Cadre pour l'amélioration de la Cybersécurité des infrastructures critiques

Version 1.1

Institut national des normes et de la technologie

16 avril 2018

https://doi.org/10.6028/NIST.CSWP.04162018fr

Traduit par / Translated by

Bachir Benyammi (https://www.linkedin.com/in/bachirbenyammi/)

Translated by Bachir Benyammi. Reviewed by Diplomatic Language Services. Official U.S. Government Translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.04162018.

Note aux lecteurs sur la mise à jour

La version 1.1 de ce cadre de cybersécurité affine, clarifie et améliore la version 1.0, qui a été publiée en février 2014. Elle intègre les commentaires reçus sur les deux brouillons de la version 1.1.

La version 1.1 est destinée à être implémentée par les utilisateurs novices et actuels du cadre. Les utilisateurs actuels devraient être en mesure de mettre en œuvre la version 1.1 avec une perturbation minimale ou nulle; la compatibilité avec la version 1.0 a été un objectif explicite.

Le tableau suivant résume les modifications apportées entre la version 1.0 et la version 1.1.

Tableau NTR-1 - Résumé des changements entre la version 1.0 et la version 1.1 du cadre.

Mise à jour	Description de la mise à jour
Clarification du fait que des termes tels que "conformité" peuvent prêter à confusion et signifier quelque chose de très différent pour diverses parties prenantes du cadre	Plus de clarté sur le fait que le cadre a une utilité en tant que structure et langage pour organiser et exprimer la conformité avec les propres exigences de cybersécurité d'une organisation. Cependant, la variété des manières dont le cadre peut être utilisé par une organisation signifie que des expressions telles que "conformité au cadre" peuvent prêter à confusion.
Une nouvelle section sur l'auto-appréciation	Ajout de la section 4.0 *auto-appréciation du risque de cybersécurité avec le cadre* pour expliquer comment le cadre peut être utilisé par les organisations pour comprendre et apprécier leur risque de cybersécurité, y compris l'utilisation de mesurages.
Explication très détaillée de l'utilisation du cadre à des fins de gestion des risques de la cyber chaîne d'approvisionnement	Une section étendue 3.3 sur la c*ommunication des exigences de cybersécurité avec les parties prenantes* aide les utilisateurs à mieux comprendre la gestion des risques de la cyber chaîne d'approvisionnement (SCRM), tandis qu'une nouvelle section 3.4 décisions d'achat met en évidence l'utilisation du cadre pour comprendre les risques associés aux produits et services commerciaux prêts à l'emploi. Des critères SCRM cybernétiques supplémentaires ont été ajoutés aux niveaux de mise en œuvre. Enfin, une catégorie de gestion des risques de la chaîne d'approvisionnement, comprenant plusieurs sous-catégories, a été ajoutée au noyau du cadre.
Améliorations pour mieux prendre en compte l'authentification, l'autorisation et la preuve d'identité	Le langage de la catégorie de contrôle d'accès a été affinée pour mieux prendre en compte l'authentification, l'autorisation et la preuve d'identité. Cela comprenait l'ajout d'une sous-catégorie pour l'authentification et la vérification d'identité. De plus, la catégorie a été renommée en gestion des identités et contrôle d'accès (PR.AC) afin de mieux représenter la portée de la catégorie et des sous-catégories correspondantes.

Meilleure explication de la relation entre les niveaux de mise en œuvre et les profiles	Ajout d'un langage à la section 3.2 *établissement ou amélioration d'un Programme de cybersécurité* sur l'utilisation des niveaux du cadre dans la mise en œuvre du cadre. Ajout d'un langage aux niveaux du cadre pour refléter l'intégration des considérations du cadre dans les programmes de gestion des risques organisationnels. Les concepts du niveau du cadre ont également été affinés. Mise à jour de la figure 2.0 pour inclure les actions des niveaux du cadre.
Considération de la divulgation coordonnée des vulnérabilités	Une sous-catégorie liée au cycle de vie de la divulgation des vulnérabilités a été ajoutée.

Comme pour la version 1.0, les utilisateurs de la version 1.1 sont encouragés à personnaliser le cadre pour maximiser la valeur organisationnelle individuelle.

Remerciements

Cette publication est le résultat d'un effort de collaboration continu impliquant l'industrie, le milieu universitaire et le gouvernement. L'institut national des normes et de la technologie (NIST) a lancé le projet en réunissant des organisations et des individus des secteurs privé et public en 2013. Publié en 2014 et révisé en 2017 et 2018, ce *cadre pour l'amélioration de la cybersécurité des infrastructures critiques* s'est appuyé sur huit ateliers publics, de multiples demandes de commentaires ou d'informations et des milliers d'interactions directes avec des parties prenantes de tous les secteurs des États-Unis ainsi que de nombreux secteurs du monde entier.

L'impulsion pour changer la version 1.0 et les changements qui apparaissent dans cette version 1.1 étaient basés sur :

- Commentaires et questions fréquemment posées au NIST depuis la sortie de la version 1,0;
- 105 réponses à la demande d'information (RFI) de décembre 2015, *opinions sur le cadre pour l'amélioration de la cybersécurité des infrastructures critiques*;
- Plus de 85 commentaires en 5 décembre 2017, un deuxième brouillon de la version 1.1 proposé;
- Plus de 120 commentaires en 10 janvier 2017, un premier brouillon de la version 1.1 proposé; et
- Contribution de plus de 1 200 participants aux ateliers du cadre de 2016 et 2017.

En outre, le NIST a précédemment publié la version 1.0 du cadre de cybersécurité avec un document d'accompagnement, *feuille de route du NIST pour l'amélioration de la cybersécurité des infrastructures critiques.* Cette feuille de route a mis en évidence des “domaines d'amélioration” clés pour un développement, un alignement et une collaboration ultérieur. Grâce aux efforts des secteurs privé et public, certains domaines d'amélioration ont avancé pour être inclus dans cette version 1.1 du cadre.

Le NIST reconnaît et remercie tous ceux qui ont contribué à ce cadre.

Sommaire exécutif

Les États-Unis dépendent du fonctionnement fiable des infrastructures critiques. Les menaces de cybersécurité exploitent la complexité et la connectivité accrues des systèmes d'infrastructure critique, mettant en danger la sécurité, l'économie et la sûreté et la santé publique de la nation. Tout comme les risques financiers et de réputation, le risque de cybersécurité affecte les résultats d'une entreprise. Cela peut monter les coûts et affecter les revenus. Cela peut nuire à la capacité d'une organisation à innover et à gagner et conserver des clients. La cybersécurité peut être une composante importante et amplificatrice de la gestion globale des risques d'une organisation.

Pour mieux adresser ces risques, la loi de 2014 sur le renforcement de la cybersécurité[1] (CEA) a mis à jour le rôle de l'institut national des normes et de la technologie (NIST) pour inclure l'identification et le développement de cadres de risque de cybersécurité pour une utilisation volontaire par les propriétaires et les opérateurs d'infrastructures critiques. Grâce au CEA, le NIST doit identifier “une approche prioritisée, flexible, reproductible, basée sur les performances et rentable, y compris des mesures et des contrôles de sécurité de l'information qui peuvent être volontairement adoptés par les propriétaires et les opérateurs d'infrastructures critiques pour les aider à identifier, apprécier et gérer les cyber risques.” Cela a officialisé les travaux antérieurs du NIST sur le développement de la version 1.0 du cadre en vertu du décret exécutif (EO) 13636, “Amélioration de la cybersécurité des infrastructures critiques” (février 2013), et a fourni des orientations pour l'évolution future du cadre. Le cadre qui a été développé en vertu de l'EO 13636, et continue d'évoluer selon le CEA, utilise un langage commun pour adresser et gérer les risques de cybersécurité de manière rentable en fonction des besoins métier et organisationnels sans imposer d'exigences réglementaires supplémentaires aux entreprises.

Le cadre se concentre sur l'utilisation de moteurs métier pour guider les activités de cybersécurité et sur la prise en compte des risques de cybersécurité dans le cadre des processus de gestion des risques de l'organisation. Le cadre se compose de trois parties : le noyau du cadre , les niveaux de mise en œuvre et les profils de cadre. Le noyau du cadre est un ensemble d'activités, de résultats et de références informatives en matière de cybersécurité qui sont communs à tous les secteurs et infrastructures critiques. Les éléments du noyau fournissent des conseils détaillés pour l’élaboration de profils organisationnels individuels. Grâce à l'utilisation de profils, le cadre aidera une organisation à aligner et à prioriser ses activités de cybersécurité avec ses exigences métier/de mission, ses tolérances au risque et ses ressources. Les niveaux fournissent un mécanisme permettant aux organisations de visualiser et de comprendre les caractéristiques de leur approche de la gestion des risques de cybersécurité, ce qui aidera à prioriser et à atteindre les objectifs de cybersécurité.

Bien que ce document ait été élaboré pour améliorer la gestion des risques de cybersécurité dans les infrastructures critiques, le cadre peut être utilisé par des organisations de n'importe quel secteur ou communauté. Le cadre permet aux organisations - quels que soient leur taille, leur degré de risque de cybersécurité ou de sophistication en matière de cybersécurité - d'appliquer les principes et les meilleures pratiques de gestion des risques pour améliorer la sécurité et la résilience.

[1] *Voir* 15 USC § 272 (e) (1) (A) (i). La loi de 2014 sur renforcement de la cybersécurité (S.1353) est devenue loi publique 113274 le 18 décembre 201 4 et peut être consultée à l'adresse : https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Le cadre fournit une structure d'organisation commune pour plusieurs approches de la cybersécurité en assemblant des normes, des lignes directrices et des pratiques qui fonctionnent efficacement aujourd'hui. De plus, parce qu'il fait référence à des normes mondialement reconnues en matière de cybersécurité, le cadre peut servir de modèle pour la coopération internationale sur le renforcement de la cybersécurité dans les infrastructures critiques ainsi que dans d'autres secteurs et communautés.

Le cadre offre un moyen flexible d'adresser la cybersécurité, y compris l'effet de la cybersécurité sur les dimensions physiques, cybernétiques et humaines. Il s'applique aux organisations s'appuyant sur la technologie, que leur cybersécurité se concentre principalement sur les technologies de l'information (TI), les systèmes de contrôle industriel (ICS), les systèmes cyber-physiques (CPS) ou les appareils connectés plus généralement, y compris l'Internet des objets (IoT). Le cadre peut aider les organisations à aborder la cybersécurité car elle affecte la vie privée des clients, des employés et d'autres parties. De plus, les résultats du cadre servent de cibles pour les activités de développement et d'évolution de l'effectif.

Le cadre n'est pas une approche unique pour gérer les risques de cybersécurité pour les infrastructures critiques. Les organisations continueront d'avoir des risques uniques – des menaces différentes, des vulnérabilités différentes, des tolérances au risque différentes. Ils varieront également dans la manière dont ils personnalisent les pratiques décrites dans le cadre. Les organisations peuvent déterminer les activités qui sont importantes pour la prestation de services critiques et peuvent prioriser les investissements pour maximiser l'impact de chaque dollar dépensé. En fin de compte, le cadre vise à réduire et à mieux gérer les risques de cybersécurité.

Pour tenir compte des besoins uniques des organisations en matière de cybersécurité, il existe une grande variété de manières d'utiliser le cadre. La décision sur la manière de l'appliquer est laissée à l'organisation de mise en œuvre. Par exemple, une organisation peut choisir d'utiliser les niveaux de mise en œuvre du cadre pour articuler les pratiques de gestion des risques envisagées. Une autre organisation peut utiliser les cinq fonctions du cadre pour analyser l'ensemble de son portefeuille de gestion des risques ; cette analyse peut s'appuyer ou non sur des conseils complémentaires plus détaillés, tels que des catalogues de contrôles. Il y a parfois des discussions sur la "conformité" avec le cadre, et le cadre a une utilité en tant que structure et langage pour organiser et exprimer la conformité avec les propres exigences de cybersécurité d'une organisation. Néanmoins, la variété des manières dont le cadre peut être utilisé par une organisation signifie que des expressions telles que "conformité avec le cadre" peuvent prêter à confusion et signifier quelque chose de très différent pour diverses parties prenantes.

Le cadre est un document évolutif et continuera d'être mis à jour et amélioré au fur et à mesure que l'industrie fournira des commentaires sur la mise en œuvre. Le NIST continuera à se coordonner avec le secteur privé et les agences gouvernementales à tous les niveaux. Au fur et à mesure que le cadre est mis en pratique, des leçons supplémentaires seront intégrées dans les versions futures. Cela garantira que le cadre répond aux besoins des propriétaires et des opérateurs d'infrastructures critiques dans un environnement dynamique et stimulant de nouvelles menaces, risques et solutions.

Une utilisation et un partage élargis et plus efficaces des meilleures pratiques de ce cadre volontaire sont les prochaines étapes pour améliorer la cybersécurité de l'infrastructure critique de notre nation - en fournissant des orientations évolutives aux organisations individuelles tout

en augmentant la posture de cybersécurité de l'infrastructure critique de la nation et de l'économie et de la société au sens large.

Table des matières

Liste des figures

Liste des tableaux

1.0 Introduction au cadre

Les États-Unis dépendent du fonctionnement fiable de leurs infrastructures critiques. Les menaces de cybersécurité exploitent la complexité et la connectivité accrues des systèmes d'infrastructures critiques, mettant en danger la sécurité, l'économie, et la sécurité et la santé publiques de la nation. Tout comme les risques financiers et de réputation, le risque de cybersécurité affecte les résultats d'une entreprise. Cela peut faire augmenter les coûts et affecter les revenus. Cela peut nuire à la capacité d'une organisation à innover et à gagner et conserver des clients. La cybersécurité peut être une composante importante et amplificatrice de la gestion globale des risques d'une organisation.

Pour renforcer la résilience de cette infrastructure, la loi de 2014 sur le renforcement de la cybersécurité[2] (CEA) a mis à jour le rôle de l'Institut national des normes et de la technologie (NIST) pour "faciliter et soutenir le développement" de cadres de risque de cybersécurité. À travers le CEA, le NIST doit identifier "une approche priorisée, flexible, reproductible, basée sur les performances et rentable, y compris des mesures et des contrôles de sécurité de l'information qui peuvent être volontairement adoptés par les propriétaires et les opérateurs d'infrastructures critiques pour les aider à identifier, apprécier, et gérer les cyber-risques." Cela a officialisé les travaux antérieurs du NIST développant la version 1.0 du cadre en vertu du décret exécutif 13636, "Amélioration de la cybersécurité des infrastructures critiques", publié en février 2013[3] et a fourni des conseils pour l'évolution future du cadre.

L'infrastructure critique[4] est défini dans l'acte patriote American de 2001[5] en tant que "systèmes et actifs, qu'ils soient physiques ou virtuels, si vitaux pour les États-Unis que l'incapacité ou la destruction de ces systèmes et actifs aurait un impact débilitant sur la sécurité, la sécurité économique nationale, la santé ou la sûreté publique nationale, ou tout autre combinaison de ces questions." En raison des pressions croissantes des menaces externes et internes, les organisations responsables des infrastructures critiques doivent adopter une approche cohérente et itérative pour identifier, apprécier et gérer les risques de cybersécurité. Cette approche est nécessaire quelle que soit la taille, l'exposition aux menaces ou la sophistication de la cybersécurité d'une organisation aujourd'hui.

La communauté des infrastructures critiques comprend des propriétaires et opérateurs publics et privés, ainsi que d'autres entités jouant un rôle dans la sécurisation des infrastructures de la nation. Les membres de chaque secteur d'infrastructure critique exécutent des fonctions qui sont prises en charge par la vaste catégorie de technologies, y compris les technologies de l'information (TI), les systèmes de contrôle industriel (ICS), les systèmes cyber-physiques (CPS) et les appareils connectés plus généralement, y compris l'Internet des objets (IoT). Cette

[2] *Voir* 15 USC § 272 (e) (1) (A) (i). La loi de 2014 sur le renforcement de la cybersécurité (S.1353) est devenue loi publique 113274 le 18 décembre 2014 et peut être consultée sur : https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Décret exécutif no. 13636, Amélioration de la cybersécurité des infrastructures critiques, DCPD-201300091, 12 février 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] Le programme d'infrastructure critique du Département de la sécurité intérieure (DHS) fournit une liste des secteurs et de leurs fonctions critiques et chaînes de valeur associées. http://www.dhs.gov/critical-infrastructure-sectors

[5] Voir 42 USC § 5195c (e)). L'acte patriote américain de 2001 (HR3162) est devenu le droit public 107-56 le 26 octobre 2001 et peut être trouvé à : https://www.congress.gov/bill/107th-congress/house-bill/3162

dépendance à l'égard de la technologie, de la communication et de l'interconnectivité a changé et élargi les vulnérabilités potentielles et accru les risques potentiels pour les opérations. Par exemple, comme la technologie, et les données qu'elle produit et qu'elle traite sont de plus en plus utilisées pour fournir des services critiques et soutenir les décisions métier/de mission, les impacts potentiels d'un incident de cybersécurité sur une organisation, la santé et la sécurité des individus, l'environnement, les communautés, et l'économie et la société au sens large devraient être prises en compte.

Pour gérer les risques de cybersécurité, une compréhension claire des moteurs métier de l'organisation et des considérations de sécurité spécifiques à son utilisation de la technologie est nécessaire. Étant donné que les risques, les priorités et les systèmes de chaque organisation sont uniques, les outils et les méthodes utilisés pour atteindre les résultats décrits par le cadre varieront.

Reconnaissant le rôle que joue la protection de la vie privée et des libertés civiles dans la création d'une plus grande confiance du public, le cadre comprend une méthodologie pour protéger la vie privée et les libertés civiles individuelles lorsque les organisations d'infrastructures critiques mènent des activités de cybersécurité. De nombreuses organisations disposent déjà de processus pour adresser la vie privée et les libertés civiles. La méthodologie est conçue pour compléter ces processus et fournir des conseils pour faciliter la gestion des risques liés à la vie privée conformément à l'approche d'une organisation en matière de gestion des risques de cybersécurité. L'intégration de la vie privée et de la cybersécurité peut profiter aux organisations en augmentant la confiance des clients, en permettant un partage plus standardisé des informations et en simplifiant les opérations entre les régimes juridiques.

Le cadre reste efficace et soutient l'innovation technique car qu'il est technologiquement neutre, tout en faisant également référence à une variété de normes, lignes directrices et pratiques existantes qui évoluent avec la technologie. En s'appuyant sur ces normes, lignes directrices et pratiques mondiales développées, gérées et mises à jour par l'industrie, les outils et méthodes disponibles pour atteindre les résultats du cadre s'étendront au-delà des frontières, reconnaîtront la nature mondiale des risques de cybersécurité et évolueront avec les avancées technologiques et les exigences métier. L'utilisation de normes existantes et émergentes permettra des économies d'échelle et favorisera le développement de produits, de services et de pratiques efficaces qui répondent aux besoins identifiés du marché. La concurrence sur le marché favorise également une diffusion plus rapide de ces technologies et pratiques et la réalisation de nombreux avantages par les acteurs de ces secteurs.

S'appuyant sur ces normes, lignes directrices et pratiques, le cadre fournit une taxonomie et un mécanisme communs permettant aux organisations de:

1) Décrire leur posture actuelle en matière de cybersécurité ;
2) Décrire leur état cible pour la cybersécurité;
3) Identifier et prioriser les opportunités d'amélioration dans le contexte d'un processus continu et reproductible;
4) Apprécier les progrès vers l'état cible;
5) Communiquer entre les parties prenantes internes et externes sur les risques de cybersécurité.

Le cadre n'est pas une approche universelle de la gestion des risques de cybersécurité pour les infrastructures critiques. Les organisations continueront d'avoir des risques uniques - différentes

menaces, différentes vulnérabilités, différentes tolérances aux risques. Ils varieront également dans la manière dont ils personnalisent les pratiques décrites dans le cadre. Les organisations peuvent déterminer les activités qui sont importantes pour la prestation de services critiques et peuvent prioriser les investissements pour maximiser l'impact de chaque investissement dépensé. En fin de compte, le cadre vise à réduire et à mieux gérer les risques de cybersécurité.

Pour tenir compte des besoins uniques des organisations en matière de cybersécurité, il existe une grande variété de manières d'utiliser le cadre. La décision sur la manière de l'appliquer est laissée à l'organisation de mise en œuvre. Par exemple, une organisation peut choisir d'utiliser les niveaux de mise en œuvre du cadre pour articuler les pratiques de gestion des risques envisagées. Une autre organisation peut utiliser les cinq fonctions du cadre pour analyser l'ensemble de son portefeuille de gestion des risques; cette analyse peut s'appuyer ou non sur des conseils complémentaires plus détaillés, tels que des catalogues de contrôles. Il y a parfois des discussions sur la "conformité" avec le cadre, et le cadre a une utilité en tant que structure et langage pour organiser et exprimer la conformité avec les propres exigences de cybersécurité d'une organisation. Néanmoins, la variété des manières dont le cadre peut être utilisé par une organisation signifie que des expressions telles que "conformité avec le cadre" peuvent prêter à confusion signifier quelque chose de très différent pour diverses parties prenantes.

Le cadre complète, et ne remplace pas, le processus de gestion des risques et le programme de cybersécurité d'une organisation. L'organisation peut utiliser ses processus actuels et tirer parti du cadre pour identifier les opportunités de renforcer et de communiquer sa gestion des risques de cybersécurité tout en s'alignant sur les pratiques de l'industrie. Alternativement, une organisation sans programme de cybersécurité existant peut utiliser le cadre comme référence pour en établir.

Bien que le cadre ait été développé pour améliorer la gestion des risques de cybersécurité en ce qui concerne les infrastructures critiques, il peut être utilisé par des organisations de n'importe quel secteur de l'économie ou de la société. Il est destiné à être utile aux entreprises, aux agences gouvernementales et aux organisations à but non lucratif, indépendamment de leur objectif ou de leur taille. La taxonomie commune des normes, lignes directrices et pratiques qu'elle fournit n'est pas non plus propre à un pays. Les organisations en dehors des États-Unis peuvent également utiliser le cadre pour renforcer leurs propres efforts de cybersécurité, et le cadre peut contribuer à développer un langage commun pour la coopération internationale sur la cybersécurité des infrastructures critiques.

1.1 Aperçu du cadre

Le cadre est une approche basée sur les risques pour la gestion des risques de cybersécurité et se compose de trois parties: le noyau du cadre , les niveaux de mise en œuvre du cadre et les profils du cadre. Chaque composant du cadre renforce le lien entre les moteurs métier/de mission et les activités de cybersécurité. Ces composants sont expliqués ci-dessous.

- Le *noyau du cadre* est un ensemble d'activités de cybersécurité, de résultats souhaités et de références applicables qui sont communs à tous les secteurs des infrastructures critiques. Le noyau présente les normes, lignes directrices et pratiques de l'industrie de manière à permettre la communication des activités et des résultats de cybersécurité dans l'ensemble de l'organisation, du niveau exécutif au niveau de la mise en œuvre/des opérations. Le noyau du cadre se compose de cinq fonctions simultanées et continues : Identifier, Protéger, Détecter, Répondre, Rétablir. Considérées ensemble, ces fonctions fournissent une vue

stratégique de haut niveau du cycle de vie de la gestion des risques de cybersécurité d'une organisation. Le noyau du cadre identifie ensuite les catégories et sous-catégories clés sous-jacentes - qui sont des résultats discrets - pour chaque fonction, et les associe à des exemples de références informatives telles que les normes, lignes directrices et pratiques existantes pour chaque sous-catégorie.

- Les *niveaux de mise en œuvre du cadre* (“Niveaux”) fournissent un contexte sur la manière dont une organisation considère le risque de cybersécurité et les processus en place pour gérer ce risque. Les niveaux décrivent le degré auquel les pratiques de gestion des risques de cybersécurité d'une organisation présentent les caractéristiques définies dans le cadre (p. ex., conscientes des risques et des menaces, reproductibles et adaptatives). Les niveaux caractérisent les pratiques d'une organisation sur une gamme allant de partielle (Niveau 1) à adaptative (Niveau 4). Ces niveaux reflètent une progression depuis des réponses informelles et réactives vers des approches agiles et tenant compte des risques. Au cours du processus de sélection de niveau, une organisation doit prendre en compte ses pratiques actuelles de gestion des risques, son environnement de menace, ses exigences légales et réglementaires, ses objectifs métier/de mission et ses contraintes organisationnelles.
- Un *profil du cadre* (“Profil”) représente les résultats basés sur les besoins métier qu'une organisation a sélectionnés dans les catégories et sous-catégories du cadre. Le profil peut être caractérisé comme l'alignement des normes, lignes directrices et pratiques sur le noyau du cadre dans un scénario de mise en œuvre particulier. Les profils peuvent être utilisés pour identifier les opportunités d'amélioration de la posture de cybersécurité en comparant un profil "Actuel" (l'état "tel quel") avec un profil "Cible" (l'état "à être"). Pour développer un profil, une organisation peut examiner toutes les catégories et sous-catégories et, sur la base des moteurs de métier/de mission et d’une appréciation des risques, déterminer lesquelles sont les plus importantes; il peut ajouter des catégories et des sous-catégories selon les besoins pour s’adresser aux risques de l'organisation. Le profil actuel peut ensuite être utilisé pour prendre en charge la priorisation et le mesurage des progrès vers le profil cible, tout en tenant compte d'autres besoins métier, notamment la rentabilité et l'innovation. Les profils peuvent être utilisés pour effectuer des auto-appréciations et communiquer au sein d'une organisation ou entre des organisations.

1.2 Gestion des risques et cadre de cybersécurité

La gestion des risques est le processus continu d'identification, d'appréciation et de réponse aux risques. Pour gérer les risques, les organisations doivent comprendre la vraisemblance qu'un événement se produise et les impacts potentiels qui en résultent. Avec ces informations, les organisations peuvent déterminer le niveau de risque acceptable pour atteindre leurs objectifs organisationnels et peuvent l'exprimer comme leur tolérance au risque.

Avec une compréhension de la tolérance au risque, les organisations peuvent prioriser les activités de cybersécurité, permettant ainsi aux organisations de prendre des décisions éclairées concernant les dépenses de cybersécurité. La mise en œuvre de programmes de gestion des risques offre aux organisations la possibilité de quantifier et de communiquer les ajustements à leurs programmes de cybersécurité. Les organisations peuvent choisir de gérer le risque de différentes manières, notamment en atténuant le risque, en transférant le risque, en évitant le risque ou en acceptant le risque, en fonction de l'impact potentiel sur la prestation de services

critiques. Le cadre utilise des processus de gestion des risques pour permettre aux organisations d'informer et de prioriser les décisions concernant la cybersécurité. Il prend en charge les appréciations des risques récurrentes et la validation des moteurs métier pour aider les organisations à sélectionner des états cibles pour les activités de cybersécurité qui reflètent les résultats souhaités. Ainsi, le noyau donne aux organisations la possibilité de sélectionner et d'orienter de manière dynamique l'amélioration de la gestion des risques de cybersécurité pour les environnements IT et ICS.

Le cadre est adaptatif pour fournir une mise en œuvre flexible et basée sur les risques qui peut être utilisée avec un large éventail de processus de gestion des risques de cybersécurité. Des exemples de processus de gestion des risques de cybersécurité incluent l'organisation internationale de normalisation (ISO) 31000:2009[6], ISO/commission électrotechnique internationale (CEI) 27005:2011[7], publication spéciale du NIST (SP) 800-39[8], et la ligne directrice sur le *processus de gestion des risques de cybersécurité du sous-secteur de l'électricité* (RMP)[9].

1.3 Aperçu du document

Le reste de ce document contient les sections et annexes suivantes :

- La section 2 décrit les composants du cadre : le noyau du cadre , les niveaux et les profiles.
- La section 3 présente des exemples d'utilisation du cadre.
- La section 4 décrit comment utiliser le cadre pour l'auto-appréciation et la démonstration de la cybersécurité via des mesurages.
- L'annexe A présente le noyau du cadre sous forme de tableau : les fonctions, les catégories, les sous-catégories et les références informatives.
- L'annexe B contient un glossaire de termes sélectionnés.
- L'annexe C répertorie les acronymes utilisés dans ce document.

[6] Organisation internationale de normalisation, *Gestion des risques - Principes et lignes directrices,* ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] Organisation Internationale de Normalisation/Commission Electrotechnique Internationale, *Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information,* ISO/CEI 27005 :2011, 2011. https://www.iso.org/standard/56742.html

[8] Initiative de transformation de la force opérationnelle interarmées, Gestion des risques liés à la sécurité de l'information : organisation, mission et vue du système d'information, publication spéciale de NIST 800-39, mars 2011. https://doi.org/10.6028/NIST.SP.80039

[9] Département américain de l'énergie, Processus de gestion des risques de cybersécurité du sous-secteur de l'électricité, DOE/OE-0003, mai 2012. https://energy.gov/sites/prod/files/Cybersecurity%2520Risk%2520Management%2520Process%2520Guideline%2520-%2520Final%2520-%2520May%25202012.pdf

2.0 Bases du noyau

Le cadre fournit un langage commun pour comprendre, gérer et exprimer les risques de cybersécurité aux parties prenantes internes et externes. Il peut être utilisé pour aider à identifier et prioriser les actions de réduction des risques de cybersécurité, et c'est un outil pour aligner les approches politiques, métier et technologiques pour gérer ce risque. Il peut être utilisé pour gérer les risques de cybersécurité dans des organisations entières ou il peut être axé sur la fourniture de services critiques au sein d'une organisation. Différents types d'entités - y compris les structures de coordination sectorielle, les associations et les organisations - peuvent utiliser le cadre à différentes fins, y compris la création de profils communs.

2.1 Noyau du cadre

Le *noyau du cadre* fournit un ensemble d'activités pour atteindre des *résultats* spécifiques en matière de cybersécurité et fait référence à des exemples de conseils pour atteindre ces résultats. Le noyau n'est pas une liste de contrôle d'actions à effectuer. Il présente les principaux résultats en matière de cybersécurité identifiés par les parties prenantes comme étant utiles dans la gestion des risques de cybersécurité. Le noyau comprend quatre éléments : les fonctions, les catégories, les sous-catégories et les références informatives, illustrées à la **figure 1**:

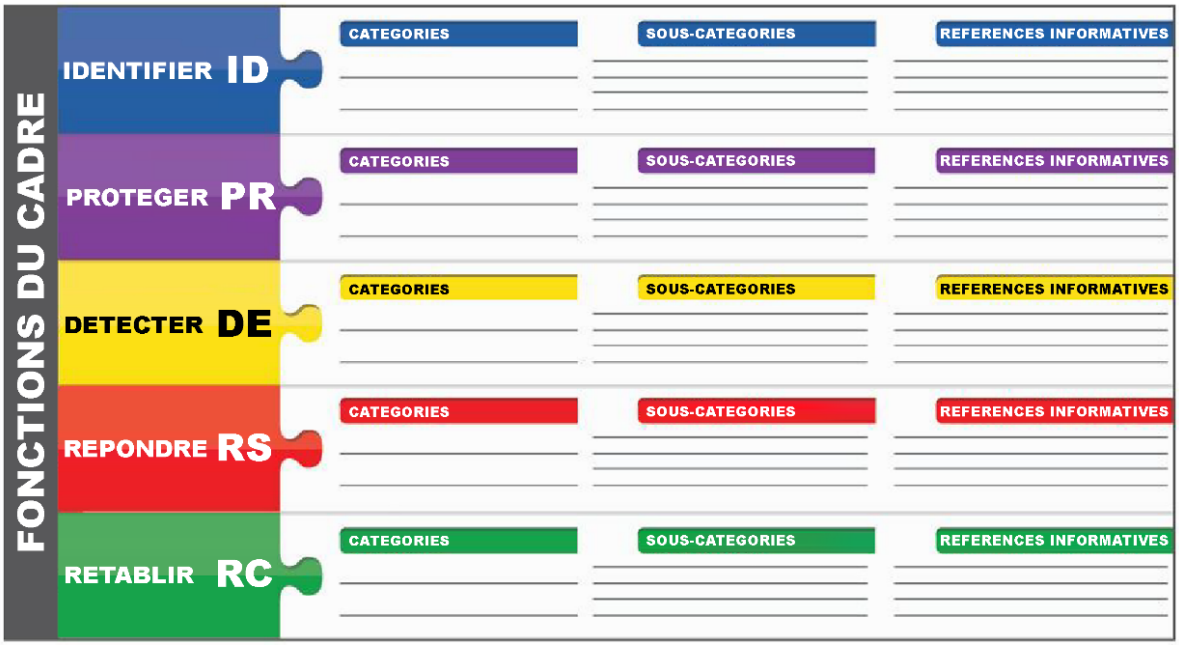

Figure 1 : Structure de noyau du cadre

Les éléments de noyau du cadre fonctionnent ensemble comme suit:

- Les **Fonctions** organisent les activités de cybersécurité de base à leur plus haut niveau . Ces fonctions sont Identifier, Protéger, Détecter, Répondre et Rétablir. Ils aident une organisation à exprimer sa gestion des risques de cybersécurité en organisant les informations, en permettant des décisions de gestion des risques, en s'adressant aux menaces et en s'améliorant en apprenant des activités précédentes. Les fonctions s'alignent également sur les méthodologies existantes pour la gestion des incidents et aident à montrer

l'impact des investissements dans la cybersécurité. Par exemple, les investissements dans la planification et les exercices soutiennent les mesures d'intervention et de rétablissement en temps opportun, ce qui réduit l'impact sur la prestation des services.

- Les **Catégories** sont les subdivisions d'une fonction en groupes de résultats de cybersécurité étroitement liés aux besoins programmatiques et à des activités particulières. Les exemples de catégories incluent "Gestion des actifs", "Gestion des identités et contrôle d'accès" et "Processus de détection".
- Les **Sous-catégories** divisent d'avantage une catégorie en résultats spécifiques d'activités techniques et/ou de gestion. Ils fournissent un ensemble de résultats qui, sans être exhaustifs, aident à soutenir l'atteinte des résultats dans chaque catégorie. Les exemples de sous-catégories incluent "Les systèmes d'information externes sont catalogués", "Les données au repos sont protégées" et "Les notifications des systèmes de détection sont étudiées."
- Les **Références informatives** sont des sections spécifiques de normes, de lignes directrices et de pratiques courantes parmi les secteurs d'infrastructures critiques qui illustrent une méthode pour atteindre les résultats associés à chaque sous-catégorie. Les références informatives présentées dans le noyau du cadre sont illustratives et non exhaustives. Ils sont basés sur les orientations intersectorielles les plus fréquemment référencées au cours du processus d'élaboration du cadre.

Les cinq fonctions principales du cadre sont définies ci-dessous. Ces fonctions ne sont pas destinées à former un chemin série ou à conduire à un état final souhaité statique. Au contraire, les fonctions doivent être exécutées simultanément et en continu pour former une culture opérationnelle qui s'adressant au risque dynamique de cybersécurité. Voir l'annexe A pour la liste complète de noyau du cadre.

- **Identifier** - Développer une compréhension organisationnelle pour gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.

  Les activités de la fonction d'identification sont fondamentales pour une utilisation efficace du cadre. Comprendre le contexte métier, les ressources qui soutiennent les fonctions critiques et les risques de cybersécurité associés permet à une organisation de concentrer et de prioriser ses efforts, conformément à sa stratégie de gestion des risques et à ses besoins métier. Des exemples de catégories de résultats au sein de cette fonction: Gestion des actifs; Environnement métier; Gouvernance; Appréciation des risques; et Stratégie de gestion des risques.

- **Protéger** - Élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la prestation des services essentiels.

  La fonction de protection prend en charge la capacité de limiter ou de contenir l'impact d'un événement de cybersécurité potentiel. Des exemples de catégories de résultats au sein de cette fonction: Gestion des identités et contrôle d'accès; Sensibilisation et formation; Sécurité des données; Procédures et procédures de protection des informations; Maintenance; et Technologie de protection.

- **Détecter** - Développer et mettre en œuvre des activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.

La fonction de détection permet la découverte en temps opportun des événements de cybersécurité. Des exemples de catégories de résultats au sein de cette fonction: Anomalies et événements; Surveillance continue de la sécurité, et; Processus de détection.

- **Répondre** - Développer et mettre en œuvre des activités appropriées pour prendre des mesures concernant un incident de cybersécurité détecté.

  La Fonction de réponse prend en charge la capacité de contenir l'impact d'un incident de cybersécurité potentiel. Des exemples de catégories de résultats au sein de cette fonction: Plan d'intervention; Communications; Analyse; Atténuation ; et Améliorations.

- **Rétablir** - Développer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et pour restaurer les capacités ou les services qui ont été altérés en raison d'un incident de cybersécurité.

  La Fonction de rétablissement prend en charge une reprise rapide des opérations normales afin de réduire l'impact d'un incident de cybersécurité. Des exemples de catégories de résultats au sein de cette fonction: Planification de la récupération; Améliorations; et Communications.

2.2 Niveaux de mise en œuvre du cadre

Les niveaux de mise en œuvre du cadre (“Niveaux”) fournissent un contexte sur la manière dont une organisation considère le risque de cybersécurité et les processus en place pour gérer ce risque. Allant de partiel (Niveau 1) à adaptatif (Niveau 4), les niveaux décrivent un degré croissant de rigueur et de sophistication dans les pratiques de gestion des risques de cybersécurité. Ils aident à déterminer dans quelle mesure la gestion des risques de cybersécurité est informée par les besoins métier et est intégrée aux pratiques globales de gestion des risques d'une organisation. Les considérations relatives à la gestion des risques incluent de nombreux aspects de la cybersécurité, y compris le degré d’intégration des considérations relatives à la vie privée et aux libertés civiles sont intégrées dans la gestion par une organisation des risques de cybersécurité et des réponses potentielles aux risques.

Le processus de sélection de niveau prend en compte les pratiques actuelles de gestion des risques d'une organisation, l'environnement de menace, les exigences légales et réglementaires, les pratiques de partage d'informations, les objectifs métier/de mission, les exigences de cybersécurité de la chaîne d'approvisionnement et les contraintes organisationnelles. Les organisations doivent déterminer le niveau souhaité, en s’assurant que le niveau sélectionné réponde aux objectifs organisationnels, est réalisable à mettre en œuvre et réduit le risque de cybersécurité pour les actifs et les ressources critiques à des niveaux acceptables pour l'organisation. Les organisations devraient envisager de tirer parti des conseils externes obtenus des ministères et organismes du gouvernement fédéral, des centres de partage et d'analyse de l'information (ISACs), des organisations de partage et d'analyse de l'information (ISAOs), des modèles de maturité existants ou d'autres sources pour les aider à déterminer le niveau souhaité.

Bien que les organisations identifiées comme étant de niveau 1 (Partiel) soient encouragées à envisager de passer au niveau 2 ou supérieur, les niveaux ne représentent pas les niveaux de maturité. Les niveaux sont destinés à soutenir la prise de décision organisationnelle sur la manière de gérer les risques de cybersécurité, ainsi que sur les dimensions de l'organisation qui sont prioritaires et pourraient recevoir des ressources supplémentaires. La progression vers des

niveaux supérieurs est encouragée lorsqu'une analyse coûts-avantages indique une réduction faisable et rentable du risque de cybersécurité.

La mise en œuvre réussie du cadre repose sur l'atteinte des résultats décrits dans le(s) profil(s) cible(s) de l'organisation et non sur la détermination du niveau. Néanmoins, la sélection et la désignation des niveaux affectent naturellement les profils de cadre. La recommandation de niveau par les gestionnaires de niveau métier/processus, telle qu'approuvée par le niveau de la haute direction, aidera à définir le ton général de la manière dont le risque de cybersécurité sera géré au sein de l'organisation et devrait influencer la priorisation au sein d'un profil cible et les appréciations des progrès accomplis pour adresser les lacunes.

Les définitions de niveau sont les suivantes:

Niveau 1: Partiel

- *Processus de gestion des risques* - Les pratiques organisationnelles de gestion des risques de cybersécurité ne sont pas formalisées et les risques sont gérés de manière *ad hoc* et parfois réactive. La priorisation des activités de cybersécurité peut ne pas être directement informée par les objectifs de risque organisationnel, l'environnement de menace ou les exigences métier/de mission.
- *Programme de gestion intégrée des risques* - La sensibilisation au risque de cybersécurité est limitée au niveau organisationnel. L'organisation met en œuvre une gestion des risques de cybersécurité de manière irrégulière, au cas par cas, en raison d'une expérience variée ou d'informations acquises auprès de sources externes. L'organisation peut ne pas avoir de processus permettant de partager les informations de cybersécurité au sein de l'organisation.
- *Participation externe* - L'organisation ne comprend pas son rôle dans l'écosystème plus large en ce qui concerne ses dépendances ou ses dépendants. L'organisation ne collabore ni ne reçoit d'informations (p. ex., renseignements sur les menaces, meilleures pratiques, technologies) d'autres entités (p. ex., acheteurs, fournisseurs, dépendances, dépendants, ISAOs, chercheurs, gouvernements), et ne partage pas d'informations. L'organisation n'est généralement pas consciente des risques de la cyber chaîne d'approvisionnement des produits et services qu'elle fournit et qu'elle utilise.

Niveau 2: Risque informé

- *Processus de gestion des* risques - Les pratiques de gestion des risques sont approuvées par la direction mais peuvent ne pas être établies en tant que politique à l'échelle de l'organisation. La priorisation des activités de cybersécurité et des besoins de protection est directement informée par les objectifs de risque organisationnel, l'environnement de menace ou les exigences métier/de mission.
- *Programme de gestion intégrée des risques* - Il existe une prise de conscience du risque de cybersécurité au niveau organisationnel, mais une approche à l'échelle de l'organisation pour gérer le risque de cybersécurité n'a pas été établie. Les informations sur la cybersécurité sont partagées au sein de l'organisation de manière informelle. La prise en compte de la cybersécurité dans les objectifs et les programmes organisationnels peut se produire à certains niveaux de l'organisation, mais pas à tous. Une appréciation des cyber risques des actifs organisationnels et externes a lieu, mais n'est généralement pas reproductible ou récurrente.

- *Participation externe* - En règle générale, l'organisation comprend son rôle dans l'écosystème plus large en ce qui concerne soit ses propres dépendances, soit ses dépendants, mais pas les deux. L'organisation collabore avec et reçoit des informations d'autres entités et génère certaines de ses propres informations, mais ne peut pas partager d'informations avec d'autres. De plus, l'organisation est consciente des risques de la cyber chaîne d'approvisionnement associés aux produits et services qu'elle fournit et utilise, mais n'agit pas de manière cohérente ou formelle face à ces risques.

Niveau 3: Répétable

- *Processus de gestion des risques* - Les pratiques de gestion des risques de l'organisation sont officiellement approuvées et exprimées sous forme de politique. Les pratiques de cybersécurité organisationnelles sont régulièrement mises à jour en fonction de l'application des processus de gestion des risques aux changements dans les exigences métier/de mission et à l'évolution du paysage des menaces et la technologie.
- *Programme de gestion intégrée des risques* - Il existe une approche à l'échelle de l'organisation pour gérer les risques de cybersécurité. Les politiques, processus et procédures tenant compte des risques sont définis, mis en œuvre comme prévu et examinés. Des méthodes cohérentes sont en place pour répondre efficacement aux changements de risque. Le personnel possède les connaissances et les compétences nécessaires pour remplir les rôles et responsabilités qui lui sont assignés. L'organisation surveille de manière cohérente et précise le risque de cybersécurité des actifs de l'organisation. Les cadres supérieurs en cybersécurité et non-cybersécurité communiquent régulièrement sur les risques de cybersécurité. Les cadres supérieurs veillent à la prise en compte de la cybersécurité dans toutes les lignes d'opération de l'organisation.
- *Participation externe* - L'organisation comprend son rôle, ses dépendances et ses dépendants dans l'écosystème plus large et peut contribuer à une compréhension plus large des risques par la communauté. Il collabore et reçoit régulièrement des informations d'autres entités qui complètent les informations générées en interne, et partage des informations avec d'autres entités. L'organisation est consciente des risques de la cyber chaîne d'approvisionnement associés aux produits et services qu'elle fournit et qu'elle utilise. De plus, il agit généralement de manière formelle sur ces risques, y compris des mécanismes tels que des accords écrits pour communiquer les exigences de base, les structures de gouvernance (p. ex., les conseils des risques), et la mise en œuvre et le suivi des politiques.

Niveau 4: Adaptatif

- *Processus de gestion des risques* - L'organisation adapte ses pratiques de cybersécurité en fonction des activités de cybersécurité précédentes et actuelles, y compris les leçons apprises et les indicateurs prédictifs. Grâce à un processus d'amélioration continue intégrant des technologies et des pratiques de cybersécurité avancées, l'organisation s'adapte activement à l'évolution du paysage des menaces et des technologies et répond de manière rapide et efficace aux menaces sophistiquées et évolutives.
- *Programme de gestion intégrée des risques* - Il existe une approche à l'échelle de l'organisation de la gestion des risques de cybersécurité qui utilise des politiques, des processus et des procédures tenant compte des risques pour s'adresser aux événements

potentiels de cybersécurité. La relation entre le risque de cybersécurité et les objectifs organisationnels est clairement comprise et prise en compte lors de la prise de décisions. Les Cadres supérieurs surveillent le risque de cybersécurité dans le même contexte que le risque financier et les autres risques organisationnels. Le budget organisationnel est basé sur une compréhension de l'environnement de risque actuel et prévu et de la tolérance au risque. Les unités d'affaires mettent en œuvre une vision exécutive et analysent les risques au niveau du système dans le contexte des tolérances au risque organisationnel. La gestion des risques de cybersécurité fait partie de la culture organisationnelle et évolue à partir d'une prise de conscience des activités précédentes et d'une conscience continue des activités sur leurs systèmes et réseaux. L'organisation peut prendre en compte rapidement et efficacement les changements apportés aux objectifs métier/de mission dans la manière dont le risque est abordé et communiqué.

- *Participation externe* - L'organisation comprend son rôle, ses dépendances et ses dépendants dans l'écosystème plus large et contribue à la compréhension plus large des risques par la communauté. Il reçoit, génère et examine les informations prioritaires qui informent une analyse continue de ses risques à mesure que les menaces et les paysages technologiques évoluent. L'organisation partage ces informations en interne et en externe avec d'autres collaborateurs. L'organisation utilise des informations en temps réel ou quasi réel pour comprendre et agir de manière cohérente sur les risques de la cyber chaîne d'approvisionnement associés aux produits et services qu'elle fournit et qu'elle utilise. De plus, il communique de manière proactive, en utilisant des mécanismes formels (p. ex., des accords) et informels pour développer et maintenir de solides relations dans la chaîne d'approvisionnement.

2.3 Profil du cadre

Le profil de cadre ("Profil") est l'alignement des fonctions, catégories et sous-catégories avec les exigences métier, la tolérance au risque et les ressources de l'organisation. Un profil permet aux organisations d'établir une feuille de route pour réduire les risques de cybersécurité qui est bien alignée sur les objectifs organisationnels et sectoriels, prend en compte les exigences légales/réglementaires et les meilleures pratiques de l'industrie, et reflète les priorités de gestion des risques. Compte tenu de la complexité de nombreuses organisations, elles peuvent être choisir d'avoir plusieurs profils, alignés sur des composants particuliers et reconnaissant leurs besoins individuels.

Les profils de cadre peuvent être utilisés pour décrire l'état actuel ou l'état cible souhaité d'activités de cybersécurité spécifiques. Le profil actuel indique les résultats en matière de cybersécurité qui sont actuellement atteints. Le profil cible indique les résultats nécessaires pour atteindre les objectifs de gestion des risques de cybersécurité souhaités. Les profils soutiennent les exigences métier/de mission et aident à communiquer les risques au sein et entre les organisations. Ce cadre ne prescrit pas de modèles de profil, permettant une flexibilité dans la mise en œuvre.

La comparaison des profils (p. ex., le profil actuel et le profil cible) peut révéler des lacunes à combler pour atteindre les objectifs de gestion des risques de cybersécurité. Un plan d'action pour adresser ces lacunes pour remplir une catégorie ou une sous-catégorie donnée peut contribuer à la feuille de route décrite ci-dessus. La priorité à l'atténuation des écarts est motivée

par les besoins métier et les processus de gestion des risques de l'organisation. Cette approche basée sur les risques permet à une organisation d'évaluer les ressources nécessaires (p. ex., recrutement, financement) pour atteindre les objectifs de cybersécurité de manière rentable et priorisée. De plus, le cadre est une approche fondée sur les risques où l'applicabilité et la réalisation d'une sous-catégorie donnée sont soumises à la portée du profil.

2.4 Coordination de la mise en œuvre du cadre

La figure 2 décrit un flux commun d'informations et de décisions aux niveaux suivants au sein d'une organisation :

- Exécutif
- Métier/Processus
- Mise en œuvre/Opérations

Le niveau exécutif communique les priorités de la mission, les ressources disponibles et la tolérance globale au risque au niveau métier/processus. Le niveau métier/processus utilise les informations comme entrées dans le processus de gestion des risques, puis collabore avec le niveau de mise en œuvre/opérations pour communiquer les besoins métier et créer un profil. Le niveau de mise en œuvre/opérations communique le progrès de mise en œuvre du profil au niveau métier/processus. Le niveau métier/processus utilise ces informations pour effectuer une appréciation d'impact. La gestion au niveau métier/processus rend compte des résultats de cette appréciation d'impact au niveau exécutif pour informer le processus global de gestion des risques de l'organisation et au niveau de mise en œuvre/opérations pour une prise conscience de l'impact métier.

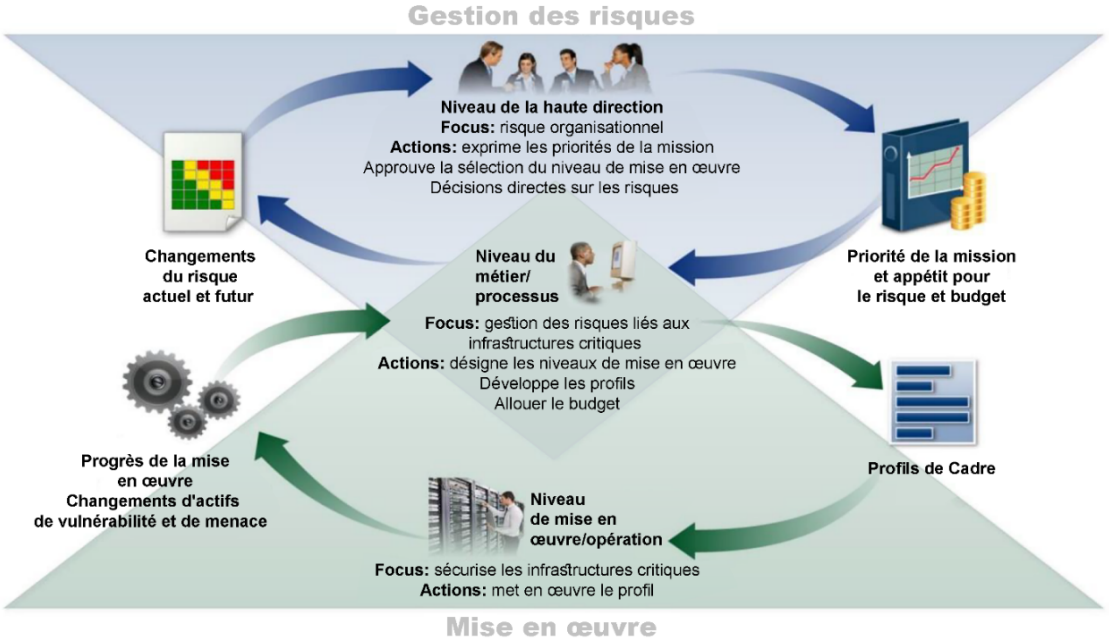

Figure 2 : Flux d'informations notionnelles et de décision au sein d'une organisation

3.0 Comment utiliser le cadre

Une organisation peut utiliser le cadre comme élément clé de son processus systématique d'identification, d'appréciation et de gestion des risques de cybersécurité. Le cadre n'est pas conçu pour remplacer les processus existants; une organisation peut utiliser son processus actuel et le superposer au cadre pour déterminer les lacunes de son approche actuelle des risques de cybersécurité et développer une feuille de route pour l'amélioration. En utilisant le cadre comme outil de gestion des risques de cybersécurité, une organisation peut déterminer les activités les plus importantes pour la prestation de services critiques et prioriser les dépenses afin de maximiser l'impact de l'investissement.

Le cadre est conçu pour compléter les opérations métier et de cybersécurité existantes. Il peut servir de base à un nouveau programme de cybersécurité ou de mécanisme d'amélioration d'un programme existant. Le cadre fournit un moyen d'exprimer les exigences de cybersécurité aux partenaires métier et aux clients et peut aider à identifier les lacunes dans les pratiques de cybersécurité d'une organisation. Il fournit également un ensemble général de considérations et de processus pour examiner les implications en matière de vie privée et de libertés civiles dans le contexte d'un programme de cybersécurité.

Le cadre peut être appliqué tout au long des phases du cycle de vie de la planification, de la conception, de la construction/achat, du déploiement, de l'exploitation et de la mise hors service. La phase de planification commence le cycle de tout système et jette les bases de tout ce qui suit. Les considérations générales en matière de cybersécurité doivent être déclarées et décrites aussi clairement que possible. Le plan devrait reconnaître que ces considérations et exigences sont susceptibles d'évoluer pendant le reste du cycle de vie. La phase de conception doit tenir compte des exigences de cybersécurité dans le cadre d'un processus d'ingénierie des systèmes multidisciplinaire plus large[10]. Une étape clé de la phase de conception est la validation que les spécifications de cybersécurité du système correspondent aux besoins et à la disposition des risques de l'organisation tels qu'ils sont capturés dans un profil de cadre. Les résultats souhaités en matière de cybersécurité classés par ordre de priorité dans un profil cible doivent être intégrés lors a) du développement du système pendant la phase de construction et b) de l'achat ou de l'externalisation du système pendant la phase d'achat. Ce même profil cible sert de liste de fonctionnalités de cybersécurité du système qui doivent être adressées lors du déploiement du système pour vérifier que toutes les fonctionnalités sont mises en œuvre. Les résultats de cybersécurité déterminés à l'aide du cadre devraient alors servir de base au fonctionnement continu du système. Cela comprend une réappréciation occasionnelle, la capture des résultats dans un profil actuel, pour vérifier que les exigences de cybersécurité sont toujours remplies. En règle générale, un réseau complexe de dépendances (p. ex., des contrôles compensatoires et communs) entre les systèmes signifie que les résultats documentés dans les profils cibles des systèmes connexes doivent être soigneusement pris en compte lors de la mise hors service des systèmes.

Les sections suivantes présentent différentes manières dont les organisations peuvent utiliser le noyau.

[10] Publication spéciale du NIST 800-160 volume 1, ingénierie de la sécurité des systèmes, considérations pour une approche multidisciplinaire dans l'ingénierie de systèmes sécurisés dignes de confiance, Ross et al, novembre 2016 (mise à jour le 21 mars 2018), https://doi.org/10.6028/NIST.SP.800-160v1

3.1 Examen de base des pratiques de cybersécurité

Le cadre peut être utilisé pour comparer les activités de cybersécurité actuelles d'une organisation avec celles décrites dans le noyau du cadre. Grâce à la création d'un profil actuel, les organisations peuvent examiner dans quelle mesure elles atteignent les résultats décrits dans les catégories et sous-catégories du noyau, alignées sur les cinq fonctions de haut niveau: Identifier, Protéger, Détecter, Répondre, et Rétablir. Une organisation peut constater qu'elle atteint déjà les résultats souhaités, gérant ainsi la cybersécurité en fonction du risque connu. Alternativement, une organisation peut déterminer qu'elle a des opportunités (ou des besoins pour) s'améliorer. L'organisation peut utiliser ces informations pour élaborer un plan d'action visant à renforcer les pratiques de cybersécurité existantes et à réduire les risques de cybersécurité. Une organisation peut également constater qu'elle surinvestit pour atteindre certains résultats. L'organisation peut utiliser ces informations pour redéfinir les priorités des ressources.

Bien qu'elles ne remplacent pas un processus de gestion des risques, ces cinq fonctions de haut niveau fourniront aux cadres supérieurs et autres un moyen concis de distiller les concepts fondamentaux du risque de cybersécurité afin qu'ils puissent apprécier comment les risques identifiés sont gérés et comment leur organisation se superpose à un niveau élevé par rapport aux normes, lignes directrices et pratiques de cybersécurité existantes. Le cadre peut également aider une organisation à répondre à des questions fondamentales, notamment "Comment allons-nous?" Ensuite, ils peuvent agir de manière plus éclairée pour renforcer leurs pratiques de cybersécurité là où et quand cela est jugé nécessaire.

3.2 Établissement ou amélioration d'un programme de cybersécurité

Les étapes suivantes illustrent comment une organisation pourrait utiliser le cadre pour créer un nouveau programme de cybersécurité ou améliorer un programme existant. Ces étapes doivent être répétées si nécessaire pour améliorer continuellement la cybersécurité.

Étape 1: Prioriser et délimiter. L'organisation identifie ses objectifs métier/de mission et ses priorités organisationnelles de haut niveau. Avec ces informations, l'organisation prend des décisions stratégiques concernant la mise en œuvre de la cybersécurité et détermine la portée des systèmes et des actifs qui prennent en charge le secteur d'activité ou le processus sélectionné. Le cadre peut être adapté pour prendre en charge les différents secteurs d'activité ou processus au sein d'une organisation, qui peuvent avoir des besoins métier différents et une tolérance au risque associée. Les tolérances au risque peuvent être reflétées dans un niveau de mise en œuvre cible.

Étape 2: Orienter. Une fois que la portée du programme de cybersécurité a été déterminée pour le secteur d'activité ou le processus, l'organisation identifie les systèmes et actifs connexes, les exigences réglementaires et l'approche globale du risque. L'organisation consulte ensuite les sources pour identifier les menaces et les vulnérabilités applicables à ces systèmes et actifs.

Étape 3: Créer un profil actuel. L'organisation élabore un profil actuel en indiquant les résultats de catégorie et sous-catégorie du noyau du cadre qui sont actuellement atteints. Si un résultat est partiellement atteint, noter ce fait aidera à soutenir les étapes suivantes en fournissant des informations de base.

Étape 4: Mener une appréciation des risques . Cette appréciation pourrait être guidée par le processus global de gestion des risques de l'organisation ou par des activités d'appréciation des risques antérieures. L'organisation analyse l'environnement opérationnel afin de discerner la vraisemblance d'un événement de cybersécurité et l'impact que l'événement pourrait avoir sur l'organisation. Il est important que les organisations identifient les risques émergents et utilisent les informations sur les cybermenaces provenant de sources internes et externes pour mieux comprendre la vraisemblance et l'impact des événements de cybersécurité.

Étape 5: Créer un profil cible. L'organisation crée un profil cible qui se concentre sur l'appréciation des catégories et sous-catégories du cadre décrivant les résultats de cybersécurité souhaités par l'organisation. Les organisations peuvent également développer leurs propres catégories et sous-catégories supplémentaires pour tenir compte des risques organisationnels uniques. L'organisation peut également prendre en compte des influences et des exigences des parties prenantes externes telles que les entités du secteur, les clients et les partenaires métier lors de la création d'un profil cible. Le profil cible doit refléter de manière appropriée les critères du niveau de mise en œuvre cible.

Étape 6: Déterminer, analyser et prioriser les écarts. L'organisation compare le profil actuel et le profil cible pour déterminer les écarts. Ensuite, il crée un plan d'action priorisé pour adresser les lacunes - reflétant les moteurs de la mission, les coûts et les avantages, et les risques - afin d'atteindre les résultats du profil cible. L'organisation détermine ensuite les ressources, y compris le financement et l'effectif, nécessaires pour adresser les lacunes. L'utilisation des profils de cette manière encourage l'organisation à prendre des décisions éclairées sur les activités de cybersécurité, prend en charge la gestion des risques et permet à l'organisation d'effectuer des améliorations ciblées et rentables.

Étape 7: Mettre en œuvre le plan d'action. L'organisation détermine les mesures à prendre pour adresser les lacunes, le cas échéant, identifiées à l'étape précédente, puis ajuste ses pratiques de cybersécurité actuelles afin d'atteindre le profil cible. Pour plus d'informations, le cadre identifie des exemples de références informatives concernant les catégories et sous-catégories, mais les organisations doivent déterminer quelles normes, lignes directrices et pratiques, y compris celles qui sont spécifiques à un secteur, conviennent le mieux à leurs besoins.

Une organisation répète les étapes nécessaires pour apprécier et améliorer en permanence sa cybersécurité. Par exemple, les organisations peuvent constater qu'une répétition plus fréquente de l'étape d'orientation améliore la qualité des appréciations des risques. En outre, les organisations peuvent suivre les progrès par le biais de mises à jour itératives du profil actuel, en comparant ensuite le profil actuel au profil cible. Les organisations peuvent également utiliser ce processus pour aligner leur programme de cybersécurité avec le niveau de mise en œuvre du cadre souhaité.

3.3 Communication des exigences de cybersécurité avec les parties prenantes

Le cadre fournit un langage commun pour communiquer les exigences entre les parties prenantes interdépendants responsables de la fourniture des produits et services d'infrastructure critique essentielle. Les exemples comprennent:

- Une organisation peut utiliser un profil cible pour exprimer les exigences de gestion des risques de cybersécurité à un fournisseur de services externe (p. ex., un fournisseur de cloud vers lequel elle exporte des données).
- Une organisation peut exprimer son état de cybersécurité par le biais d'un profil actuel pour rapporter des résultats ou pour comparer avec les exigences d'acquisition.
- Un propriétaire/opérateur d'infrastructure critique, ayant identifié un partenaire externe dont dépend cette infrastructure, peut utiliser un profil cible pour transmettre les catégories et sous-catégories requises.
- Un secteur d'infrastructure critique peut établir un profil cible qui peut être utilisé parmi ses constituants comme profil de base initial pour construire leurs profils cibles personnalisés.
- Une organisation peut mieux gérer les risques de cybersécurité parmi les parties prenantes en appréciant leur position dans l'infrastructure critique et l'économie numérique au sens large à l'aide des niveaux de mise en œuvre.

La communication est particulièrement importante entre les parties prenantes en amont et en aval des chaînes d'approvisionnement. Les chaînes d'approvisionnement sont des ensembles de ressources et de processus complexes, répartis à l'échelle mondiale et interconnectés entre plusieurs niveaux d'organisation. Les chaînes d'approvisionnement commencent par l'approvisionnement en produits et services et s'étendent de la conception, du développement, de la fabrication, du traitement, de la manutention et de la livraison des produits et services à l'utilisateur final. Compte tenu de ces relations complexes et interconnectées, la gestion des risques de la chaîne d'approvisionnement (SCRM) est une fonction organisationnelle essentielle.[11]

La Cyber SCRM est l'ensemble des activités nécessaires pour gérer les risques de cybersécurité associé aux parties externes. Plus précisément, la cyber SCRM s'adresse à la fois l'effet de cybersécurité qu'une organisation sur les parties externes et l'effet de cybersécurité que des parties externes ont sur une organisation.

Un objectif principal de la cyber SCRM est d'identifier, d'apprécier et d'atténuer "les produits et services qui peuvent contenir des fonctionnalités potentiellement malveillantes, sont contrefaits ou sont vulnérables en raison de mauvaises pratiques de fabrication et de développement au sein de la cyber-chaîne d'approvisionnement[12]." Les activités de la cyber SCRM peuvent inclure:

- Déterminer les exigences de cybersécurité pour les fournisseurs,
- Adopter des exigences de cybersécurité par le biais d'un accord formel (p. ex., contrats),
- Communiquer aux fournisseurs comment ces exigences de cybersécurité seront vérifiées et validées,
- Vérifier que les exigences en matière de cybersécurité sont satisfaites grâce à une variété de méthodologies d'appréciation, et
- Gouverner et gérer les activités ci-dessus.

[11] La communication des exigences de cybersécurité (section 3.3) et les décisions d'achat (section 3.4) n'adressent que de deux utilisations du cadre pour la cyber SCRM et ne vise pas à adresser la cyber SCRM de manière exhaustive.

[12] Publication spéciale du NIST 800-161, pratiques de gestion des risques de la chaîne d'approvisionnement pour les systèmes d'information et les organisations fédérales, Boyens et al, avril 2015, https://doi.org/10.6028/NIST.SP.800-161

Comme le montre la figure 3, la cyber SCRM englobe les fournisseurs et acheteurs de technologie, ainsi que les fournisseurs et acheteurs non technologiques, où la technologie est composée au minimum de technologies de l'information (TI), de systèmes de contrôle industriel (ICS), de systèmes cyber-physiques (CPS), et les appareils connectés plus généralement, y compris l'Internet des objets (IoT). La figure 3 illustre une organisation à un moment donné. Cependant, dans le cours normal des opérations métier, la plupart des organisations seront à la fois un fournisseur en amont et un acheteur en aval par rapport à d'autres organisations ou utilisateurs finaux.

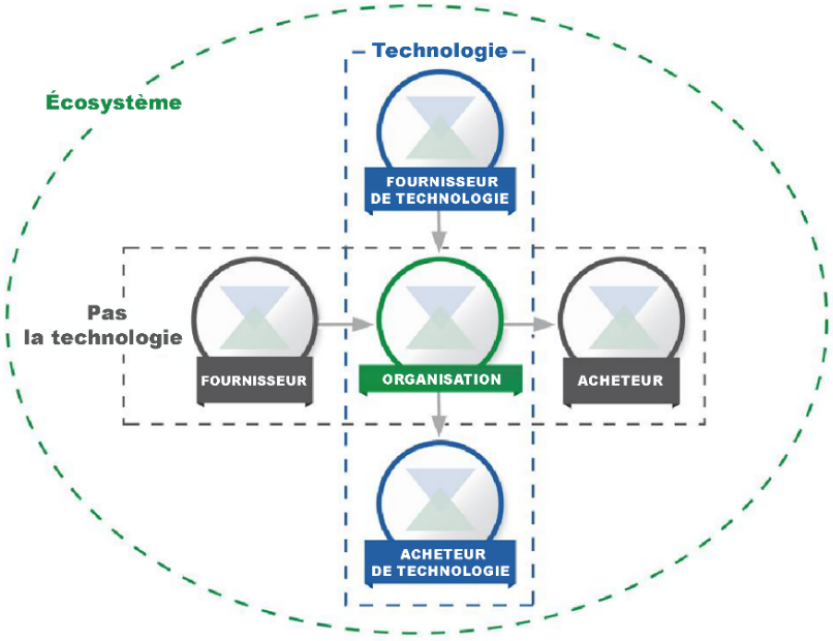

Figure 3 : Relations de la cyber chaîne d'approvisionnement

Les parties décrites à la figure 3 constituent l'écosystème de cybersécurité d'une organisation. Ces relations mettent en évidence le rôle crucial de la cyber SCRM dans la gestion des risques de cybersécurité dans les infrastructures critiques et l'économie numérique au sens large. Ces relations, les produits et services qu'elles fournissent et les risques qu'elles présentent doivent être identifiés et pris en compte dans les capacités de protection et de détection des organisations, ainsi que dans leurs protocoles de réponse et de récupération.

Dans la figure ci-dessus, "Acheteur" fait référence aux personnes ou aux organisations en aval qui consomment un produit ou un service donné d'une organisation, y compris les organisations à but lucratif et non lucratif. "Fournisseur" englobe les fournisseurs de produits et de services en amont qui sont utilisés à des fins internes d'une organisation (p. ex., l'infrastructure informatique) ou intégrés aux produits ou services fournis à l'acheteur. Ces conditions s'appliquent aux produits et services technologiques et non technologiques.

Qu'il s'agisse de considérer les sous-catégories individuelles du noyau ou les considérations complètes d'un profil, le cadre offre aux organisations et à leurs partenaires une méthode pour aider à garantir que le nouveau produit ou service répond aux résultats de sécurité critiques. En sélectionnant d'abord les résultats pertinents au contexte (p. ex., la transmission d'informations personnellement identifiables (PII), la prestation de services essentiels à la mission, les services de vérification des données, l'intégrité du produit du service), l'organisation peut ensuite évaluer

les partenaires en fonction de ces critères. Par exemple, si un système est acheté qui surveillera la technologie opérationnelle (OT) pour les communications réseau anormales, la disponibilité peut être un objectif de cybersécurité particulièrement important à atteindre et devrait conduire une évaluation du fournisseur de technologie par rapport aux sous- catégories applicables (p. ex., ID.BE- 4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Décisions d'achat

Étant donné qu'un profil cible de cadre est une liste priorisée d'exigences de cybersécurité organisationnelles, les profils cibles peuvent être utilisés pour éclairer les décisions d'achat de produits et de services. Cette transaction diffère de la communication des exigences en matière de cybersécurité avec les parties prenantes (adressée dans la section 3.3) en ce qu'il peut ne pas être possible d'imposer un ensemble d'exigences en matière de cybersécurité au fournisseur. L'objectif devrait être de prendre la meilleure décision d'achat parmi plusieurs fournisseurs, compte tenu d'une liste soigneusement déterminée d'exigences en matière de cybersécurité. Souvent, cela signifie un certain degré de compromis, en comparant plusieurs produits ou services avec des lacunes connues par rapport au profil cible.

Une fois qu'un produit ou un service est acheté, le profil peut également être utilisé pour suivre et adresser les risques de cybersécurité résiduel. Par exemple, si le service ou le produit acheté n'a pas atteint tous les objectifs décrits dans le profil cible, l'organisation peut adresser le risque résiduel par d'autres actions de gestion. Le profil fournit également à l'organisation une méthode pour apprécier si le produit répond aux résultats de cybersécurité grâce à des mécanismes d'examen et de test périodiques.

3.5 Identification des opportunités de références informatives nouvelles ou révisées

Le cadre peut être utilisé pour identifier les opportunités de normes, des lignes directrices ou pratiques nouvelles ou révisées où des références informatives supplémentaires aideraient les organisations pour s'adresser aux besoins émergents. Une organisation mettant en œuvre une sous-catégorie donnée, ou développant une nouvelle sous-catégorie, peut découvrir qu'il existe peu de références informatives, voire aucun, pour une activité connexe. Pour s'adresser à ce besoin, l'organisation peut collaborer avec des leaders technologiques et/ou des organismes de normalisation pour rédiger, développer et coordonner des normes, des lignes directrices ou des pratiques.

3.6 Méthodologie de protection de la vie privée et des libertés civiles

Cette section décrit une méthodologie pour adresser les implications individuelles en matière de la vie privée et des libertés civiles qui peuvent résulter de la cybersécurité. Cette méthodologie est destinée à être un ensemble général de considérations et de processus car les implications en matière de vie privée et de libertés civiles peuvent différer selon le secteur ou dans le temps et les organisations peuvent adresser ces considérations et processus avec une gamme de mises en œuvre techniques. Néanmoins, toutes les activités d'un programme de cybersécurité n'engendrent pas des considérations relatives à la vie privée et aux libertés civiles. Des normes techniques de confidentialité, des lignes directrices et des meilleures pratiques supplémentaires peuvent être développées pour prendre en charge des implémentations techniques améliorées.

La vie privée et la cybersécurité sont étroitement liées. Les activités de cybersécurité d'une organisation peuvent également créer des risques pour la vie privée et les libertés civiles lorsque des informations personnelles sont utilisées, collectées, traitées, conservées ou divulguées. Voici quelques exemples: activités de cybersécurité qui entraînent une collecte excessive ou une conservation excessive d'information personnelles; la divulgation ou l'utilisation de renseignement personnels non liées aux activités de cybersécurité; et les activités d'atténuation de la cybersécurité qui entraînent un déni de service ou d'autres impacts potentiellement négatifs similaires, y compris certains types de détection ou de surveillance d'incidents susceptibles d'entraver la liberté d'expression ou d'association.

Le gouvernement et ses agents ont la responsabilité de protéger les libertés civiles découlant des activités de cybersécurité. Comme indiqué dans la méthodologie ci-dessous, le gouvernement ou ses agents qui possèdent ou exploitent une infrastructure critique doivent avoir mis en place un processus en place pour soutenir la conformité des activités de cybersécurité avec les lois, réglementations et exigences constitutionnelles applicables en matière de vie privée.

Pour adresser les implications en matière de vie privée, les organisations peuvent envisager comment leur programme de cybersécurité pourrait intégrer des principes de vie privée tels que: la minimisation des données dans la collecte, la divulgation et la conservation des informations personnelles liées à l'incident de cybersécurité; utiliser des limitations en dehors des activités de cybersécurité sur toute information collectée spécifiquement pour les activités de cybersécurité; transparence pour certaines activités de cybersécurité; consentement individuel et réparation pour les impacts négatifs résultant de l'utilisation d'informations personnelles dans les activités de cybersécurité; la qualité, l'intégrité et la sécurité des données; et la responsabilité et l'audit.

Au fur et à mesure que les organisations apprécient le noyau du cadre de l'annexe A, les processus et activités suivants peuvent être considérés comme un moyen pour adresser les implications susmentionnées sur la vie privée et les libertés civiles:

Gouvernance du risque de cybersécurité

- L'appréciation par une organisation des risques de cybersécurité et des réponses potentielles aux risques tient compte des implications de son programme de cybersécurité sur la vie privée.
- Les personnes exerçant des responsabilités en matière de vie privée liées à la cybersécurité relèvent de la direction appropriée et sont correctement formées.
- Un processus est en place pour soutenir la conformité des activités de cybersécurité avec les lois, réglementations et exigences constitutionnelles applicables en matière de vie privée.
- Un processus est en place pour apprécier la mise en œuvre des mesures et contrôles organisationnels ci-dessus.

Approches pour identifier, authentifier et autoriser les individus à accéder aux actifs et aux systèmes de l'organisation

- Des étapes sont prises pour identifier et adresser les implications sur la vie privée de la gestion de l'identité et des mesures de contrôle d'accès dans la mesure où elles impliquent la collecte, la divulgation ou l'utilisation de renseignements personnels.

Mesures de sensibilisation et de formation

- Les informations applicables des politiques de vie privée de l'organisation sont incluses dans les activités de formation et de sensibilisation de l'effectif en cybersécurité.

- Les fournisseurs de services qui fournissent des services liés à la cybersécurité pour l'organisation sont informés des politiques de vie privée applicables de l'organisation.

Détection des activités anormales et surveillance du système et des actifs

- Un processus est en place pour effectuer un examen de la vie privée de la détection des activités anormales et de la surveillance de la cybersécurité d'une organisation.

Activités d'intervention, y compris le partage d'informations ou d'autres efforts d'atténuation

- Un processus est en place pour apprécier et adresser si, quand, comment et dans quelle mesure les informations personnelles sont partagées en dehors de l'organisation dans le cadre des activités de partage d'informations sur la cybersécurité.
- Un processus est en place pour effectuer un examen de la vie privée des efforts d'atténuation de la cybersécurité d'une organisation.

4.0 Auto-appréciation des risques de cybersécurité avec le cadre

Le cadre de cybersécurité est conçu pour réduire les risques en améliorant la gestion des risques de cybersécurité par rapport aux objectifs organisationnels. Idéalement, les organisations qui utilisent le cadre seront en mesure de mesurer et d'attribuer des valeurs à leur risque *ainsi que* le coût et les avantages des mesures prises pour réduire le risque à des niveaux acceptables. Mieux une organisation est en mesure de mesurer les risques, les coûts et les avantages des stratégies et des étapes de cybersécurité, plus son approche et ses investissements en matière de cybersécurité seront rationnels, efficaces et précieux.

Au fil du temps, l'auto-appréciation et le mesurage devraient améliorer la prise de décision en matière d'investissement priorités. Par exemple, mesurer - ou au moins caractériser de manière robuste - les aspects de l'état et des tendances de la cybersécurité d'une organisation au fil du temps peut permettre à cette organisation de comprendre et de transmettre des informations significatives sur les risques aux dépendent, fournisseurs, acheteurs et autres parties. Une organisation peut accomplir cela en interne ou en demandant une appréciation par un tiers. Si elles sont effectuées correctement et avec une appréciation des limites, ces mesurages peuvent fournir une base pour de solides relations de confiance, à la fois à l'intérieur et à l'extérieur d'une organisation.

Pour examiner l'efficacité des investissements, une organisation doit d'abord avoir une compréhension claire de ses objectifs organisationnels, de la relation entre ces objectifs et les résultats de cybersécurité favorables, et comment ces résultats de cybersécurité discrets sont mis en œuvre et gérés. Bien que les mesurages de tous ces éléments dépassent la portée du cadre, les résultats en matière de cybersécurité du noyau du cadre soutiennent l'auto-appréciation de l'efficacité des investissements et des activités de cybersécurité des manières suivantes:

- Faire des choix sur la manière dont les différentes parties de l'opération de cybersécurité devraient influencer le choix des niveaux de mise en œuvre cibles,
- Évaluer l'approche de l'organisation en matière de gestion des risques de cybersécurité en déterminant les niveaux de mise en œuvre actuels,
- Prioriser les résultats de la cybersécurité en développant des profils cibles,
- Déterminer dans quelle mesure des étapes de cybersécurité spécifiques permettent d'atteindre les résultats souhaités en matière de cybersécurité en appréciant les profils actuels, et
- Mesurer le degré de mise en œuvre des catalogues de contrôles ou des conseils techniques répertoriés comme références informatives.

Le développement de mesures de performance en matière de cybersécurité évolue. Les organisations doivent être réfléchies, créatives et prudentes quant à la manière dont elles utilisent les mesurages pour optimiser l'utilisation, tout en évitant de s'appuyer se fier à des indicateurs artificiels de l'état actuel et des progrès dans l'amélioration de la gestion des risques de cybersécurité. Juger le cyber-risque nécessite de la discipline et doit être revu périodiquement. Chaque fois que des mesurages sont utilisées dans le cadre du processus du cadre, les organisations sont encouragées à identifier clairement et à savoir pourquoi ces mesurages sont importantes et comment elles contribueront à la gestion globale des risques de cybersécurité. Ils doivent également être clairs sur les limites des mesurages utilisées.

Par exemple, le suivi des mesures de sécurité et des résultats métier peut fournir des informations utiles sur la manière dont les modifications apportées aux contrôles de sécurité granulaires affectent la réalisation des objectifs organisationnels. La vérification de la réalisation de certains objectifs organisationnels nécessite d'analyser les données uniquement *après* que cet objectif ait été atteint. Ce type de mesure retardée est plus absolu. Cependant, il est souvent plus utile de prédire si un risque de cybersécurité *peut* survenir et l'impact qu'il *pourrait avoir*, en utilisant une mesure avancée.

Les organisations sont encouragées à innover et à personnaliser la manière dont elles intègrent les mesurages dans leur application du cadre en tenant pleinement compte de leur utilité et leurs limites.

Annexe A: Noyau du cadre

Cette annexe présente le noyau du cadre : une liste de fonctions, de catégories, de sous-catégories et de références informatives qui décrivent des activités de cybersécurité spécifiques qui sont communes à tous les secteurs d'infrastructures critiques. Le format de présentation choisi pour le noyau du cadre ne suggère pas d'ordre de mise en œuvre spécifique ni n'implique un degré d'importance des catégories, sous-catégories et références informatives. Le noyau du cadre présenté dans cette annexe représente un ensemble commun d'activités de gestion des risques de cybersécurité. Bien que le cadre ne soit pas exhaustif, il est extensible, permettant aux organisations, secteurs et autres entités d'utiliser des sous-catégories et des références informatives qui sont rentables et efficaces et qui leur permettent de gérer leur risque de cybersécurité. Les activités peuvent être sélectionnées dans noyau du cadre pendant le processus de création du profil et des catégories, sous-catégories et références informatives supplémentaires peuvent être ajoutées au profil. Les processus de gestion des risques d'une organisation, les exigences légales/réglementaires, les objectifs métier/de mission et les contraintes organisationnelles guident la sélection de ces activités lors de la création du profil. Les informations personnelles sont considérées comme une composante des données ou des actifs référencés dans les catégories lors de l'appréciation des risques de sécurité et des protections.

Bien que les résultats escomptés identifiés dans les fonctions, catégories et sous-catégories soient les mêmes pour l'IT et les ICS, les environnements opérationnels et les considérations pour l'IT et les ICS diffèrent. Les ICS ont un effet direct sur le monde physique, y compris les risques potentiels pour la santé et la sécurité des individus, et l'impact sur l'environnement. De plus, les ICS ont des exigences de performances et de fiabilité uniques par rapport à l'IT, et les objectifs de sécurité et d'efficacité doivent être pris en compte lors de la mise en œuvre des mesures de cybersécurité.

Pour faciliter l'utilisation, chaque composant de noyau du cadre se voit attribuer un identifiant unique. Les fonctions et les catégories ont chacune un identifiant alphabétique unique, comme indiqué dans le Tableau 1. Les sous-catégories au sein de chaque catégorie sont référencées numériquement; l'identifiant unique pour chaque sous-catégorie est inclus dans le Tableau 2.

Des supports supplémentaires, y compris des références informatives, concernant le cadre peuvent être disponible sur le site web du NIST à l'adresse https://www.nist.gov/cyberframework.

Tableau 1: Identificateurs uniques de fonction et de catégorie

Identifiant unique de fonction	Fonction	Identifiant unique de catégorie	Catégorie
ID	Identifier	ID.AM	Gestion des actifs
		ID.BE	Environnement métier
		ID.GV	Gouvernance
		ID.RA	Appréciation des risques
		ID.RM	Stratégie de gestion des risques
		ID.SC	Gestion des risques de la chaîne d'approvisionnement
PR	Protéger	PR.AC	Gestion des identités et contrôle d'accès
		PR.AT	Sensibilisation et formation
		PR.DS	Sécurité des données
		PR.IP	Processus et procédures de protection des informations
		PR.MA	Maintenance
		PR.PT	Technologie de protection
DE	Détecter	DE.AE	Anomalies et événements
		DE.CM	Surveillance continue de la sécurité
		DE.DP	Processus de détection
RS	Répondre	RS.RP	Plan d'intervention
		RS.CO	Communications
		RS.AN	Analyse
		RS.MI	Atténuation
		RS.IM	Améliorations
RC	Rétablir	RC.RP	Planification de la récupération
		RC.IM	Améliorations
		RC.CO	Communications

Tableau 2: Noyau du cadre

Fonction	Catégorie	Sous-catégorie	Références informatives
IDENTIFIER (ID)	**Gestion des actifs (ID.AM):** Les données, le personnel, les appareils, les systèmes et les installations qui permettent à l'organisation d'atteindre les objectifs métier sont identifiés et gérés conformément à leur importance relative pour les objectifs organisationnels et la stratégie de risques de l'organisation.	**ID.AM-1:** Les appareils et systèmes physiques au sein de l'organisation sont inventoriés	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/CEI 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rév. 4** CM-8, PM-5
		ID.AM-2: Les plates-formes logicielles et les applications au sein de l'organisation sont inventoriées	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/CEI 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rév. 4** CM-8, PM-5
		ID.AM-3: La communication organisationnelle et les flux de données sont cartographiés	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/CEI 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rév. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Les systèmes d'information externes sont catalogués	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/CEI 27001:2013** A.11.2.6 **NIST SP 800-53 Rév. 4** AC-20, SA-9
		ID.AM-5: Les ressources (p. ex., le matériel, les appareils, les données, le temps, le personnel et les logiciels) sont priorisées en fonction de leur classification, de leur criticité et de leur valeur métier	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/CEI 27001:2013** A.8.2.1 **NIST SP 800-53 Rév. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Les rôles et responsabilités en matière de	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Fonction	Catégorie	Sous-catégorie	Références informatives
		cybersécurité pour l'ensemble de l'effectif et les parties prenantes tierces (p. ex., fournisseurs, clients, partenaires) sont établis	**ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/CEI 27001:2013** A.6.1.1 **NIST SP 800-53 Rév. 4** CP-2, PS-7, PM-11
	Environnement métier (ID.BE): La mission, les objectifs, les parties prenantes et les activités de l'organisation sont compris et priorisés; ces informations sont utilisées pour informer les rôles, les responsabilités et les décisions de gestion des risques en matière de cybersécurité.	**ID.BE-1:** Le rôle de l'organisation dans la chaîne d'approvisionnement est identifié et communiqué	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/CEI 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rév. 4** CP-2, SA-12
		ID.BE-2: La place de l'organisation dans les infrastructures critiques et son secteur industriel est identifiée et communiquée	**COBIT 5** APO02.06, APO03.01 **ISO/CEI 27001:2013** Clause 4.1 **NIST SP 800-53 Rév. 4** PM-8
		ID.BE-3: Les priorités de la mission, des objectifs et des activités de l'organisation sont établies et communiquées	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rév. 4** PM-11, SA-14
		ID.BE-4: Les dépendances et les fonctions critiques pour la fourniture de services critiques sont établies	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/CEI 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rév. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Les exigences de résilience pour soutenir la prestation de services critiques sont établies pour tous les états opérationnels (p. ex. sous la contrainte/attaque, pendant la récupération, opérations normales)	**COBIT 5** BAI03.02, DSS04.02 **ISO/CEI 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rév. 4** CP-2, CP-11, SA-13, SA-14
	Gouvernance (ID.GV): Les politiques, procédures et processus pour gérer et surveiller les exigences réglementaires, juridiques, de risque, environnementales et opérationnelles de l'organisation sont comprises et informent la gestion du risque de cybersécurité.	**ID.GV-1:** Une politique organisationnelle de cybersécurité est établie et communiquée	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/CEI 27001:2013** A.5.1.1 **NIST SP 800-53 Rév. 4** Contrôles -1 de toutes les familles de contrôle de sécurité
		ID.GV-2: Les rôles et responsabilités en matière de cybersécurité sont	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04

Fonction	Catégorie	Sous-catégorie	Références informatives
		coordonnés et alignés avec les rôles internes et les partenaires externes	**ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rév. 4** PS-7, PM-1, PM-2
		ID.GV-3: Les exigences légales et réglementaires en matière de cybersécurité, y compris les obligations en matière de vie privée et de libertés civiles, sont comprises et gérées	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/CEI 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rév. 4** Contrôles -1 de toutes les familles de contrôle de sécurité
		ID.GV-4: Les processus de gouvernance et de gestion des risques adressent les risques de cybersécurité	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/CEI 27001:2013** Clause 6 **NIST SP 800-53 Rév. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Appréciation des risques (ID.RA): L'organisation comprend le risque de cybersécurité pour les opérations organisationnelles (y compris la mission, les fonctions, l'image ou la réputation), les actifs organisationnels et les individus.	**ID.RA-1:** Les vulnérabilités des actifs sont identifiées et documentées	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/CEI 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rév. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Les renseignements sur les cybermenaces proviennent de forums et de sources de partage d'informations	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/CEI 27001:2013** A.6.1.4 **NIST SP 800-53 Rév. 4** SI-5, PM-15, PM-16
		ID.RA-3: Les menaces, internes et externes, sont identifiées et documentées	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/CEI 27001:2013** Clause 6.1.2

Fonction	Catégorie	Sous-catégorie	Références informatives
			NIST SP 800-53 Rév. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Les impacts métier potentiels et les vraisemblances sont identifiés	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/CEI 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rév. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Les menaces, les vulnérabilités, les vraisemblances et les impacts sont utilisés pour déterminer le risque	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/CEI 27001:2013** A.12.6.1 **NIST SP 800-53 Rév. 4** RA-2, RA-3, PM-16
		ID.RA-6: Les réponses aux risques sont identifiées et priorisées	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/CEI 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rév. 4** PM-4, PM-9
	Stratégie de gestion des risques (ID.RM): Les priorités, les contraintes, les tolérances au risque et les hypothèses de l'organisation sont établies et utilisées pour appuyer 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	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/CEI 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rév. 4** PM-9
		ID.RM-2: La tolérance au risque organisationnelle est déterminée et clairement exprimée	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/CEI 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rév. 4** PM-9
		ID.RM-3: La détermination de la tolérance au risque de l'organisation est éclairée par son rôle dans les infrastructures critiques et l'analyse des risques spécifiques au secteur	**COBIT 5** APO12.02 **ISO/CEI 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rév. 4** SA-14, PM-8, PM-9, PM-11
			CIS CSC 4

Fonction	Catégorie	Sous-catégorie	Références informatives
	Gestion des risques de la chaîne d'approvisionnement (ID.SC): Les priorités, les contraintes, les tolérances au risque et les hypothèses sont établies et utilisées pour étayer les décisions relatives aux risques associées à la gestion des risques de la chaîne d'approvisionnement. L'organisation a établi et mis en œuvre les processus pour identifier, apprécier et gérer les risques liés à la chaîne d'approvisionnement.	**ID.SC-1:** Les processus de gestion des risques de la cyber chaîne d'approvisionnement sont identifiés, établis, appréciés, gérés et acceptés par les parties prenantes de l'organisation	**COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/CEI 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rév. 4** SA-9, SA-12, PM-9
		ID.SC-2: Les fournisseurs et les partenaires tiers des systèmes d'information, des composants et des services sont identifiés, priorisées et appréciés à l'aide d'un processus d'appréciation des risques de la cyber chaîne d'approvisionnement	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2 .3.14 **ISO/CEI 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rév. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		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 d'une organisation et du plan de gestion des risques de la cyber chaîne d'approvisionnement	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/CEI 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rév. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Les fournisseurs et les partenaires tiers sont régulièrement appréciés à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluation pour confirmer qu'ils respectent leurs obligations contractuelles.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/CEI 27001:2013** A.15.2.1, A.15.2.2 NIST SP 800-53 Rev.4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: La planification et les tests de réponse et de récupération sont effectués avec des fournisseurs et prestataires tiers	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/CEI 27001:2013** A.17.1.3

Fonction	Catégorie	Sous-catégorie	Références informatives
			NIST SP 800-53 Rév. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTÉGER (PR)	**Gestion des identités, authentification et contrôle d'accès (PR.AC):** L'accès aux actifs physiques et logiques et aux installations associées est limité aux utilisateurs, processus et appareils autorisés, et est géré conformément au risque apprécié d'accès non autorisé aux activités et transactions autorisées.	**PR.AC-1:** Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, utilisateurs et processus autorisés	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/CEI 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A .9.4.3 NIST SP 800-53 Rev.4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA -9, IA-10, IA-11
		PR.AC-2: L'accès physique aux actifs est géré et protégé	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/CEI 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A .11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rév. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: L'accès à distance est géré	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/CEI 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rév. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Les autorisations d'accès et les autorisations sont gérées, en intégrant les principes du moindre privilège et de la séparation des tâches	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/CEI 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rév. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
			CIS CSC 9, 14, 15, 18

Fonction	Catégorie	Sous-catégorie	Références informatives
		PR.AC-5: L'intégrité du réseau est protégée (p. ex., ségrégation du réseau, segmentation du réseau)	**COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/CEI 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rév. 4** AC-4, AC-10, SC-7
		PR.AC-6: Les identités sont vérifiées et liées aux informations d'identification et affirmées dans les interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/CEI 27001:2013**, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev.4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA -8, PE-2, PS-3
		PR.AC-7: Les utilisateurs, appareils et autres actifs sont authentifiés (p. ex., à un facteur, à plusieurs facteurs) en fonction du risque de la transaction (p. ex., risques pour la sécurité et la vie privée des individus et autres risques organisationnels)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7 , 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/CEI 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev.4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA -5, IA-8, IA-9, IA-10, IA-11
	Sensibilisation et formation (PR.AT): Le personnel et les partenaires de l'organisation reçoivent une formation sur la sensibilisation à la cybersécurité et sont formés pour s'acquitter de leurs tâches et responsabilités liées à la cybersécurité conformément	**PR.AT-1:** Tous les utilisateurs sont informés et formés	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/CEI 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rév. 4** AT-2, PM-13
		PR.AT-2: Les utilisateurs privilégiés comprennent leurs rôles et responsabilités	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3

Fonction	Catégorie	Sous-catégorie	Références informatives
	aux politiques, procédures et accords connexes.		**ISO/CEI 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rév. 4** AT-3, PM-13
		PR.AT-3: Les parties prenantes tierces (p. ex., fournisseurs, clients, partenaires) comprennent leurs rôles et responsabilités	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rév. 4** PS-7, SA-9, SA-16
		PR.AT-4: Les cadres supérieurs comprennent leurs rôles et responsabilités	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rév. 4** AT-3, PM-13
		PR.AT-5: Le personnel physique et de cybersécurité comprend ses rôles et responsabilités	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rév. 4** AT-3, IR-2, PM-13
	Sécurité des données (PR.DS): Les informations et les enregistrements (données) sont gérés conformément à la stratégie de gestion des risques de l'organisation pour protéger la confidentialité, l'intégrité et la disponibilité des informations.	**PR.DS-1:** Les données au repos sont protégées	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/CEI 27001:2013** A.8.2.3 **NIST SP 800-53 Rév. 4** MP-8, SC-12, SC-28
		PR.DS-2: Les données en transit sont protégées	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/CEI 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rév. 4** SC-8, SC-11, SC-12
			CIS CSC 1

Fonction	Catégorie	Sous-catégorie	Références informatives
		PR.DS-3: Les actifs sont officiellement gérés tout au long du retrait, des transferts et de la disposition	**COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/CEI 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rév. 4** CM-8, MP-6, PE-16
		PR.DS-4: Une capacité adéquate est maintenue pour garantir la disponibilité	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/CEI 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rév. 4** AU-4, CP-2, SC-5
		PR.DS-5: Les protections contre les fuites de données sont mises en œuvre	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/CEI 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A .9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2 .1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rév. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI -4
		PR.DS-6: Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des micrologiciels et des informations	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/CEI 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rév. 4** SC-16, SI-7
		PR.DS-7: Les environnements de développement et de test sont séparés de l'environnement de production	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/CEI 27001:2013** A.12.1.4 **NIST SP 800-53 Rév. 4** CM-2
			COBIT 5 BAI03.05

Fonction	Catégorie	Sous-catégorie	Références informatives
		PR.DS-8: Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité du matériel	**ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/CEI 27001:2013** A.11.2.4 **NIST SP 800-53 Rév. 4** SA-10, SI-7
	Processus et procédures de protection de l'information (PR.IP): Les politiques de sécurité (qui adressent de l'objectif, de la portée, des rôles, des responsabilités, de l'engagement de la direction et de la coordination entre les entités organisationnelles), des processus et des procédures sont maintenus et utilisés pour gérer la protection des systèmes d'information et des actifs .	**PR.IP-1:** Une configuration de base des technologies de l'information/systèmes de contrôle industriel est créée et maintenue en incorporant les principes de sécurité (p. ex., le concept de moindre fonctionnalité)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/CEI 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rév. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Un cycle de vie de développement de système pour gérer les systèmes est mis en œuvre	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/CEI 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rév. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI -13, SI-14, SI-16, SI-17
		PR.IP-3: Les processus de contrôle des changements de configuration sont en place	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/CEI 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rév. 4** CM-3, CM-4, SA-10
		PR.IP-4: Les sauvegardes d'informations sont effectuées, maintenues et testées	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/CEI 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rév. 4** CP-4, CP-6, CP-9
			COBIT 5 DSS01.04, DSS05.05

Fonction	Catégorie	Sous-catégorie	Références informatives
		PR.IP-5: La politique et les réglementations concernant l'environnement d'exploitation physique des actifs de l'organisation sont respectées	**ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/CEI 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rév. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Les données sont détruites conformément à la politique	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/CEI 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rév. 4** MP-6
		PR.IP-7: Les processus de protection sont améliorés	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/CEI 27001:2013** A.16.1.6, Article 9, Article 10 **NIST SP 800-53 Rév. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: L'efficacité des technologies de protection est partagée	**COBIT 5** BAI08.04, DSS03.04 **ISO/CEI 27001:2013** A.16.1.6 **NIST SP 800-53 Rév. 4** AC-21, CA-7, SI-4
		PR.IP-9: Les plans d'intervention (réponse aux incidents et continuité des activités) et les plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/CEI 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rév. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Les plans d'intervention et de reprise sont testés	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/CEI 27001:2013** A.17.1.3 **NIST SP 800-53 Rév. 4** CP-4, IR-3, PM-14
			CIS CSC 5, 16

Fonction	Catégorie	Sous-catégorie	Références informatives
		PR.IP-11: La cybersécurité est incluse dans les pratiques des ressources humaines (p. ex., déprovisionnement, filtrage du personnel)	**COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/CEI 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rév. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/CEI 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rév. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): La maintenance et les réparations des composants de contrôle industriel et du système d'information sont effectuées conformément aux politiques et procédures.	**PR.MA-1:** La maintenance et la réparation des actifs de l'organisation sont effectuées et enregistrées, avec des outils approuvés et contrôlés	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/CEI 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rév. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: La maintenance à distance des actifs de l'organisation est approuvée, enregistrée et effectuée de manière à empêcher tout accès non autorisé	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/CEI 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rév. 4** MA-4
	Technologie de protection (PR.PT): Les solutions de sécurité technique sont gérées pour assurer la sécurité et la résilience des systèmes et des actifs, conformément aux politiques, procédures et accords connexes.	**PR.PT-1:** Les enregistrements d'audit/journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/CEI 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 Famille **NIST SP 800-53 Rév. 4** AU
		PR.PT-2: Les supports amovibles sont protégés et leur utilisation est	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06

Fonction	Catégorie	Sous-catégorie	Références informatives
		restreinte conformément à la politique	**ISA 62443-3-3:2013** SR 2.3 **ISO/CEI 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rév. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Le principe de moindre fonctionnalité est incorporé en configurant les systèmes pour ne fournir que les capacités critiques	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7 , 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3 .3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1 , SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/CEI 27001:2013** A.9.1.2 **NIST SP 800-53 Rév. 4** AC-3, CM-7
		PR.PT-4: Les réseaux de communication et de contrôle sont protégés	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/CEI 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rév. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC -24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Les mécanismes (p. ex., sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/CEI 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rév. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DÉTECTER (DE)	**Anomalies et événements (DE.AE):** Une activité anormale est détectée et	**DE.AE-1:** Une base de référence des opérations réseau et des flux de	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Fonction	Catégorie	Sous-catégorie	Références informatives
	l'impact potentiel des événements est compris.	données attendus pour les utilisateurs et les systèmes est établie et gérée	**ISO/CEI 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rév. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Les événements détectés sont analysés pour comprendre les cibles et les méthodes d'attaque	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/CEI 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rév. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Les données d'événements sont collectées et corrélées à partir de plusieurs sources et capteurs	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/CEI 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rév. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: L'impact des événements est déterminé	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/CEI 27001:2013** A.16.1.4 **NIST SP 800-53 Rév. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Les seuils d'alerte d'incident sont établis	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/CEI 27001:2013** A.16.1.4 **NIST SP 800-53 Rév. 4** IR-4, IR-5, IR-8
	Surveillance continue de la sécurité (DE.CM): 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	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rév. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: L'environnement physique est surveillé pour détecter	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8

Fonction	Catégorie	Sous-catégorie	Références informatives
		les événements potentiels de cybersécurité	**ISO/CEI 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rév. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: L'activité du personnel est surveillée pour détecter les événements potentiels de cybersécurité	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/CEI 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rév. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Le code malveillants est détecté	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/CEI 27001:2013** A.12.2.1 **NIST SP 800-53 Rév. 4** SI-3, SI-8
		DE.CM-5: Le code mobile non autorisé est détecté	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/CEI 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 800-53 Rév. 4** SC-18, SI-4, SC-44
		DE.CM-6: L'activité des prestataires de services externes est surveillée pour détecter les événements potentiels de cybersécurité	**COBIT 5** APO07.06, APO10.05 **ISO/CEI 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rév. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est effectuée	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/CEI 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rév. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Les analyses de vulnérabilité sont effectuées	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7

Fonction	Catégorie	Sous-catégorie	Références informatives
			ISO/CEI 27001:2013 A.12.6.1 **NIST SP 800-53 Rév. 4** RA-5
	Processus de détection (DE.DP): Les processus et procédures de détection sont maintenus et testés pour assurer la prise de conscience des événements anormaux.	**DE.DP-1:** Les rôles et les responsabilités en matière de détection sont bien définis pour garantir l'imputabilité	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rév. 4** CA-2, CA-7, PM-14
		DE.DP-2: Les activités de détection sont conformes à toutes les exigences applicables	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/CEI 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rév. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Les processus de détection sont testés	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/CEI 27001:2013** A.14.2.8 **NIST SP 800-53 Rév. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Les informations de détection d'événement sont communiquées	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/CEI 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rév. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Les processus de détection sont continuellement améliorés	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/CEI 27001:2013** A.16.1.6 **NIST SP 800-53 Rév. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
REPONDRE (RS)	**Plan d'intervention (RS.RP):** Les processus et procédures d'intervention sont exécutés et	**RS.RP-1:** Le plan d'intervention est exécuté pendant ou après un incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1

Fonction	Catégorie	Sous-catégorie	Références informatives
	maintenus pour garantir la réponse aux incidents de cybersécurité détectés.		**ISO/CEI 27001:2013** A.16.1.5 **NIST SP 800-53 Rév. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Les activités d'intervention sont coordonnées avec les parties prenantes internes et externes (p. ex., le soutien externe des forces de l'ordre).	**RS.CO-1:** Le personnel connaît ses rôles et l'ordre des opérations lorsqu'une intervention est nécessaire	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/CEI 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rév. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Les incidents sont signalés conformément aux critères établis	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/CEI 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rév. 4** AU-6, IR-6, IR-8
		RS.CO-3: Les informations sont partagées conformément aux plans d'intervention	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/CEI 27001:2013** A.16.1.2, article 7.4, article 16.1.2 **NIST SP 800-53 Rév. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: La coordination avec les parties prenantes se fait conformément aux plans d'intervention	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/CEI 27001:2013** Clause 7.4 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-8
		RS.CO-5: Un partage volontaire d'informations a lieu avec des parties prenantes externes pour parvenir à une meilleure connaissance de la situation en matière de cybersécurité	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/CEI 27001:2013** A.6.1.4 **NIST SP 800-53 Rév. 4** SI-5, PM-15
	Analyse (RS.AN): Une analyse est menée pour assurer	**RS.AN-1:** Les notifications des systèmes de détection sont étudiées	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07

Fonction	Catégorie	Sous-catégorie	Références informatives
	une intervention efficace et soutenir les activités de récupération.		**ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/CEI 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rév. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: L'impact de l'incident est compris	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/CEI 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rév. 4** CP-2, IR-4
		RS.AN-3: Les forensique sont effectuées	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/CEI 27001:2013** A.16.1.7 **NIST SP 800-53 Rév. 4** AU-7, IR-4
		RS.AN-4: Les incidents sont classés conformément aux plans de reprise	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/CEI 27001:2013** A.16.1.4 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Les processus sont établis pour recevoir, analyser et répondre aux vulnérabilités divulguées à l'organisation à partir de sources internes et externes (p. ex., des tests internes, des bulletins de sécurité ou des chercheurs en sécurité)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rév. 4** SI-5, PM-15
	Atténuation (RS.MI): Les activités sont effectuées pour empêcher l'expansion d'un événement, atténuer ses effets et résoudre l'incident.	**RS.MI-1:** Les incidents sont contenus	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/CEI 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rév. 4** IR-4

Fonction	Catégorie	Sous-catégorie	Références informatives
		RS.MI-2: Les incidents sont atténués	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/CEI 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rév. 4** IR-4
		RS.MI-3: Les vulnérabilités nouvellement identifiées sont atténuées ou documentées comme des risques acceptés	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/CEI 27001:2013** A.12.6.1 **NIST SP 800-53 Rév. 4** CA-7, RA-3, RA-5
	Améliorations (RS.IM): Les activités de réponse organisationnelle sont améliorées en incorporant les leçons tirées des activités de détection/réponse actuelles et précédentes.	**RS.IM-1:** Les plans d'intervention intègrent les leçons apprises	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/CEI 27001:2013** A.16.1.6, Article 10 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-8
		RS.IM-2: Les stratégies d'intervention sont mises à jour	**COBIT 5** BAI01.13, DSS04.08 **ISO/CEI 27001:2013** A.16.1.6, Article 10 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-8
RÉTABLIR (RC)	**Planification de la récupération (RC.RP):** Les processus et procédures de récupération sont exécutés et maintenus pour garantir la restauration des systèmes ou des actifs affectés par des incidents de cybersécurité.	**RC.RP-1:** Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/CEI 27001:2013** A.16.1.5 **NIST SP 800-53 Rév. 4** CP-10, IR-4, IR-8
	Améliorations (RC.IM): La planification et les processus de récupération sont améliorés en incorporant les leçons apprises dans les activités futures.	**RC.IM-1:** Les plans de récupération intègrent les leçons apprises	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/CEI 27001:2013** A.16.1.6, Article 10 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-8
		RC.IM-2: Les stratégies de récupération sont mises à jour	**COBIT 5** APO12.06, BAI07.08 **ISO/CEI 27001:2013** A.16.1.6, Article 10 **NIST SP 800-53 Rév. 4** CP-2, IR-4, IR-8

Fonction	Catégorie	Sous-catégorie	Références informatives
	Communications (RC.CO): Les activités de restauration sont coordonnées avec les parties internes et externes (p. ex. les centres de coordination, les fournisseurs d'accès Internet, les propriétaires de systèmes d'attaque, les victimes, les autres CSIRT et les fournisseurs).	**RC.CO-1:** Les relations publiques sont gérées	**COBIT 5** EDM03.02 **ISO/CEI 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: La réputation est réparée après un incident	**COBIT 5** MEA03.02 **ISO/CEI 27001:2013** Clause 7.4
		RC.CO-3: Les activités de récupération sont communiquées aux parties prenantes internes et externes ainsi qu'aux équipes de direction et de gestion	**COBIT 5** APO12.06 **ISO/CEI 27001:2013** Clause 7.4 **NIST SP 800-53 Rév. 4** CP-2, IR-4

Les informations concernant les références informatives décrites dans l'annexe A peuvent être trouvées aux emplacements suivants:

- Objectifs de contrôle de l'information et des technologies connexes (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Contrôles de sécurité critiques CIS pour une cyberdéfense efficace (contrôles CIS): https://www.cisecurity.org
- Institut national de normalisation américain/Société d'automatisation internationale (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Sécurité pour les systèmes d'automatisation et de contrôle industriels: Etablissement d'un programme de sécurité des systèmes d'automatisation et de contrôle industriels* : https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03) -2013, *Sécurité des systèmes d'automatisation et de contrôle industriels: Exigences de sécurité du système et niveaux de sécurité* : https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/CEI 27001, *Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences* : https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev.4 - Publication spéciale NIST 800-53 révision 4, *Contrôles de sécurité et de vie privée pour les systèmes et organisations d'information fédéraux*, avril 2013 (y compris les mises à jour au 22 janvier 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Les références informatives ne sont mappées qu'au niveau de contrôle, bien que toute amélioration de contrôle puisse être jugée utile pour atteindre un résultat de sous-catégorie.

Les correspondances entre les sous-catégories principales de noyau du cadre et les sections spécifiées dans les références informatives ne sont pas destinées à déterminer de manière définitive si les sections spécifiées dans les références informatives fournissent le résultat souhaité de la sous-catégorie.

Les références informatives ne sont pas exhaustives, dans la mesure où tous les éléments (p. ex., contrôle, exigence) d'une référence informative donnée ne sont pas mappés aux sous-catégories principales de noyau du cadre.

Annexe B: Glossaire

Cette annexe définit certains termes utilisés dans la publication.

Tableau 3: Glossaire du cadre

Acheteur	Les personnes ou les organisations qui consomment un produit ou un service donné.
Catégorie	La subdivision d'une fonction en groupes de résultats de cybersécurité, étroitement liés aux besoins programmatiques et à des activités particulières. Des exemples de catégories incluent "Gestion des actifs", "Gestion des identités et contrôle d'accès" et "Processus de détection".
Infrastructure critique	Systèmes et actifs, qu'ils soient physiques ou virtuels, si vitaux pour les États-Unis que l'incapacité ou la destruction de ces systèmes et actifs aurait un impact débilitant sur la cybersécurité, la sécurité économique nationale, la santé ou la sécurité publiques nationales, ou toute combinaison de ces questions.
Cybersécurité	Le processus de protection des informations par la prévention, la détection et la réponse aux attaques.
Événement de cybersécurité	Un changement de cybersécurité qui peut avoir un impact sur les opérations organisationnelles (y compris la mission, les capacités ou la réputation).
Incident de cybersécurité	Un événement de cybersécurité dont il a été déterminé qu'il a un impact sur l'organisation, ce qui entraîne le besoin d'une réponse et d'une récupération.
Détecter (fonction)	Développer et mettre en œuvre les activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.
Cadre	Une approche basée sur les risques pour réduire les risques de cybersécurité composée de trois parties: le noyau du cadre , le profil du cadre et les niveaux de mise en œuvre du cadre. Aussi connu sous le nom de "Cadre de cybersécurité".
Noyau du cadre	Un ensemble d'activités et de références de cybersécurité qui sont communes à tous les secteurs d'infrastructures critiques et sont organisées autour de résultats particuliers. Le noyau du cadre comprend quatre types d'éléments: fonctions, catégories, sous-catégories et références informatives.
Niveau de mise en œuvre du cadre	Une lentille à travers laquelle visualiser les caractéristiques de l'approche du risque d'une organisation - comment une organisation perçoit le risque de cybersécurité et les processus en place pour gérer ce risque.

Profil de cadre	Une représentation des résultats qu'un système ou une organisation particulière a sélectionnés parmi les catégories et sous-catégories du cadre.
Fonction	L'un des principaux composants du cadre. Les fonctions fournissent le plus haut niveau de structure pour organiser les activités de cybersécurité de base en catégories et sous-catégories. Les cinq fonctions sont Identifier, Protéger, Détecter, Réagir et Rétablir.
Identifier (fonction)	Développer la compréhension organisationnelle pour gérer les risques de cybersécurité pour les systèmes, les actifs, les données et les capacités.
Référence informative	Une section spécifique de normes, de lignes directrices et de pratiques communes aux secteurs des infrastructures critiques qui illustre une méthode pour atteindre les résultats associés à chaque sous-catégorie. Un exemple de référence informative est le contrôle ISO/CEI 27001 A.10 .8.3, qui prend en charge la sous-catégorie "Les données en transit sont protégées" de la catégorie "Sécurité des données" dans la fonction "Protéger".
Code mobile	Un programme (p. ex., un script, une macro ou une autre instruction portable) qui peut être livré inchangé à une collection hétérogène de plates-formes et exécuté avec une sémantique identique.
Protéger (fonction)	Développer et mettre en œuvre les garanties appropriées pour assurer la prestation des services d'infrastructure critiques.
Utilisateur privilégié	Un utilisateur qui est autorisé (et donc de confiance) à exécuter des fonctions liées à la sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter.
Réagir (fonction)	Développer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et pour restaurer les capacités ou les services qui ont été altérés en raison d'un événement de cybersécurité.
Rétablir (fonction)	Développer et mettre en œuvre les activités appropriées pour prendre des mesures concernant un événement de cybersécurité détecté.
Risque	Une mesure de l'étendue dans laquelle une entité est menacée par une circonstance ou un événement potentiel, et généralement en fonction: (i) des effets défavorables qui surviendraient si la circonstance ou l'événement se produisait; et (ii) la vraisemblance d'occurrence.
Gestion des risques	Le processus d'identification, d'appréciation et de réponse aux risques.

Sous-catégorie	La subdivision d'une catégorie en résultats spécifiques d'activités techniques et/ou de gestion. Des exemples de sous-catégories incluent "Les systèmes d'information externes sont catalogués", "Les données au repos sont protégées" et "Les notifications des systèmes de détection sont enquêtées."
Fournisseur	Fournisseurs de produits et de services utilisés à des fins internes à une organisation (p. ex., infrastructure informatique) ou intégrés aux produits de services fournis aux acheteurs de cette organisation.
Taxonomie	Un schéma de classification.

Annexe C: Acronymes

Cette annexe définit certains acronymes utilisés dans la publication.

ANSI	Institut national de normalisation américain
CEA	Loi de 2014 sur le renforcement de la cybersécurité
CIS	Centre de sécurité Internet
COBIT	Objectifs de contrôle de l'information et des technologies associées
CPS	Systèmes cyber-physiques
CSC	Contrôle de sécurité critique
DHS	Département de la sécurité intérieure
EO	Ordre exécutif
ICS	Systèmes de contrôle industriels
CEI	Commission électrotechnique internationale
IoT	Internet des objets
IR	Rapport inter-institutions
ISA	Société d'automatisation internationale
ISAC	Centre de partage et d'analyse d'informations
ISAO	Organisation de partage et d'analyse d'informations
ISO	Organisation internationale de normalisation
IT	Technologie de l'information
NIST	Institut national des normes et de la technologie
OT	Technologie opérationnelle
PII	Donnée à caractère personnel
RFI	Demande d'information
RMP	Processus de gestion des risques
SCRM	Gestion des risques de la chaîne d'approvisionnement
SP	Publication spéciale