fil, la connexion d'un dispositif mobile, la modification des paramètres de configuration, l'inventaire contrasté des composants du système, l'utilisation d'outils de maintenance et la maintenance non locale, l'accès physique, la température et l'humidité, la livraison et le retrait d'équipements, les communications aux frontières du système d'information, l'utilisation d'un code mobile, l'utilisation de la voix sur IP (VoIP) et la divulgation de logiciels malveillants.

## DE.DP-5 Les processus de détection sont améliorés en permanence.

**Les améliorations découlant de la surveillance, de la mesure, de l'évaluation, des tests, de l'examen et des enseignements tirés seront incorporées dans les révisions du processus de détection.**

### Orientation

- Il en résulte une amélioration continue des processus de détection.
- Le recours à des équipes indépendantes pour évaluer le processus de détection pourrait être envisagé.

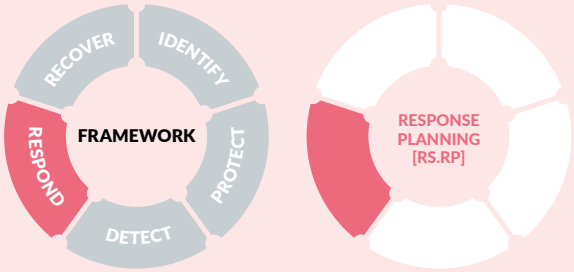
**L'organisation doit effectuer des évaluations spécialisées, notamment une surveillance approfondie, un scannage de vulnérabilité, des tests d'utilisateurs malveillants, une évaluation de la menace interne, des tests de performance/charge, ainsi que des tests de vérification et de validation sur les systèmes critiques de l'organisation.**

### Orientation

Ces activités peuvent être externalisées, de préférence auprès d'organisations accrédités.

# RÉPONDRE

# Respond



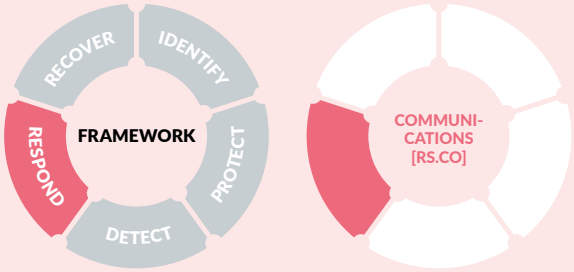

Les processus et procédures de réponse sont exécutés et maintenus, afin de garantir une réponse aux incidents de cybersécurité détectés.

## RS.RP-1 Le plan de réponse est exécuté pendant ou après un incident.

**Un processus de réponse aux incidents, comprenant les rôles, les responsabilités et les pouvoirs, doit être exécuté pendant ou après un événement lié à l'information ou à la cybersécurité sur les systèmes critiques de l'organisation.**

### Orientation

- Il convient que le processus de réponse aux incidents inclue un ensemble prédéterminé d'instructions ou de procédures pour détecter, répondre et limiter les conséquences d'une cyber-attaque malveillante.
- Il convient que les rôles, les responsabilités et les pouvoirs prévus dans le plan de réponse aux incidents soient précis quant aux personnes impliquées, leurs coordonnées, leurs différents rôles et responsabilités, à la personne qui prend la décision de lancer les procédures de rétablissement et à celle qui sera le contact avec les parties prenantes externes appropriées.
- Il convient d'envisager de déterminer les causes d'un événement de sécurité de l'information/cybersécurité et de mettre en œuvre une action corrective afin que l'événement ne se reproduise plus ou ne se produise pas ailleurs (une infection par un code malveillant sur une machine ne s'est pas propagée ailleurs dans le réseau). Il convient que l'efficacité de toute mesure corrective prise soit examinée. Il convient que les actions correctives soient adaptées aux effets de l'événement de sécurité de l'information/cybersécurité rencontré.




Les activités de réponse sont coordonnées avec les parties prenantes internes et externes (par exemple, le soutien externe des forces de l'ordre).

## RS.CO-1 Le personnel connaît ses rôles et l'ordre des opérations lorsqu'une réponse est nécessaire.

L'organisation doit s'assurer que le personnel comprend ses rôles, ses objectifs, les priorités de restauration, les séquences de tâches (ordre des opérations) et les responsabilités d'affectation pour la réponse aux événements.

### Orientation

Envisagez d'utiliser le Guide de gestion des incidents du CCB pour vous guider dans cet exercice et envisagez de faire appel à des experts extérieurs si nécessaire. Testez votre plan régulièrement et ajustez-le après chaque incident.

## RS.CO-2 Les incidents sont signalés conformément aux critères établis.

L'organisation doit mettre en place un système de notification des incidents liés à la sécurité de l'information/cybersécurité sur ses systèmes critiques, dans un délai défini par l'organisation, à l'intention du personnel ou des rôles définis par l'organisation.

### Orientation

Il convient que tous les utilisateurs aient un point de contact unique pour signaler tout incident et soient encouragés à le faire.

Les événements doivent être signalés conformément aux critères établis.

### Orientation

Il convient que les critères de signalement soient inclus dans le plan de réponse aux incidents.

## RS.CO-3 Les informations sont partagées conformément aux plans de réponse.

Les informations relatives aux incidents de cybersécurité doivent être communiquées et partagées avec les employés de l'organisation dans un format qu'ils peuvent comprendre.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit partager les informations relatives aux incidents de cybersécurité avec les parties prenantes concernées, comme prévu dans le plan de réponse aux incidents.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## RS.CO-4 La coordination avec les parties prenantes se fait conformément aux plans de réponse.

L'organisation doit coordonner les actions de réponse aux incidents de sécurité de l'information/cybersécurité avec toutes les parties prenantes prédéfinies.

### Orientation

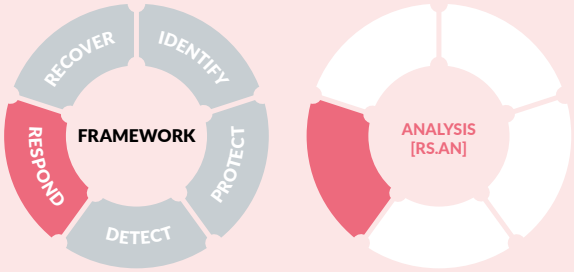
- Les parties prenantes de la réponse aux incidents comprennent par exemple les gestionnaires de la mission/de l'activité, les gestionnaires des systèmes critiques de l'organisation, les intégrateurs, les fournisseurs, les bureaux des ressources humaines, les bureaux de la sécurité physique et du personnel, les services juridiques, le personnel des opérations et les bureaux des achats.
- La coordination avec les parties prenantes se fait conformément aux plans de réponse aux incidents.

## RS.CO-5 Le partage volontaire d'informations se fait avec des parties prenantes externes afin d'obtenir une meilleure connaissance de la situation en matière de cybersécurité.

L'organisation doit partager volontairement les informations sur les événements de cybersécurité, le cas échéant, avec les parties prenantes externes, les groupes de sécurité de l'industrie... afin de parvenir à une connaissance plus large de la situation en matière d'information et de cybersécurité.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Une analyse est effectuée pour garantir une réponse efficace et soutenir les activités de rétablissement.

## RS.AN-1 Les notifications des systèmes de détection sont examinées.

**L'organisation doit enquêter sur les notifications relatives à l'information/la cybersécurité générées par les systèmes de détection.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit mettre en œuvre des mécanismes automatisés pour faciliter l'enquête et l'analyse des notifications liées à l'information/la cybersécurité.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

## RS.AN-2 L'impact de l'incident est compris.

**Une enquête approfondie et l'analyse des résultats doivent permettre de comprendre toutes les implications de l'incident de sécurité de l'information/cybersécurité.**

### Orientation

- L'analyse des résultats peut consister à déterminer la corrélation entre les informations de l'événement détecté et les résultats des évaluations des risques. De cette façon, on obtient un aperçu de l'impact de l'événement sur l'ensemble de l'organisation.
- Envisager d'inclure la détection des modifications non autorisées de ses systèmes critiques dans ses capacités de réponse aux incidents.

**L'organisation doit mettre en œuvre des mécanismes automatisés pour soutenir l'analyse de l'impact des incidents.**

### Orientation

La mise en œuvre peut aller d'un système de billetterie à un système de gestion des informations et des événements de sécurité (SIEM).

## RS.AN-3 L'analyse forensique est réalisée.

**L'organisation doit fournir un examen, une analyse et un rapport d'audit à la demande pour les enquêtes après coup sur les incidents liés à l'information et à la cybersécurité.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.

**L'organisation doit effectuer une analyse forensique des informations collectées/des informations sur les événements de cybersécurité afin de déterminer la cause d'origine.**

### Orientation

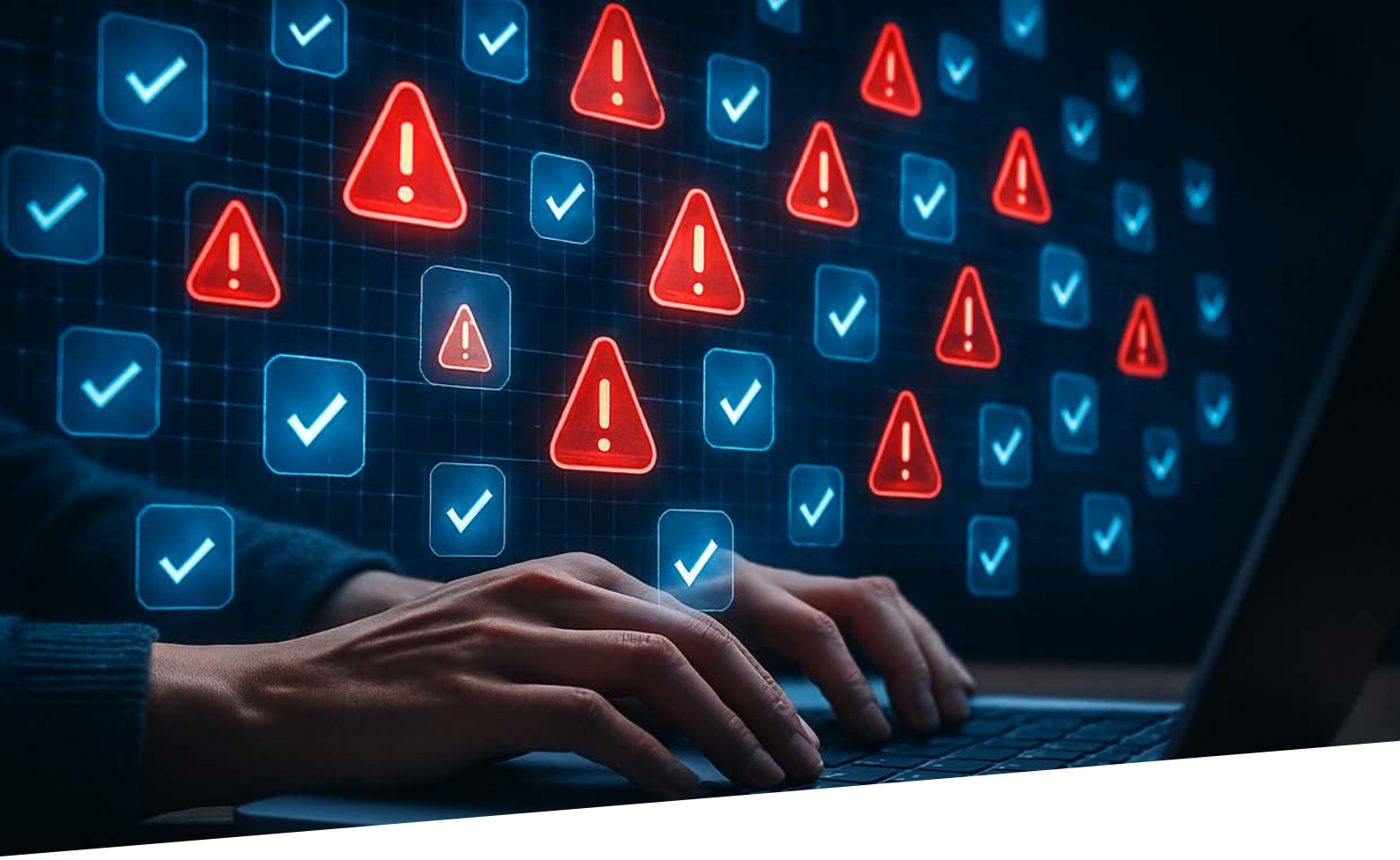
Envisagez de déterminer la cause d'origine d'un incident. Si nécessaire, utilisez l'analyse forensique des informations recueillies/des informations sur les événements de cybersécurité pour y parvenir.

## RS.AN-4 Les incidents sont classés par catégories conformément aux plans de réponse.

**Les incidents liés à l'information et à la cybersécurité sont classés en fonction de leur niveau de gravité et de leur impact, conformément aux critères d'évaluation inclus dans le plan de réponse aux incidents.**

### Orientation

- Il convient d'envisager de déterminer les causes d'un incident de sécurité de l'information/cybersécurité et de mettre en œuvre une action corrective afin que l'incident ne se reproduise plus ou ne se reproduise pas ailleurs.
- Il convient que l'efficacité de toute mesure corrective prise soit examinée.
- Il convient que les actions correctives soient adaptées aux effets de l'incident de sécurité de l'information/cybersécurité rencontré.



## RS.AN-5 Des processus sont établis pour recevoir, analyser et répondre aux vulnérabilités divulguées à l'organisation par des sources internes et externes (par exemple, tests internes, bulletins de sécurité ou chercheurs en sécurité).

L'organisation doit mettre en œuvre des processus et des procédures de gestion des vulnérabilités qui comprennent le traitement, l'analyse et la correction des vulnérabilités provenant de sources internes et externes.

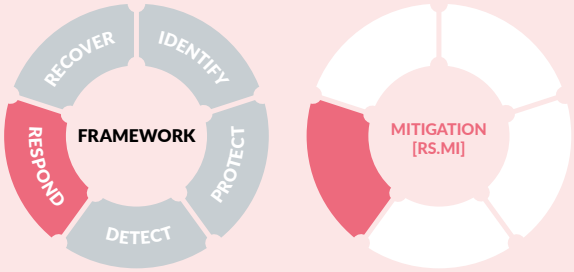
### Orientation

Aucune Orientation supplémentaire sur ce sujet.

L'organisation doit mettre en place des mécanismes automatisés pour diffuser et suivre les efforts de remédiation pour les informations de vulnérabilités, capturées à partir de sources internes et externes, auprès des principales parties prenantes.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.



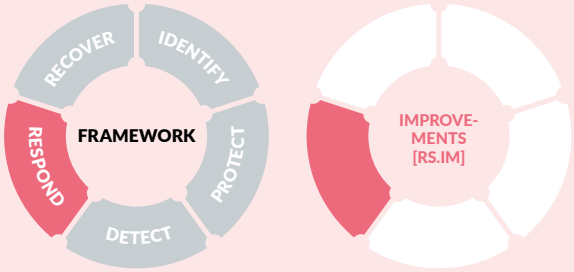

Les activités de réponse de l'organisation sont améliorées par l'intégration des enseignements tirés des activités de détection/réponse actuelles et précédentes.

## RS.MI-1 Les incidents sont contenus.

**L'organisation doit mettre en œuvre une capacité de traitement des incidents de sécurité de l'information/cybersécurité sur ses systèmes essentiels à l'activité, qui comprend la préparation, la détection et l'analyse, le confinement, l'éradication, le rétablissement et l'acceptation documentée des risques.**

### Orientation

Une acceptation des risques documentée concerne les risques que l'organisation évalue comme non dangereux pour les systèmes critiques de l'organisation et pour lesquels le propriétaire du risque accepte formellement le risque (en relation avec l'appétit de l'organisation pour le risque).




Les activités de réponse de l'organisation sont améliorées par l'intégration des enseignements tirés des activités de détection/réponse actuelles et précédentes.

## RS.IM-1 Les plans de réponse intègrent les leçons apprises.

**L'organisation doit procéder à des évaluations post-incident afin d'analyser les enseignements tirés de la réponse à l'incident et du rétablissement, et par conséquent améliorer les processus/procédures/technologies pour renforcer sa cyber-résilience.**

### Orientation

Envisagez de réunir les personnes concernées après chaque incident et réfléchissez ensemble aux moyens d'améliorer ce qui s'est passé, comment cela s'est passé, comment nous avons réagi, comment cela aurait pu mieux se passer, ce qui devrait être fait pour éviter que cela ne se reproduise, etc.

**Les enseignements tirés du traitement des incidents sont traduits en procédures de traitement des incidents actualisées ou nouvelles qui sont testées, approuvées et enseignées.**

### Orientation

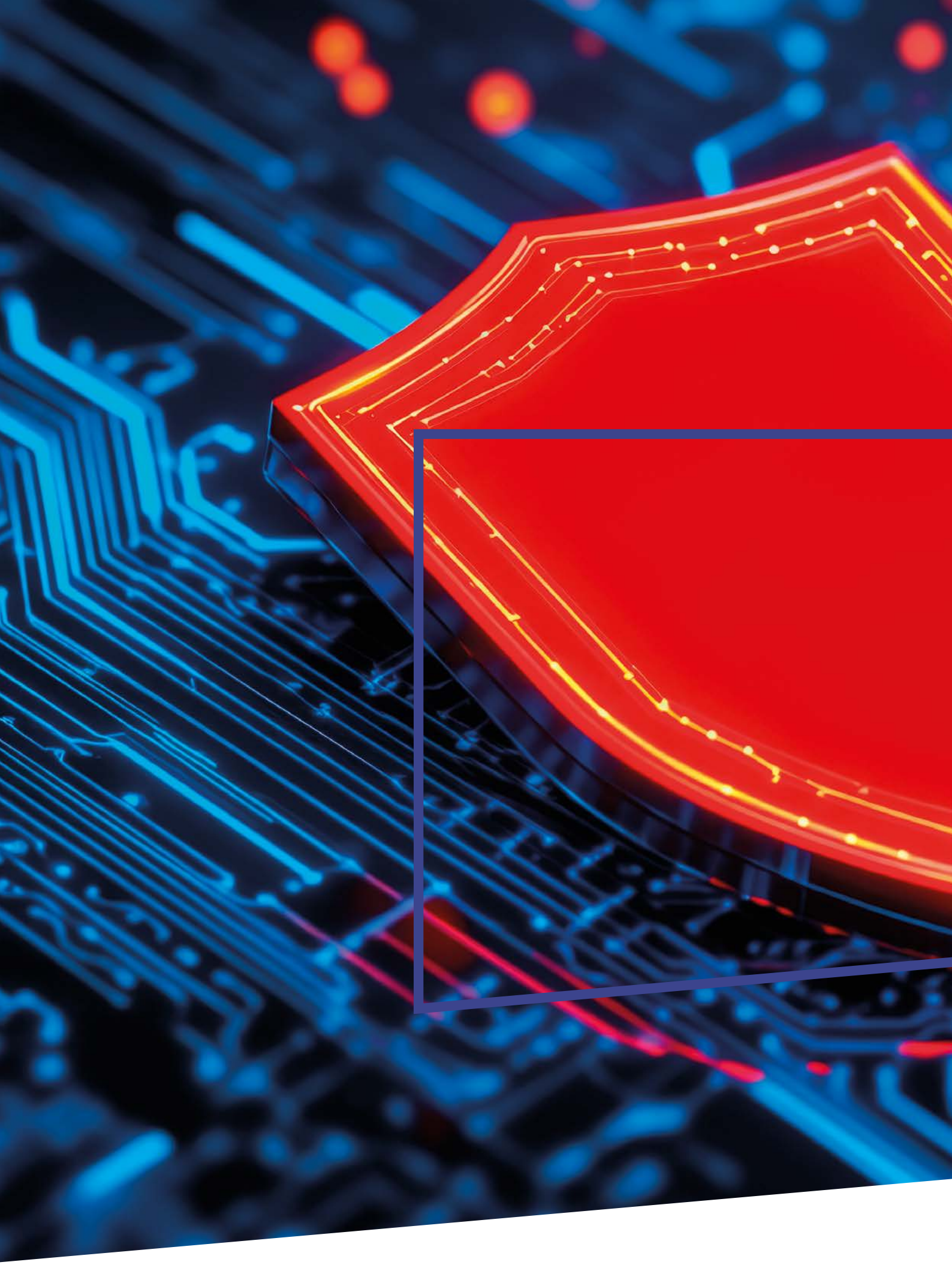
Aucune Orientation supplémentaire sur ce sujet.

## RS.IM-2 Les plans de réponse intègrent les leçons apprises.

**L'organisation doit mettre à jour les plans de réponse et de rétablissement pour tenir compte des changements survenus dans son contexte.**

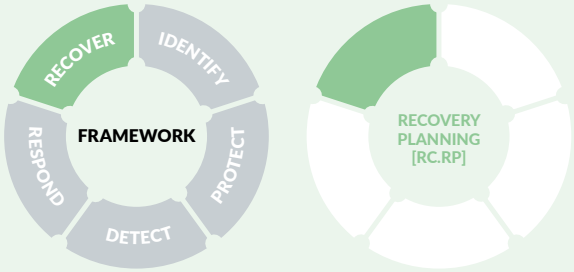
### Orientation

Le contexte de l'organisation concerne la structure organisationnelle, ses systèmes critiques, les vecteurs d'attaque, les nouvelles menaces, les améliorations technologiques, l'environnement d'exploitation, les problèmes rencontrés lors de la mise en œuvre/exécution/test du plan et les enseignements tirés.



# RÉTABLIR

# Recover




Des processus et des procédures de rétablissement sont exécutés et maintenus pour assurer la restauration des systèmes ou des actifs touchés par des incidents de cybersécurité.

## RC.RP-1 Le plan de reprise est exécuté pendant ou après un incident de cybersécurité.

**Un processus de rétablissement en cas de catastrophes et d'incidents liés à l'information et à la cybersécurité est élaboré et exécuté selon les besoins.**

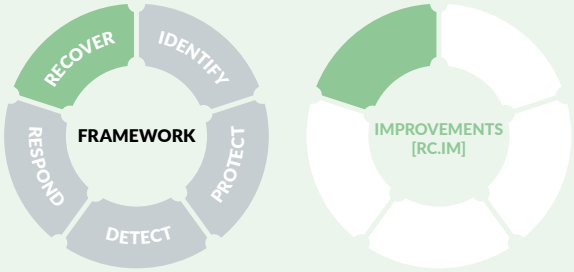
### Orientation

- Il convient qu'un processus soit élaboré pour déterminer les mesures immédiates à prendre en cas d'incendie, d'urgence médicale, de cambriolage, de catastrophe naturelle ou d'incident de sécurité informatique.
- Il convient de prendre en compte dans le processus :
  - Rôles et responsabilités, y compris qui prend la décision de lancer les procédures de rétablissement et qui sera le contact avec les parties prenantes externes appropriées.
  - Ce qu'il faut faire avec les informations et les systèmes d'information de l'organisation en cas d'incident. Cela comprend l'arrêt ou le verrouillage des ordinateurs, le déplacement vers un site de secours, le retrait physique des documents importants, etc.
  - Qui appeler en cas d'incident.

**Les fonctions et services de l'organisation essentielle doivent être poursuivis avec peu ou pas de perte de continuité opérationnelle et la continuité doit être maintenue jusqu'à la restauration complète du système.**

### Orientation

Aucune Orientation supplémentaire sur ce sujet.




Des processus et des procédures de rétablissement sont améliorés en intégrant les leçons apprises dans les activités futures.

## RC.IM-1 Les plans de rétablissement intègrent les leçons apprises.

L'organisation doit intégrer les enseignements tirés des activités de rétablissement des incidents dans les procédures de rétablissement du système, nouvelles ou mises à jour, et, après les avoir testées, les encadrer par une formation appropriée.

### Orientation

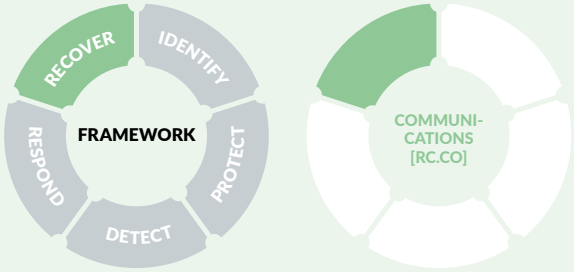
Aucune Orientation supplémentaire sur ce sujet.

## RC.IM-2 Les stratégies de rétablissement sont mises à jour.

Cette exigence est combinée avec RS.IM-2.

### Orientation

Aucune Orientation supplémentaire sur ce sujet.


Les activités de récupération sont coordonnées avec des parties internes et externes (par exemple, les centres de coordination, les fournisseurs d'accès Internet, les propriétaires des systèmes attaquants, les victimes, les autres CSIRT et les fournisseurs).

## RC.CO-1 Les relations publiques sont gérées.

L'organisation doit centraliser et coordonner la manière dont les informations sont diffusées et gérer la manière dont l'organisation est présentée au public.

### Orientation

La gestion des relations publiques peut comprendre, par exemple, la gestion des interactions avec les médias, la coordination et l'enregistrement de toutes les demandes d'interviews, le traitement et le triage des appels téléphoniques et des demandes par e-mail, la mise en relation des demandes des médias avec les experts internes appropriés et disponibles qui sont prêts à être interviewés, le filtrage de toutes les informations fournies aux médias, l'assurance que le personnel connaît bien les politiques en matière de relations publiques et de confidentialité.

Un responsable des relations publiques est désigné.

### Orientation

Il convient que le responsable des relations publiques envisage l'utilisation de contacts externes prédéfinis (par exemple, la presse, les régulateurs, les groupes d'intérêt).

## RC.CO-2 La réputation est réparée après un incident.

L'organisation doit mettre en œuvre une stratégie de réponse aux crises afin de protéger l'organisation des conséquences négatives d'une crise et de contribuer à restaurer sa réputation.

### Orientation

Les stratégies de réponse aux crises comprennent, par exemple, des actions visant à déterminer les attributions de la crise, à modifier les perceptions de l'organisation en crise et à réduire l'effet négatif généré par la crise.

## RC.CO-3 Les activités de rétablissement sont communiquées aux parties prenantes internes et externes, ainsi qu'aux équipes de direction et de gestion.

L'organisation doit communiquer les activités de rétablissement aux parties prenantes prédéfinies, aux équipes de direction et de gestion.

### Orientation

La communication des activités de rétablissement à toutes les parties prenantes concernées ne s'applique qu'aux entités soumises à la législation NIS.

# ANNEXE

# ANNEXE A : LISTE DES MESURES CLÉS POUR LE NIVEAU D'ASSURANCE «BASIC».

## PROTÉGER

**PR.AC-1 Les identités et les identifiants sont émis, gérés, vérifiés, révoqués et audités pour les dispositifs, les utilisateurs et les processus autorisés.**

(1) Les identités et les identifiants des dispositifs et des utilisateurs autorisés doivent être gérés.

**PR.AC-3 L'accès à distance est géré.**

(2) Les réseaux de l'organisation auxquels on accède à distance doivent être sécurisés, notamment par une authentification multifactorielle (MFA).

**PR.AC-4 Les permissions et les autorisations d'accès sont gérées en intégrant les principes du moindre privilège et de la séparation des tâches.**

(3) Les autorisations d'accès des utilisateurs aux systèmes de l'organisation doivent être définies et gérées.

(4) Il convient d'identifier qui doit avoir accès aux informations et aux technologies critiques de l'organisation et les moyens d'y accéder.

(5) L' accès des employés aux données et aux informations est limité aux systèmes et aux informations spécifiques dont ils ont besoin pour faire leur travail.

(6) Personne ne doit avoir de privilèges d'administrateur pour les tâches quotidiennes.

**PR.AC-5 L'intégrité du réseau est protégée (par exemple, séparation du réseau, segmentation du réseau).**

(7) Des pare-feu doivent être installés et activés sur tous les réseaux de l'organisation.

(8) Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par l'intégration de la segmentation et de la ségrégation du réseau.

**PR.IP-4 Des sauvegardes des informations sont effectuées, maintenues et testées.**

(9) Les sauvegardes des données critiques de l'organisation doivent être effectuées et stockées sur un système différent du dispositif sur lequel résident les données originales.

**PR.MA-1** L'entretien et la réparation des actifs de l'organisation sont effectués et consignés, avec des outils approuvés et contrôlés.

(10) Les correctifs et les mises à jour de sécurité pour les systèmes d'exploitation et les composants critiques du système doivent être installés.

**PR.PT-1** Les enregistrements d'audit/logs sont déterminés, documentés, mis en œuvre et revus conformément à la politique.

(11) Les logs doivent être tenus, documentés et examinés.

## DÉTECTER

**DE.AE-3** Les données d'événements sont collectées et corrélées à partir de sources et de capteurs multiples.

(12) La fonctionnalité d'enregistrement des activités du matériel ou du logiciel de protection/détection (par exemple, les pare-feu, les antivirus) doit être activée, sauvegardée et examinée.

**DE.CM-4** Un code malveillant est détecté.

(13) Les programmes anti-virus, anti-spyware et autres programmes malveillants doivent être installés et mis à jour.

# ANNEXE B : LISTE DES MESURES CLÉS SUPPLÉMENTAIRES POUR LE NIVEAU D'ASSURANCE «IMPORTANT» ET «ESSENTIEL».

La liste ci-dessous s'**ajoute** aux mesures clés du niveau d'assurance «Basic».

## IDENTIFIER

**ID.AM-6 Les rôles, responsabilités et pouvoirs en matière de cybersécurité pour l'ensemble du personnel et les parties prenantes tierces sont établis.**

(1) Les rôles, les responsabilités et les pouvoirs en matière de sécurité de l'information et de cybersécurité au sein de l'organisation sont documentés, examinés, autorisés et mis à jour, et alignés sur les rôles internes de l'organisation et les partenaires externes.

## PROTÉGER

**PR.AC-3 L'accès à distance est géré.**

(2) Les restrictions d'utilisation, les exigences de connexion, les conseils de mise en œuvre et les autorisations d'accès à distance à l'environnement des systèmes critiques de l'organisation doivent être identifiés, documentés et mis en œuvre.

**PR.AC-5 L'intégrité du réseau est protégée (par exemple, séparation du réseau, segmentation du réseau).**

(3) Le cas échéant, l'intégrité du réseau des systèmes critiques de l'organisation doit être protégée par (1) l'identification, la documentation et le contrôle des connexions entre les composants du système et (2) la limitation des connexions externes aux systèmes critiques de l'organisation.

(4) L'organisation doit surveiller et contrôler les connexions et les communications à la frontière externe et aux principales frontières internes des systèmes critiques de l'organisation en mettant en œuvre des dispositifs de protection des frontières, le cas échéant.

**PR.DS-5 Des protections contre les fuites de données sont mises en place.**

(5) L'organisation doit prendre des mesures appropriées aboutissant à la surveillance de ses systèmes critiques aux frontières extérieures et aux points internes critiques lorsqu'un accès et des activités non autorisés, y compris une fuite de données, sont détectés.

**PR.IP-1** **Une configuration de base des systèmes de contrôle des technologies de l'information/ de l'industrie est créée et maintenue en intégrant les principes de sécurité.**

(6) L'organisation doit développer, documenter et maintenir une configuration de base pour ses systèmes critiques.

## DÉTECTER

**DE.CM-1** **Le réseau est surveillé pour détecter les événements potentiels de cybersécurité.**

(7) L'organisation doit surveiller et identifier l'utilisation non autorisée de ses systèmes critiques pour l'organisation par la détection des connexions locales, des connexions réseau et des connexions à distance non autorisées.

## RÉPONDRE

**RS.AN-5** **Des processus sont établis pour recevoir, analyser et répondre aux vulnérabilités divulguées à l'organisation par des sources internes et externes.**

(8) L'organisation doit mettre en œuvre des processus et des procédures de gestion des vulnérabilités qui comprennent le traitement, l'analyse et la correction des vulnérabilités provenant de sources internes et externes.

# ANNEXE C : LISTE DES MESURES CLÉS SUPPLÉMENTAIRES POUR LE NIVEAU D'ASSURANCE «ESSENTIEL».

La liste ci-dessous s'**ajoute** aux mesures clés du niveau d'assurance «Basic» et «Important».

## IDENTIFIER

**ID.SC-3 Les contrats avec les fournisseurs et les partenaires tiers sont utilisés pour mettre en œuvre des mesures appropriées conçues pour atteindre les objectifs du programme de cybersécurité et du plan de gestion des risques de la chaîne d'approvisionnement de l'organisation.**

(1) Des exigences contractuelles en matière de «sécurité de l'information et de cybersécurité» pour les fournisseurs et les partenaires tiers sont mises en œuvre pour garantir un processus vérifiable de correction des failles et pour garantir la correction des failles identifiées lors des tests et des évaluations de «sécurité de l'information et de cybersécurité».

(2) L'organisation doit établir des exigences contractuelles lui permettant d'examiner les programmes de «sécurité des informations et de cybersécurité» mis en œuvre par les fournisseurs et les partenaires tiers.

## PROTÉGER

**PR.AC-7 Les identités sont prouvées et liées aux identifiants et présentées dans les interactions.**

(3) L'organisation doit effectuer une évaluation des risques documentée sur les transactions des systèmes critiques de l'organisation et authentifier les utilisateurs, les dispositifs et les autres actifs (par exemple, à un ou plusieurs facteurs) en fonction du risque de la transaction (par exemple, les risques pour la sécurité et la vie privée des individus et les autres risques pour l'organisation).

**PR.MA-1 L'entretien et la réparation des actifs de l'organisation sont effectués et consignés, avec des outils approuvés et contrôlés.**

(4) L'organisation doit empêcher le retrait non autorisé des équipements de maintenance contenant des informations critiques sur les systèmes de l'organisation.

(5) Les outils de maintenance et les dispositifs de stockage portables doivent être inspectés lorsqu'ils sont introduits dans l'établissement et doivent être protégés par des solutions anti-malware afin qu'ils soient analysés pour détecter les codes malveillants avant d'être utilisés sur les systèmes de l'organisation.

(6) L'organisation doit vérifier les contrôles de sécurité à la suite de la maintenance ou de la réparation/du correctif du matériel et des logiciels et prendre les mesures qui s'imposent.

**PR.PT-2** **Les supports amovibles sont protégés et leur utilisation est limitée conformément à la politique.**

(7) Les dispositifs de stockage portables contenant des données système doivent être contrôlés et protégés pendant leur transport et leur stockage.

## DÉTECTER

**DE.AE-1** **Une base de référence des opérations du réseau et des flux de données attendus pour les utilisateurs et les systèmes est établie et gérée.**

(8) L'organisation doit s'assurer qu'une base de référence des opérations du réseau et des flux de données attendus pour ses systèmes critiques est développée, documentée et maintenue pour suivre les événements.

## Avis de non-responsabilité

Le présent document et ses annexes ont été élaborés par le Centre pour la Cybersécurité de Belgique (CCB), une administration fédérale créée par l'arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.



Ce document contient des informations techniques rédigées principalement en français. Ces informations concernent la sécurité des réseaux et des systèmes d'information s'adresse aux services informatiques et peuvent utiliser des termes anglais du langage informatique. Une traduction en anglais, néerlandais et allemand de ces informations techniques sont également rendu accessible par le CCB.

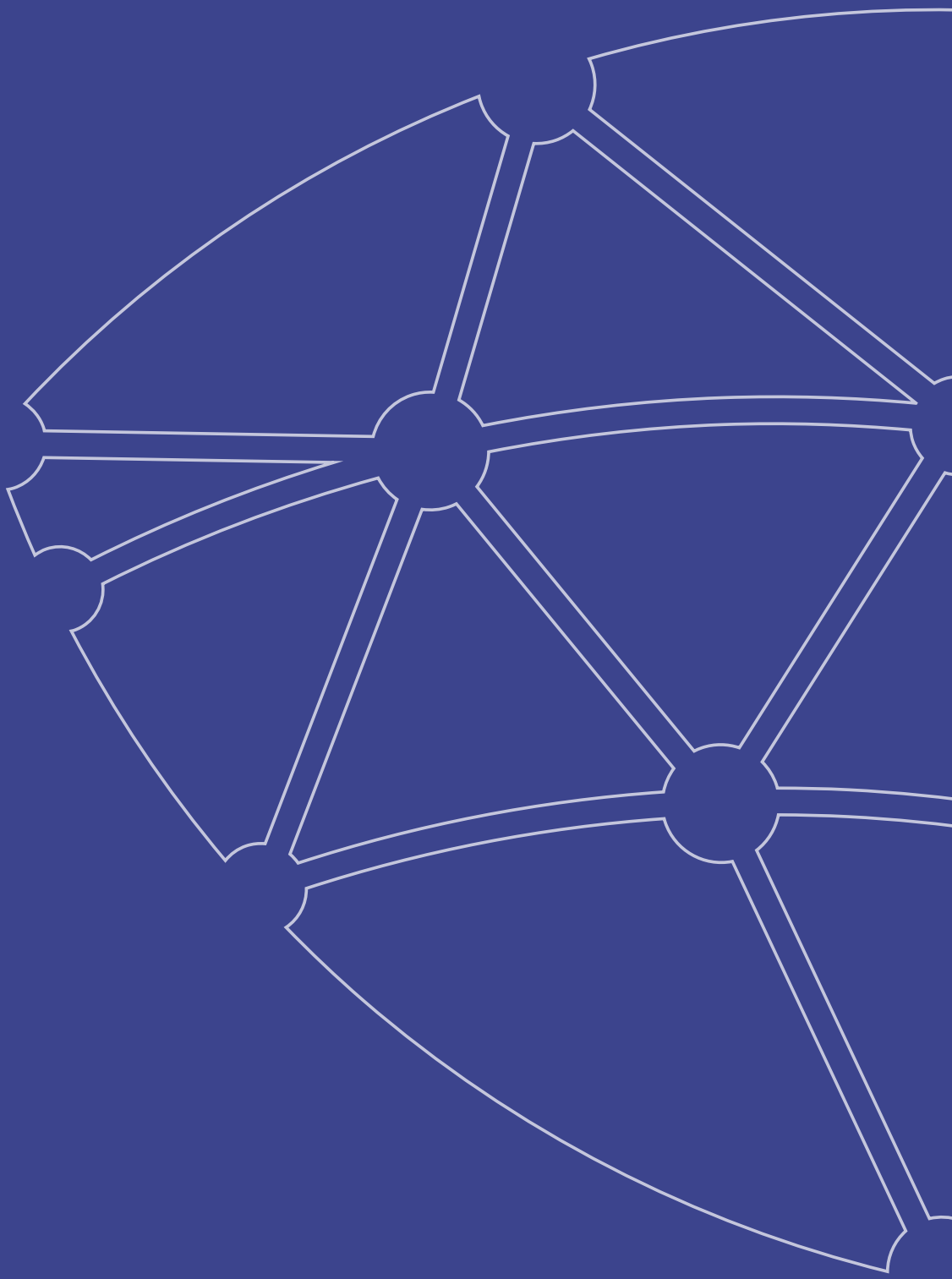
Le CCB n'accepte **aucune responsabilité quant au contenu** de ce document.
Les informations fournies :

- sont exclusivement de nature générale et ne visent pas à prendre en considération toutes les situations particulières.
- ne sont pas nécessairement exhaustives, précises ou à jour sur tous les points.

**Rédacteur responsable**

Centre pour la Cybersécurité de Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18
1000 Bruxelles

**Dépôt légal**
D/2023/14828/001



Centre pour la Cybersécurité Belgique

Rue de la Loi, 18

1000, Bruxelles