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

NIST Cybersecurity Framework 2.0:

Guide de démarrage rapide pour les petites entreprises

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Publication spéciale du NIST
NIST SP 1300
https://doi.org/10.6028/NIST.SP.1300.fre
Février 2024

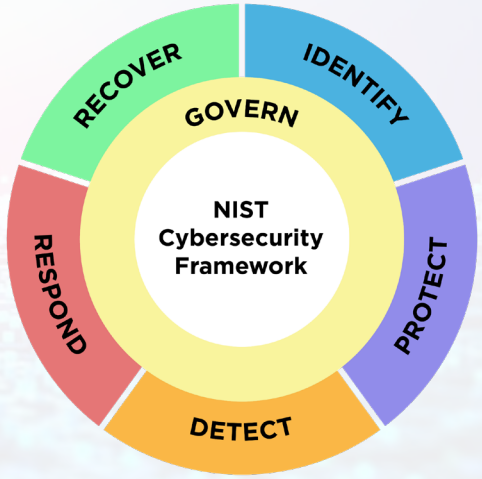
Cadre de cybersécurité NIST 2.0 : Guide de démarrage rapide pour les petites entreprises

Objectif

Ce guide fournit aux petites et moyennes entreprises (PME), en particulier à celles qui n'ont que peu ou pas de plans de cybersécurité en place, des éléments permettant de lancer leur stratégie de gestion des risques de cybersécurité en utilisant le cadre de cybersécurité (CSF) 2.0 du NIST. Ce guide peut également aider d'autres organisations relativement petites, telles que les organisations à but non lucratif, les agences gouvernementales et les écoles. Il s'agit d'un complément au NIST CSF et n'est pas destiné à le remplacer.

Qu'est-ce que le cadre de cybersécurité du NIST ?

Le cadre de cybersécurité du NIST est un guide volontaire qui aide les organisations, quels que soient leur taille, leur secteur ou leur maturité, à mieux comprendre, évaluer, hiérarchiser et communiquer leurs efforts en matière de cybersécurité. Le cadre n'est pas une approche unique de la gestion des risques liés à la cybersécurité. Ce supplément et le CSF 2.0 complet peuvent aider les organisations à prendre en compte et à enregistrer leurs propres tolérances au risque, priorités, menaces, vulnérabilités, exigences, etc.



Le cadre de cybersécurité : pour commencer

Le CCA organise les résultats de la cybersécurité en six fonctions de haut niveau : Gouverner, Identifier, Protéger, Détecter, Répondre et Récupérer. Considérées dans leur ensemble, ces fonctions offrent une vision globale de la gestion des risques liés à la cybersécurité. Les activités énumérées pour chaque fonction dans le présent guide peuvent constituer un bon point de départ pour votre entreprise. Pour obtenir des exemples spécifiques, orientés vers l'action, sur la manière de réaliser les activités énumérées, reportez-vous aux exemples de mise en œuvre du CCA 2.0. Si vous ne comprenez pas certaines activités ou si vous ne vous sentez pas à l'aise pour les aborder vous-même, ce guide peut servir de point de départ à une discussion avec la personne que vous avez choisie pour vous aider à réduire les risques liés à la cybersécurité, par exemple un fournisseur de services de sécurité gérés (MSSP).

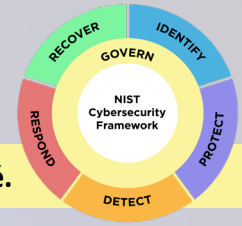
EXPLORER D'AUTRES RESSOURCES CSF 2.0

nist.gov/cyberframework

Trouvez rapidement ce dont vous avez besoin, y compris :

- ✓Une série de NOUVEAUX guides de démarrage rapide
- ✓Exemples de mise en œuvre
- ✓Outils de recherche
- ✓FAQ
- ✓Et bien plus encore !

GOUVERNER



La fonction de gouvernance vous aide à établir et à contrôler la stratégie, les attentes et la politique de votre entreprise en matière de gestion des risques liés à la cybersécurité.

Actions à envisager

Comprendre

- Comprennez comment les risques de cybersécurité peuvent perturber la réalisation de la mission de votre entreprise. *(GV.OC-01)*
- Comprennez les exigences légales, réglementaires et contractuelles en matière de cybersécurité. *(GV.OC-03)*
- Déterminez qui, au sein de l'entreprise, sera responsable de l'élaboration et de la mise en œuvre de la stratégie de cybersécurité. *(GV.RR-02)*

Évaluer

- Évaluez l'impact potentiel d'une perte totale ou partielle des actifs et opérations critiques de l'entreprise. *(GV.0C-04)*
- Déterminez si l'assurance cybersécurité est appropriée pour votre entreprise. *(GV.RM-04)*
- Évaluez les risques de cybersécurité posés par les fournisseurs et autres tiers avant de nouer des relations formelles. *(GV.SC-06)*

Fixer des priorités

- Donnez la priorité à la gestion des risques liés à la cybersécurité, au même titre que les autres risques de l'entreprise. *(GV.RM-03)*

Communiquer

- Communiquez le soutien de la direction à une culture consciente des risques, éthique et en constante amélioration. *(GV.RR-01)*
- Communiquez, appliquez et maintenez des politiques de gestion des risques liés à la cybersécurité. *(GV.PO-01)*

Démarrer la gouvernance de la cybersécurité

Vous pouvez utiliser ces tableaux pour commencer à réfléchir à votre stratégie de gouvernance en matière de cybersécurité.

Mise en place du contexte organisationnel	
Notre mission d'entreprise :	
Quels sont les risques de cybersécurité qui pourraient nous empêcher de mener à bien cette mission ?	

Documenter les exigences en matière de cybersécurité	
Dressez la liste de vos obligations légales :	
Dressez la liste de vos exigences réglementaires :	
Dressez la liste de vos exigences contractuelles :	

Plongée technique : Mise en scène des risques de cybersécurité pour la gestion des risques d'entreprise et le contrôle de la gouvernance

Questions à examiner

- À mesure que notre entreprise se développe, à quelle fréquence révisons-nous notre stratégie de cybersécurité ?
- Devons-nous améliorer les compétences de notre personnel, recruter des talents ou faire appel à un partenaire externe pour nous aider à mettre en place et à gérer notre plan de cybersécurité ?
- Avons-nous mis en place des politiques d'utilisation acceptable pour l'entreprise et pour les appareils appartenant aux employés qui accèdent aux ressources de l'entreprise ? Les employés ont-ils été sensibilisés à ces politiques ?

Ressources connexes

- Manuel de ressources sur la sécurisation des chaînes d'approvisionnement des petites et moyennes entreprises
- Choix d'un vendeur/prestataire de services

Voir toutes les ressources du NIST CSF 2.0 ici

IDENTIFIER

La fonction d'identification vous aide à déterminer le risque actuel de cybersécurité pour l'entreprise.

Actions à envisager

Comprendre

- Comprennez sur quels actifs repose votre entreprise en créant et en tenant à jour un inventaire du matériel, des logiciels, des systèmes et des services. *(ID.AM-01/02/04)*

Évaluer

- Évaluez les vulnérabilités potentielles de vos actifs (informatiques et physiques). *(ID.RA-01)*
- Évaluez l'efficacité du programme de cybersécurité de l'entreprise afin d'identifier les points à améliorer. *(ID.IM-01)*

Fixer des priorités

- Donnez la priorité à l'inventaire et à la classification des données de l'entreprise. *(ID.AM-07)*
- Établissez un ordre de priorité dans la documentation des menaces internes et externes en matière de cybersécurité et des réponses associées à l'aide d'un registre des risques. *(ID.RA)*

Communiquer

- Communiquez les plans, les politiques et les meilleures pratiques en matière de cybersécurité à l'ensemble du personnel et aux tiers concernés. *(ID.IM-04)*
- Communiquez au personnel l'importance d'identifier les améliorations à apporter aux processus, procédures et activités de gestion des risques liés à la cybersécurité. *(ID.IM)*

Commencer à identifier les risques actuels de cybersécurité pour votre entreprise

Avant de pouvoir protéger vos actifs, vous devez les identifier. Vous pourrez ensuite déterminer le niveau de protection approprié pour chaque actif en fonction de sa sensibilité et de sa criticité pour la mission de votre entreprise. Vous pouvez utiliser cet exemple de tableau pour commencer à dresser l'inventaire de vos actifs informatiques. Au fur et à mesure que votre entreprise se développe, vous pouvez envisager d'utiliser une solution automatisée d'inventaire des biens ou un fournisseur de services de sécurité gérés pour vous aider à gérer l'ensemble des biens de votre entreprise.

Logiciels/ matériel/ système/ service	Utilisation officielle de l'actif :	Administrateur ou propriétaire des biens :	Identifier les données sensibles auxquelles le bien a accès :	Une authentification multifactorielle est-elle nécessaire pour accéder à ce bien ?	Risque pour l'entreprise si nous perdons l'accès à cet actif

Plongée technique : Intégrer la cybersécurité et la gestion des risques d'entreprise

Questions à examiner

- Quels sont les actifs les plus critiques de notre entreprise (données, matériel, logiciels, systèmes, installations, services, personnel, etc.
- Quels sont les risques en matière de cybersécurité et de protection de la vie privée associés à chaque actif ?
- Quels sont les technologies ou les services utilisés par le personnel pour accomplir son travail ? Ces services ou technologies sont-ils sécurisés et leur utilisation approuvée ?

Ressources connexes

- Modèle de registre des risques NIST
- Faire le point. Connaître les informations sensibles dont vous disposez
- Évaluer votre résilience opérationnelle et vos pratiques en matière de cybersécurité

Voir toutes les ressources du NIST CSF 2.0 ici

PROTÉGER

La fonction de protection vous permet d'utiliser des mesures de protection pour prévenir ou réduire les risques liés à la cybersécurité.

Actions à envisager

Comprendre

- Comprendre quelles sont les informations auxquelles les employés devraient avoir ou ont accès. Restreindre l'accès aux informations sensibles aux seuls employés qui en ont besoin pour faire leur travail. *(PR.AA-05)*

Évaluer

- Évaluez l'opportunité, la qualité et la fréquence de la formation à la cybersécurité dispensée par votre entreprise à ses employés. *(PR.AT-01/02)*

Fixer des priorités

- Exiger en priorité l'authentification multifactorielle pour tous les comptes qui la proposent et envisagez d'utiliser des gestionnaires de mots de passe pour vous aider, vous et votre personnel, à créer et à protéger des mots de passe forts. *(PR.AA-03)*
- Donner la priorité à la modification des mots de passe par défaut des fabricants. *(PR.AA-01)*
- Accorder la priorité à la mise à jour régulière et à l'application de correctifs aux logiciels et aux systèmes d'exploitation. Activer les mises à jour automatiques pour vous en souvenir. *(PR.PS-02)*
- Donner la priorité à la sauvegarde régulière de vos données et au test de vos sauvegardes. *(PR.DS-11)*
- Configurer en priorité vos tablettes et ordinateurs portables pour activer le chiffrement intégral du disque afin de protéger les données. *(PR.DS-01)*

Communiquer

- Expliquer à votre personnel comment reconnaître les attaques courantes, signaler les attaques ou les activités suspectes et effectuer des tâches d'hygiène informatique de base. *(PR.AT-01/02)*

Commencer à protéger son entreprise

L'activation de l'authentification multifactorielle (AMF) est l'un des moyens les plus rapides et les moins coûteux de protéger vos données. Commencez par les comptes qui peuvent accéder aux informations les plus sensibles. Utilisez cette liste de contrôle pour vous donner une longueur d'avance, mais n'oubliez pas que votre propre liste sera plus longue que celle-ci :

Compte	MFA activé (O/N)
Compte(s) bancaire(s)	
Compte(s) comptable(s) et fiscal(aux)	
Compte(s) marchand(s)	
Compte(s) Google, Microsoft et/ou Apple ID	
Compte(s) de messagerie	
Gestionnaire(s) de mots de passe	
Compte(s) Internet	

Approfondissement technique : Lignes directrices du NIST sur l'identité numérique

Questions à examiner

- Limitons-nous l'accès et les privilèges aux seules personnes qui en ont besoin ? Supprimons-nous l'accès lorsqu'ils n'en ont plus besoin ?
- Comment assainissons-nous et détruisons-nous en toute sécurité les données et les dispositifs de stockage de données lorsqu'ils ne sont plus nécessaires ?
- Les employés possèdent-ils les connaissances et les compétences nécessaires pour accomplir leur travail en tenant compte de la sécurité ?

Ressources connexes

- Ressources de formation à la cybersécurité
- Authentification multifactorielle
- Protéger votre entreprise contre l'hameçonnage

Voir toutes les ressources du NIST CSF 2.0 ici

DÉTECTER

La fonction de détection fournit des résultats qui vous aident à trouver et à analyser d'éventuelles attaques et compromissions en matière de cybersécurité.

Actions à envisager

Comprendre

- Comprennez comment identifier les indicateurs communs d'un incident de cybersécurité. *(DE.CM)*

Évaluer

- Évaluez vos technologies informatiques et vos services externes pour détecter les écarts par rapport au comportement attendu ou typique. *(DE.CM-06/09)*
- Évaluez votre environnement physique pour y déceler des signes d'altération ou d'activité suspecte. *(DE.CM-02)*

Fixer des priorités

- Donnez la priorité à l'installation et à la maintenance de logiciels antivirus et anti-malware sur tous les appareils de l'entreprise, y compris les serveurs, les ordinateurs de bureau et les ordinateurs portables. *(DE.CM-09)*
- Si vous ne disposez pas des ressources nécessaires pour le faire en interne, engagez en priorité un prestataire de services pour surveiller les ordinateurs et les réseaux à la recherche d'activités suspectes. *(DE.CM)*

Communiquer

- Communiquez avec votre intervenant autorisé en cas d'incident, tel qu'un MSSP, sur les détails pertinents de l'incident afin de l'aider à l'analyser et à l'atténuer. *(DE.AE-06/07)*

Premiers pas dans la détection des incidents

Voici quelques indicateurs courants d'un incident de cybersécurité :

- Perte de l'accès habituel aux données, applications ou services
- Réseau anormalement lent
- Les logiciels antivirus émettent des alertes lorsqu'ils détectent qu'un hôte est infecté par un logiciel malveillant.
- Plusieurs tentatives de connexion échouées
- Un administrateur de messagerie voit de nombreux courriels renvoyés dont le contenu est suspect.
- Un administrateur de réseau remarque un écart inhabituel par rapport aux flux de trafic typiques du réseau

Plongée technique : Guide de traitement des incidents de sécurité informatique du NIST

Questions à examiner

- Les appareils utilisés dans le cadre de notre activité, qu'ils appartiennent à l'entreprise ou aux employés, sont-ils dotés d'un logiciel antivirus ?
- Les employés savent-ils comment détecter d'éventuelles attaques de cybersécurité et comment les signaler ?
- Comment notre entreprise surveille-t-elle ses journaux et ses alertes pour détecter d'éventuels cyberincidents ?

Ressources connexes

- Protection contre les ransomwares et réponse
- Détection d'une intrusion potentielle
- Ressources de formation à la cybersécurité

Voir toutes les ressources du NIST CSF 2.0 ici

RÉPONDRE

La fonction "réagir" vous permet de prendre des mesures en cas d'incident de cybersécurité détecté.

Actions à envisager

Comprendre

- Comprendre ce qu'est votre plan d'intervention en cas d'incident et savoir qui a l'autorité et la responsabilité de mettre en œuvre les différents aspects du plan. *(RS.MA-01)*

Évaluer

- Évaluer votre capacité à répondre à un incident de cybersécurité. *(RS.MA-01)*
- Évaluer l'incident pour déterminer sa gravité, ce qui s'est passé et sa cause profonde. *(RS.AN-03, RS.MA-03)*

Fixer des priorités

- Prendre en priorité des mesures pour contenir et éradiquer l'incident afin d'éviter d'autres dommages. *(RS.MI)*

Communiquer

- Communiquer un incident de cybersécurité confirmé à toutes les parties prenantes internes et externes (par exemple, les clients, les partenaires commerciaux, les autorités chargées de l'application de la loi, les organismes de réglementation) comme l'exigent les lois, les règlements, les contrats ou les politiques. *(RS.CO-02/03)*

Démarrer avec un plan d'intervention en cas d'incident

Avant qu'un incident ne se produise, vous devez être prêt à mettre en place un plan d'intervention de base. Ce plan sera personnalisé en fonction de l'entreprise, mais il devrait comprendre les éléments suivants

- ✓ **Un champion de l'entreprise** : Une personne responsable de l'élaboration et de la mise à jour de votre plan d'intervention en cas d'incident.
- ✓ **Qui appeler ?** Dressez la liste de toutes les personnes susceptibles de participer à vos efforts de réponse à l'incident. Indiquez leurs coordonnées, leurs responsabilités et leur autorité.
- ✓ **Quoi/quand/comment signaler :** Dressez la liste des responsabilités de votre entreprise en matière de communication/rapport, conformément aux lois, réglementations, contrats ou politiques.

Plongée technique : Guide de traitement des incidents de sécurité informatique du NIST

Contact	Téléphone
Chef d'entreprise :	
Contact technique :	
Police d'État :	
Juridique :	
Banque :	
Assurance :	

Questions à examiner

- Disposons-nous d'un plan de réponse aux incidents de cybersécurité ? Dans l'affirmative, l'avons-nous mis en pratique pour voir s'il est réalisable ?
- Savons-nous qui sont les principaux acteurs et décideurs internes et externes qui nous aideront en cas d'incident de cybersécurité confirmé ?

Ressources connexes

- Les bases du plan d'intervention en cas d'incident
- Internet Crime Complaint Center du FBI
- Réponse aux violations de données : Un guide pour les entreprises
- Bonnes pratiques en matière d'intervention auprès des victimes et de signalement des cyberincidents

Voir toutes les ressources du NIST CSF 2.0 ici

RÉCUPÉRER

La fonction de récupération implique des activités visant à restaurer les biens et les opérations qui ont été affectés par un incident de cybersécurité.

Actions à envisager

Comprendre

- Comprendre qui, à l'intérieur et à l'extérieur de votre entreprise, a des responsabilités en matière de récupération. *(RC.RP-01)*

Évaluer

- Évaluez ce qui s'est passé en préparant un rapport après action - par vous-même ou en consultation avec un fournisseur/partenaire - qui documente l'incident, les mesures d'intervention et de rétablissement prises et les leçons tirées. *(RC.RP-06)*
- Évaluez l'intégrité de vos données et actifs sauvegardés avant de les utiliser pour la restauration. *(RC.RP-03)*

Fixer des priorités

- Priorisez vos actions de récupération en fonction des besoins de l'organisation, des ressources et des biens touchés. *(RC.RP-02)*

Communiquer

- Communiquez régulièrement et en toute sécurité avec les parties prenantes internes et externes. *(RC.CO)*
- Communiquez et documenter la fin de l'incident et la reprise des activités normales. *(RC.RP-06)*

Démarrer avec un manuel de récupération
Un cahier de jeu comprend généralement les éléments essentiels suivants :

- ✓ Un ensemble de processus formels de récupération
- ✓ Documentation de la criticité des ressources de l'organisation (par exemple, les personnes, les installations, les composants techniques, les services externes)
- ✓ Documentation des systèmes qui traitent et stockent les informations de l'organisation, en particulier les actifs clés. Cela permettra d'établir l'ordre des priorités de restauration.
- ✓ Une liste du personnel qui sera responsable de la définition et de la mise en œuvre des plans de récupération
- ✓ Un plan de communication complet pour la reprise

Plongée technique approfondie : Guide du NIST pour la récupération des événements de cybersécurité

Questions à examiner

- Quels sont les enseignements que nous avons tirés ? Comment pouvons-nous réduire au minimum les risques d'incident de cybersécurité à l'avenir ?
- Quelles sont nos obligations légales, réglementaires et contractuelles en matière de communication avec les parties prenantes internes et externes en cas d'incident de cybersécurité ?
- Comment s'assurer que les mesures de redressement que nous prenons n'introduisent pas de nouvelles vulnérabilités dans notre entreprise ?

Ressources connexes

- Ressources de formation à la cybersécurité
- Création d'un plan de reprise après sinistre informatique
- Sauvegarde et récupération des ressources

Voir toutes les ressources du NIST CSF 2.0 ici

Profils et ressources complémentaires

Utiliser les profils organisationnels pour mettre en œuvre le cadre de cybersécurité

Un *profil organisationnel CCA* décrit la position actuelle et/ou cible d'une organisation en matière de cybersécurité en fonction des résultats du CCA en matière de cybersécurité. Chaque profil organisationnel comprend l'un des éléments suivants ou les deux :

1. Un **profil actuel** spécifie les résultats souhaités qu'une organisation atteint actuellement (ou tente d'atteindre) et caractérise comment ou dans quelle mesure chaque résultat est atteint.
2. Un **profil cible** précise les résultats qu'une organisation a sélectionnés et classés par ordre de priorité pour atteindre ses objectifs de gestion des risques liés à la cybersécurité.
    - Vous pouvez également utiliser un **profil de communauté** comme base pour votre profil de cible. Un profil de communauté est une base de référence des résultats ciblés pour un secteur, une technologie, un type de menace ou un autre cas d'utilisation particulier.
    - Vous pouvez également choisir d'utiliser les **niveaux du CCA** pour créer votre profil. Les niveaux caractérisent la rigueur actuelle ou ciblée des pratiques d'une organisation par fonction ou catégorie du CCA. Pour plus d'informations sur les niveaux et leur utilisation, consultez le *Guide de démarrage rapide pour l'utilisation des niveaux du CCA*.

Consultez le *Guide de démarrage rapide pour la création et l'utilisation de profils d'organisation* pour obtenir des informations plus détaillées sur la manière de commencer à créer des profils actuels et cibles pour votre organisation.

Ressources complémentaires

L'outil de référence du cadre de cybersécurité du NIST permet aux utilisateurs d'explorer l'intégralité du CSF 2.0 Core dans des versions lisibles par l'homme et par la machine (en JSON et Excel), tout en conservant des ressources contenant des informations qui vous aideront à atteindre les résultats souhaités, comme par exemple :

- Cartographie : Les références informatives sont des cartographies indiquant les relations entre le CCA 2.0 et diverses normes, lignes directrices, réglementations et autres contenus. Elles permettent de savoir comment une organisation peut atteindre les résultats du CSC.
- Les exemples de mise en œuvre illustrent des étapes concises et orientées vers l'action pour guider les organisations dans la réalisation des résultats du CCA. Ces exemples ne constituent pas une liste exhaustive de toutes les mesures qui pourraient être prises par une organisation, ni une base de référence des mesures requises ; il s'agit d'une série d'exemples utiles pour amener les organisations à réfléchir à des mesures concrètes.

L'outil de référence du NIST pour la cybersécurité et la protection de la vie privée (CPRT) offre un moyen simple d'accéder aux données de référence de diverses normes, lignes directrices et cadres du NIST en matière de cybersécurité et de protection de la vie privée, téléchargeables dans des formats courants (XLSX et JSON).

La norme NIST SP 800-53 fournit un catalogue de contrôles de sécurité et de protection de la vie privée parmi lesquels vous pouvez choisir. Ces contrôles sont flexibles, personnalisables et mis en œuvre dans le cadre d'un processus de gestion des risques à l'échelle de l'organisation. Visualiser et exporter à partir de l'outil de référence pour la cybersécurité et la protection de la vie privée (CPRT).

Le cadre pour les effectifs en cybersécurité (cadre NICE) aide les employeurs à atteindre les résultats du CCA 2.0 en les aidant à identifier les lacunes critiques dans les effectifs et les capacités en matière de cybersécurité, à déterminer et à communiquer les responsabilités des postes et les descriptions des tâches, et à fournir une formation au personnel et des parcours de carrière.