Le Cadre de Cybersécurité du NIST (CSF) 2.0

Institut National des Normes et de la Technologie
Cette publication est disponible gratuitement sur : https://doi.org/10.6028/NIST.CSWP.29.fre

26 février 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Résumé

Le cadre de cybersécurité du NIST (CSF) 2.0 fournit des conseils à l'industrie, aux agences gouvernementales et à d'autres organisations pour gérer les risques de cybersécurité. Il propose une taxonomie de résultats de haut niveau de cybersécurité qui peuvent être utilisés par toute organisation, quelle que soit sa taille, son secteur ou sa maturité, pour mieux comprendre, évaluer, hiérarchiser et communiquer ses efforts en matière de cybersécurité. Le CSF ne prescrit pas comment les résultats doivent être atteints. Il renvoie plutôt à des ressources en ligne qui fournissent des conseils supplémentaires sur les pratiques et les contrôles qui pourraient être utilisés pour atteindre ces résultats. Ce document décrit le CSF 2.0, ses composants et certaines des nombreuses façons dont il peut être utilisé.

Mots-clés

cybersécurité ; Cadre de Cybersécurité (CSF) ; gouvernance des risques de cybersécurité ; gestion des risques de cybersécurité ; gestion des risques d'entreprise ; Profils ; Niveaux.

Public

Les personnes responsables du développement et de la direction des programmes de cybersécurité constituent le public cible principal du CSF. Le CSF peut également être utilisé par d'autres acteurs impliqués dans la gestion des risques – notamment les dirigeants, les conseils d'administration, les professionnels des acquisitions, les professionnels de la technologie, les gestionnaires de risques, les avocats, les spécialistes des ressources humaines et les auditeurs en cybersécurité et gestion des risques – pour guider leurs décisions en matière de cybersécurité. En outre, le CSF peut être utile à ceux qui élaborent et influencent les politiques (par exemple, les associations, les organisations professionnelles, les régulateurs) qui définissent et communiquent les priorités en matière de gestion des risques de cybersécurité.

Contenu supplémentaire

Le NIST continuera de créer et d'héberger des ressources supplémentaires pour aider les organisations à mettre en œuvre le CSF, notamment des Guides de Démarrage Rapide et des Profils Communautaires. Toutes les ressources sont mises à disposition du public sur le site web du NIST CSF. Les suggestions de ressources supplémentaires à référencer sur le site web du CSF du NIST peuvent toujours être partagées avec le NIST à cyberframework@nist.gov.

Note aux lecteurs

Sauf indication contraire, les documents cités, référencés ou extraits dans cette publication ne sont pas entièrement incorporés dans cette publication.

Avant la version 2.0, le Cadre de Cybersécurité s'appelait « Cadre pour l'amélioration de la cybersécurité des infrastructures critiques ». Ce titre n'est pas utilisé pour le CSF 2.0.

Remerciements

Le CSF est le résultat d'un effort collaboratif de plusieurs années entre l'industrie, le monde universitaire et le gouvernement aux États-Unis et dans le monde. Le NIST reconnaît et remercie tous ceux qui ont contribué à la révision de ce CSF. Des informations sur le processus de développement du CSF sont disponibles sur le site web du NIST CSF. Les leçons apprises sur l'utilisation du CSF peuvent toujours être partagées avec le NIST à cyberframework@nist.gov.

Traduit par / Translated by Bachir Benyammi

Traduit avec l'aimable autorisation de l'Institut National des Normes et de la Technologie (NIST). La traduction a été relue pour le compte du NIST par TaikaTranslations LLC sous le contrat {133ND23PNB770271}. Traduction officielle du gouvernement américain. Tous droits réservés, Secrétaire au Commerce des USA.

Translated with permission courtesy of the National Institute of Standards and Technology (NIST). Translation reviewed on behalf of NIST by TaikaTranslations LLC under contract {133ND23PNB770271}. Official U.S. Government Translation. All rights reserved, US Secretary of Commerce.

Table des matières

Liste des figures

Préface

Le Cadre de Cybersécurité (CSF) 2.0 est conçu pour aider les organisations de toutes tailles et de tous secteurs (y compris l'industrie, le gouvernement, le milieu universitaire et les organisations à but non lucratif) à gérer et à réduire leurs risques de cybersécurité. Il est utile quel que soit le niveau de maturité et la sophistication technique des programmes de cybersécurité d'une organisation. Néanmoins, le CSF n'adopte pas une approche universelle. Chaque organisation a des risques communs et uniques, ainsi que des appétences et des tolérances au risque différents, des missions spécifiques et des objectifs pour atteindre ces missions. Par nécessité, la manière dont les organisations mettent en œuvre le CSF variera.

Idéalement, le CSF sera utilisé pour s'adresser aux risques de cybersécurité ainsi que d'autres risques de l'entreprise, notamment ceux qui sont de nature financière, de vie privée, de chaîne d'approvisionnement, de réputation, technologiques ou physiques.

Le CSF *décrit* les résultats souhaités qui sont destinés à être compris par un large public, notamment des dirigeants, des gestionnaires et des praticiens, quelle que soit leur expertise en de cybersécurité. Étant donné que ces résultats sont neutres en termes de secteur, de pays et de technologie, ils offrent à une organisation la flexibilité nécessaire pour s'adresser à ses propres risques, technologies et considérations de mission uniques. Les résultats sont directement mappés à une liste de contrôles de sécurité potentiels à prendre en compte immédiatement pour atténuer les risques de cybersécurité.

Bien qu'il ne soit pas prescriptif, le CSF aide ses utilisateurs à se renseigner sur des résultats spécifiques et à les sélectionner. Des suggestions sur la manière d'atteindre des résultats spécifiques sont fournies dans une série croissante de ressources en ligne qui complètent le CSF, y compris une série de Guides de Démarrage Rapide (QSG). En outre, divers outils proposent des formats téléchargeables pour aider les organisations qui choisissent d'automatiser certains de leurs processus. Les QSG suggèrent des façons initiales d'utiliser le CSF et invitent le lecteur à explorer le CSF et les ressources associées plus en profondeur. Disponibles sur le site web du NIST CSF, le CSF et ces ressources supplémentaires du NIST et d'autres doivent être considérés comme un « portefeuille CSF » pour aider à gérer et à réduire les risques. Quelle que soit la manière dont il est appliqué, le CSF incite ses utilisateurs à considérer leur posture de cybersécurité dans son contexte puis à adapter le CSF à leurs besoins spécifiques.

S'appuyant sur les versions précédentes, le CSF 2.0 contient de nouvelles fonctionnalités qui soulignent l'importance de *la gouvernance* et *des chaînes d'approvisionnement*. Une attention particulière est accordée aux QSG pour garantir que le CSF est pertinent et facilement accessible par les petites organisations ainsi que leurs homologues plus grandes. Le NIST fournit désormais *des Exemples de Mise en Œuvre* et *des Références Informatives*, qui sont disponibles en ligne et mis à jour régulièrement. La création de *Profils Organisationnels* d'état actuel et cible aide les organisations à comparer où elles se trouvent et où elles veulent ou doivent être et leur permet de mettre en œuvre et d'évaluer les contrôles de sécurité plus rapidement.

Les risques de cybersécurité sont en constante augmentation et la gestion de ces risques doit être un processus continu. Cela est vrai, que l'organisation commence tout juste à faire face à

ses défis en matière de cybersécurité ou qu'elle soit active depuis de nombreuses années avec une équipe de cybersécurité sophistiquée et bien dotée en ressources. Le CSF est conçu pour être utile à tout type d'organisation et devrait fournir des conseils appropriés sur une longue période.

1. Aperçu du Cadre de Cybersécurité (CSF)

Ce document est la version 2.0 du Cadre de Cybersécurité du NIST (*Cadre* ou *CSF*). Il comprend les composants suivants :

- ***Noyau du CSF***, le cœur du CSF, qui est une taxonomie de résultats de cybersécurité de haut niveau pouvant aider toute organisation à gérer ses risques de cybersécurité. Les composants du Noyau du CSF sont une hiérarchie de Fonctions, Catégories et Sous-catégories qui détaillent chaque résultat. Ces résultats peuvent être compris par un large public, notamment des dirigeants, des gestionnaires et des praticiens, quelle que soit leur expertise en cybersécurité. Étant donné que les résultats sont neutres en termes de secteur, de pays et de technologie, ils offrent à une organisation la flexibilité nécessaire pour répondre à ses risques, technologies et considérations de mission uniques.
- ***Profils Organisationnels du CSF***, qui sont un mécanisme permettant de décrire la posture de cybersécurité actuelle et/ou cible d'une organisation en termes de résultats du Noyau du CSF.
- ***Niveaux du CSF***, qui peuvent être appliqués aux Profils Organisationnels du CSF pour caractériser la rigueur des pratiques de gouvernance et de gestion des risques de cybersécurité d'une organisation. Les niveaux peuvent également fournir un contexte sur la façon dont une organisation perçoit les risques de cybersécurité et les processus en place pour gérer ces risques.

Ce document décrit les résultats souhaitables qu'une organisation peut aspirer à atteindre. Il ne *prescrit pas* de résultats ni *la manière* dont ils peuvent être atteints. Des descriptions de *la manière dont* une organisation peut atteindre ces résultats sont fournies dans une série de ressources en ligne qui complètent le CSF et sont disponibles sur le site web du NIST CSF. Ces ressources offrent des conseils supplémentaires sur les pratiques et les contrôles qui pourraient être utilisés pour atteindre des résultats et sont destinées à aider une organisation à comprendre, adopter et utiliser le CSF. Elles comprennent :

- *Références Informatives* qui pointent vers des sources d'orientation sur chaque résultat à partir des normes, lignes directrices, cadres, réglementations, politiques, etc. mondiaux existants.
- *Exemples de Mise en Œuvre* illustrant les moyens potentiels pour atteindre chaque résultat
- *Guides de Démarrage Rapide* qui fournissent des conseils pratiques sur l'utilisation du CSF et de ses ressources en ligne, y compris la transition des versions précédentes du CSF vers la version 2.0.
- *Profils Communautaires et Modèles de Profils Organisationnels* qui aident une organisation à mettre en pratique le CSF et à définir des priorités pour la gestion des risques de cybersécurité.

Une organisation peut utiliser le Noyau, les profils et les niveaux du CSF avec les ressources supplémentaires pour comprendre, évaluer, hiérarchiser et communiquer les risques de cybersécurité.

- **Comprendre et évaluer :** Décrire la posture de cybersécurité actuelle ou cible d'une partie ou de la totalité d'une organisation, déterminer les lacunes et évaluez les progrès réalisés pour combler ces lacunes.
- **Prioriser :** Identifier, organiser et hiérarchiser les actions de gestion des risques de cybersécurité qui correspondent à la mission de l'organisation, aux exigences légales et réglementaires, ainsi qu'aux attentes en matière de gestion des risques et de gouvernance.
- **Communiquer :** Fournir un langage commun pour communiquer à l'intérieur et à l'extérieur de l'organisation sur les risques, les capacités, les besoins et les attentes en matière de cybersécurité.

Le CSF est conçu pour être utilisé par des organisations de toutes tailles et de tous secteurs, y compris l'industrie, le gouvernement, le monde universitaire et les organisations à but non lucratif, quel que soit le niveau de maturité de leurs programmes de cybersécurité. Le CSF est une ressource fondamentale qui peut être adoptée volontairement et par le biais de politiques et de mandats gouvernementaux. La taxonomie du CSF et les normes, lignes directrices et pratiques référencées ne sont pas spécifiques à un pays, et les versions précédentes du CSF ont été exploitées avec succès par de nombreux gouvernements et autres organisations à l'intérieur et à l'extérieur des États-Unis.

Le CSF doit être utilisé conjointement avec d'autres ressources (p. ex., cadres, normes, lignes directrices, pratiques exemplaires) pour mieux gérer les risques de cybersécurité et éclairer la gestion globale des risques liés aux technologies de l'information et des communications (TIC) au niveau de l'entreprise. Le CSF est un cadre flexible destiné à être adapté à l'utilisation par toutes les organisations, quelle que soit leur taille. Les organisations continueront d'avoir des risques, notamment des menaces et des vulnérabilités différentes, et des tolérances aux risques uniques ainsi des objectifs et des exigences de mission uniques. Ainsi, les approches des organisations en matière de gestion des risques et leurs mises en œuvre du CSF varieront.

Le reste de ce document est structuré comme suit :

- La section 2 explique les bases du Noyau du CSF : Fonctions, Catégories et Sous-catégories.
- La section 3 définit les concepts de Profils et de Niveaux du CSF.
- La section 4 fournit un aperçu des composants sélectionnés de la suite de ressources en ligne du CSF : Références Informatives, Exemples de Mise en Œuvre et Guides de Démarrage Rapide.
- La section 5 explique comment une organisation peut intégrer le CSF à d'autres programmes de gestion des risques.
- Annexe A est le Noyau du CSF.

- Annexe B contient une illustration notionnelle des Niveaux du CSF.
- Annexe C est un glossaire de la terminologie du CSF.

2. Introduction au Noyau du CSF

Annexe A est le Noyau du CSF - un ensemble de résultats de cybersécurité classés par Fonction, puis par Catégorie et enfin par Sous-catégorie, comme illustré dans Fig. 1. Ces résultats ne constituent pas une liste de contrôle des actions à effectuer ; les actions spécifiques entreprises pour atteindre un résultat varient selon l'organisation et le cas d'utilisation, tout comme la personne responsable de ces actions. De plus, l'ordre et la taille des Fonctions, Catégories et Sous-catégories dans le Noyau n'impliquent pas la séquence ou l'importance de leur réalisation. La structure du Noyau est destinée à trouver un plus grand écho auprès des personnes chargées de rendre opérationnelle la gestion des risques au sein d'une organisation.

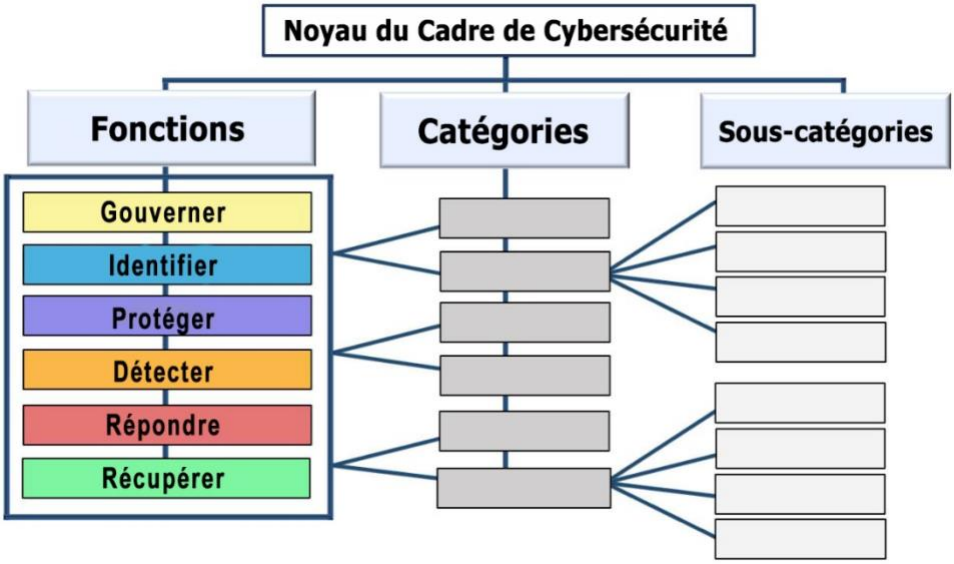

Fig. 1. Structure du Noyau du CSF

Les Fonctions du Noyau du CSF — GOUVERNER, IDENTIFIER, PROTEGER, DETECTER, REPONDRE et RECUPERER — organisent les résultats de cybersécurité à leur plus haut niveau.

- **GOUVERNER (GV)** — *La stratégie, les attentes et la politique de gestion des risques de cybersécurité de l'organisation sont établies, communiquées et surveillées.* La Fonction GOUVERNER fournit des résultats pour informer ce qu'une organisation peut faire pour atteindre et prioriser les résultats des cinq autres Fonctions dans le contexte de sa mission et des attentes des parties prenantes. Les activités de gouvernance sont essentielles pour intégrer la cybersécurité dans la stratégie plus large de gestion des risques d'entreprise (ERM) d'une organisation. GOUVERNER aborde la compréhension du contexte organisationnel ; l'établissement d'une stratégie de cybersécurité et de gestion des risques de la chaîne d'approvisionnement en cybersécurité; les rôles, les responsabilités et les autorités; la politique; et la supervision de la stratégie de cybersécurité.
- **IDENTIFIER (ID)** — *Les risques de cybersécurité actuels de l'organisation sont compris.* La compréhension des actifs de l'organisation (p. ex., données, matériel, logiciels, systèmes, installations, services, personnes), des fournisseurs et des risques de

cybersécurité associés permet à une organisation de prioriser ses efforts en cohérence avec sa stratégie de gestion des risques et aux besoins de la mission identifiés sous GOUVERNER. Cette Fonction comprend également l'identification des opportunités d'amélioration des politiques, plans, processus, procédures et pratiques de l'organisation qui soutiennent la gestion des risques de cybersécurité afin d'éclairer les efforts dans le cadre des six Fonctions.

- **PROTEGER (PR)** — *Des mesures de protection sont utilisées pour gérer les risques de cybersécurité de l'organisation.* Une fois les actifs et les risques identifiés et priorisés, PROTEGER prend en charge la capacité à sécuriser ces actifs pour prévenir ou réduire la probabilité et l'impact d'événements de cybersécurité indésirables, ainsi que pour augmenter la probabilité et l'impact de tirer parti des opportunités. Les résultats couverts par cette Fonction comprennent la gestion des identités, l'authentification et le contrôle d'accès ; la sensibilisation et la formation ; la sécurité des données; la sécurité de la plateforme (c.-à-d. la sécurisation du matériel, des logiciels et des services des plateformes physiques et virtuelles); et la résilience de l'infrastructure technologique.
- **DETECTER (DE)** — *Les attaques et compromissions de cybersécurité possibles sont détectées et analysées.* DETECTER permet la découverte et l'analyse en temps opportun des anomalies, des indicateurs de compromission et d'autres événements potentiellement indésirables qui peuvent indiquer que des attaques et des incidents de cybersécurité se produisent. Cette Fonction prend en charge les activités réussies de réponse aux incidents et de récupération.
- **REPONDRE (RS)** — *Des mesures concernant un incident de cybersécurité détecté sont prises.* REPONDRE soutient la capacité à contenir les effets des incidents de cybersécurité. Les résultats au sein de cette Fonction couvrent la gestion, l'analyse, l'atténuation, la production de rapports et la communication des incidents.
- **RECUPERER (RC)** — *Les actifs et les opérations affectés par un incident de cybersécurité sont restaurés.* RECUPERER prend en charge la restauration rapide des opérations normales afin de réduire les effets des incidents de cybersécurité et de permettre une communication appropriée pendant les efforts de récupération.

Bien que de nombreuses activités de gestion des risques liés à la cybersécurité visent à empêcher la survenance d'événements négatifs, elles peuvent également contribuer à tirer parti d'opportunités positives. Les actions visant à réduire les risques de cybersécurité peuvent bénéficier à une organisation d'autres manières, comme l'augmentation des revenus. (P. ex., en offrant d'abord un espace excédentaire à un fournisseur d'hébergement commercial pour héberger ses propres centres de données et ceux d'autres organisations, puis en déplaçant un système financier majeur du centre de données interne de l'organisation vers le fournisseur d'hébergement pour réduire les risques de cybersécurité).

La Fig. 2 montre les Fonctions du CSF sous forme de roue car toutes les Fonctions sont liées les unes aux autres. Par exemple, une organisation classera les actifs sous IDENTIFIER et prendra des

mesures pour sécuriser ces actifs sous PROTEGER. Les investissements dans la planification et les tests dans les Fonctions GOUVERNER et IDENTIFIER permettront de détecter en temps opportun les événements inattendus dans la Fonction DETECTER, ainsi que la mise en place d'actions de réponse et de récupération en cas d'incident de cybersécurité dans les Fonctions REPONDRE et RECUPERER. GOUVERNER est au centre de la roue car elle informe sur la manière dont une organisation mettra en œuvre les cinq autres Fonctions.

Fig. 2. Fonctions du CSF

Les Fonctions doivent être traitées simultanément. Les actions qui prennent en charge GOUVERNER, IDENTIFIER, PROTEGER et DETECTER doivent toutes se produire en continu, et les actions qui prennent en charge REPONDRE et RECUPERER doivent être prêtes à tout moment et se produire lorsque des incidents de cybersécurité se produisent. Toutes les Fonctions ont des rôles essentiels liés aux incidents de cybersécurité. Les résultats de GOUVERNER, IDENTIFIER et PROTEGER aident à prévenir et à se préparer aux incidents, tandis que les résultats de GOUVERNER, DETECTER, REPONDRE et RECUPERER aident à découvrir et à gérer les incidents.

Chaque Fonction est nommée d'après un verbe qui résume son contenu. Chaque Fonction est divisée en *catégories*, qui sont des résultats de cybersécurité connexes qui constituent collectivement la Fonction. *Les Sous-catégories* divisent ensuite chaque catégorie en résultats plus spécifiques d'activités techniques et de gestion. Les Sous-catégories ne sont pas exhaustives, mais elles décrivent des résultats détaillés qui soutiennent chaque catégorie.

Les Fonctions, Catégories et Sous-catégories s'appliquent à toutes les TIC utilisées par une organisation, y compris les technologies de l'information (IT), l'Internet des objets (IoT) et la technologie opérationnelle (OT). Elles s'appliquent également à tous les types d'environnements technologiques, y compris les systèmes cloud, mobiles et d'intelligence artificielle. Le Noyau du CSF est tourné vers l'avenir et est destiné à s'appliquer aux changements futurs des technologies et des environnements.

3. Introduction aux Profils et aux Niveaux du CSF

Cette section définit les concepts de Profils et de Niveaux du CSF.

3.1. Profils du CSF

Un *Profil Organisationnel du CSF* décrit la posture actuelle et/ou cible de cybersécurité d'une organisation en termes de résultats du Noyau. Les Profils Organisationnels sont utilisés pour comprendre, adapter, évaluer, hiérarchiser et communiquer les résultats du Noyau en tenant compte des objectifs de mission d'une organisation, des attentes des parties prenantes, du paysage des menaces et des exigences. Une organisation peut alors prioriser ses actions pour atteindre des résultats spécifiques et communiquer ces informations aux parties prenantes.

Chaque Profil Organisationnel comprend un ou les deux éléments suivants :

1. Un *Profil Actuel* précise les résultats du Noyau qu'une organisation atteint actuellement (ou tente d'atteindre) et caractérise comment ou dans quelle mesure chaque résultat est atteint.
2. Un *Profil Cible* spécifie les résultats souhaités qu'une organisation a sélectionnés et priorisés pour atteindre ses objectifs de gestion des risques de cybersécurité. Un Profil Cible prend en compte les changements anticipés dans la posture de cybersécurité de l'organisation, tels que les nouvelles exigences, l'adoption de nouvelles technologies et les tendances en matière de renseignement sur les menaces.

> Un Profil Communautaire est une base de résultats du CSF qui est créé et publié pour s'adresser aux intérêts et objectifs partagés par un certain nombre d'organisations. Un Profil Communautaire est généralement développé pour un secteur, un sous-secteur, une technologie, un type de menace ou un autre cas d'utilisation particulier. Une organisation peut utiliser un Profil Communautaire comme base pour son propre profil cible. Des Exemples de Profils Communautaires peuvent être trouvés sur le site web du NIST CSF.

Les étapes présentées dans Fig. 3 et résumées ci-dessous illustrent une manière dont une organisation pourrait utiliser un Profil Organisationnel pour contribuer à l'amélioration continue de sa cybersécurité.

Fig. 3. Étapes de création et d'utilisation d'un profil organisationnel du CSF

1. **Définir la portée du Profil Organisationnel.** Documenter les faits et hypothèses de haut niveau sur lesquels le Profil sera basé pour définir sa portée. Une organisation peut avoir autant de profils organisationnels que souhaité, chacun ayant une portée différente. Par exemple, un Profil peut s'adresser à une organisation entière ou être limité aux systèmes financiers d'une organisation ou à la lutte contre les menaces de ransomware et à la gestion des incidents de ransomware impliquant ces systèmes financiers.
2. **Rassembler les informations nécessaires pour préparer le Profil organisationnel.** Des exemples d'informations peuvent inclure des politiques organisationnelles, des priorités et des ressources en matière de gestion des risques, des profils de risque d'entreprise, des registres d'analyse d'impact sur les activités (BIA), des exigences et des normes de cybersécurité suivies par l'organisation, des pratiques et des outils (p. ex., des procédures et des mesures de protection) et des rôles professionnels.
3. **Créer le Profil Organisationnel.** Déterminer les types d'informations que le profil doit inclure pour les résultats du CSF sélectionnés et documenter les informations nécessaires. Tenir compte des implications en matière de risques du Profil Actuel pour éclairer la planification et la priorisation du Profil Cible. Envisager également d'utiliser un Profil Communautaire comme base pour le Profil Cible.
4. **Analyser les écarts entre les Profils Actuel et Cible et créer un plan d'action.** Effectuer une analyse des écarts pour identifier et analyser les différences entre les Profils Actuel et Cible, et élaborer un plan d'action priorisé (p. ex., registre des risques, rapport détaillé des risques, Plan d'Action et Jalons [POA&M]) pour s'adresser à ces écarts.
5. **Mettre en œuvre le plan d'action et mettre à jour le Profil Organisationnel.** Suivre le plan d'action pour s'adresser aux écarts et faire progresser l'organisation vers le Profil Cible. Un plan d'action peut avoir une échéance globale ou être continu.

Etant donné de l'importance de l'amélioration continue, une organisation peut répéter ces étapes aussi souvent que nécessaire.

Il existe des utilisations supplémentaires pour les Profils Organisationnels. Par exemple, un profil actuel peut être utilisé pour documenter et communiquer les capacités de cybersécurité de l'organisation et les opportunités d'amélioration connues aux parties prenantes externes, telles que des partenaires commerciaux ou des clients potentiels. En outre, un Profil Cible peut aider à exprimer les exigences et les attentes de l'organisation en matière de gestion des risques de cybersécurité aux fournisseurs, partenaires et autres tiers en tant qu'objectif à atteindre pour ces parties.

3.2. Niveaux du CSF

Une organisation peut choisir d'utiliser les niveaux pour informer ses Profils Actuels et Cibles. *Les Niveaux* caractérisent la rigueur des pratiques de gouvernance et de gestion des risques de cybersécurité d'une organisation, et ils fournissent un contexte sur la façon dont une organisation perçoit les risques de cybersécurité et les processus en place pour gérer ces risques. Les niveaux, tels qu'ils sont indiqués dans Fig. 4 et illustrés de manière notionnelle dans l'Annexe B, reflètent les pratiques d'une organisation en matière de gestion des risques de cybersécurité comme suit : Partiel (Niveau 1), Informé sur les risques (Niveau 2), Répétable (Niveau 3) et Adaptative (Niveau 4). Les niveaux décrivent une progression depuis des réponses informelles et ad hoc vers des approches agiles, tenant compte des risques et en constante amélioration. La sélection des niveaux permet de donner le ton général de la manière dont une organisation gérera ses risques de cybersécurité.

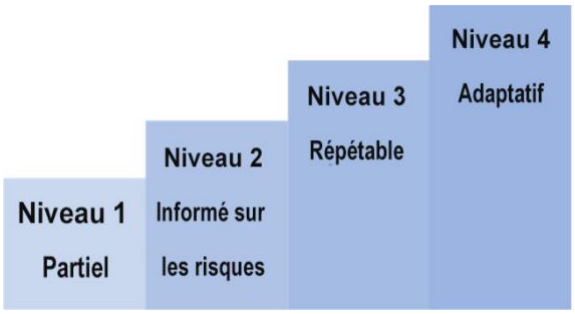

Fig. 4. Niveaux du CSF pour la gouvernance et la gestion des risques de cybersécurité

Les Niveaux doivent compléter la méthodologie de gestion des risques de cybersécurité d'une organisation plutôt que de la remplacer. Par exemple, une organisation peut utiliser les Niveaux pour communiquer en interne comme référence pour une approche à l'échelle de l'organisation[1] en matière de gestion des risques de cybersécurité. La progression vers des Niveaux supérieurs est encouragée lorsque les risques ou les mandats sont plus importants ou lorsqu'une analyse coûts-bénéfices indique une réduction réalisable et rentable des risques négatifs de cybersécurité.

Le site web du NIST CSF fournit des informations supplémentaires sur l'utilisation des Profils et des Niveaux. Il comprend des pointeurs vers des modèles de Profils Organisationnels hébergés

[1]Pour les besoins de ce document, les termes « à l'échelle de l'organisation » et « entreprise » ont la même signification.

par le NIST et un référentiel de Profils Communautaires dans divers formats lisibles par machine et utilisables par l'homme.

4. Introduction aux ressources en ligne qui complètent le CSF

Le NIST et d'autres organisations ont produit une série de ressources en ligne qui aident les organisations à comprendre, adopter et utiliser le CSF. Etat hébergées en ligne, ces ressources supplémentaires peuvent être mises à jour plus fréquemment que ce document, qui est mis à jour peu fréquemment pour assurer la stabilité de ses utilisateurs, et être disponible dans des formats lisibles par machine. Cette section fournit un aperçu de trois types de ressources en ligne : Références Informatives, Exemples de Mise en Œuvre et Guides de Démarrage Rapide.

Références Informatives sont des mappages qui indiquent les relations entre le Noyau et diverses normes, lignes directrices, réglementations et autres contenus. Les références informatives aident à informer sur la manière dont une organisation peut atteindre les résultats du Noyau. Les Références Informatives peuvent être spécifiques à un secteur ou à une technologie. Elles peuvent être produites par le NIST ou une autre organisation. Certaines Références Informatives ont une portée plus restreinte qu'une Sous-catégorie. Par exemple, un contrôle particulier de la SP 800-53, *Contrôles de Sécurité et de Vie Privée pour les Systèmes d'Information et les Organisations*, peut être l'une des nombreuses références nécessaires pour atteindre le résultat décrit dans une Sous-catégorie. D'autres Références Informatives peuvent être de niveau supérieur, comme une exigence d'une politique qui répond partiellement à de nombreuses Sous-catégories. En utilisant le CSF, une organisation peut identifier les Références Informatives les plus pertinentes.

Exemples de Mise en Œuvre fournir des exemples notionnels d'étapes concises et orientées vers l'action pour aider à atteindre les résultats des Sous-catégories. Les verbes utilisés pour exprimer les exemples incluent partager, documenter, développer, exécuter, surveiller, analyser, évaluer et exercer. Les exemples ne constituent pas une liste exhaustive de toutes les actions qui pourraient être entreprises par une organisation pour atteindre un résultat, ni ne représentent une base de références des actions requises pour s'adresser aux risques de cybersécurité.

Guides de Démarrage Rapide (QSG) sont de brefs documents sur des sujets spécifiques liés au CSF et sont souvent adaptés à des publics spécifiques. Les QSG peuvent aider une organisation à mettre en œuvre le CSF, car ils distillent des parties spécifiques du CSF en "premières étapes" concrètes qu'une organisation peut envisager pour améliorer sa posture de cybersécurité sa gestion des risques associés. Les guides sont révisés selon leurs propres délais et de nouveaux guides sont ajoutés selon le besoin.

Les suggestions de nouvelles références informatives pour CSF 2.0 peuvent toujours être partagées avec le NIST à olir@nist.gov. Les suggestions d'autres ressources à référencer sur le site Web du NIST CSF, y compris des sujets supplémentaires des QSG, doivent être adressées à cyberframework@nist.gov.

5. Améliorer la communication et l'intégration des risques liés à la cybersécurité

L'utilisation du CSF varie en fonction de la mission et des risques uniques d'une organisation. En comprenant les attentes des parties prenantes, de leur appétence et tolérance au risque (comme indiqué dans GOUVERNER), une organisation peut prioriser les activités de cybersécurité afin de prendre des décisions éclairées sur les dépenses et les actions en matière de cybersécurité. Une organisation peut choisir de gérer les risques d'une ou plusieurs manières – notamment en atténuant, transférant, évitant ou acceptant les risques négatifs et en réalisant, partageant, améliorant ou acceptant des risques positifs – en fonction des impacts et des probabilités potentiels. Il est important de noter qu'une organisation peut utiliser le CSF à la fois en interne pour gérer ses capacités de cybersécurité et en externe pour superviser ou communiquer avec des tiers.

Quelle que soit l'utilisation du CSF, une organisation peut bénéficier de l'utilisation du CSF comme guide pour l'aider à comprendre, évaluer, hiérarchiser et communiquer les risques de cybersécurité et les actions qui permettront de gérer ces risques. Les résultats sélectionnés peuvent être utilisés pour se concentrer sur les décisions stratégiques et les mettre en œuvre afin d'améliorer les postures de cybersécurité et de maintenir la continuité des fonctions essentielles à la mission tout en tenant compte des priorités et des ressources disponibles.

5.1. Améliorer la communication sur la gestion des risques

Le CSF fournit une base pour une meilleure communication concernant les attentes, la planification et les ressources en matière de cybersécurité. Le CSF favorise un flux d'informations bidirectionnel (comme indiqué dans la moitié supérieure de Fig. 5) entre les dirigeants qui se concentrent sur les priorités et l'orientation stratégique de l'organisation et les gestionnaires qui gèrent des risques de cybersécurité spécifiques qui pourraient affecter la réalisation de ces priorités. Le CSF prend également en charge un flux similaire (comme le montre la moitié inférieure de Fig. 5) entre les gestionnaires et les praticiens qui mettent en œuvre et exploitent les technologies. Le côté gauche de la figure indique l'importance pour les praticiens de partager leurs mises à jour, leurs idées et leurs préoccupations avec les gestionnaires et les dirigeants.

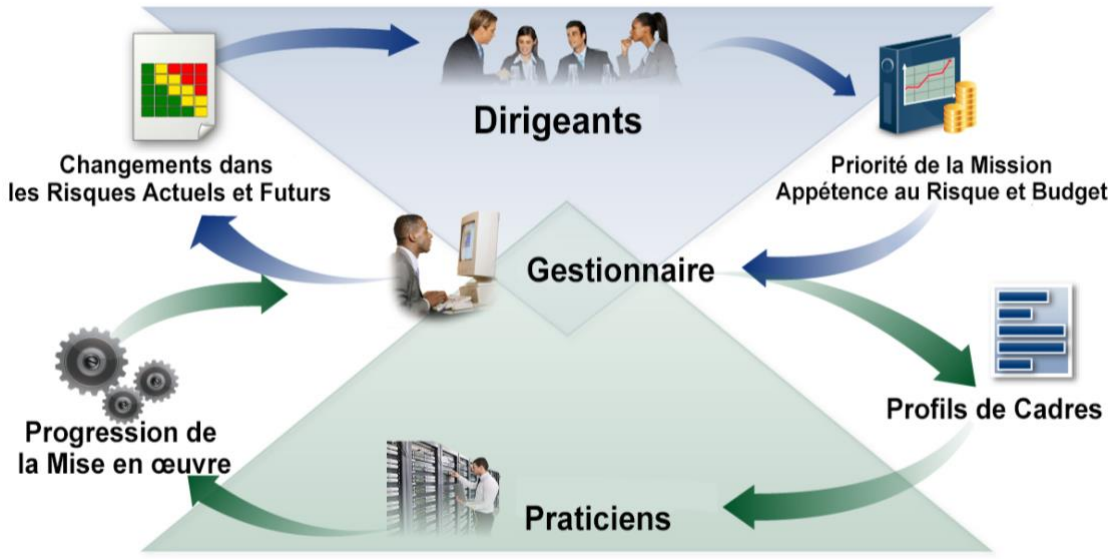

Fig. 5. Utiliser le CSF pour améliorer la communication sur la gestion des risques

La préparation à la création et à l'utilisation des Profils Organisationnels implique de recueillir des informations sur les priorités organisationnelles, les ressources et l'orientation des risques auprès des dirigeants. Les gestionnaires collaborent ensuite avec les praticiens pour communiquer les besoins opérationnels et créer des Profils Organisationnels tenant compte des risques. Les actions visant à combler les écarts identifiés entre les Profils Actuels et Cibles seront mises en œuvre par les gestionnaires et les praticiens et fourniront des apports clés aux plans au niveau du système. Au fur et à mesure que l'état cible est atteint dans toute l'organisation – notamment grâce aux contrôles et à la surveillance appliqués au niveau du système – les résultats mis à jour peuvent être partagés via des registres de risques et des rapports d'avancement. Dans le cadre de l'évaluation continue, les gestionnaires acquièrent des connaissances pour procéder à des ajustements qui réduisent davantage les préjudices potentiels et augmentent les avantages potentiels.

La Fonction GOUVERNER soutient la communication de risques organisationnels auprès des **dirigeants**. Les discussions des dirigeants portent sur la stratégie, en particulier sur la manière dont les incertitudes liées à la cybersécurité pourraient affecter la réalisation des objectifs organisationnels. Ces discussions de gouvernance soutiennent le dialogue et l'accord sur les stratégies de gestion des risques (y compris les risques liés à la chaîne d'approvisionnement en cybersécurité) ; les rôles, les responsabilités et les autorités; les politiques; et la surveillance. Lorsque les dirigeants établissent des priorités et des objectifs de cybersécurité en fonction de ces besoins, ils communiquent leurs attentes en matière d'appétence au risque, de responsabilité et de ressources. Les dirigeants sont également responsables de l'intégration de la gestion des risques de cybersécurité aux programmes ERM et aux programmes de gestion des risques de niveau inférieur (voir Sec. 5.2). Les communications reflétées dans la moitié supérieure de Fig. 5peuvent inclure des considérations sur la ERM et les programmes de niveau inférieur et, ainsi, informer les gestionnaires et les praticiens.

Les objectifs généraux de cybersécurité fixés par les dirigeants sont informés et transmis aux **gestionnaires**. Dans une entité commerciale, ceux-ci peuvent s'appliquer à un secteur d'activité ou à une division opérationnelle. Pour les entités gouvernementales, il peut s'agir de considérations au niveau d'une division ou d'une branche. Lors de la mise en œuvre du CSF, les gestionnaires se concentreront sur la manière d'atteindre les objectifs de risque grâce à des services communs, des contrôles et une collaboration, tels qu'exprimés dans le profil cible et améliorés grâce aux actions suivies dans le plan d'action (p., ex., registre des risques, rapport détaillé des risques, POA&M).

Les **praticiens** se concentrent sur la mise en œuvre de l'état cible et sur la mesure des changements dans le risque opérationnel pour aider à planifier, réaliser et surveiller des activités de cybersécurité spécifiques. Au fur et à mesure que les contrôles sont mis en œuvre pour gérer le risque à un niveau acceptable, les praticiens fournissent aux gestionnaires et aux dirigeants les informations (p. ex., les indicateurs de performance clés, les indicateurs de risque clés) dont ils ont besoin pour comprendre la posture de cybersécurité de l'organisation, prendre des décisions éclairées et maintenir ou ajuster la stratégie de risque en conséquence. Les dirigeants peuvent également combiner ces données sur les risques de cybersécurité avec des informations sur d'autres types de risques au sein de l'organisation. Les mises à jour des attentes et des priorités sont incluses dans les profils organisationnels mis à jour au fur et à mesure que le cycle se répète.

5.2. Améliorer l'intégration avec d'autres programmes de gestion des risques

Chaque organisation est confrontée à de nombreux types de risques liés aux TIC (p., ex., vie privée, chaîne d'approvisionnement, intelligence artificielle) et peut utiliser des cadres et des outils de gestion spécifiques à chaque risque. Certaines organisations intègrent les TIC et tous les autres efforts de gestion des risques à un niveau élevé en utilisant l'ERM, tandis que d'autres séparent les efforts pour garantir une attention adéquate à chacun. Les petites organisations, par leur nature, peuvent surveiller les risques au niveau de l'entreprise, tandis que les grandes entreprises peuvent maintenir des efforts de gestion des risques distincts intégrés dans l'ERM.

Les organisations peuvent utiliser une approche ERM pour équilibrer un *portefeuille* de considérations de risques, notamment la cybersécurité, et prendre des décisions éclairées. Les dirigeants reçoivent des informations importantes sur les activités de risque actuelles et planifiées lorsqu'ils intègrent les stratégies de gouvernance et de risque aux résultats des utilisations précédentes du CSF. Le CSF aide les organisations à traduire leur terminologie relative à la cybersécurité et à la gestion des risques de cybersécurité en un langage général de gestion des risques que les dirigeants comprendront.

Les ressources du NIST qui décrivent la relation mutuelle entre la gestion des risques de cybersécurité et la ERM comprennent :

- *Cadre de cybersécurité du NIST 2.0 – Guide de Démarrage Rapide pour la Gestion des Risques d'Entreprise*

- Rapport Interagences (IR) 8286 du NIST, *Intégration de la Cybersécurité et de la Gestion des Risques d'Entreprise (ERM)*
- IR 8286A, *Identification et Estimation des Risques de Cybersécurité pour la Gestion des Risques d'Entreprise*
- IR 8286B, *Priorisation des Risques de Cybersécurité pour la Gestion des Risques d'Entreprise*
- IR 8286C, *Mise en Scène des Risques de Cybersécurité pour la Gestion des Risques d'Entreprise et la Surveillance de la Gouvernance*
- IR 8286D, *Utilisation de l'Analyse d'Impact sur les Activités pour Eclairer la Priorisation et la Réponse aux Risques*
- SP 800-221, *Impact sur l'Entreprise des Risques liés aux Technologies de l'Information et des Communications : Gouvernance et Gestion des Programmes de Risques liés aux TIC au sein d'un Portefeuille de Risques d'Entreprise*
- SP 800-221A, *Résultats des Risques liés aux Technologies de l'information et des Communications (TIC) : Intégration des Programmes de Gestion des Risques liés aux TIC au Portefeuille de Risques d'Entreprise*

Une organisation peut également trouver le CSF utile pour intégrer la gestion des risques de cybersécurité aux programmes individuels de gestion des risques liés aux TIC, tels que :

- **Gestion et évaluation des risques de cybersécurité:** Le CSF peut être intégré aux programmes établis de gestion et d'évaluation des risques de cybersécurité, tels que SP 800-37, Cadre de Gestion des Risques pour les Systèmes d'Information et les Organisations, et SP 800-30, Guide pour la Réalisation d'Evaluations des Risques du cadre de gestion des risques du NIST (RMF). Pour une organisation utilisant le RMF du NIST et sa suite de publications, le CSF peut être utilisé pour compléter l'approche du CGR en matière de sélection et de priorisation des contrôles du SP 800-53, *Contrôles de Sécurité et de Vie Privée pour les Systèmes d'Information et les Organisations*.
- **Risques liés à la vie privée :** Bien que la cybersécurité et la vie privée soient des disciplines indépendantes, leurs objectifs se chevauchent dans certaines circonstances, comme illustré dans Fig. 6.

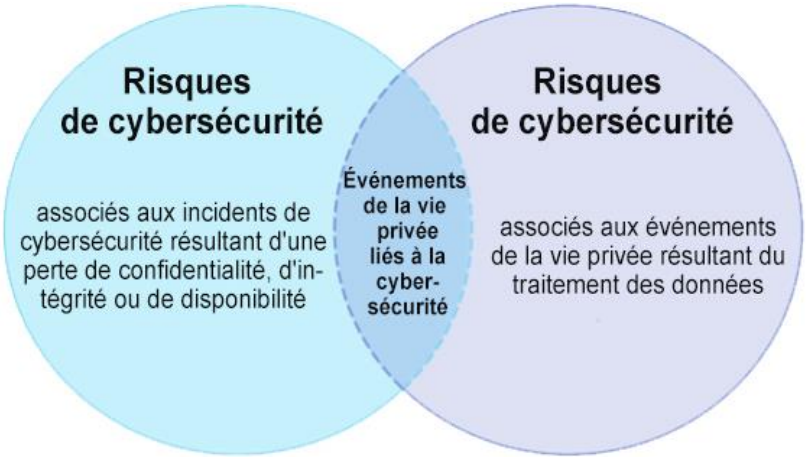

Fig. 6. Relation entre les risques liés à la cybersécurité et à la vie privée

La gestion des risques de cybersécurité est essentielle pour s'adresser aux risques d'atteinte à la vie privée liés à la perte de confidentialité, d'intégrité et de disponibilité des données des individus. Par exemple, les violations de données peuvent conduire à un vol d'identité. Cependant, les risques pour la vie privée peuvent également survenir par des moyens sans rapport avec des incidents de cybersécurité.

Une organisation traite des données pour atteindre ses objectifs de mission ou d'affaires, ce qui peut parfois donner lieu à *des événements de vie privée* dans lesquels les individus peuvent rencontrer des problèmes en raison du traitement des données. Ces problèmes peuvent être exprimés de diverses manières, mais le NIST les décrit comme allant d'effets de type dignité (p., ex., embarras ou stigmatisation) à des préjudices plus tangibles (p., ex., discrimination, perte économique ou préjudice physique). Le Cadre de Vie Privée du NIST et le cadre de cybersécurité peuvent être utilisés ensemble pour aborder les différents aspects de la cybersécurité et des risques liés à la vie privée. En outre, la Méthodologie d'Evaluation des Risques pour la Vie Privée (PRAM) du NIST propose un catalogue d'exemples de problèmes à utiliser dans les évaluations des risques pour la vie privée.

- **Risques de la chaîne d'approvisionnement :** Une organisation peut utiliser le CSF pour favoriser la surveillance et la communication des risque de cybersécurité avec les parties prenantes de toutes les chaînes d'approvisionnement. Tous les types de technologies reposent sur un écosystème de chaîne d'approvisionnement complexe, distribué à l'échelle mondiale, étendu et interconnecté, avec des itinéraires géographiquement diversifiés et de multiples niveaux d'externalisation. Cet écosystème est composé d'entités des secteurs public et privé (p. ex., des acquéreurs, des fournisseurs, des développeurs, des intégrateurs de systèmes, des fournisseurs de services système externes et d'autres fournisseurs de services liés à la technologie) qui interagissent pour rechercher, développer, concevoir, fabriquer, acquérir, livrer, intégrer, exploiter, entretenir, éliminer et utiliser ou gérer de toute autre manière des produits et services technologiques. Ces interactions sont façonnées et influencées par les technologies, les lois, les politiques, les procédures et les pratiques.

Compte tenu des relations complexes et interconnectées dans cet écosystème, la gestion des risques de la chaîne d'approvisionnement (SCRM) est essentielle pour les organisations. La SCRM de cybersécurité (C-SCRM) est un processus systématique de gestion de l'exposition aux risques de cybersécurité dans l'ensemble des chaînes d'approvisionnement et de développement de stratégies, politiques, processus et procédures de réponse appropriés. Les Sous-catégories de la catégorie C-SCRM du CSF [GV.SC] fournissent un lien entre les résultats qui se concentrent uniquement sur la cybersécurité et ceux qui se concentrent sur le C-SCRM. SP 800-161r1 (Révision 1), *Pratiques de Gestion des Risques de la Chaîne d'Approvisionnement en Cybersécurité pour les Systèmes et les Organisations*, fournit des informations détaillées sur la C-SCRM.

- **Risques liés aux technologies émergentes :** à mesure que de nouvelles technologies et de nouvelles applications technologiques deviennent disponibles, de nouveaux risques deviennent évidents. Un exemple contemporain est celui de l'intelligence artificielle (IA), qui présente des risques en matière de cybersécurité et de vie privée, ainsi que de nombreux autres types de risques. Le Cadre de Gestion des Risques liés à l'Intelligence Artificielle (AI RMF) du NIST a été développé pour aider à s'adresser à ces risques. Traiter les risques liés à l'IA parallèlement à d'autres risques d'entreprise (par exemple, financiers, cybersécurité, réputation et vie privée) permettra d'obtenir des résultats plus intégrés et une meilleure efficacité organisationnelle. Les considérations et approches de gestion des risques liés à la cybersécurité et à la vie privée s'appliquent à la conception, au développement, au déploiement, à l'évaluation et à l'utilisation de systèmes d'IA. Le Noyau du AI RMF utilise des Fonctions, des Catégories et des Sous-catégories pour décrire les résultats de l'IA et aider à gérer les risques liés à l'IA.

Annexe A. Noyau du CSF

Cette annexe décrit les Fonctions, Catégories et Sous-catégories du Noyau CSF. Le Tableau 1 répertorie les noms des Fonctions et des Catégories du Noyau CSF 2.0 ainsi que leurs identifiants alphabétiques uniques. Chaque nom de Fonction dans le tableau est lié à sa partie de l'annexe. L'ordre des Fonctions, Catégories et Sous-catégories du Noyau n'est pas alphabétique ; il est destiné à trouver un écho auprès des personnes chargées de rendre de mettre en œuvre la gestion des risques au sein d'une organisation. La numérotation des Sous-catégories n'est intentionnellement pas séquentielle ; les lacunes dans la numérotation indiquent les Sous-catégories CSF 1.1 qui ont été déplacées dans CSF 2.0.

Tableau 1. Noms et identifiants de Fonctions et de Catégories du noyau du CSF 2.0

Fonction	Catégorie	Identificateur de Catégorie
Gouverner (GV)	Contexte organisationnel	GV.OC
	Stratégie de gestion des risques	GV.RM
	Rôles, responsabilités et autorités	GV.RR
	Politique	GV.PO
	Surveillance	GV.OV
	Gestion des risques de la chaîne d'approvisionnement en cybersécurité	GV.SC
Identifier (ID)	Gestion d'actifs	ID.AM
	Evaluation des risques	ID.RA
	Amélioration	ID.IM
Protéger (RP)	Gestion des identités, authentification et contrôle d'accès	PR.AA
	Sensibilisation et formation	PR.AT
	Sécurité des données	PR.DS
	Sécurité de la plateforme	PR.PS
	Résilience des infrastructures technologiques	PR.IR
Détecter (DE)	Contrôle continu	DE.CM
	Analyse des événements indésirables	DE.AE
Répondre (RS)	Gestion des incidents	RS.MA
	Analyse des incidents	RS.AN
	Rapports et communications en matière de réponse aux incidents	RS.CO
	Atténuation des incidents	RS.MI
Récupérer (RC)	Exécution du plan de récupération après incident	RC.RP
	Communication de récupération après incident	RC.CO

Le Noyau du CSF, les Références Informatives et les Exemples de Mise en Œuvre sont disponibles sur le site web CSF 2.0 et via l'Outil de Référence CSF 2.0, qui permet aux utilisateurs de les explorer et de les exporter dans des formats lisibles par l'homme et la par

machine. Le Noyau du CSF 2.0 est également disponible dans un format hérité similaire à celui du CSF 1.1.

GOUVERNER (GV) : La stratégie, les attentes et la politique de gestion des risques de cybersécurité de l'organisation sont établies, communiquées et surveillées

- **Contexte organisationnel (GV.OC) :** Les circonstances (mission, attentes des parties prenantes, dépendances et exigences légales, réglementaires et contractuelles) entourant les décisions de gestion des risques de cybersécurité de l'organisation sont comprises
  - **GV.OC-01 :** La mission organisationnelle est comprise et informe la gestion des risques de cybersécurité
  - **GV.OC-02 :** Les parties prenantes internes et externes sont comprises, et leurs besoins et attentes en matière de gestion des risques de cybersécurité sont compris et pris en compte
  - **GV.OC-03 :** Les exigences légales, réglementaires et contractuelles en matière de cybersécurité, y compris les obligations en matière de vie privée et de libertés civiles, sont comprises et gérées
  - **GV.OC-04 :** Les objectifs, capacités et services critiques dont dépendent les parties prenantes externes ou qu'ils attendent de l'organisation sont compris et communiqués
  - **GV.OC-05 :** Les résultats, les capacités et les services dont dépend l'organisation sont compris et communiqués
- **Stratégie de gestion des risques (GV.RM) :** Les priorités, les contraintes, les déclarations de tolérance et d'appétence au risque et les hypothèses de l'organisation sont établies, communiquées et utilisées pour soutenir les décisions en matière de risques opérationnels
  - **GV.RM-01 :** Les objectifs de gestion des risques sont établis et acceptés par les parties prenantes organisationnelles
  - **GV.RM-02 :** Les déclarations d'appétence et de tolérance au risque sont établies, communiquées et maintenues
  - **GV.RM-03 :** Les activités et les résultats de la gestion des risques de cybersécurité sont inclus dans les processus de gestion des risques de l'entreprise
  - **GV.RM-04 :** Une orientation stratégique décrivant les options de réponse aux risques appropriées est établie et communiquée
  - **GV.RM-05 :** Les lignes de communication au sein de l'organisation sont établies pour les risques de cybersécurité, y compris les risques liés aux fournisseurs et autres tiers
  - **GV.RM-06 :** Une méthode normalisée de calcul, de documentation, de catégorisation et de priorisation des risques de cybersécurité est établie et communiquée
  - **GV.RM-07 :** Les opportunités stratégiques (c-à-d., les risques positifs) sont caractérisées et incluses dans les discussions sur les risques de cybersécurité organisationnels

- **Rôles, responsabilités et autorités (GV.RR):** Les rôles, responsabilités et autorités en matière de cybersécurité visant à la responsabilisation, l'évaluation des performances et l'amélioration continue sont établis et communiqués
  - **GV.RR-01 :** La direction organisationnelle est responsable des risques liés à la cybersécurité et favorise une culture consciente des risques, éthique et en constante amélioration
  - **GV.RR-02 :** Les rôles, responsabilités et autorités liés à la gestion des risques de cybersécurité sont établis, communiqués, compris et appliqués
  - **GV.RR-03 :** Les ressources adéquates sont allouées en fonction de la stratégie, des rôles, des responsabilités et des politiques en matière de risques de cybersécurité
  - **GV.RR-04 :** La cybersécurité est incluse dans les pratiques en matières des ressources humaines

- **Politique (GV.PO) :** La politique de cybersécurité organisationnelle est établie, communiquée et appliquée
  - **GV.PO-01 :** La politique de gestion des risques de cybersécurité est établie en fonction du contexte organisationnel, de la stratégie de cybersécurité et des priorités, et est communiquée et appliquée
  - **GV.PO-02 :** La politique de gestion des risques de cybersécurité est revue, mise à jour, communiquée et appliquée pour refléter les changements dans les exigences, les menaces, la technologie et la mission organisationnelle

- **Surveillance (GV.OV) :** Les résultats des activités et des performances de gestion des risques de cybersécurité à l'échelle de l'organisation sont utilisés pour informer, améliorer et ajuster la stratégie de gestion des risques
  - **GV.OV-01 :** Les résultats de la stratégie de gestion des risques de cybersécurité sont examinés pour éclairer et ajuster la stratégie et l'orientation
  - **GV.OV-02 :** La stratégie de gestion des risques de cybersécurité est revue et ajustée pour garantir la couverture des exigences et des risques organisationnels
  - **GV.OV-03 :** La performance de la gestion des risques de cybersécurité organisationnelle est évaluée et révisée pour les ajustements nécessaires

- **Gestion des risques de la chaîne d'approvisionnement de cybersécurité (GV.SC) :** Les processus de gestion des risques de la chaîne d'approvisionnement en matière de cybersécurité sont identifiés, établis, gérés, surveillés et améliorés par les parties prenantes de l'organisation
  - **GV.SC-01 :** Un programme, une stratégie, des objectifs, des politiques et des processus de gestion des risques liés à la chaîne d'approvisionnement en matière de cybersécurité sont établis et acceptés par les parties prenantes de l'organisation

- **GV.SC-02 :** Les rôles et responsabilités en matière de cybersécurité pour les fournisseurs, les clients et les partenaires sont établis, communiqués et coordonnés en interne et en externe
- **GV.SC-03 :** La gestion des risques de la chaîne d'approvisionnement en cybersécurité est intégrée aux processus de cybersécurité et de gestion des risques d'entreprise, d'évaluation des risques et d'amélioration
- **GV.SC-04 :** Les fournisseurs sont connus et priorisés par criticité
- **GV.SC-05 :** Les exigences visant à s'adresser aux risques de cybersécurité dans les chaînes d'approvisionnement sont établies, priorisées et intégrées dans les contrats et autres types d'accords avec les fournisseurs et autres tiers concernés
- **GV.SC-06** : La planification et la diligence raisonnable sont effectuées pour réduire les risques avant d'entrer dans des relations formelles avec des fournisseurs ou d'autres tiers
- **GV.SC-07 :** Les risques posés par un fournisseur, ses produits et services et d'autres tiers sont compris, enregistrés, priorisés, évalués, traités et surveillés tout au long de la relation
- **GV.SC-08 :** Les fournisseurs concernés et autres tiers sont inclus dans les activités de planification, de réponse et de récupération en cas d'incident
- **GV.SC-09 :** Les pratiques de sécurité de la chaîne d'approvisionnement sont intégrées aux programmes de cybersécurité et de gestion des risques d'entreprise, et leurs performances sont surveillées tout au long du cycle de vie des produits et services technologiques
- **GV.SC-10 :** Les plans de gestion des risques de la chaîne d'approvisionnement en matière de cybersécurité comprennent des dispositions pour les activités qui se produisent après la conclusion d'un accord de partenariat ou de service

IDENTIFIER (ID) : Les risques actuels de cybersécurité de l'organisation sont compris

- **Gestion des actifs (ID.AM) :** Les actifs (p. ex., données, matériel, logiciels, systèmes, installations, services, personnes) qui permettent à l'organisation d'atteindre ses objectifs commerciaux sont identifiés et gérés en fonction de leur importance relative par rapport aux objectifs organisationnels et à la stratégie de risque de l'organisation
  - **ID.AM-01 :** Les inventaires du matériel géré par l'organisation sont maintenus
  - **ID.AM-02 :** Les inventaires des logiciels, services et systèmes gérés par l'organisation sont maintenus
  - **ID.AM-03 :** Les représentations des communications réseau autorisées de l'organisation et des flux de données réseau internes et externes sont maintenues
  - **ID.AM-04 :** Les inventaires des services fournis par les fournisseurs sont maintenus

- **ID.AM-05 :** Les actifs sont priorisés en fonction de la classification, de la criticité, des ressources et de l'impact sur la mission
- **ID.AM-07 :** Les inventaires de données et les métadonnées correspondantes pour les types de données désignés sont maintenus
- **ID.AM-08 :** Les systèmes, matériels, logiciels, services et données sont gérés tout au long de leur cycle de vie

- **Évaluation des risques (ID.RA) :** Le risque de cybersécurité pour l'organisation, les actifs et les individus est compris par l'organisation
  - **ID.RA-01 :** Les vulnérabilités des actifs sont identifiées, validées et enregistrées
  - **ID.RA-02 :** Les renseignements sur les cybermenaces sont reçus de forums et de sources de partage d'informations
  - **ID.RA-03 :** Les menaces internes et externes à l'organisation sont identifiées et enregistrées
  - **ID.RA-04 :** Les impacts potentiels et les probabilités des menaces exploitant les vulnérabilités sont identifiés et enregistrés
  - **ID.RA-05 :** Les menaces, les vulnérabilités, les probabilités et les impacts sont utilisés pour comprendre les risques inhérents et informer la priorisation des réponses aux risques.
  - **ID.RA-06 :** Les réponses aux risques sont choisies, priorisées, planifiées, suivies et communiquées
  - **ID.RA-07 :** Les changements et les exceptions sont gérés, évalués en termes d'impact sur les risques, enregistrés et suivis
  - **ID.RA-08 :** Les processus de réception, d'analyse et de réponse aux divulgations de vulnérabilités sont établis
  - **ID.RA-09 :** L'authenticité et l'intégrité du matériel et des logiciels sont évaluées avant l'acquisition et l'utilisation.
  - **ID.RA-10 :** Les fournisseurs critiques sont évalués avant l'acquisition

- **Amélioration (ID.IM) :** Les améliorations aux processus, procédures et activités de gestion des risques de cybersécurité organisationnels sont identifiées dans toutes les Fonctions du CSF.
  - **ID.IM-01 :** Les améliorations sont identifiées à partir des évaluations
  - **ID.IM-02 :** Les améliorations sont identifiées à partir de tests et d'exercices de sécurité, y compris ceux effectués en coordination avec les fournisseurs et les tiers concernés
  - **ID.IM-03 :** Les améliorations sont identifiées à partir de l'exécution des processus opérationnels, des procédures et des activités

- **ID.IM-04 :** Les plans de réponse aux incidents et d'autres plans de cybersécurité qui affectent les opérations sont établis, communiqués, maintenus et améliorés

PROTEGER (PR) : Les mesures de protection pour gérer les risques de cybersécurité de l'organisation sont utilisées

- **Gestion des identités, authentification et contrôle d'accès (PR.AA) :** L'accès aux actifs physiques et logiques est limité aux utilisateurs, services et matériels autorisés et géré en fonction du risque évalué d'accès non autorisé
  - **PR.AA-01 :** Les identités et les informations d'identification des utilisateurs, services et matériels autorisés sont gérées par l'organisation
  - **PR.AA-02 :** Les identités sont vérifiées et liées aux informations d'identification en fonction du contexte des interactions
  - **PR.AA-03 :** Les utilisateurs, les services et le matériel sont authentifiés
  - **PR.AA-04 :** Les affirmations d'identité sont protégées, transmises et vérifiées
  - **PR.AA-05 :** Les autorisations d'accès, les droits et les autorisations sont définis dans une politique, gérés, appliqués et revus, et intègrent les principes du moindre privilège et de la séparation des tâches
  - **PR.AA-06 :** L'accès physique aux actifs est géré, surveillé et appliqué en fonction du risque
- **Sensibilisation et formation (PR.AT) :** Le personnel de l'organisation reçoit une sensibilisation et une formation à la cybersécurité afin qu'il puisse accomplir ses tâches liées à la cybersécurité
  - **PR.AT-01 :** Le personnel est sensibilisé et formé afin qu'il possède les connaissances et les compétences nécessaires pour effectuer des tâches générales en tenant compte des risques de cybersécurité
  - **PR.AT-02 :** Les personnes occupant des postes spécialisés reçoivent une sensibilisation et une formation afin qu'elles possèdent les connaissances et les compétences nécessaires pour effectuer des tâches pertinentes en tenant compte des risques de cybersécurité
- **Sécurité des données (PR.DS) :** Les données sont gérées conformément à la stratégie de risque de l'organisation afin de protéger la confidentialité, l'intégrité et la disponibilité des informations
  - **PR.DS-01 :** La confidentialité, l'intégrité et la disponibilité des données au repos sont protégées
  - **PR.DS-02 :** La confidentialité, l'intégrité et la disponibilité des données en transit sont protégées

- **PR.DS-10 :** La confidentialité, l'intégrité et la disponibilité des données en cours d'utilisation sont protégées
- **PR.DS-11 :** Les sauvegardes des données sont créées, protégées, maintenues et testées

- **Sécurité de la plateforme (PR.PS) :** Le matériel, les logiciels (p. ex., les micrologiciels, les systèmes d'exploitation, les applications) et les services des plateformes physiques et virtuelles sont gérés conformément à la stratégie de risque de l'organisation pour protéger leur confidentialité, leur intégrité et leur disponibilité.
  - **PR.PS-01 :** Les pratiques de gestion de la configuration sont établies et appliquées
  - **PR.PS-02 :** Le logiciel est maintenu, remplacé et supprimé en fonction du risque
  - **PR.PS-03 :** Le matériel est entretenu, remplacé et retiré en fonction du risque
  - **PR.PS-04 :** Les enregistrements de journaux sont générés et mis à disposition pour une surveillance continue
  - **PR.PS-05 :** L'installation et l'exécution de logiciels non autorisés sont empêchées
  - **PR.PS-06 :** Les pratiques de développement de logiciels sécurisés sont intégrées et leurs performances sont surveillées tout au long du cycle de vie du développement logiciel

- **Résilience de l'infrastructure technologique (PR.IR) :** Les architectures de sécurité sont gérées avec la stratégie de risque de l'organisation pour protéger la confidentialité, l'intégrité et la disponibilité des actifs, ainsi que la résilience organisationnelle
  - **PR.IR-01 :** Les réseaux et les environnements sont protégés contre les accès logiques et les utilisations non autorisés
  - **PR.IR-02 :** Les actifs technologiques de l'organisation sont protégés contres les menaces environnementales
  - **PR.IR-03 :** Les mécanismes sont mis en œuvre pour satisfaire aux exigences de résilience dans des situations normales et défavorables
  - **PR.IR-04 :** Les capacité de ressources adéquate pour assurer la disponibilité sont maintenues

DETECTER (DE) : Les attaques et compromissions possibles en matière de cybersécurité sont détectées et analysées

- **Surveillance continue (DE.CM) :** Les actifs sont surveillés pour détecter des anomalies, des indicateurs de compromission et d'autres événements potentiellement indésirables
  - **DE.CM-01 :** Les réseaux et services réseau sont surveillés pour détecter les événements potentiellement indésirables
  - **DE.CM-02 :** L'environnement physique est surveillé pour détecter les événements potentiellement indésirables

- **DE.CM-03 :** L'activité du personnel et l'utilisation de la technologie sont surveillées pour détecter les événements potentiellement indésirables
- **DE.CM-06 :** Les activités et services des prestataires de services externes sont surveillés pour détecter les événements potentiellement indésirables
- **DE.CM-09 :** Le matériel informatique et les logiciels, les environnements d'exécution et leurs données sont surveillés pour détecter les événements potentiellement indésirables

- **Analyse des événements indésirables (DE.AE) :** Les anomalies, les indicateurs de compromission et d'autres événements potentiellement indésirables sont analysés pour caractériser les événements et détecter les incidents de cybersécurité
  - **DE.AE-02 :** Les événements potentiellement indésirables sont analysés pour mieux comprendre les activités associées
  - **DE.AE-03 :** Les informations sont corrélées à partir de sources multiples
  - **DE.AE-04 :** L'impact et la portée estimés des événements indésirables sont compris
  - **DE.AE-06 :** Les informations sur les événements indésirables sont fournies au personnel et aux outils autorisés
  - **DE.AE-07 :** Les renseignements sur les cybermenaces et d'autres informations contextuelles sont intégrés dans l'analyse
  - **DE.AE-08 :** Les incidents sont déclarés lorsque les événements indésirables répondent aux critères d'incident définis

RÉPONDRE (RS) : Des mesures concernant un incident de cybersécurité détecté sont prises

- **Gestion des incidents (RS.MA) :** Les réponses aux incidents de cybersécurité détectés sont gérées
  - **RS.MA-01 :** Le plan de réponse aux incidents est exécuté en coordination avec les tiers concernés une fois qu'un incident est déclaré
  - **RS.MA-02 :** Les rapports d'incidents sont triés et validés
  - **RS.MA-03 :** Les incidents sont catégorisés et priorisés
  - **RS.MA-04 :** Les incidents sont escaladés ou augmentés selon les besoins
  - **RS.MA-05 :** Les critères d'initiation de la reprise après incident sont appliqués
- **Analyse des incidents (RS.AN) :** Des enquêtes sont menées pour garantir une réponse efficace et soutenir les activités criminalistiques et de récupération.
  - **RS.AN-03 :** Une analyse est effectuée pour établir ce qui s'est passé lors d'un incident et la cause profonde de l'incident

- **RS.AN-06 :** Les actions effectuées au cours d'une enquête sont enregistrées et l'intégrité et la provenance des enregistrements sont préservées
- **RS.AN-07 :** Les données et métadonnées relatives aux incidents sont collectées, et leur intégrité et leur provenance sont préservées
- **RS.AN-08 :** L'ampleur d'un incident est estimée et validée

- **Rapports et communications en matière de réponse aux incidents (RS.CO) :** Les activités de réponse sont coordonnées avec les parties prenantes internes et externes, comme l'exigent les lois, les réglementations ou les politiques
  - **RS.CO-02 :** Les parties prenantes internes et externes sont informées des incidents
  - **RS.CO-03 :** Les informations sont partagées avec des parties prenantes internes et externes désignées

- **Atténuation des incidents (RS.MI) :** Les activités sont réalisées pour empêcher l'expansion d'un événement et atténuer ses effets
  - **RS.MI-01 :** Les incidents sont contenus
  - **RS.MI-02 :** Les incidents sont éradiqués

RECUPERER (RC) : Les actifs et les opérations affectés par un incident de cybersécurité sont restaurés

- **Exécution du plan de reprise après incident (RC.RP) :** Les activités de restauration sont effectuées pour garantir la disponibilité opérationnelle des systèmes et services affectés par les incidents de cybersécurité.
  - **RC.RP-01 :** La partie récupération du plan de réponse aux incidents est exécutée une fois lancée à partir du processus de réponse aux incidents.
  - **RC.RP-02 :** Les actions de récupération sont sélectionnées, délimitées, priorisées et exécutées
  - **RC.RP-03 :** L'intégrité des sauvegardes et autres actifs de restauration est vérifiée avant de les utiliser pour la restauration
  - **RC.RP-04 :** Les fonctions critiques de la mission et la gestion des risques de cybersécurité sont considérées pour établir des normes opérationnelles après incident.
  - **RC.RP-05 :** L'intégrité des actifs restaurés est vérifiée, les systèmes et services sont restaurés et l'état de fonctionnement normal est confirmé
  - **RC.RP-06 :** La fin de la reprise après incident est déclarée sur la base de critères et la documentation relative à l'incident est complétée.

- **Communication de récupération après incident (RC.CO) :** Les activités de restauration sont coordonnées avec les parties internes et externes.

- **RC.CO-03 :** Les activités de récupération et les progrès réalisés dans la restauration des capacités opérationnelles sont communiqués aux parties prenantes internes et externes désignées.
- **RC.CO-04 :** Les mises à jour publiques sur la récupération après incident sont partagées à l'aide de méthodes et de messages approuvés.

Annexe B. Niveaux du CSF

Tableau 2 contient une illustration notionnelle des Niveaux du CSF discutés à la Sec. 3. Les Niveaux caractérisent la rigueur des pratiques de gouvernance des risques de cybersécurité (GOUVERNER) et des pratiques de gestion des risques de cybersécurité (IDENTIFIER, PROTEGER, DETECTER, REPONDRE et RECUPERER) d'une organisation.

Tableau 2. Illustration notionnelle des Niveaux du CSF

Niveau	Gouvernance des Risques de Cybersécurité	Gestion des Risques de Cybersécurité
Niveau 1 : Partiel	L'application de la stratégie organisationnelle de gestion des risques de cybersécurité est gérée de manière ad hoc. La priorisation est ponctuelle et ne repose pas formellement sur des objectifs ou un environnement de menace.	La sensibilisation aux risques de cybersécurité est limitée au niveau organisationnel. L'organisation met en œuvre une gestion des risques de cybersécurité de manière irrégulière et au cas par cas. L'organisation peut ne pas disposer de processus permettant de partager des informations sur la cybersécurité au sein de l'organisation. L'organisation n'est généralement pas consciente des risques de cybersécurité associés à ses fournisseurs et aux produits et services qu'elle acquiert et utilise.
Niveau 2 : Informé sur les risques	Les pratiques de gestion des risques sont approuvées par la direction mais ne peuvent pas être établies comme une politique à l'échelle de l'organisation. La priorisation des activités de cybersécurité et des besoins de protection est directement influencée par les objectifs de risque organisationnels, l'environnement de menace ou les exigences de l'entreprise/la mission.	Il existe une prise de conscience des risques de cybersécurité au niveau organisationnel, mais une approche à l'échelle de l'organisation pour gérer les risques de cybersécurité n'a pas été établie. La prise en compte de la cybersécurité dans les objectifs et programmes organisationnels peut avoir lieu à certains niveaux de l'organisation, mais pas à tous. L'évaluation des cyber-risques liés aux actifs organisationnels et externes a lieu, mais n'est généralement pas reproductible ou récurrente. Les informations sur la cybersécurité sont partagées au sein de l'organisation de manière informelle. L'organisation est consciente des risques de cybersécurité associés à ses fournisseurs et aux produits et services qu'elle acquiert et utilise, mais elle n'agit pas de manière cohérente ou formelle en réponse à ces risques.

Niveau	Gouvernance des Risques de Cybersécurité	Gestion des Risques de Cybersécurité
Niveau 3 : Répétable	Les pratiques de gestion des risques de l'organisation sont formellement approuvées et exprimées sous forme de politique. Les politiques, processus et procédures tenant compte des risques sont définis, mis en œuvre comme prévu et examinés. Les pratiques organisationnelles en matière de cybersécurité sont régulièrement mises à jour en fonction de l'application de processus de gestion des risques aux changements dans les exigences de l'entreprise/la mission, les menaces et le paysage technologique.	Il existe une approche à l'échelle de l'organisation pour gérer les risques de cybersécurité. Les informations sur la cybersécurité sont régulièrement partagées dans toute l'organisation. 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 confiés. L'organisation surveille de manière cohérente et précise les risques de cybersécurité des actifs. Les hauts dirigeants en cybersécurité et autres communiquent régulièrement sur les risques liés à la cybersécurité. Les dirigeants veillent à ce que la cybersécurité soit prise en compte dans toutes les lignes opérationnelles de l'organisation. La stratégie de risque de l'organisation est éclairée par les risques de cybersécurité associés à ses fournisseurs et aux produits et services qu'elle acquiert et utilise. Le personnel agit formellement sur ces risques par le biais de mécanismes tels que des accords écrits pour communiquer les exigences de base, les structures de gouvernance (par exemple, les conseils des risques) et la mise en œuvre et le suivi des politiques. Ces actions sont mises en œuvre de manière cohérente et comme prévu et sont continuellement surveillées et examinées.

Niveau	Gouvernance des Risques de Cybersécurité	Gestion des Risques de Cybersécurité
Niveau 4 : Adaptatif	Il existe une approche à l'échelle de l'organisation pour gérer les risques de cybersécurité qui utilise des politiques, des processus et des procédures tenant compte des risques pour faire face aux événements potentiels de cybersécurité. La relation entre les risques de cybersécurité et les objectifs organisationnels est clairement comprise et prise en compte lors de la prise de décision. Les dirigeants surveillent les risques de cybersécurité dans le même contexte que les risques financiers et 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 commerciales mettent en œuvre la vision de la direction et analysent les risques au niveau du système dans le contexte des tolérances au risque de l'organisation. La gestion des risques de cybersécurité fait partie de la culture organisationnelle. Il évolue à partir d'une conscience des activités antérieures et d'une conscience continue des activités sur les systèmes et réseaux organisationnels. L'organisation peut prendre en compte rapidement et efficacement les changements apportés aux objectifs de l'entreprise/la mission dans la manière dont les risques sont abordés et communiqués.	L'organisation adapte ses pratiques de cybersécurité en fonction des activités de cybersécurité antérieures et actuelles, y compris les leçons apprises et les indicateurs prédictifs. Grâce à un processus d'amélioration continue qui intègre des technologies et des pratiques avancées en matière de cybersécurité, l'organisation s'adapte activement à un paysage technologique changeant et répond de manière rapide et efficace aux menaces évolutives et sophistiquées. L'organisation utilise des informations en temps réel ou quasi réel pour comprendre et agir de manière cohérente sur les risques de cybersécurité associés à ses fournisseurs et aux produits et services qu'elle acquiert et utilise. Les informations sur la cybersécurité sont constamment partagées dans toute l'organisation et avec des tiers autorisés.

Annexe C. Glossaire

Catégorie du CSF
Un groupe de résultats liés à la cybersécurité qui constituent collectivement une Fonction du CSF.

Profil Communautaire du CSF
Une base de résultats du CSF créée et publiée pour s'adresser aux intérêts et objectifs partagés par un certain nombre d'organisations. Un Profil Communautaire est généralement développé pour un secteur, un sous-secteur, une technologie, un type de menace ou un autre cas d'utilisation particulier. Une organisation peut utiliser un profil communautaire comme base pour son propre profil cible.

Noyau du CSF
Une taxonomie des résultats de de cybersécurité haut niveau qui peut aider toute organisation à gérer ses risques en matière de cybersécurité. Ses composants sont une hiérarchie de Fonctions, Catégories et Sous-catégories qui détaillent chaque résultat.

Profil Actuel du CSF
Une partie d'un Profil Organisationnel qui spécifiée les principaux résultats qu'une organisation atteint actuellement (ou tente d'atteindre) et caractérise comment ou dans quelle mesure chaque résultat est atteint.

Fonction du CSF
Le plus haut niveau d'organisation pour les résultats de cybersécurité. Il existe six Fonctions du CSF : Gouverner, Identifier, Protéger, Détecter, Répondre et Récupérer.

Exemple de Mise en Œuvre du CSF
Une illustration notionnelle concise, orientée vers l'action d'une manière d'aider à atteindre un résultat du Noyau du CSF.

Référence Informative du CSF
Une cartographie qui indique une relation entre un résultat du Noyau du CSF et une norme, une ligne directrice, une réglementation ou un autre contenu existant.

Profil Organisationnel du FSC
Un mécanisme permettant de décrire la posture de cybersécurité actuelle et/ou cible d'une organisation en termes de résultats du Noyau du CSF.

Guide de Démarrage Rapide du CSF
Une ressource supplémentaire qui fournit des conseils brefs et pratiques sur des sujets spécifiques liés au CSF.

Sous-catégorie du CSF
Un groupe de résultats plus spécifiques des activités techniques et de gestion de cybersécurité qui constituent une Catégorie du CSF.

Profil Cible du CSF
Une partie d'un Profil Organisationnel qui spécifie les résultats du Noyau souhaités qu'une organisation a sélectionnés et priorisés pour atteindre ses objectifs de gestion des risques de cybersécurité.

Niveau du CSF
Une caractérisation de la rigueur des pratiques de gouvernance et de gestion des risques de cybersécurité d'une organisation. Il existe quatre niveaux : Partiel (Niveau 1), Informé sur les risques (Niveau 2), Répétable (Niveau 3) et Adaptatif (Niveau 4).

Certains équipements, instruments, logiciels ou matériels, commerciaux ou non commerciaux, sont identifiés dans cet article afin de préciser de manière adéquate la procédure expérimentale. Une telle identification n'implique pas une recommandation ou une approbation d'un produit ou d'un service par le NIST, ni que les matériaux ou équipements identifiés sont nécessairement les meilleurs disponibles à cet effet.

Politiques de la série technique du NIST
Déclarations de droits d'auteur, d'utilisation et de licence
Syntaxe de l'identifiant de publication de la série technique NIST

Comment citer cette publication de la série technique du NIST :
Institut National des Normes et de la Technologie (2024) Le Cadre de Cybersécurité du NIST (CSF) 2.0. (Institut National des Normes et Technologies, Gaithersburg, MD), Livre Blanc du NIST sur la Cybersécurité (CSWP) NIST CSWP 29 fre. https://doi.org/10.6028/NIST.CSWP.29.fre

Coordonnées
cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899–2000

Tous les commentaires sont sujets à publication en vertu de la Loi sur la Liberté d'Information (FOIA).