AYI NEDJIMI Consultants

Maturité cybersécurité : modèles CMMC et NIST CSF 2.0

Catégorie : Conformité Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Comparez les modèles CMMC et NIST CSF 2.0 pour évaluer votre maturité cybersécurité. Guide avec critères, mapping NIS 2 et feuille de route pratique.

Résumé exécutif

L'évaluation du niveau de maturité cybersécurité d'une organisation est devenue un exercice incontournable pour piloter la progression de la posture de sécurité, justifier les investissements auprès de la direction et répondre aux exigences croissantes des régulateurs, clients et partenaires commerciaux. Ce guide analyse en profondeur les deux principaux modèles de maturité utilisés dans le monde occidental, le NIST Cybersecurity Framework version 2.0 et le Cybersecurity Maturity Model Certification, en détaillant leurs structures respectives, leurs critères d'évaluation, leurs domaines d'application privilégiés et leur complémentarité pour les organisations européennes soumises simultanément aux exigences réglementaires continentales comme NIS 2 et DORA et aux standards internationaux imposés par leurs partenaires et donneurs d'ordre américains, tout en fournissant des critères de sélection objectifs et des recommandations pratiques pour choisir le modèle le plus adapté à votre contexte organisationnel spécifique.

Mesurer la maturité cybersécurité d'une organisation est un exercice fondamentalement différent d'un simple audit de conformité ou d'un test d'intrusion technique ponctuel. Là où l'audit vérifie la conformité à un référentiel normatif à un instant précis et où le pentest évalue la résistance technique à des attaques simulées, l'évaluation de maturité mesure la capacité globale et systémique de l'organisation à gérer ses risques cyber de manière répétable, prévisible et en amélioration continue dans la durée. Les modèles de maturité fournissent un cadre de référence structuré permettant de positionner l'organisation sur une échelle de progression, d'identifier les lacunes prioritaires à combler et de définir une feuille de route stratégique crédible et budgétisable pour atteindre le niveau cible défini par la direction. En 2026, deux modèles dominent le paysage international de la maturité cybersécurité : le **NIST Cybersecurity Framework** version 2.0 publié en février 2024 par le National Institute of Standards and Technology américain, et le *Cybersecurity Maturity Model Certification* (CMMC) développé par le Department of Defense américain pour sécuriser sa chaîne d'approvisionnement industrielle. Leur compréhension approfondie et leur application intelligente permettent aux organisations européennes de structurer leur démarche de progression en cybersécurité tout en répondant aux exigences multiples de conformité qui s'imposent à elles.

Comment fonctionne le NIST CSF version 2.0 ?

Le NIST Cybersecurity Framework version 2.0, publié en février 2024, représente une évolution majeure du cadre de référence le plus utilisé au monde pour la gestion des risques cyber. La version 2.0 introduit une sixième fonction fondamentale, **Govern**, qui s'ajoute aux cinq fonctions historiques (Identify, Protect, Detect, Respond, Recover) pour structurer explicitement la gouvernance de la cybersécurité au niveau stratégique de l'organisation. Cette addition reflète la prise de conscience globale que la cybersécurité est un enjeu de direction générale.

Chaque fonction se décline en catégories puis en sous-catégories qui constituent des résultats attendus mesurables. Le NIST CSF 2.0 propose également des **tiers d'implémentation** (Implementation Tiers) qui caractérisent le degré de rigueur et de sophistication des pratiques de gestion des risques : partiel (Tier 1), informé (Tier 2), reproductible (Tier 3) et adaptatif (Tier 4). Ces tiers ne constituent pas des niveaux de maturité prescriptifs mais des profils descriptifs qui aident l'organisation à évaluer sa posture actuelle et à définir son profil cible en fonction de son contexte de risque et de ses objectifs stratégiques, en lien avec la conformité NIS 2.

Savez-vous réellement à quel tier du NIST CSF se situe votre organisation aujourd'hui, ou reposez-vous sur une auto-évaluation optimiste jamais confrontée à un regard externe ?

Quelles sont les spécificités du modèle CMMC ?

Le *Cybersecurity Maturity Model Certification* (CMMC) version 2.0 a été développé par le Department of Defense américain pour renforcer la protection des informations sensibles dans sa chaîne d'approvisionnement industrielle. Contrairement au NIST CSF qui est un cadre volontaire d'auto-évaluation, le CMMC impose une **certification par un tiers indépendant** accrédité pour accéder aux contrats du DoD, ce qui en fait un standard contraignant avec des conséquences commerciales directes pour les fournisseurs concernés.

Le CMMC 2.0 s'organise en trois niveaux de certification progressifs. Le **niveau 1** (Foundational) couvre 17 pratiques de cyberhygiène de base et repose sur une auto-évaluation annuelle. Le **niveau 2** (Advanced) aligne 110 pratiques sur le standard NIST SP 800-171 et exige une évaluation par un tiers certifié (C3PAO) pour les programmes critiques. Le **niveau 3** (Expert) ajoute des pratiques avancées issues du NIST SP 800-172 et nécessite une évaluation gouvernementale directe. Pour les entreprises européennes fournissant le DoD, la conformité CMMC est devenue une condition sine qua non d'accès au marché américain de la défense.

Mon avis : Le NIST CSF 2.0 est le meilleur cadre de référence disponible pour structurer une démarche de maturité cybersécurité dans les organisations européennes, grâce à sa flexibilité, sa couverture exhaustive et sa compatibilité native avec NIS 2 et ISO 27001. Le CMMC est pertinent uniquement pour les organisations ayant des relations contractuelles avec le DoD américain. Pour les autres, je recommande de se concentrer sur le NIST CSF complété par les exigences spécifiques des réglementations européennes applicables.

Comment réaliser une évaluation de maturité cybersécurité ?

La réalisation d'une évaluation de maturité cybersécurité suit une méthodologie structurée en quatre phases. La **phase de cadrage** définit le périmètre d'évaluation, sélectionne le modèle de référence adapté, identifie les parties prenantes à interviewer et collecte la documentation préliminaire. La **phase de collecte** combine l'analyse documentaire, les entretiens avec les responsables opérationnels et techniques, et des vérifications factuelles ciblées pour évaluer chaque domaine du modèle retenu.

La **phase d'analyse** positionne l'organisation sur l'échelle de maturité pour chaque domaine évalué, identifie les écarts par rapport au profil cible défini et priorise les actions d'amélioration selon une matrice impact-effort. La **phase de restitution** produit un rapport détaillé avec une cartographie visuelle de la maturité par domaine, des recommandations priorisées et une feuille de route pluriannuelle budgétisée. Les résultats doivent être présentés au COMEX en lien avec le volet protection des données et les objectifs stratégiques de l'organisation.

Critère de comparaison	NIST CSF 2.0	CMMC 2.0
Nature du cadre	Volontaire et flexible	Obligatoire pour fournisseurs DoD
Niveaux de maturité	4 tiers d'implémentation	3 niveaux de certification
Nombre de contrôles	6 fonctions, 22 catégories, 106 sous-catégories	17 à 110+ pratiques selon niveau
Évaluation	Auto-évaluation recommandée	Certification par tiers obligatoire (niv.2-3)
Couverture	Tous secteurs, toutes tailles	Chaîne d'approvisionnement défense US
Compatibilité NIS 2	Forte (mapping direct disponible)	Partielle (focus protection CUI)
Coût d'évaluation	Variable (auto-évaluation à externe)	50k à 200k USD pour certification L2

L'attaque Marriott révélée en 2018, qui a exposé les données personnelles de 500 millions de clients suite à une compromission non détectée pendant quatre ans héritée de l'acquisition de Starwood, illustre parfaitement les conséquences d'un déficit de maturité en cybersécurité, particulièrement dans les fonctions Identify et Detect du NIST CSF. Une évaluation de maturité pré-acquisition aurait révélé les lacunes critiques du dispositif de sécurité de Starwood et permis de conditionner la transaction à un plan de remédiation chiffré intégré dans le prix d'achat.

Comment mapper le NIST CSF sur les exigences NIS 2 ?

Le mapping entre le NIST CSF 2.0 et les exigences de la directive NIS 2 est une démarche essentielle pour les organisations européennes souhaitant utiliser le cadre américain comme colonne vertébrale de leur programme de cybersécurité tout en garantissant leur conformité réglementaire européenne. La bonne nouvelle est que la correspondance est naturellement

forte : les six fonctions du NIST CSF couvrent l'essentiel des mesures de gestion des risques exigées par l'article 21 de NIS 2, incluant la gestion des incidents, la continuité d'activité, la sécurité de la supply chain et le chiffrement.

Cependant, NIS 2 impose des obligations spécifiques qui ne trouvent pas de correspondance directe dans le NIST CSF, notamment les obligations de **notification des incidents** aux autorités compétentes dans des délais stricts (alerte précoce sous 24 heures, notification sous 72 heures), les exigences de **formation obligatoire des dirigeants** et les obligations de supervision de la sécurité de la chaîne d'approvisionnement. Ces exigences spécifiquement européennes doivent être ajoutées en complément du cadre NIST pour garantir une couverture exhaustive, en coordination avec le processus de gestion des vulnérabilités et le plan de réponse aux incidents.

Faut-il viser le niveau de maturité le plus élevé ?

La tentation naturelle est de viser le niveau de maturité le plus élevé possible, mais cette approche est rarement pertinente et peut s'avérer contre-productive. Le niveau de maturité cible doit être proportionné au **profil de risque** de l'organisation, à son secteur d'activité, à ses obligations réglementaires et aux ressources disponibles. Une PME industrielle de 200 personnes n'a ni les mêmes besoins ni les mêmes moyens qu'un opérateur d'importance vitale ou une banque systémique.

L'approche recommandée consiste à définir un profil de maturité cible différencié par domaine, en concentrant les efforts sur les domaines les plus critiques pour l'organisation. Par exemple, une organisation fortement exposée aux ransomwares privilégiera les fonctions Protect et Recover, tandis qu'une organisation manipulant des données sensibles investira prioritairement dans les fonctions Identify et Protect. La feuille de route doit prévoir une progression graduelle et réaliste sur trois à cinq ans, avec des paliers intermédiaires mesurables et des quick wins visibles dès la première année pour maintenir la dynamique et le soutien de la direction. Cette approche pragmatique alimente le reporting de la cyberhygiène préconisée par l'ANSSI.

Comment suivre la progression de la maturité dans le temps ?

Le suivi de la progression de la maturité cybersécurité nécessite un dispositif de mesure régulier et objectif. L'évaluation complète doit être reconduite annuellement pour mesurer la progression globale, identifier les nouveaux écarts apparus et ajuster la feuille de route en conséquence. Entre les évaluations annuelles, des indicateurs intermédiaires permettent de suivre la dynamique de progression : taux de mise en œuvre des actions de la feuille de route, évolution des KPIs de sécurité opérationnelle, résultats des audits internes et des tests techniques.

La visualisation de la progression utilise typiquement des **graphiques radar** comparant le profil actuel au profil cible et au profil de l'évaluation précédente pour chaque domaine du modèle. Les résultats doivent être contextualisés par rapport aux benchmarks sectoriels disponibles pour démontrer le positionnement relatif de l'organisation par rapport à ses pairs. Le rapport de

maturité annuel constitue un élément clé du reporting au COMEX et au conseil d'administration, démontrant la progression tangible de l'investissement en cybersécurité et justifiant les budgets futurs auprès de la direction financière, en lien avec l'ENISA.

Sources et références : CNIL · ANSSI

Comment intégrer l'évaluation de maturité dans la stratégie d'entreprise ?

L'évaluation de maturité cybersécurité prend toute sa valeur lorsqu'elle est intégrée dans la stratégie globale de l'entreprise et non traitée comme un exercice technique isolé. Les résultats doivent alimenter le processus de planification stratégique annuel en fournissant au COMEX une vision claire et objectivement mesurée du niveau de protection de l'organisation face aux risques numériques, du positionnement par rapport aux standards sectoriels et des investissements nécessaires pour atteindre le niveau cible validé par la direction dans le contexte de sa tolérance au risque globale.

L'intégration stratégique implique également d'aligner le profil de maturité cible sur les objectifs de développement de l'organisation. Une entreprise en phase d'expansion internationale devra anticiper les exigences de maturité des marchés visés. Une organisation préparant une introduction en bourse devra démontrer un niveau de maturité cohérent avec les attentes des investisseurs institutionnels et des analystes ESG qui intègrent désormais la cybersécurité dans leurs critères d'évaluation. Une société positionnée sur des marchés B2B réglementés devra prouver une maturité alignée sur les exigences de ses clients grands comptes. Cette vision stratégique transforme l'évaluation de maturité d'un diagnostic technique ponctuel en un outil de pilotage stratégique continu au service de la création de valeur et de la compétitivité durable de l'organisation.

À retenir : Le NIST CSF 2.0 est le cadre de maturité le plus universel et flexible pour les organisations européennes, compatible nativement avec NIS 2 et ISO 27001. Le CMMC est pertinent uniquement pour les fournisseurs du DoD américain. Le niveau de maturité cible doit être proportionné aux risques et aux moyens de l'organisation, avec une progression graduelle sur trois à cinq ans. L'évaluation annuelle et le suivi continu des indicateurs de progression sont indispensables pour piloter efficacement la montée en maturité.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr