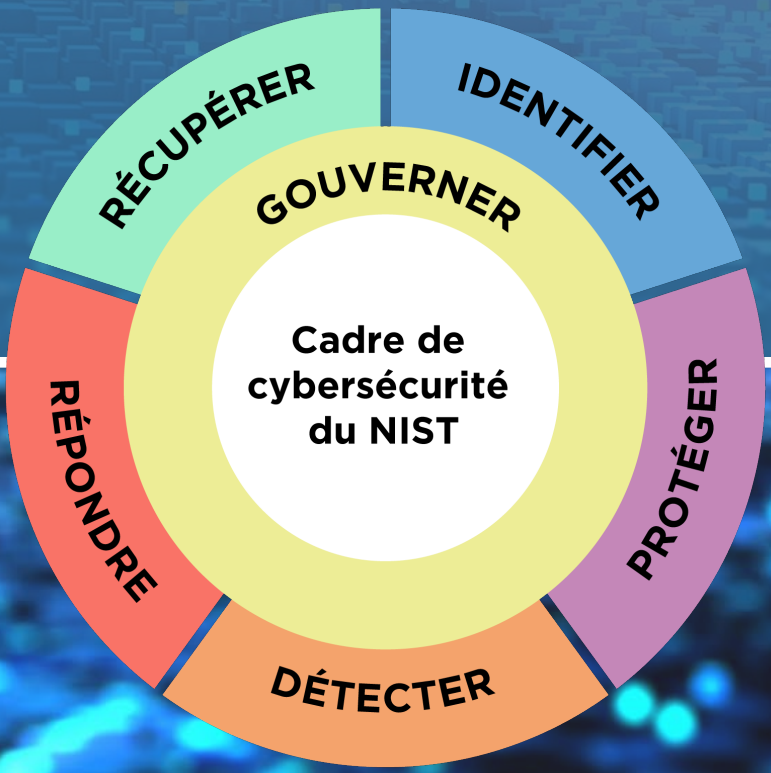
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:

GUIDE DES RESSOURCES ET DE L'APERÇU



Publication spéciale du NIST
NIST SP 1299 fre

https://doi.org/10.6028/NIST.SP.1299.fre
Février 2024

NIST CSF 2.0 :
GUIDE DES RESSOURCES ET DE L'APERÇU

QU'EST-CE QUE LE CSF 2.0... ET COMMENT L'UTILISER ?

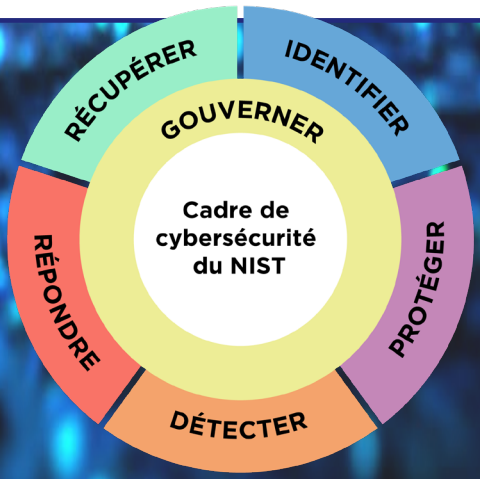
Le cadre de cybersécurité (CSF) 2.0 du NIST peut aider les organisations à gérer et à réduire les risques liés à la cybersécurité lorsqu'elles lancent ou améliorent leur programme de cybersécurité. Le CSF décrit les résultats spécifiques que les organisations peuvent atteindre pour faire face aux risques. D'autres ressources du NIST permettent d'expliquer les actions spécifiques qui peuvent être entreprises pour atteindre chaque résultat. *Ce guide est un complément au CSF du NIST et n'est pas destiné à le remplacer.*

Le CSF 2.0, ainsi que les ressources complémentaires du NIST, peuvent être utilisés par les organisations pour comprendre, évaluer, hiérarchiser et communiquer les risques liés à la cybersécurité ; il est particulièrement utile pour favoriser la communication interne et externe entre les équipes, ainsi que pour s'intégrer dans des stratégies plus larges de gestion des risques.

Le CSF 2.0 s'articule autour de six fonctions : **gouverner, identifier, protéger, détecter, réagir et récupérer**. Ensemble, ces fonctions offrent une vue d'ensemble de la gestion des risques liés à la cybersécurité. Le présent guide de ressources et d'aperçu fournit des informations détaillées sur chaque fonction, qui peuvent servir de point de départ.

Le CCA 2.0 est composé des éléments suivants :

- CSF Core - Une taxonomie de résultats de haut niveau en matière de cybersécurité qui peut aider toute organisation à gérer ses risques de cybersécurité.
- Profils organisationnels du CSF - Mécanisme permettant de décrire la position actuelle et/ou cible d'une organisation en matière de cybersécurité en fonction des résultats du CSF.
- Les niveaux du CSF - 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.



NIST CSF 2.0 :
GUIDE DES RESSOURCES ET DE L'APERÇU

EXPLORER D'AUTRES RESSOURCES CSF 2.0

Références informatives	**Visualiser et créer des correspondances entre le CCA 2.0 et d'autres documents.** Vous souhaitez soumettre vos correspondances avec les documents du NIST et les faire figurer sur notre site ? Veuillez suivre le lien à gauche ou envoyer un e-mail à olir@nist.gov si vous avez des questions.
Outil de référence pour la cybersécurité et la protection de la vie privée (CPRT)	**Parcourez et téléchargez le contenu principal et cartographié du CSF 2.0.** Le CPRT fournit un mécanisme centralisé, normalisé et modernisé pour la gestion des ensembles de données de référence (et offre un format cohérent pour l'accès aux données de référence provenant de diverses normes, lignes directrices et cadres du NIST en matière de cybersécurité et de protection de la vie privée).
Exemples de mise en œuvre	Visualiser et télécharger des exemples fictifs d'étapes concises et orientées vers l'action pour aider à atteindre les résultats des sous-catégories du CSF 2.0, en plus des conseils fournis dans les références informatives.
Outil de référence du CSF 2.0	Accéder à des versions du Core lisibles par l'homme et par la machine (en JSON et Excel). Vous pouvez également visualiser et exporter des parties du Core en utilisant des termes de recherche clés.

Des ressources supplémentaires sont disponibles :

Profils de communautés et modèles de profils (pour aider les organisations à mettre le CSF en pratique)

Outils de recherche (simplifier et rationaliser la recherche d'informations spécifiques)

Documents de réflexion (pour en savoir plus sur les différents thèmes du CSF)

FAQ (voir ce que les autres demandent et obtenir des réponses aux questions les plus fréquentes)

Explorer la suite du référentiel de ressources CSF 2.0 du NIST

NIST CSF 2.0 :
GUIDE DES RESSOURCES ET DE L'APERÇU

NAVIGATION DANS LES GUIDES DE DÉMARRAGE RAPIDE (QSG) du CSF 2.0 du NIST

Type QSG	Description	Explorer
Petites entreprises (PME)	Fournit aux PME, en particulier à celles qui n'ont que peu ou pas de plans de cybersécurité en place, des éléments pour lancer leur stratégie de gestion des risques liés à la cybersécurité.	Voir le QSG
Création et utilisation de profils organisationnels	Fournit à toutes les organisations des considérations sur la création et l'utilisation des profils actuels et/ou cibles pour mettre en œuvre le CSF 2.0.	Voir le QSG
Utilisation des niveaux du CSF	Explique comment toute organisation peut appliquer les niveaux du CSF aux profils organisationnels pour caractériser la rigueur de ses pratiques de gouvernance et de gestion des risques liés à la cybersécurité.	Voir le QSG
Projet de gestion des risques de la chaîne d'approvisionnement en matière de cybersécurité (C-SCRM)	Aide toutes les organisations à devenir des acquéreurs et des fournisseurs avisés de produits et de services technologiques en améliorant leurs processus C-SCRM.	Voir le QSG
Projet pour les praticiens de la gestion du risque d'entreprise (ERM)	Explique comment les praticiens de la gestion des risques d'entreprise peuvent utiliser les résultats fournis dans le CSF 2.0 pour améliorer la gestion des risques de cybersécurité au sein de l'organisation.	Voir le QSG

...et d'autres suivront à l'avenir.

Voir le dépôt en ligne actuel du QSG

NIST CSF 2.0 : GUIDE DES RESSOURCES ET DE L'APERÇU

GOUVERNER

La stratégie, les attentes et la politique de l'organisation en matière de gestion des risques liés à la cybersécurité sont établies, communiquées et contrôlées.

Comprendre et évaluer les besoins spécifiques en matière de cybersécurité. Déterminer les risques et les besoins propres à votre organisation. Discuter de l'environnement de risque actuel et prévu et du niveau de risque que votre organisation est prête à accepter. Solliciter la contribution et les idées de l'ensemble de l'organisation. Comprendre ce qui a fonctionné ou non dans le passé et en discuter ouvertement.

Élaborer une stratégie sur mesure en matière de risques de cybersécurité. Elle doit être fondée sur les objectifs spécifiques de votre organisation en matière de cybersécurité, sur l'environnement de risque et sur les enseignements tirés du passé - et des autres. Gérer, mettre à jour et discuter de la stratégie à intervalles réguliers. Les rôles et les responsabilités doivent être clairs.

Établir des politiques définies de gestion des risques. Les politiques doivent être approuvées par la direction, s'appliquer à l'ensemble de l'organisation, être reproductibles et récurrentes, et s'aligner sur le contexte actuel des menaces pour la cybersécurité, les risques (qui évolueront au fil du temps) et les objectifs de la mission. Intégrer les politiques dans la culture de l'entreprise afin de favoriser et d'inspirer la capacité à prendre des décisions éclairées. Rendre compte des obligations légales, réglementaires et contractuelles.

Développer et communiquer les pratiques organisationnelles en matière de cybersécurité. Celles-ci doivent être simples et communiquées régulièrement. Ils doivent refléter l'application de la gestion des risques à l'évolution des exigences de la mission ou de l'activité, des menaces et du paysage technique global. Documenter les pratiques et les partager en tenant compte du retour d'information et en faisant preuve de souplesse pour changer de cap.

Mettre en place une gestion des risques de la chaîne d'approvisionnement en matière de cybersécurité et en assurer le suivi. Établir une stratégie, une politique, des rôles et des responsabilités, y compris pour la supervision des fournisseurs, des clients et des partenaires. Intégrer les exigences dans les contrats. Impliquer les partenaires et les fournisseurs dans la planification, la réponse et le rétablissement.

Mettre en place une surveillance continue et des points de contrôle. Analyser les risques à intervalles réguliers et les surveiller en permanence (comme vous le feriez pour les risques financiers).

IDENTIFIER

Les risques actuels de l'organisation en matière de cybersécurité sont compris.

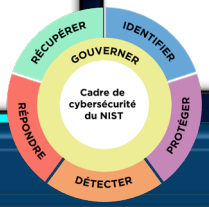
Identifier les processus et les actifs critiques de l'entreprise. Réfléchir aux activités de votre organisation qui doivent absolument être poursuivies pour être viables. Il peut s'agir, par exemple, de gérer un site web pour récupérer les paiements, de protéger en toute sécurité les informations relatives aux clients/patients ou de veiller à ce que les informations essentielles à votre organisation restent accessibles et exactes.

Tenir des inventaires du matériel, des logiciels, des services et des systèmes. Sachez quels sont les ordinateurs et les logiciels utilisés par votre organisation - y compris les services fournis par les fournisseurs - car ce sont souvent les points d'entrée des acteurs malveillants. Cet inventaire peut être aussi simple qu'une feuille de calcul. Envisager d'inclure les appareils et applications personnels des employés, qu'ils soient possédés ou loués.

Documenter les flux d'informations. Réfléchir au type d'informations que votre organisation recueille et utilise (ainsi qu'à l'endroit où se trouvent les données et à la manière dont elles sont utilisées), en particulier lorsque des contrats et des partenaires externes sont impliqués.

Identifier les menaces, les vulnérabilités et les risques pour les biens. Sur la base de la connaissance des menaces internes et externes, les risques doivent être identifiés, évalués et documentés. Parmi les moyens de les documenter, on peut citer les registres des risques, qui contiennent des informations sur les risques, y compris des données sur les risques au fil du temps. Veiller à ce que les réponses aux risques soient identifiées, hiérarchisées et exécutées, et à ce que les résultats soient contrôlés.

Les enseignements tirés sont utilisés pour identifier les améliorations à apporter. Dans la conduite des activités quotidiennes, il est important d'identifier les moyens d'affiner ou d'améliorer les performances, y compris les possibilités de mieux gérer et de réduire les risques liés à la cybersécurité. Cela nécessite un effort délibéré de la part de votre organisation à tous les niveaux. En cas d'incident, évaluez ce qui s'est passé. Préparer un rapport après action qui documente l'incident, l'intervention, les mesures de rétablissement prises et les enseignements tirés.



NIST CSF 2.0 : GUIDE DES RESSOURCES ET DE L'APERÇU

PROTÉGER

Des mesures de protection des personnes sont utilisées pour gérer les risques de cybersécurité de l'organisation.

Gérer l'accès. Créez des comptes uniques pour les employés et veillez à ce que les utilisateurs n'aient accès qu'aux ressources nécessaires. Authentifier les utilisateurs avant de leur accorder l'accès aux informations, aux ordinateurs et aux applications. Gérer et suivre l'accès physique aux installations/appareils.

Utilisateurs du train. Former régulièrement les employés pour s'assurer qu'ils connaissent les politiques et les procédures de cybersécurité et qu'ils ont les connaissances et les compétences nécessaires pour effectuer des tâches générales et spécifiques ; expliquer comment reconnaître les attaques courantes et signaler toute activité suspecte. Certaines fonctions peuvent nécessiter une formation supplémentaire.

Protéger et surveiller vos appareils. Envisager d'utiliser des produits de sécurité pour les points finaux. Appliquer des configurations uniformes aux appareils et contrôler les modifications apportées aux configurations des appareils. Désactiver les services ou les fonctionnalités qui ne soutiennent pas les fonctions de la mission. Configurer les systèmes et les services pour qu'ils génèrent des enregistrements. Veiller à ce que les appareils soient mis au rebut de manière sûre.

Protéger les données sensibles. Veiller à ce que les données sensibles stockées ou transmises soient protégées par cryptage. Envisagez d'utiliser le contrôle d'intégrité afin que seules les modifications approuvées soient apportées aux données. Effacer et/ou détruire les données en toute sécurité lorsqu'elles ne sont plus nécessaires ou requises.

Gérer et entretenir les logiciels. Mettre régulièrement à jour les systèmes d'exploitation et les applications ; activer les mises à jour automatiques. Remplacer les logiciels en fin de vie par des versions compatibles. Envisagez d'utiliser des outils logiciels pour analyser les appareils afin de détecter d'autres vulnérabilités et d'y remédier.

Effectuer des sauvegardes régulières. Sauvegardez les données selon un calendrier convenu ou utilisez les fonctions de sauvegarde intégrées ; les logiciels et les solutions en nuage peuvent automatiser ce processus. Conservez au moins un ensemble de données sauvegardées hors ligne pour les protéger contre les ransomwares. Test pour s'assurer que les données sauvegardées peuvent être restaurées avec succès dans les systèmes.

DÉTECTER

Les éventuelles attaques et compromissions en matière de cybersécurité sont trouvées et analysées.

Surveiller en permanence les réseaux, les systèmes et les installations afin de détecter les événements potentiellement néfastes. Élaborer et tester des processus et des procédures pour détecter les indicateurs d'un incident de cybersécurité sur le réseau et dans l'environnement physique. Collecter des informations de journal à partir de plusieurs sources organisationnelles afin de faciliter la détection d'activités non autorisées.

Déterminer et analyser l'impact et la portée estimés des événements indésirables. Si un événement de cybersécurité est détecté, votre organisation doit travailler rapidement et de manière approfondie pour comprendre l'impact de l'incident. La compréhension des détails relatifs à tout incident de cybersécurité contribuera à éclairer la réponse.

Fournir des informations sur les événements indésirables au personnel et aux outils autorisés. Lorsque des événements indésirables sont détectés, fournir des informations sur l'événement en interne au personnel autorisé afin de s'assurer que les mesures appropriées de réponse à l'incident sont prises.

NIST CSF 2.0 : GUIDE DES RESSOURCES ET DE L'APERÇU

RÉPONDRE

Des mesures sont prises en cas d'incident de cybersécurité détecté.

Mettre en œuvre un plan d'intervention en cas d'incident déclaré, en coordination avec les tiers concernés. Pour exécuter correctement un plan d'intervention en cas d'incident, il faut s'assurer que chacun connaît ses responsabilités, ce qui implique de comprendre toutes les exigences (par exemple en matière de réglementation, de rapports légaux et de partage d'informations).

Classer les incidents par catégorie et par ordre de priorité et les transmettre à un échelon supérieur si nécessaire. Analyser ce qui s'est passé, déterminer la cause première de l'incident et établir un ordre de priorité pour les incidents qui requièrent en premier lieu l'attention de votre organisation. Communiquer cet ordre de priorité à votre équipe et veiller à ce que chacun comprenne à qui les informations doivent être communiquées concernant un incident prioritaire lorsqu'il se produit.

Collecter les données relatives aux incidents et préserver leur intégrité et leur provenance. La collecte d'informations en toute sécurité facilitera la réaction de votre organisation en cas d'incident. Veiller à ce que les données soient toujours sécurisées après l'incident afin de préserver la réputation de votre organisation et la confiance des parties prenantes. Le stockage de ces informations en toute sécurité peut également contribuer à améliorer l'efficacité des plans d'intervention mis à jour et futurs.

Notifier les parties prenantes internes et externes de tout incident et partager avec elles les informations relatives à l'incident, conformément aux politiques établies par votre organisation. Partager en toute sécurité les informations conformément aux plans d'intervention et aux accords de partage d'informations. Notifier les incidents aux partenaires commerciaux et aux clients conformément aux exigences contractuelles.

Contenir et éradiquer les incidents. L'exécution d'un plan d'intervention élaboré et testé aidera votre organisation à contenir les effets d'un incident et à l'éradiquer. Une coordination et une communication efficaces avec les parties prenantes peuvent permettre de réagir plus efficacement et d'atténuer les effets de l'incident.

RÉCUPÉRER

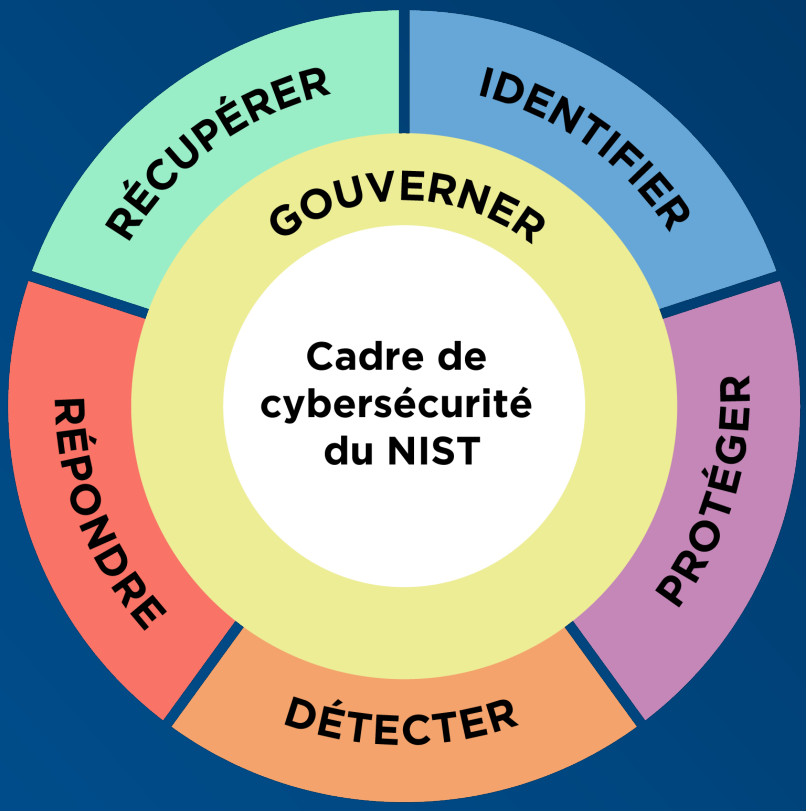
Les actifs et les opérations touchés par un incident de cybersécurité sont rétablis.

Comprendre les rôles et les responsabilités. Comprendre qui, à l'intérieur et à l'extérieur de votre entreprise, a des responsabilités en matière de récupération. Sachez qui a accès et est habilité à prendre des décisions pour mener à bien vos efforts de réponse au nom de l'entreprise.

Exécutez votre plan de reprise. Assurer la disponibilité opérationnelle des systèmes et des services concernés ; établir des priorités et effectuer des tâches de récupération.

Vérifiez deux fois votre travail. Il est important de s'assurer de l'intégrité des sauvegardes et des autres éléments de récupération avant de les utiliser pour reprendre les activités normales de l'entreprise.

Communiquer avec les parties prenantes internes et externes. Déterminer avec soin quelles informations seront partagées avec les différentes parties prenantes, comment et quand, afin que toutes les parties intéressées reçoivent les informations dont elles ont besoin, mais qu'aucune information inappropriée ne soit partagée. Communiquez à votre personnel les enseignements tirés et les révisions apportées aux processus, procédures et technologies (conformément aux politiques déjà établies par l'organisation). C'est le bon moment pour former ou recycler le personnel sur les meilleures pratiques en matière de cybersécurité.



Département du commerce des États-Unis
Gina M. Raimondo, Secrétaire

Institut national des normes et de la technologie
Laurie E. Locascio, directeur du NIST et sous-secrétaire au commerce pour les normes et la technologie