EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CADRE D'ÉVALUATION DES CAPACITÉS NATIONALES

DÉCEMBRE 2020

À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations, consultez: www.enisa.europa.eu.

CONTACT

Pour contacter les auteurs, veuillez utiliser l'adresse team@enisa.europa.eu.
Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

AUTEURS

Anna Sarri, Pinelopi Kyranoudi – Agence européenne pour la cybersécurité (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique – Wavestone

REMERCIEMENTS

L'ENISA tient à remercier tous les experts qui ont participé et apporté une contribution précieuse à ce rapport, et plus particulièrement les personnes suivantes, par ordre alphabétique:

Bureau central de l'État pour le développement de la société numérique (Croatie), Marin Ante Pivcevic

Centre pour la cybersécurité (Belgique)

CFCS – Center for Cybersikkerhed (Danemark), Thomas Wulff

Centre européen de lutte contre la cybercriminalité – EC3, Alzofra Martinez Alvaro

Centre européen de lutte contre la cybercriminalité – EC3, Adrian-Ionut Bobeica

Ministère fédéral de l'intérieur (Allemagne), Sascha-Alexander Lettgen

Administration de la sécurité de l'information (République de Slovénie), Marjan Kavčič

Gouvernement italien (Italie)

Agence des technologies de l'information de Malte (Malte), Katia Bonello et Martin Camilleri

Ministère de la justice et de la sécurité publique (Norvège), Robin Bakke

Ministère de la politique numérique (Grèce), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali et Sotiris Vasilos

Ministère des affaires économiques et de la communication (Estonie), Anna-Liisa Pärnalaas

Agence nationale de sécurité informatique et cybernétique (République tchèque), Veronika Netolická

Autorité de sécurité nationale (Slovaquie)

Département de sécurité nationale (Espagne), Maria Mar Lopez Gil

NCTV, Ministère de la justice et de la sécurité (Pays-Bas)

Centre national de cybersécurité du Portugal (Portugal), Alexandre Leite et Pedro Matos

Division de la politique de cybersécurité, Département de l'environnement, du climat et des communications (Irlande), James Caffrey

Université d'Oxford – Centre de capacité de la cybersécurité mondiale, Carolin Weisser Harris

L'ENISA souhaite également remercier tous les experts qui ont apporté une précieuse contribution à cette étude, mais qui préfèrent rester anonymes.

AVIS JURIDIQUE

Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA, à moins d'être adoptée en vertu du règlement (UE) nº 2019/881.
Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

DÉCLARATION CONCERNANT LES DROITS D'AUTEUR

© Agence de l'Union européenne pour la cybersécurité (ENISA), 2020
Reproduction autorisée, moyennant mention de la source.

Pour toute utilisation ou reproduction de photos ou d'autres matériels non couverts par le droit d'auteur de l'ENISA, l'autorisation doit être obtenue directement auprès des titulaires du droit d'auteur.

ISBN: 978-92-9204-483-1

DOI: 10.2824/46758

CATALOGUE: TP-02-21-253-FR-N

1. TABLE DES MATIÈRES

GLOSSAIRE

SIGLE OU ACRONYME	DÉFINITION
AELE	Association européenne de libre-échange
ALN	Agents de liaison nationaux
AR	Agence répressive
ARCC	Arrangement de reconnaissance des critères communs
C2M2	Modèle de maturité des capacités en matière de cybersécurité
CEC	Cadre européen des certifications
CMMC	Certification du modèle de maturité de la cybersécurité
CSIRT	Centre de réponse aux incidents de sécurité informatique
DCV	Divulgation coordonnée des vulnérabilités
DPA	Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
ECSO	Organisation européenne pour la cybersécurité
EM	État membre
GECC	Groupe européen de certification de cybersécurité
IA	Intelligence artificielle
ICP	Indice de cyberpuissance
IIC	Infrastructure d'information critique
IMCS	Indice mondial de la cybersécurité
MCAI	Modèle des capacités d'audit interne dans le secteur public
MECS	Mois européen de la cybersécurité
MMC	Modèle de maturité des capacités en matière de cybersécurité pour les nations
MMCSC	Modèle de maturité de la cybersécurité communautaire
MMSI	Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework
MNU	Marché numérique unique
NIST	Institut national des normes et des technologies
OSE	Opérateurs de services essentiels
PME	Petites et moyennes entreprises

PPP	Partenariats public-privé
Q-C2M2	Modèle de maturité des capacités en matière de cybersécurité au Qatar
R&D	Recherche et développement
RGPD	Règlement général sur la protection des données
SGIP	Système de gestion des informations personnelles
SNCS	Stratégies nationales de cybersécurité
SNG	Service numérique du gouvernement
SOG-IS ARM	Comité consultatif pour les actions à mener dans le domaine de la sécurité des systèmes d'information, accord de reconnaissance mutuelle
SRI	Sécurité des réseaux et de l'information
TIC	Technologies de l'information et de la communication
TO	Technologie opérationnelle
TPVP	Technologies de protection de la vie privée
UE	Union européenne
UIT	Union internationale des télécommunications

SYNTHÈSE

Alors que la menace informatique se renforce et que les cyberattaques continuent d'augmenter en intensité et en nombre, les États membres de l'UE doivent réagir efficacement en développant et en adaptant davantage leurs stratégies nationales de cybersécurité (SNCS). Depuis la publication par l'ENISA, en 2012, des premières études liées aux SNCS, les États membres de l'UE et les pays de l'AELE ont réalisé de grands progrès dans la mise au point et la mise en œuvre de leurs stratégies.

Ce rapport présente le travail effectué par l'ENISA pour établir un cadre d'évaluation des capacités nationales (CECN).

Ce cadre vise à fournir aux États membres une autoévaluation de leur niveau de maturité en appréciant les objectifs de leur SNCS. Cette autoévaluation a pour but de les aider à améliorer et renforcer leurs capacités en matière de cybersécurité sur les plans tant stratégique qu'opérationnel.

Il présente une vue simple et représentative du niveau de maturité de l'État membre en matière de cybersécurité. Le CECN est un outil qui aide les États membres:

- en fournissant des informations utiles pour l'élaboration d'une stratégie à long terme (par exemple, bonnes pratiques, lignes directrices);
- en les aidant à identifier les éléments manquants dans leur SNCS;
- en les aidant à renforcer leurs capacités en matière de cybersécurité;
- en étayant le bien-fondé des actions politiques;
- en donnant de la crédibilité vis-à-vis du grand public et des partenaires internationaux;
- en soutenant leur rayonnement et en renforçant leur image publique en tant qu'organisation transparente;
- en contribuant à anticiper les défis de demain;
- en contribuant à identifier les enseignements tirés et les meilleures pratiques;
- en fournissant une base de référence sur les capacités en matière de cybersécurité dans l'UE pour faciliter les discussions; et
- en aidant à évaluer les capacités nationales en matière de cybersécurité.

Ce cadre a été conçu avec le soutien des experts en la matière de l'ENISA ainsi que des représentants de 19 États membres et pays de l'AELE[1]. Le public cible de ce rapport est constitué de décideurs, d'experts, de représentants du gouvernement responsables de ou

[1] Les représentants des États membres et pays de l'AELE suivants ont été interrogés: Allemagne, Belgique, Croatie, Danemark, Espagne, Estonie, Grèce, Hongrie, Irlande, Italie, Lichtenstein, Malte, Norvège, Pays-Bas, Portugal, République tchèque, Slovaquie, Slovénie, Suède.

impliqués dans la conception, la mise en œuvre et l'évaluation de la SNCS et, à plus large échelle, des capacités en matière de cybersécurité.

Le cadre d'évaluation des capacités nationales couvre 17 objectifs stratégiques et s'articule autour de quatre groupes principaux:

- Groupe nº 1: Gouvernance et normes en matière de cybersécurité
  1. Élaborer un plan d'urgence cybernétique national
  2. Établir des mesures de sécurité de base
  3. Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques

- Groupe nº 2: Renforcement des capacités et sensibilisation
  4. Organiser des exercices de cybersécurité
  5. Établir une capacité de réponse aux incidents
  6. Sensibiliser les utilisateurs
  7. Renforcer les programmes de formation et d'enseignement
  8. Encourager la R&D
  9. Inciter le secteur privé à investir dans des mesures de sécurité
  10. Améliorer la cybersécurité de la chaîne d'approvisionnement

- Groupe nº 3: Cadre juridique et réglementaire
  11. Protéger l'infrastructure d'information critique, les OSE et les FSN
  12. Lutter contre la cybercriminalité
  13. Mettre en place des mécanismes de signalement des incidents
  14. Renforcer la protection de la vie privée et des données

- Groupes nº 4: Coopération
  15. Établir un partenariat public-privé
  16. Institutionnaliser la coopération entre les organismes publics
  17. S'engager dans la coopération internationale

1. INTRODUCTION

La directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI), publiée en juillet 2016, exige que les États membres de l'UE adoptent une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, également appelée SNCS (stratégie nationale de cybersécurité), ainsi que le prévoient les articles 1er et 7. Dans ce contexte, une SNCS se définit comme un cadre qui établit des principes stratégiques, des lignes directrices, des objectifs stratégiques, des priorités, des politiques appropriées et des mesures réglementaires. L'objectif prévu d'une SNCS est d'atteindre et de maintenir un niveau élevé de sécurité des réseaux et des systèmes, permettant ainsi aux États membres d'atténuer les menaces éventuelles. De plus, la SNCS peut aussi être un catalyseur de développement industriel et de progrès économique et social.

Conformément au règlement de l'Union européenne sur la cybersécurité, l'ENISA encourage la diffusion des meilleures pratiques dans la définition et la mise en œuvre d'une SNCS en soutenant les États membres dans l'adoption de la directive SRI et en recueillant de précieuses informations sur leurs expériences. À cette fin, l'ENISA a mis au point plusieurs outils destinés à aider les États membres à élaborer, mettre en œuvre et évaluer leurs stratégies nationales de cybersécurité (SNCS).

Dans le cadre de son mandat, l'ENISA vise à développer un cadre d'autoévaluation des capacités nationales afin de mesurer le niveau de maturité des diverses SNCS. L'objectif de ce rapport est de présenter l'étude réalisée pour la définition du cadre d'autoévaluation.

1.1 PORTÉE ET OBJECTIFS DE L'ÉTUDE

Le principal objectif de cette étude est de créer un cadre d'autoévaluation des capacités nationales, abrégé en CECN, pour mesurer le niveau de maturité des capacités de cybersécurité des États membres. Plus spécifiquement, le cadre devrait donner aux États membres les moyens:

- d'évaluer leurs capacités nationales en matière de cybersécurité;
- de mieux cerner le niveau de maturité du pays;
- d'identifier les domaines d'amélioration; et
- de renforcer les capacités en matière de cybersécurité.

Ce cadre devrait aider les États membres, et en particulier les décideurs nationaux, à réaliser un exercice d'autoévaluation dans le but d'améliorer les capacités nationales en matière de cybersécurité.

1.2 APPROCHE MÉTHODOLOGIQUE

L'approche méthodologique utilisée pour concevoir le cadre d'autoévaluation des capacités nationales repose sur quatre grandes étapes:

1. **Des recherches documentaires**: la première étape a consisté à effectuer une analyse bibliographique approfondie pour recueillir les meilleures pratiques concernant l'élaboration d'un cadre d'évaluation de la maturité des stratégies de cybersécurité nationales. La recherche documentaire consiste principalement en une analyse systématique des documents pertinents sur le renforcement des capacités et la définition de la stratégie de cybersécurité, sur les SNCS existantes au sein des États

membres et sur une comparaison des modèles de maturité existants en matière de cybersécurité. Un test de performance a été réalisé sur les modèles de maturité existants par l'adoption d'un cadre d'analyse mis au point aux fins de cette étude. Le cadre d'analyse s'appuie sur la méthodologie de Becker[2] pour le développement de modèles de maturité. Cette méthodologie définit une procédure générique et consolidée pour la conception des modèles de maturité et établit des exigences claires pour leur mise au point. Le cadre d'analyse a été adapté pour répondre aux besoins de cette étude.

2. **La consultation des experts et des parties prenantes**: sur la base des données recueillies lors de la recherche documentaire et des résultats préliminaires de l'analyse, cette étape consistait à identifier des experts ayant de l'expérience dans l'élaboration et la mise en œuvre d'une SNCS ou des modèles de maturité et à les inviter pour un entretien. L'ENISA a contacté son groupe d'experts en stratégies de cybersécurité nationales ainsi que les agents de liaison nationaux (ALN) afin de trouver les experts pertinents dans chaque État membre. En outre, plusieurs experts impliqués dans la mise au point de modèles de maturité ont également été invités pour un entretien. Au total, 22 entretiens ont été menés, dont 19 avec des représentants d'agences en charge de la cybersécurité au sein de divers États membres (et pays de l'AELE).
3. **L'analyse de l'ensemble des données recueillies:** les données recueillies dans le cadre de la recherche documentaire et lors des entretiens ont ensuite été analysées afin d'identifier les meilleures pratiques en vue de l'élaboration d'un cadre d'autoévaluation visant à mesurer la maturité des SNCS, afin de comprendre les besoins des États membres et de déterminer les données qu'il est possible de collecter dans les différents pays européens[3]. Cette analyse a permis de peaufiner le modèle préliminaire mis au point lors des étapes précédentes et d'affiner l'ensemble des indicateurs inclus dans le modèle, les niveaux de maturité et ses dimensions.
4. **La finalisation du modèle:** par la suite, une version actualisée du cadre d'autoévaluation des capacités nationales a été examinée par les experts de l'ENISA, puis validée par des experts à l'occasion d'un atelier organisé en octobre 2020 avant la publication.

1.3 PUBLIC CIBLE

Le public cible de ce rapport est constitué de décideurs, d'experts, de représentants du gouvernement responsables de ou impliqués dans la conception, la mise en œuvre et l'évaluation de la SNCS et, à plus large échelle, des capacités en matière de cybersécurité. En outre, les conclusions formalisées dans ce document peuvent s'avérer utiles pour les experts et les chercheurs en matière de politique de cybersécurité à l'échelle nationale ou européenne.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application,» Business & Information Systems Engineering, vol. 1, nº 3, pp. 213–222, Juin 2009.
[3] Aux fins de cette étude, les «pays européens» auxquels il est fait référence dans ce rapport comprennent les 27 États membres de l'UE.

2. CONTEXTE

2.1 TRAVAUX ANTÉRIEURS SUR LE CYCLE DE VIE DES SNCS

Comme indiqué dans le règlement de l'Union européenne sur la cybersécurité, l'un des principaux objectifs de l'ENISA est de soutenir les États membres dans l'élaboration de stratégies nationales en matière de sécurité des réseaux et des systèmes d'information, de promouvoir la diffusion de ces stratégies et de surveiller leur mise en œuvre. Dans le cadre de son mandat, l'ENISA a produit plusieurs documents sur ce sujet afin d'encourager le partage des bonnes pratiques et de soutenir la mise en œuvre des SNCS dans toute l'UE:

- le «Practical guide on the development and execution phase of NCSS»[4] publié en 2012;
- le document intitulé «Setting the course for national efforts to strengthen security in cyberspace»[5] publié en 2012;
- le premier cadre de l'ENISA pour l'évaluation de la SNCS d'un État membre[6] publié en 2014;
- l'«Online NCSS Interactive Map»[7] publiée en 2014;
- le «NCSS Good Practice Guide»[8] publié en 2016;
- le «National Cybersecurity Strategies Evaluation Tool»[9] publié en 2018;
- les «Good practices in innovation on Cybersecurity under the NCSS»[10] publiées en 2019.

L'ANNEXE A fournit un aperçu des principales publications de l'ENISA sur ce sujet.

Les guides et documents mentionnés ci-dessus ont été étudiés dans le cadre de la recherche documentaire. En particulier, le «National Cybersecurity Strategies Evaluation Tool»[11] est un élément fondamental du CECN. Le CECN s'appuie sur les objectifs couverts dans l'outil d'évaluation en ligne des SNCS.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, actualisée en 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Ce document est une mise à jour du guide de 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 OBJECTIFS COMMUNS IDENTIFIÉS PARMI LES SNCS EUROPÉENNES

La disparité entre les différents États membres rend difficile l'identification d'activités ou de plans d'action communs parmi les divers contextes nationaux, cadres juridiques et agendas politiques. Toutefois, les SNCS des États membres présentent souvent des objectifs stratégiques articulés autour des mêmes thèmes. Ainsi, sur la base des travaux antérieurs de l'ENISA et de l'analyse des SNCS des États membres, 22 objectifs stratégiques ont été identifiés. Quinze de ces objectifs stratégiques avaient déjà été identifiés lors des travaux antérieurs de l'ENISA, deux objectifs ont été ajoutés dans cette étude et cinq objectifs ont été identifiés pour être examinés plus en détail par la suite.

2.2.1 Objectifs stratégiques communs couverts par les États membres

Sur la base des travaux précédents de l'ENISA, et tout particulièrement du National Cybersecurity Strategies Evaluation Tool[12], le tableau suivant montre l'ensemble des 15 objectifs stratégiques mentionnés ci-dessus qui sont communément couverts dans les SNCS des États membres. Les finalités décrivent le cœur de la «philosophie nationale» globale par rapport à l'objectif en question. Pour plus d'informations sur les objectifs décrits ci-dessous, veuillez vous référer au rapport de l'ENISA «NCSS Good Practice Guide»[13].

Tableau 1: Objectifs stratégiques communs couverts par les États membres dans leur SNCS

ID	Objectifs stratégiques de la SNCS	Finalités
1	**Élaborer des plans d'urgence cybernétique nationaux**	▶ Présenter et expliquer les critères à utiliser pour définir une situation comme étant une crise; ▶ Définir les processus et actions clés pour la gestion de la crise; ▶ Définir clairement les rôles et responsabilités des diverses parties prenantes lors d'une cybercrise; et ▶ Présenter et expliquer les critères de sortie de crise et/ou déterminer qui est habilité à déclarer que la crise est terminée.
2	**Établir des mesures de sécurité de base**	▶ Harmoniser les différentes pratiques suivies par les organisations dans les secteurs public et privé; ▶ Créer un langage commun aux autorités publiques compétentes et aux organisations et ouvrir des canaux de communication sécurisés; ▶ Permettre aux diverses parties prenantes de vérifier et de comparer leurs capacités en termes de cybersécurité; ▶ Partager des informations sur les bonnes pratiques en matière de cybersécurité dans chaque secteur d'activité; et ▶ Aider les parties prenantes à hiérarchiser leurs investissements dans le domaine de la sécurité.
3	**Organiser des exercices de cybersécurité**	▶ Identifier ce qui doit être testé (plans et processus, personnes, infrastructures, capacités de réponse, capacités de coopération, communication, etc.); ▶ Mettre sur pied une équipe nationale de planification des cyberexercices, avec un mandat clair; et ▶ Intégrer les cyberexercices dans le cycle de vie de la stratégie nationale de cybersécurité ou du plan d'urgence cybernétique national.
4	**Établir une capacité de réponse aux incidents**	▶ Mandat – il s'agit des pouvoirs, rôles et responsabilités qui doivent être attribués à l'équipe par le gouvernement concerné;

[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Ce document est une mise à jour du guide de 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	Objectifs stratégiques de la SNCS	Finalités
		▶ Portefeuille de services – il s'agit des services qu'une équipe fournit à son public cible ou qu'elle utilise pour son propre fonctionnement interne; ▶ Capacités opérationnelles – il s'agit des exigences techniques et opérationnelles auxquelles une équipe doit se conformer; et ▶ Capacités de coopération – il s'agit des exigences relatives au partage d'information avec des équipes non couvertes par les trois catégories précédentes, par exemple, les décideurs, l'armée, les organismes de contrôle, les opérateurs (d'infrastructure d'information critique), les autorités répressives.
5	**Sensibiliser les utilisateurs**	▶ Identifier les lacunes dans les connaissances en matière de cybersécurité ou les problèmes relatifs à la sécurité de l'information; et ▶ Combler les lacunes par la sensibilisation ou l'acquisition/le renforcement des bases de connaissances.
6	**Renforcer les programmes de formation et d'enseignement**	▶ Augmenter les capacités opérationnelles des professionnels de la sécurité de l'information en place; ▶ Encourager les étudiants à s'intéresser à la thématique et les préparer à entrer dans le domaine de la cybersécurité; ▶ Promouvoir et encourager les relations entre le secteur de la sécurité de l'information et les milieux universitaires correspondants; et ▶ Faire correspondre la formation en cybersécurité aux besoins des entreprises.
7	**Encourager la R&D**	▶ Identifier les véritables causes des vulnérabilités au lieu de réparer les conséquences; ▶ Réunir des experts de diverses disciplines afin d'apporter des solutions aux problèmes multidimensionnels et complexes tels que les cybermenaces physiques; ▶ Jeter des ponts entre les besoins de l'industrie et les résultats de la recherche, facilitant ainsi le passage de la théorie à la pratique; et ▶ Trouver des moyens non seulement de maintenir mais aussi d'accroître le niveau de cybersécurité des produits et services qui soutiennent les cyberinfrastructures existantes.
8	**Inciter le secteur privé à investir dans des mesures de sécurité**	▶ Identifier les incitations possibles pour les entreprises privées à investir dans des mesures de sécurité; et ▶ Fournir aux entreprises des incitations pour encourager les investissements dans la sécurité.
9	**Protéger l'infrastructure d'information critique (IIC), les OSE et les FSN**	▶ Identifier l'infrastructure d'information critique; et ▶ Identifier et atténuer les risques pertinents relatifs à l'IIC.
10	**Lutter contre la cybercriminalité**	▶ Établir des lois dans le domaine de la cybercriminalité; et ▶ Accroître l'efficacité des agences répressives.
11	**Mettre en place des mécanismes de signalement des incidents**	▶ Apprendre à mieux connaître l'environnement global de la menace; ▶ Évaluer l'impact des incidents (par exemple, atteintes à la sécurité, défaillances du réseau, interruptions du service); ▶ Acquérir des connaissances au sujet des vulnérabilités et types d'attaques nouveaux et existants; ▶ Mettre à jour les mesures de sécurité en conséquence; et ▶ Mettre en œuvre les dispositions de la directive SRI en matière de signalement des incidents.
12	**Renforcer la protection de la vie privée et des données**	▶ Contribuer au renforcement des droits fondamentaux en matière de vie privée et de protection des données.
13	**Établir un partenariat public-privé (PPP)**	▶ Dissuader (dissuader les malfaiteurs); ▶ Protéger (sur la base de la recherche sur les nouvelles menaces à l'encontre de la sécurité); ▶ Détecter (utiliser le partage d'information pour faire face aux nouvelles menaces); ▶ Réagir (assurer la capacité à gérer l'impact initial d'un incident); et ▶ Récupérer (assurer la capacité à résoudre l'impact final d'un incident).

ID	Objectifs stratégiques de la SNCS	Finalités
14	Institutionnaliser la coopération entre les organismes publics	▶ Accroître la coopération entre les organismes publics ayant des responsabilités et des compétences liées à la cybersécurité; ▶ Éviter le chevauchement des compétences et des ressources entre les organismes publics; et ▶ Améliorer et institutionnaliser la coopération entre les organismes publics dans les différents domaines de la cybersécurité.
15	S'engager dans la coopération internationale (pas seulement avec les États membres de l'UE)	▶ Bénéficier de la création d'une base de connaissances commune aux États membres de l'UE; ▶ Créer des effets de synergie entre les autorités de cybersécurité nationales; et ▶ Permettre et intensifier la lutte contre la criminalité transnationale.

2.2.2 Objectifs stratégiques supplémentaires

Sur la base de la recherche documentaire effectuée et des entretiens menés par l'ENISA, des objectifs stratégiques supplémentaires ont été identifiés. Ces sujets se font toujours plus présents dans la SNCS et les plans d'action des États membres. Des exemples d'activités mises en œuvre par les États membres sont également fournis. Lorsqu'un exemple provient d'une source accessible au public, une référence est indiquée. Lorsque les exemples sont basés sur des entretiens confidentiels avec des fonctionnaires des États membres de l'UE, aucune référence n'est communiquée.

Les objectifs stratégiques supplémentaires suivants ont été identifiés:

- Améliorer la cybersécurité de la chaîne d'approvisionnement; et
- Sécuriser l'identité électronique et instaurer la confiance dans les services publics numériques.

Améliorer la cybersécurité de la chaîne d'approvisionnement

Les petites et moyennes entreprises (PME) sont les piliers de l'économie européenne. Elles représentent 99 % de toutes les entreprises de l'Union européenne[14] et, en 2015, on estimait qu'elles étaient à l'origine d'environ 85 % de la création d'emplois et de deux tiers de l'emploi total au sein du secteur privé de l'UE. Dans la mesure où les PME fournissent des services aux grandes entreprises et travaillent de plus en plus avec les administrations publiques[15], il faut noter que, dans le contexte interconnecté actuel, elles constituent le maillon faible en ce qui concerne les cyberattaques. En effet, ce sont les PME qui sont les plus exposées à ces attaques informatiques. Or, souvent, elles ne peuvent pas se permettre d'investir suffisamment dans la cybersécurité[16]. L'amélioration de la cybersécurité de la chaîne d'approvisionnement devra donc mettre l'accent sur les PME.

En plus de cette approche systémique, les États membres peuvent également mettre l'accent sur leurs efforts en matière de cybersécurité de services et produits TIC spécifiques considérés comme essentiels: les technologies TIC utilisées dans l'infrastructure d'information critique, les mécanismes de sécurité appliqués dans le secteur des télécommunications (contrôles au niveau des FAI, etc.), les services de confiance tels que définis dans le règlement eIDAS, et les fournisseurs de services en nuage. Par exemple, dans sa stratégie nationale de cybersécurité pour 2019-2024[17], la Pologne s'est engagée à mettre au point un système national d'évaluation

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

et de certification de la cybersécurité en tant que mécanisme d'assurance de la qualité dans la chaîne d'approvisionnement. Ce système de certification sera aligné sur le cadre de certification de l'UE pour les produits, services et processus numériques des TIC établi par le règlement de l'Union européenne sur la cybersécurité (2019/881).

L'amélioration de la cybersécurité de la chaîne d'approvisionnement revêt donc une importance capitale. Cette amélioration peut être obtenue en établissant des politiques fortes pour promouvoir les PME, en fournissant des lignes directrices pour les exigences de cybersécurité dans les procédures de passation de marchés des administrations publiques, en encourageant la coopération au sein du secteur privé, en construisant des PPP, en faisant la promotion de mécanismes de divulgation coordonnée des vulnérabilités (DCV)[18], en construisant un système de certification des produits, en incluant des éléments de cybersécurité dans les initiatives numériques pour les PME, et en finançant le renforcement des compétences, entre autres.

Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques

En février 2020, la Commission a exposé sa vision de la transformation numérique de l'UE dans la communication «Façonner l'avenir numérique de l'Europe»[19]. Pour la Commission, cette transformation doit fournir des technologies inclusives qui sont au service des personnes et qui respectent les valeurs fondamentales de l'UE. En particulier, la communication indique que la promotion de la transformation numérique des administrations publiques dans toute l'Europe est cruciale. À cet égard, il est primordial de renforcer la confiance dans le gouvernement en ce qui concerne l'identité numérique, de même que la confiance dans les services publics. C'est d'autant plus important que les transactions et les échanges de données du secteur public sont souvent de nature sensible.

De nombreux pays ont exprimé leur intention d'aborder ce sujet dans leur SNCS. C'est notamment le cas des pays suivants: Danemark, Espagne, Estonie, France, Luxembourg, Malte, Pays-Bas et Royaume-Uni. Parmi ces pays, certains ont également affirmé que cet objectif stratégique pourrait être abordé dans le cadre d'un plan plus large:

- L'Estonie associe son plan d'action sur la sécurité de l'identité électronique et la capacité d'authentification électronique à l'initiative plus large de l'Agenda numérique 2020 pour l'Estonie.
- La SNCS française indique que le secrétaire d'État chargé des technologies numériques supervise l'établissement d'une feuille de route visant à «protéger la vie numérique, la vie privée et les données personnelles des Français».
- La SNCS néerlandaise stipule que la cybersécurité dans les administrations publiques, ainsi que les services publics fournis aux citoyens et aux entreprises sont abordés plus en détail dans l'Agenda général pour un gouvernement numérique.
- Alors que le gouvernement britannique continue à proposer de plus en plus de services en ligne, il a chargé le Service numérique du gouvernement (SNG) de s'assurer que tous les nouveaux services numériques mis au point ou achetés par le gouvernement sont également «sécurisés par défaut», avec le soutien du Centre national de cybersécurité britannique (NCSC).

[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Façonner l'avenir numérique de l'Europe, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_fr.pdf

2.2.3 Autres objectifs stratégiques envisagés

Lors de la phase de recherche documentaire et dans le cadre des entretiens menés par l'ENISA, d'autres objectifs stratégiques ont été étudiés. Cependant, il a été décidé que ces objectifs ne feraient pas partie du cadre d'autoévaluation. L'ANNEXE C – Autres objectifs étudiés

fournit des définitions pour chacun de ces objectifs pouvant être utilisées pour alimenter de futures discussions sur les améliorations possibles des SNCS.

Les objectifs stratégiques suivants ont été étudiés en tant que considérations futures:

- Développer des stratégies de cybersécurité sectorielles spécifiques;
- Lutter contre les campagnes de désinformation;
- Sécuriser les technologies de pointe (5G, IA, informatique quantique, etc.);
- Assurer la souveraineté des données; et
- Fournir des incitations pour le développement du secteur de la cyberassurance.

2.3 PRINCIPAUX ENSEIGNEMENTS TIRÉS DU TEST DE PERFORMANCE

La recherche documentaire sur les modèles de maturité existants en matière de cybersécurité a été menée dans le but de recueillir des informations et des preuves pour soutenir l'élaboration du cadre d'autoévaluation des capacités nationales relatif aux SNCS. Dans ce contexte, une analyse bibliographique approfondie des modèles existants a été réalisée pour compléter les résultats de la recherche initiale sur la portée des modèles de maturité de la cybersécurité et des SNCS existants, abordés aux sections 2.1 et 2.2. Cet examen systématique sous-tend la sélection et la justification des niveaux de maturité du cadre d'évaluation, ainsi que la définition des différents indicateurs et dimensions.

Dans le cadre de l'examen systématique des modèles de maturité, dix modèles ont été retenus et analysés sur la base de leurs caractéristiques clés. La vue d'ensemble des caractéristiques clés de chaque modèle analysé dans le cadre de cette étude est disponible dans le Tableau 2: Vue d'ensemble des modèles **de maturité analysés**. Une analyse plus détaillée est en outre fournie à l'ANNEXE A.

Tableau 2: Vue d'ensemble des modèles de maturité analysés

Nom du modèle	Nbre de niveaux de maturité	Nbre d'attributs	Méthode d'évaluation	Représentation des résultats
Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC)	5	5 dimensions principales	Collaboration avec une organisation locale pour peaufiner le modèle avant de l'appliquer au contexte national	Radar à 5 sections
Modèle de maturité des capacités en matière de cybersécurité (C2M2)	4	10 domaines clés	Méthodologie et outils d'autoévaluation	Tableau de bord avec graphiques circulaires
Cadre pour l'amélioration de la cybersécurité des infrastructures critiques	s.o. (4 ranches)	5 fonctions principales	Autoévaluation	s.o.
Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2)	5	5 domaines clés	s.o.	s.o.

Certification du modèle de maturité de la cybersécurité (CMMC)	5	17 domaines clés	Évaluation par des auditeurs tiers	s.o.
Modèle de maturité de la cybersécurité communautaire (MMCSC)	5	6 dimensions principales	Évaluation au sein des communautés avec une contribution de l'État et des agences répressives fédérales	s.o.
Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework (MMSI)	5	23 domaines évalués	s.o.	s.o.
Modèle des capacités d'audit interne (MCAI) dans le secteur public	5	6 éléments	Autoévaluation	s.o.
Indice mondial de la cybersécurité (IMCS)	s.o.	5 piliers	Autoévaluation	Tableau de classement
L'Indice de cyberpuissance (ICP)	s.o.	4 catégories	Évaluation comparative par l'Economist Intelligence Unit	Tableau de classement

Cet examen systématique a permis de tirer des conclusions sur les meilleures pratiques adoptées dans les modèles existants afin d'alimenter l'élaboration du modèle conceptuel du modèle de maturité actuel. En particulier, le test de performance a contribué à la définition des niveaux de maturité, à la création de groupes de dimensions et à la sélection d'indicateurs, ainsi qu'à la mise en place d'une méthodologie de visualisation appropriée pour les résultats du modèle. Les résultats les plus pertinents pour chacun de ces éléments sont détaillés dans le Tableau 3.

Tableau 3: Principaux enseignements tirés du test de performance

Caractéristique	Principaux enseignements
Niveaux de maturité	▶ Une échelle de maturité à cinq niveaux pour les cadres d'évaluation des capacités en matière de cybersécurité est communément acceptée et permet de fournir des résultats d'évaluation avec une bonne granularité (cf. Tableau 6 Comparaison des niveaux de **maturité** pour la définition détaillée des niveaux de maturité de chaque modèle); ▶ Tous les modèles fournissent une définition de haut niveau de chaque niveau de maturité, qui est ensuite adaptée aux différentes dimensions ou aux groupes de dimensions; ▶ Deux aspects principaux sont généralement évalués lors de la mesure de la maturité des capacités en matière de cybersécurité: la maturité des stratégies et la maturité des processus mis en place pour mettre en œuvre les stratégies.
Attributs	▶ L'analyse comparative des attributs des modèles de maturité existants montre des résultats hétérogènes avec un nombre moyen d'attributs par modèle variant entre quatre et cinq; ▶ Un modèle qui repose sur environ quatre ou cinq attributs fournit aux pays le bon degré de granularité des données en regroupant les dimensions pertinentes et en assurant la lisibilité des résultats (cf. Tableau 7: Comparaison des attributs/dimensions pour une description des attributs de chaque modèle); ▶ Le principe clé adopté par tous les modèles lors de la définition des groupes est basé sur la cohérence des éléments rassemblés au sein de chaque groupe.
Méthode d'évaluation	▶ Les méthodes d'évaluation utilisées varient dans les différents modèles analysés; ▶ La méthode d'évaluation la plus courante est basée sur l'autoévaluation.
Représentation des résultats	▶ Il est important de présenter les résultats avec différents niveaux de granularité; ▶ La méthodologie de visualisation doit être explicite et facile à lire.

Le modèle conceptuel a été construit sur la base du test de performance appliqué aux différents modèles de maturité et sur la base des travaux antérieurs de l'ENISA. En outre, il a été décidé de s'appuyer sur l'*outil interactif en ligne de l'ENISA* pour concevoir des indicateurs de maturité pour chaque attribut.

2.4 PROBLÉMATIQUES DE L'ÉVALUATION DES SNCS

Les États membres sont confrontés à de nombreuses problématiques dans le cadre du renforcement de leurs capacités en matière de cybersécurité et, plus particulièrement, lorsqu'ils tentent de s'assurer que leurs capacités correspondent bien aux derniers développements. Vous trouverez ci-dessous un résumé des problématiques identifiées par les États membres et examinées avec ceux-ci dans le cadre de cette étude:

- **Difficultés de coordination et de coopération:** coordonner les efforts de cybersécurité à l'échelle nationale afin d'avoir une réponse efficace aux problèmes de cybersécurité peut être problématique en raison du grand nombre de parties prenantes impliquées.
- **Manque de ressources pour mener à bien l'évaluation:** selon le contexte local et la structure de gouvernance nationale en matière de cybersécurité, l'évaluation de la SNCS et de ses objectifs peut prendre jusqu'à plus de 15 jours-personnes.
- **Manque de soutien en faveur du renforcement des capacités de cybersécurité:** certains États membres ont indiqué que, pour défendre un budget et obtenir un soutien en vue de renforcer les capacités de cybersécurité, ils doivent d'abord passer par une phase d'évaluation pour identifier les lacunes et les limitations.

- **Difficultés à attribuer les réussites ou les changements à la stratégie:** dans la mesure où les menaces évoluent chaque jour et où la technologie s'améliore, les plans d'action doivent constamment être adaptés en conséquence. Cependant, évaluer une SNCS et confirmer que les changements sont bel et bien le résultat de la stratégie reste une tâche ardue, ce qui rend difficile l'identification des limitations et des lacunes de la SNCS.
- **Difficultés à mesurer l'efficacité de la SNCS:** des indicateurs peuvent être collectés pour mesurer différents domaines, tels que les progrès, la mise en œuvre, la maturité et l'efficacité. Bien qu'il soit relativement facile de mesurer les progrès et la mise en œuvre plutôt que de mesurer l'efficacité, ce dernier paramètre reste plus significatif pour l'évaluation des résultats et des impacts d'une SNCS. Sur la base des entretiens menés par l'ENISA, un grand nombre d'États membres ont déclaré qu'il est important de mesurer quantitativement l'efficacité d'une SNCS, mais qu'il s'agit aussi d'une tâche très exigeante pouvant même s'avérer impossible dans certains cas.
- **Difficulté à adopter un cadre commun:** les États membres de l'UE opèrent dans des contextes différents en termes de politique, d'organisations, de culture, de structure de la société et de maturité de la SNCS. Certains États membres interrogés dans le cadre de cette étude ont indiqué qu'il pourrait s'avérer difficile de défendre et d'utiliser un cadre d'autoévaluation «universel».

2.5 AVANTAGES D'UNE ÉVALUATION DES CAPACITÉS NATIONALES

Depuis 2017, tous les États membres de l'UE disposent d'une SNCS[20]. Bien qu'il s'agisse d'une évolution positive, il est aussi important que les États membres soient en mesure d'évaluer correctement ces SNCS, apportant ainsi une valeur ajoutée à leur planification stratégique et à leur mise en œuvre.

L'un des objectifs du cadre d'évaluation des capacités nationales est d'évaluer les capacités de cybersécurité en fonction des priorités définies dans les différentes SNCS. Fondamentalement, le cadre mesure le niveau de maturité des capacités de cybersécurité des États membres dans les domaines définis par les objectifs de la SNCS. Ainsi, les résultats du cadre aident les décideurs des États membres à définir la stratégie nationale en matière de cybersécurité en leur fournissant des renseignements sur la situation dans leur pays[21]. Le CECN a pour but ultime d'aider les États membres à identifier les domaines d'amélioration et à renforcer leurs capacités.

Le cadre vise à fournir aux États membres une autoévaluation de leur niveau de maturité en évaluant les objectifs de leur SNCS. Cette autoévaluation a pour but de les aider à améliorer et renforcer leurs capacités en matière de cybersécurité sur les plans tant stratégique qu'opérationnel.

D'un point de vue plus pratique, basé sur les entretiens menés par l'ENISA avec plusieurs agences responsables du domaine de la cybersécurité dans différents États membres, les avantages suivants du cadre d'évaluation des capacités nationales ont été identifiés et soulignés:

- Fournir des informations utiles pour l'élaboration d'une stratégie à long terme (par exemple, bonnes pratiques, lignes directrices);
- Aider à identifier les éléments manquants dans leur SNCS;
- Aider à renforcer leurs capacités en matière de cybersécurité;

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

- Étayer le bien-fondé des actions politiques;
- Donner de la crédibilité vis-à-vis du grand public et des partenaires internationaux;
- Soutenir leur rayonnement et renforcer leur image publique en tant qu'organisation transparente;
- Aider à anticiper les défis de demain;
- Aider à identifier les enseignements tirés et les meilleures pratiques;
- Fournir une base de référence sur les capacités en matière de cybersécurité dans l'UE pour faciliter les discussions; et
- Aider à évaluer les capacités nationales en matière de cybersécurité.

3. MÉTHODOLOGIE DU CADRE D'ÉVALUATION DES CAPACITÉS NATIONALES

3.1 OBJECTIF GÉNÉRAL

L'**objectif principal** du CECN est de mesurer le niveau de maturité des capacités de cybersécurité des **États membres** afin de les aider à mener une évaluation de leurs capacités nationales en matière de cybersécurité, à mieux connaître le niveau de maturité du pays, à identifier les domaines d'amélioration et à renforcer les capacités de cybersécurité.

3.2 NIVEAUX DE MATURITÉ

Le cadre est basé sur **cinq niveaux de maturité** définissant les étapes par lesquelles les États membres passent pour mettre en place des capacités de cybersécurité dans le domaine couvert par chaque objectif de la SNCS. Les niveaux de maturité vont croissant. Tout en bas de l'échelle, on trouve le **niveau 1**, dans lequel les États membres n'ont pas d'approche clairement définie pour le renforcement des capacités en matière de cybersécurité dans les domaines couverts par les objectifs de la SNCS. L'échelle se termine au **niveau 5**, dans lequel la stratégie de renforcement des capacités en matière de cybersécurité est dynamique et adaptable aux évolutions de l'environnement. Le Tableau 4 montre l'échelle des niveaux de maturité avec une description de chaque niveau.

Tableau 4: L'échelle de maturité à cinq niveaux du cadre d'évaluation des capacités nationales de l'ENISA

NIVEAU 1 – INITIAL/ACTIONS PONCTUELLES	NIVEAU 2 – DÉBUT DE DÉFINITION	NIVEAU 3 – MISE EN ŒUVRE	NIVEAU 4 – OPTIMISATION	NIVEAU 5 – ADAPTABILITÉ
L'État membre n'a pas d'approche clairement définie pour le renforcement des capacités en matière de cybersécurité dans les domaines couverts par les objectifs de la SNCS. Néanmoins, le pays peut avoir mis en place certains objectifs génériques et avoir réalisé certaines études (techniques, politiques, stratégiques) pour améliorer les capacités nationales.	L'approche nationale en faveur du renforcement des capacités dans le domaine couvert par les objectifs de la SNCS a été définie. Les plans d'action ou les activités visant à atteindre les résultats sont en place mais n'en sont qu'à leurs débuts. De plus, des parties prenantes actives peuvent avoir été identifiées et/ou engagées.	Le plan d'action pour le renforcement des capacités dans le domaine couvert par les objectifs de la SNCS est clairement défini et soutenu par les parties prenantes correspondantes. Les pratiques et les activités sont appliquées et mises en œuvre de manière uniforme à l'échelle nationale. Les activités sont définies et documentées avec une allocation des ressources et une gouvernance claires, ainsi qu'un ensemble d'échéances.	Le plan d'action est évalué régulièrement: des priorités y sont établies, il est optimisé et durable. La performance des activités de renforcement des capacités en matière de cybersécurité est régulièrement mesurée. Les facteurs de réussite, les défis et les lacunes dans la mise en œuvre des activités sont identifiés.	La stratégie de renforcement des capacités en matière de cybersécurité est dynamique et adaptative. L'attention constante portée aux évolutions de l'environnement (progrès technologiques, conflits mondiaux, nouvelles menaces, etc.) favorise une capacité de décision rapide et une aptitude à agir vite pour obtenir des améliorations.

3.3 GROUPES ET STRUCTURE GLOBALE DU CADRE D'AUTOÉVALUATION

Le cadre d'autoévaluation se caractérise par **quatre groupes**: (I) Gouvernance et normes en matière de cybersécurité, (II) Renforcement des capacités et sensibilisation, (III) Législation et réglementation et (IV) Coopération. Chacun de ces groupes couvre un domaine thématique clé pour le renforcement des capacités de cybersécurité dans un pays et contient un ensemble d'objectifs que les États membres pourraient inclure dans leur SNCS. En particulier:

- **(I) Gouvernance et normes en matière de cybersécurité**: ce groupe mesure la capacité des États membres à établir une gouvernance, des normes et des bonnes pratiques adéquates dans le domaine de la cybersécurité. Cette dimension prend en compte différents aspects de la cyberdéfense et de la résilience tout en soutenant le développement de l'industrie nationale de la cybersécurité et en renforçant la confiance dans les gouvernements;
- **(II) Renforcement des capacités et sensibilisation**: ce groupe évalue la capacité des États membres à sensibiliser aux risques et aux menaces en matière de cybersécurité et à la manière de les combattre. En outre, cette dimension évalue la capacité du pays à renforcer continuellement ses capacités en matière de cybersécurité et à accroître le niveau général des connaissances et des compétences dans ce domaine. Ce groupe aborde le développement du marché de la cybersécurité et les progrès de la R&D en matière de cybersécurité. Il rassemble tous les objectifs qui préparent le terrain pour le renforcement des capacités à venir;
- **(III) Législation et réglementation**: ce groupe mesure la capacité des États membres à mettre en place les instruments juridiques et réglementaires nécessaires pour lutter contre la montée de la cybercriminalité et des cyberincidents correspondants, et pour protéger l'infrastructure d'information critique. De plus, cette dimension évalue aussi la

capacité des États membres à créer un cadre juridique pour protéger les citoyens et les entreprises, comme lorsqu'il est question de l'équilibre entre sécurité et vie privée; et

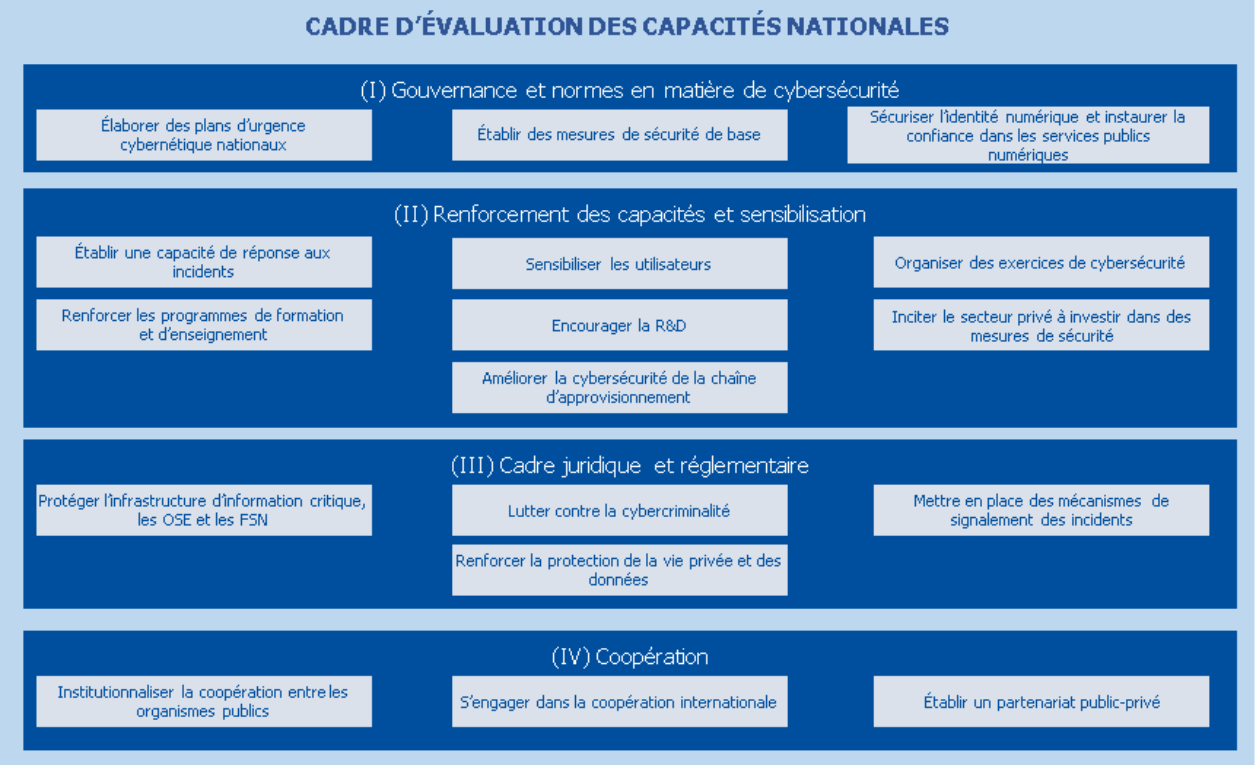
- **(IV) Coopération**: ce groupe évalue la coopération et le partage d'information entre les différents groupes de parties prenantes à l'échelle nationale et internationale, en tant qu'outil essentiel pour mieux comprendre et répondre à un environnement de menaces en constante évolution.

Les objectifs qui ont été inclus dans le modèle sont ceux qui sont communément adoptés par les États membres, et ils ont été sélectionnés parmi les objectifs énumérés à la section 2.2. Le modèle évalue en particulier les objectifs suivants:

- 1. Élaborer des plans d'urgence cybernétique nationaux (I)
- 2. Établir des mesures de sécurité de base (I)
- 3. Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques (I)
- 4. Établir une capacité de réponse aux incidents (II)
- 5. Sensibiliser les utilisateurs (II)
- 6. Organiser des exercices de cybersécurité (II)
- 7. Renforcer les programmes de formation et d'enseignement (II)
- 8. Encourager la R&D (II)
- 9. Inciter le secteur privé à investir dans des mesures de sécurité (II)
- 10. Améliorer la cybersécurité de la chaîne d'approvisionnement (II)
- 11. Protéger l'infrastructure d'information critique, les OSE et les FSN (III)
- 12. Lutter contre la cybercriminalité (III)
- 13. Mettre en place des mécanismes de signalement des incidents (III)
- 14. Renforcer la protection de la vie privée et des données (III)
- 15. Institutionnaliser la coopération entre les organismes publics (IV)
- 16. S'engager dans la coopération internationale (IV)
- 17. Établir un partenariat public-privé (IV)

Les quatre groupes et les objectifs sous-jacents sont combinés dans le modèle pour obtenir une vue globale de la maturité des capacités de cybersécurité des États membres. La Figure 1 présente la structure globale du cadre d'autoévaluation et montre comment ces éléments, à savoir les objectifs, les groupes et le cadre d'autoévaluation, sont liés à l'évaluation de la performance d'un pays.

Figure 1: Structure du cadre d'autoévaluation



Pour chaque objectif inclus dans le cadre d'autoévaluation, il existe une série d'indicateurs répartis entre les cinq niveaux de maturité. Chaque indicateur est basé sur une question dichotomique (oui/non). L'indicateur peut être un élément nécessaire ou accessoire.

3.4 MÉCANISME DES SCORES

Le **mécanisme des scores** du cadre d'autoévaluation prend en considération les éléments mentionnés ci-dessus et les principes énumérés à la section 3.5. En fait, le modèle fournit un score basé sur la valeur de deux paramètres, le **niveau de maturité** et le **taux de couverture**. Chacun de ces paramètres peut être calculé à différents niveaux: (i) par objectif, (ii) par groupe d'objectifs ou (iii) globalement.

Scores par objectif

Le **score de niveau de maturité** donne un aperçu du niveau de maturité en montrant quelles capacités et pratiques ont été mises en place. Le score de niveau de maturité est calculé comme le niveau le plus élevé pour lequel le répondant satisfait à toutes les exigences (c'est-à-dire pour lequel il a répondu OUI à toutes les questions portant sur des éléments nécessaires), en plus d'avoir rempli toutes les exigences des niveaux de maturité précédents.

Le **taux de couverture** montre l'étendue de la couverture de tous les indicateurs pour lesquels la réponse est positive, quel que soit leur niveau. C'est une valeur complémentaire qui prend en compte l'ensemble des indicateurs mesurant un objectif. Le taux de couverture est calculé comme la proportion entre le nombre total de questions dans l'objectif et le nombre de questions pour lesquelles la réponse est positive.

Il est important de préciser que, dans le reste du document, le mot ***score*** est utilisé pour désigner à la fois les valeurs du niveau de maturité et celles du taux de couverture.

La Figure 2 – Mécanisme des scores par objectif fournit une visualisation du mécanisme d'évaluation qui est décrit à la section 3.1 et qui sera abordé plus en détail ci-dessous.

Figure 2: Mécanisme des scores par objectif

La *Figure 2 montre un exemple de calcul du niveau de maturité par objectif. Il est à noter que le répondant remplissait toutes les exigences des trois premiers niveaux de maturité et ne remplissait que partiellement celles du niveau 4. Dès lors, le score indique que le* ***niveau de maturité du répondant est niveau 3 pour l'objectif «Organiser des exercices de cybersécurité»****.*

Cependant, dans l'exemple présenté dans la Figure 2, le niveau de maturité de l'objectif ne tient pas compte des informations fournies par les indicateurs dont le score est positif et qui sont supérieurs au niveau 3 de maturité. Dans ce cas, le taux de couverture peut fournir une vue d'ensemble de tous les éléments mis en œuvre par le répondant pour atteindre cet objectif, quel que soit son niveau de maturité réel. Dans l'exemple, la proportion entre le nombre total de questions dans l'objectif et le nombre de questions pour lesquelles la réponse est positive est égale à 19/27, ce qui signifie que ***le taux de couverture est de 70 %****.*

De plus, pour s'adapter aux spécificités des États membres tout en permettant une vue d'ensemble cohérente, le score est calculé à partir de deux échantillons différents au niveau des groupes et au niveau global:

- **Scores généraux**: un échantillon complet couvrant tous les objectifs inclus dans le groupe ou dans le cadre général (de 1 à 17);
- **Scores spécifiques**: un échantillon spécifique couvrant uniquement les objectifs sélectionnés par l'État membre (correspondant généralement aux objectifs présents dans la SNCS du pays concerné) au sein du groupe ou du cadre général.

Scores par groupe

Le **niveau de maturité général de chaque groupe** est calculé comme la moyenne arithmétique du niveau de maturité de tous les objectifs de ce groupe.

Le **niveau de maturité spécifique de chaque groupe** est calculé comme la moyenne arithmétique du niveau de maturité des objectifs au sein de ce groupe que l'État membre a choisi d'évaluer (il s'agit généralement des objectifs présents dans la SNCS du pays en question).

Par exemple, la Figure 1 montre que le groupe (I) Gouvernance et normes en matière de cybersécurité se compose de trois objectifs. En supposant que le répondant a choisi d'évaluer seulement les deux premiers objectifs, mais pas le troisième, et en supposant que les deux premiers objectifs présentent respectivement un niveau de maturité de 2 et 4, alors le niveau de maturité du groupe en tenant compte de tous les objectifs est le niveau 2 (niveau de maturité général pour le groupe (I) = (2+4)/3), tandis que le niveau de maturité du groupe en tenant compte seulement des objectifs spécifiques sélectionnés par l'évaluateur est le niveau 3 (niveau de maturité spécifique pour le groupe (I) = (2+4)/2).

Le **taux de couverture général de chaque groupe** est calculé comme la proportion entre le nombre total de questions dans le groupe et le nombre de questions auxquelles la réponse est positive.

Le **taux de couverture spécifique de chaque groupe** est calculé comme la proportion entre le nombre total de questions au sein du groupe concernant les objectifs que l'État membre a choisi d'évaluer (il s'agit généralement des objectifs figurant dans la SNCS du pays spécifique) et le nombre de questions pour lesquelles la réponse est positive.

Scores globaux

Le **niveau de maturité général global d'un pays** est calculé comme la moyenne arithmétique du niveau de maturité de tous les objectifs au sein du cadre, de 1 à 17.

Le **niveau de maturité spécifique global d'un pays** est calculé comme la moyenne arithmétique du niveau de maturité des objectifs au sein du cadre que l'État membre a choisi d'évaluer (il s'agit généralement des objectifs figurant dans la SNCS du pays concerné).

Le **taux de couverture général global d'un pays** est calculé comme la proportion entre le nombre total de questions portant sur tous les objectifs inclus dans le cadre (de 1 à 17) et le nombre de questions pour lesquelles la réponse est positive.

Le **taux de couverture spécifique global d'un pays** est calculé comme la proportion entre le nombre total de questions portant sur les objectifs du cadre que l'État membre a choisi d'évaluer (il s'agit généralement des objectifs figurant dans la SNCS du pays concerné) et le nombre de questions pour lesquelles la réponse est positive.

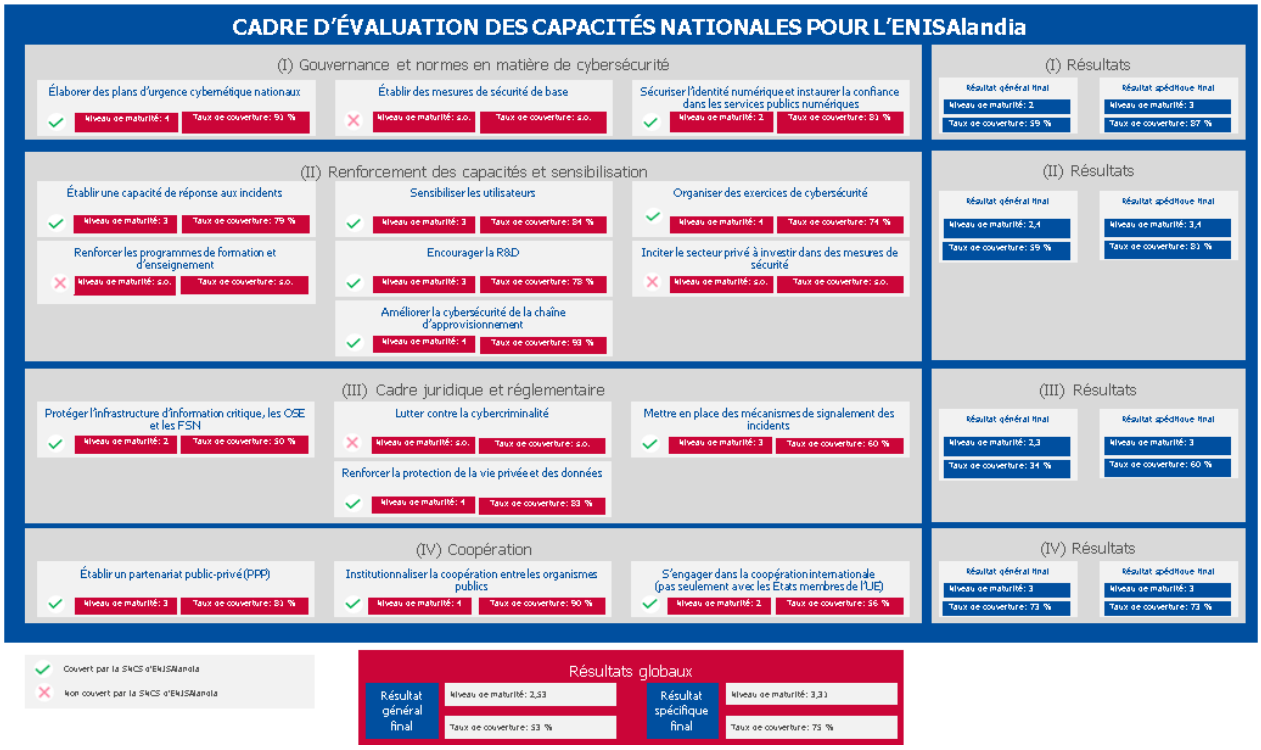
Pour chaque indicateur, les répondants peuvent sélectionner une troisième option de réponse «ne sait pas/non applicable». Dans ce cas, l'indicateur est exclu du calcul total des résultats.

Les niveaux de maturité au niveau des groupes et au niveau global sont calculés avec une moyenne arithmétique afin de montrer la progression entre deux évaluations. En effet, l'alternative consistant à calculer les niveaux de maturité des groupes et global comme le niveau de maturité de l'objectif le moins mature – bien que pertinente du point de vue de la maturité – ne peut pas rendre compte des progrès réalisés dans les domaines couverts par d'autres objectifs.

Comme le niveau des groupes et le niveau global sont consolidés à des fins d'établissement de rapports, le choix a été fait d'utiliser la moyenne arithmétique. Pour plus de précision, veuillez utiliser les scores au niveau des objectifs aux fins d'établissement de rapports.

La figure 3 ci-dessous résume les mécanismes des scores à travers les différents niveaux du modèle (objectif, groupe, global).

Figure 3: Mécanisme des scores global



3.5 EXIGENCES POUR LE CADRE D'AUTOÉVALUATION

Le cadre d'évaluation des capacités nationales présenté dans cette section est basé sur les besoins mis en évidence par les États membres et il est construit autour d'un ensemble d'exigences énumérées ci-après:

- Le CECN est déployé sur une base volontaire par l'État membre en tant que cadre d'autoévaluation;
- Le CECN vise à mesurer les capacités des États membres en matière de cybersécurité par rapport aux 17 objectifs. Toutefois, l'État membre peut choisir les objectifs qu'il souhaite évaluer et n'évaluer qu'un sous-ensemble des 17 objectifs;
- Le cadre d'autoévaluation vise à mesurer le niveau de maturité des capacités de cybersécurité de l'État membre;
- Les résultats de l'évaluation ne sont pas publiés, sauf si l'État membre décide de le faire de sa propre initiative;
- L'État membre peut afficher les résultats de l'évaluation en présentant le niveau de maturité des capacités de cybersécurité du pays, d'un groupe d'objectifs, voire d'un seul objectif;
- Tous les objectifs évalués ont une pertinence équivalente dans le cadre d'évaluation, ils ont donc la même importance. Il en va de même pour les indicateurs déployés dans ce cadre; et
- L'État membre est en mesure de suivre sa progression dans le temps.

Le cadre d'autoévaluation vise à aider les États membres à renforcer leurs capacités en matière de cybersécurité. Par conséquent, il comprend aussi un ensemble de recommandations ou d'orientations pour guider les pays européens dans l'amélioration de leur niveau de maturité.

Remarque: ces recommandations ou orientations sont génériques et basées sur les publications de l'ENISA et les enseignements tirés d'autres pays, et elles dépendront du résultat de l'autoévaluation.

4. INDICATEURS DE CECN

4.1 INDICATEURS DU CADRE

Cette section présente les indicateurs du cadre d'évaluation des capacités nationales de l'ENISA. Les sections suivantes sont organisées par groupe.

Pour chaque groupe, un tableau présente l'ensemble des indicateurs sous forme de questions représentatives d'un niveau de maturité donné. Le questionnaire est l'instrument principal de l'autoévaluation. Pour chaque objectif, il y a deux séries d'indicateurs:

- Une série de questions génériques sur la maturité de la stratégie (9 questions génériques), notées de «a» à «c» pour chaque niveau de maturité, répétées pour chaque objectif; et
- Une série de questions sur la capacité de cybersécurité (319 questions sur la capacité de cybersécurité), numérotées de «1» à «10» pour chaque niveau de maturité, spécifiques au domaine couvert par l'objectif.

Chaque question s'accompagne d'une balise (0-1), qui indique si la question est un indicateur nécessaire (1) ou accessoire (0) pour le niveau de maturité.

Chaque question est caractérisée par son numéro d'identification composé:

- Du numéro de l'objectif;
- Du niveau de maturité; et
- Du numéro de la question.

Par exemple, la question ID 1.2.4 est la quatrième question du niveau de maturité 2 de l'objectif stratégique (I) «Élaborer des plans d'urgence cybernétique nationaux».

Il convient de noter que, tout au long du questionnaire, les questions portent sur la situation nationale, sauf indication contraire. Dans toutes les questions, le pronom «vous» fait référence à l'État membre de manière générique et ne se réfère pas à la personne ou à l'organisme public qui effectue l'évaluation.

Vous trouverez la définition de chaque objectif au chapitre 2.2 - Objectifs communs identifiés parmi les SNCS européennes.

4.1.1 Groupe nº 1: Gouvernance et normes en matière de cybersécurité

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
1 – Élaborer des plans d'urgence cybernétique nationaux	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans le cadre de la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous commencé à travailler à l'élaboration de plans d'urgence cybernétique nationaux? Par exemple, en définissant les objectifs généraux, la portée et/ou les principes des plans d'urgence, etc.	1	Avez-vous une doctrine/stratégie nationale qui inclut la cybersécurité comme un facteur de crise (c.-à-d. un plan, une politique, etc.)?	1	Disposez-vous d'un plan de gestion des cybercrises à l'échelle nationale?	1	Êtes-vous satisfait du nombre ou du pourcentage de secteurs critiques inclus dans le plan d'urgence cybernétique national?	1	Avez-vous mis en place un processus d'apprentissage permettant de tirer les enseignements des cyberexercices ou de crises réelles au niveau national?	1
	2	Est-il généralement admis que les cyberincidents constituent un facteur de crise susceptible de menacer la sécurité nationale?	0	Disposez-vous d'une plate-forme d'acquisition des informations et d'information des décideurs? C'est-à-dire tout type de méthodes, plates-formes ou lieux permettant à tous les acteurs de la réponse aux crises d'accéder aux mêmes informations en temps réel à propos de la cybercrise.	1	Disposez-vous de procédures spécifiques en cas de cybercrise à l'échelle nationale?	1	Organisez-vous assez souvent des activités (c'est-à-dire des exercices) liées à la planification nationale en cas d'urgence cybernétique?	1	Avez-vous un processus pour tester régulièrement le plan national?	1
	3	Des études (techniques, opérationnelles, politiques) ont-elles été réalisées dans le domaine de la planification des cyberurgences?	0	Les ressources pertinentes sont-elles engagées pour superviser l'élaboration et l'exécution des plans d'urgence cybernétique nationaux?	1	Avez-vous une équipe de communication spécialement formée pour répondre aux cybercrises et informer le public?	1	Disposez-vous d'effectifs en suffisance pour la planification de crise, l'examen des enseignements tirés et la mise en œuvre des changements?	1	Disposez-vous d'outils et de plates-formes adéquats pour renforcer la conscience situationnelle?	1
	4	-		Disposez-vous d'une méthodologie d'évaluation de la cybermenace à l'échelle nationale qui comprend des procédures d'analyse d'impact?	0	Faites-vous appel à toutes les parties prenantes nationales concernées (sécurité nationale, défense, protection civile, forces de l'ordre, ministères, autorités, etc.)?	1	Disposez-vous de suffisamment de personnes formées pour répondre aux cybercrises à l'échelle nationale?	1	Suivez-vous un modèle de maturité spécifique pour surveiller et améliorer le plan d'urgence cybernétique?	0
	5	-		-		Disposez-vous d'installations et de cellules de crise adéquates pour la gestion des crises?	1	-		Disposez-vous de ressources spécialisées dans l'anticipation des menaces ou travaillant sur la	0

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
										cybersécurité prospective pour faire face aux crises futures ou aux défis de demain?	
	6	-		-		Vous engagez-vous auprès des parties prenantes internationales dans l'UE si nécessaire?	0	-		-	
	7	-		-		Vous engagez-vous auprès des parties prenantes internationales hors UE si nécessaire?	0	-		-	
2 – Établir des mesures de sécurité de base	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans le cadre de la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous réalisé une étude pour identifier les exigences et les lacunes des organismes **publics** sur la base de normes internationalement reconnues? Par exemple, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS, etc.	1	Les mesures de sécurité sont-elles conformes aux normes internationales/nationales?	1	Des mesures de sécurité de base sont-elles obligatoires?	1	Existe-t-il un processus de mise à jour fréquente des mesures de sécurité de base?	1	Avez-vous un processus visant à durcir les TIC lorsque les incidents ne sont pas traités par les mesures?	1
	2	Avez-vous réalisé une étude pour identifier les exigences et les lacunes des organisations **privées** sur la base de normes internationalement reconnues? Par exemple, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, UIT, ISA, IEC, CIS, etc.	1	Le secteur privé et les autres parties prenantes sont-ils consultés lors de la définition des mesures de sécurité de base?	1	Mettez-vous en œuvre des mesures de sécurité horizontales parmi les secteurs critiques?	1	Existe-t-il un mécanisme de surveillance pour examiner l'application des mesures de sécurité de base?	1	Évaluez-vous la pertinence des nouvelles normes élaborées en réponse aux derniers développements dans le paysage de la menace?	1
	3	-		-		Mettez-vous en œuvre des mesures de sécurité spécifiques	1	Existe-t-il une autorité nationale chargée de vérifier si les mesures	1	Disposez-vous d'un processus de divulgation coordonnée des vulnérabilités (DCV) ou	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
						au secteur dans les secteurs critiques?		de sécurité de base sont appliquées ou non?		encouragez-vous son élaboration?	
	4	-				Les mesures de sécurité de base sont-elles conformes aux programmes de certification pertinents?	1	Avez-vous mis en place un processus pour identifier les organisations non conformes dans un délai précis?	1	-	
	5	-		-		Existe-t-il un processus d'autoévaluation des risques pour les mesures de sécurité de base?	1	Existe-t-il un processus d'audit pour s'assurer que les mesures de sécurité sont correctement appliquées?	1	-	
2 – Établir des mesures de sécurité de base	6	-		-		Examinez-vous les mesures de sécurité de base obligatoires dans les procédures de passation de marchés des organismes gouvernementaux?	0	Définissez-vous ou encouragez-vous activement l'adoption de normes sécurisées pour le développement de produits IT/OT critiques (équipements médicaux, véhicules connectés et autonomes, radio professionnelle, équipements de l'industrie lourde, etc.)?	0	-	
3 – Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous réalisé des études ou des analyses des lacunes pour identifier les besoins de sécurisation des services publics numériques au profit des citoyens et des entreprises?	1	Effectuez-vous des analyses des risques pour déterminer le profil de risque des actifs ou des services avant de les transférer dans le cloud ou de lancer des projets de transformation numérique?	1	Faites-vous la promotion des méthodologies de protection de la vie privée dès la conception dans tous les projets d'e-gouvernement?	1	Recueillez-vous des indicateurs sur les incidents de cybersécurité impliquant une atteinte à la sécurité des services publics numériques?	1	Participez-vous à des groupes de travail européens pour la maintenance des normes et/ou la conception de nouvelles exigences pour les services de confiance (signatures électroniques, sceaux électroniques, enregistrement électronique pour la prestation de services, horodatage, authentification de sites web)? Par exemple, ETSI/CEN/CENELEC, ISO, IETF, NIST, UIT, etc.	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
3 – Sécuriser l'identité numérique et instaurer la confiance dans les services publics numériques	2	-		Avez-vous une stratégie pour construire ou promouvoir des schémas d'identification électronique (eID) nationaux sécurisés pour les citoyens et les entreprises?	1	Faites-vous participer les parties prenantes privées à la conception et à la fourniture de services publics numériques sécurisés?	1	Avez-vous mis en œuvre la reconnaissance mutuelle des moyens d'identification électronique avec d'autres États membres?	1	Participez-vous activement aux examens par les pairs dans le cadre de la notification des schémas d'eID à la Commission européenne?	1
	3	-		Avez-vous une stratégie pour créer ou promouvoir des services de confiance nationaux sécurisés (signatures électroniques, sceaux électroniques, enregistrement électronique pour la prestation de services, horodatage, authentification de sites web) pour les citoyens et les entreprises?	1	Appliquez-vous un socle de sécurité minimum pour tous les services publics numériques?	1	-		-	
	4	-		Avez-vous une stratégie concernant le cloud gouvernemental (une stratégie de cloud computing ciblée sur le gouvernement et les organismes publics tels que les ministères, les agences gouvernementales et les administrations publiques, etc.) qui prend en compte les implications en termes de sécurité?	0	Existe-t-il des schémas d'identification électronique accessibles aux citoyens et aux entreprises avec un niveau de garantie élevé ou substantiel tel que défini dans l'annexe du règlement eIDAS (UE) nº 910/2014?	1	-		-	
	5	-		-		Disposez-vous de services publics numériques nécessitant des schémas d'identification électronique avec un niveau de garantie élevé ou substantiel tel que défini dans l'annexe du règlement eIDAS (UE) nº 910/2014?	1	-		-	
	6	-		-		Avez-vous des prestataires de services de confiance pour les citoyens et les entreprises (signatures électroniques, sceaux électroniques, enregistrement électronique pour la prestation de services, horodatage, authentification de sites web)?	1	-		-	
	7	-		-		Favorisez-vous l'adoption de mesures de sécurité de base pour tous les modèles de déploiement	0	-		-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
						dans le cloud (par exemple, IaaS, PaaS, SaaS privés, publics, hybrides)?					

4.1.2 Groupe nº 2: Renforcement des capacités et sensibilisation

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
4 – Établir une capacité de réponse aux incidents	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Disposez-vous de capacités informelles de réponse aux incidents gérées au sein des secteurs public et privé ou conjointement par ces secteurs?	1	Avez-vous au moins un CSIRT national officiel?	1	Disposez-vous de capacités de réponse aux incidents pour les secteurs visés à l'annexe II de la directive SRI?	1	Avez-vous défini des pratiques standardisées pour les procédures de réponse aux incidents et les systèmes de classification des incidents et en avez-vous fait la promotion?	1	Disposez-vous de mécanismes de détection précoce, d'identification, de prévention, de réponse et d'atténuation des vulnérabilités zéro-jour?	1
	2	-		Votre ou vos CSIRT nationaux ont-ils un champ d'intervention clairement défini? Par exemple, en fonction du secteur ciblé, des types d'incidents, des impacts.	1	Existe-t-il un mécanisme de coopération CSIRT dans votre pays pour répondre aux incidents?	1	Évaluez-vous votre capacité de réponse aux incidents pour vous assurer que vous disposez des ressources et des compétences adéquates pour effectuer les tâches définies à l'annexe I, point 2), de la directive SRI?	1	-	
	3	-		Votre ou vos CSIRT nationaux ont-ils des relations clairement définies avec d'autres parties prenantes nationales concernant le paysage national de la cybersécurité et les pratiques de réponse aux incidents (par exemple, AR, armée, FAI, centre national de cybersécurité)?	0	Votre ou vos CSIRT nationaux disposent-ils d'une capacité de réponse aux incidents conforme à l'annexe I de la directive SRI, notamment en matière de disponibilité, de sécurité physique, de continuité des activités, de coopération internationale, de suivi des incidents, de capacité d'alerte et d'avertissement précoces, de réponse aux incidents, d'analyse des risques et de conscience situationnelle, de coopération avec le secteur privé, de pratiques standard, etc.?	1	-		-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
4 – Établir une capacité de réponse aux incidents	4	-				Existe-t-il un mécanisme de coopération avec des pays voisins concernant les incidents?	1	-		-	
	5	-		-		Avez-vous formellement défini des politiques et des procédures claires de gestion des incidents?	1	-		-	
	6	-		-		Votre ou vos CSIRT nationaux participent-ils à des exercices de cybersécurité à l'échelle tant nationale qu'internationale?	1	-		-	
	7	-		-		Votre ou vos CSIRT nationaux sont-ils membres du FIRST (Forum of Incident Response and Security Teams)?	0	-		-	
5 – Sensibiliser les utilisateurs	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Y a-t-il un minimum de reconnaissance de la part du gouvernement, du secteur privé et des utilisateurs en général quant à la nécessité d'éveiller les consciences sur les questions de cybersécurité et de respect de la vie privée?	1	Avez-vous identifié un public cible spécifique pour la sensibilisation des utilisateurs? Par exemple, les utilisateurs généraux, les jeunes, les utilisateurs professionnels (qui peuvent encore être subdivisés comme suit: PME, OSE, FSN, etc.).	1	Avez-vous élaboré des plans/stratégies de communication pour les campagnes?	1	Préparez-vous des indicateurs pour évaluer votre campagne pendant la phase de planification?	1	Avez-vous mis en place des mécanismes pour garantir que les campagnes de sensibilisation sont constamment pertinentes par rapport aux progrès technologiques, aux changements dans le paysage de la menace, à la législation et aux réglementations, et aux directives de sécurité nationale?	1
	2	Les organismes publics mènent-ils ponctuellement des campagnes de sensibilisation à la cybersécurité au sein de leur organisation? Par exemple à la	0	Établissez-vous un plan de projet pour sensibiliser aux questions de sécurité de l'information et de protection de la vie privée?	1	Avez-vous un processus de création de contenu au niveau gouvernemental?	1	Évaluez-vous vos campagnes après leur exécution?	1	Effectuez-vous des évaluations ou des études périodiques pour mesurer les changements d'attitude ou de comportement en matière de cybersécurité et de	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
		suite d'un incident de cybersécurité.								protection de la vie privée dans les secteurs privé et public?	
5 – Sensibiliser les utilisateurs	3	Les organismes publics mènent-ils ponctuellement des campagnes de sensibilisation à la cybersécurité auprès du grand public? Par exemple, à la suite d'un incident de cybersécurité.	0	Avez-vous des ressources disponibles et facilement identifiables (par exemple, un portail unique en ligne, des kits de sensibilisation) pour tout utilisateur qui cherche à s'informer sur les questions de cybersécurité et de respect de la vie privée?	1	Disposez-vous de mécanismes pour identifier les domaines cibles de la sensibilisation (à savoir rapport de l'ENISA concernant le paysage des menaces, paysages nationaux, paysages internationaux, rétroactions des centres nationaux de lutte contre la cybercriminalité, etc.)?	1	Avez-vous mis en place des mécanismes pour identifier le média ou le canal de communication le plus pertinent en fonction du public cible afin de maximiser le rayonnement et l'engagement? Par exemple, différents types de médias numériques, des brochures, des e-mails, du matériel pédagogique, des affiches dans des zones très fréquentées, la télévision, la radio, etc.	1	Consultez-vous des experts en comportement pour adapter votre campagne au public cible?	1
	4	-		-		Réunissez-vous les parties prenantes avec des experts et des équipes de communication afin de créer du contenu?	1			-	
	5	-		-		Impliquez-vous et engagez-vous le secteur privé dans vos efforts de sensibilisation pour promouvoir les messages et les diffuser à un public plus large?	1	-		-	
	6	-		-		Préparez-vous des initiatives de sensibilisation spécifiques pour les cadres des secteurs public, privé, universitaire ou de la société civile?	1	-		-	
	7	-		-		Participez-vous aux campagnes du mois européen de la cybersécurité (ECSM) de l'ENISA?	0	-		-	
6 – Organiser des exercices de cybersécurité	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans le cadre de la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
6 – Organiser des exercices de cybersécurité	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Effectuez-vous des exercices de crise dans d'autres secteurs (autres que la cybersécurité) à l'échelle nationale ou paneuropéenne?	1	Avez-vous un programme d'exercices de cybersécurité à l'échelle nationale?	1	Impliquez-vous toutes les autorités des pouvoirs publics concernées? (même si le scénario est spécifique au secteur)	1	Rédigez-vous des rapports après action/des rapports d'évaluation?	1	Avez-vous une capacité d'analyse des enseignements tirés en matière de cybernétique (processus d'établissement de rapports, d'analyse, d'atténuation)?	1
	2	Avez-vous des ressources affectées à la conception et à la planification d'exercices de gestion de crise?	1	Effectuez-vous des exercices de gestion de cybercrises sur les fonctions sociétales vitales et les infrastructures critiques ou hiérarchisez-vous de tels exercices?	1	Impliquez-vous le secteur privé dans la planification et l'exécution des exercices?	1	Testez-vous des plans et des procédures à l'échelle nationale?	1	Avez-vous un processus établi en matière d'enseignements tirés?	1
	3	-		Avez-vous chargé un organe de coordination de superviser la conception et la planification des exercices de cybersécurité (organisme public, société de conseil, etc.)?	0	Organisez-vous des exercices spécifiques aux secteurs à l'échelle nationale et/ou internationale?	1	Participez-vous à des exercices de cybersécurité à l'échelle paneuropéenne?	1	Adaptez-vous les scénarios des exercices en fonction des derniers développements (progrès technologiques, conflits mondiaux, paysage de la menace, etc.)?	1
	4	-		-		Organisez-vous des exercices dans tous les secteurs critiques mentionnés à l'annexe II de la directive SRI?	1	-		Alignez-vous vos procédures de gestion de crise sur celles des autres États membres afin de garantir une gestion de crise paneuropéenne efficace?	1
	5	-		-		Organisez-vous des exercices de cybersécurité intersectoriels et/ou transversaux?	1	-		Disposez-vous d'un mécanisme d'adaptation rapide de la stratégie, des plans et des procédures à partir des enseignements tirés des exercices?	0
	6	-		-		Organisez-vous des exercices de cybersécurité spécifiques à différents niveaux (technique et opérationnel, procédural, décisionnel, politique, etc.)?	0	-		-	
7 – Renforcer les programmes de formation et d'enseignement	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Envisagez-vous d'élaborer des programmes de formation et des programmes éducatifs consacrés à la cybersécurité?	1	Instaurez-vous des cours consacrés à la cybersécurité?	1	Votre pays intègre-t-il la culture de la cybersécurité à un stade précoce dans le parcours d'enseignement ou de formation des étudiants? Par exemple, mettez-vous la cybersécurité en avant au collège et au lycée?	1	Insistez-vous pour que le personnel des secteurs privé et public soit agréé ou certifié?	1	Avez-vous mis en place des mécanismes pour garantir que les formations et programmes éducatifs sont constamment pertinents par rapport aux évolutions technologiques actuelles et émergentes, aux changements dans le paysage de la menace, à la législation et aux réglementations, et aux directives de sécurité nationale?	1
	2	-		Les universités de votre pays proposent-elles des doctorats en cybersécurité en tant que discipline indépendante et non en tant que matière liée à l'informatique?	1	Disposez-vous de laboratoires de recherche nationaux et d'établissements d'enseignement spécialisés dans la cybersécurité?	1	Votre pays a-t-il mis en place des programmes de formation ou de mentorat en matière de cybersécurité afin de soutenir les jeunes entreprises et les PME nationales?	1	Établissez-vous des centres universitaires d'excellence en matière de cybersécurité destinés à servir de plates-formes de recherche et d'éducation?	1
	3	-		Prévoyez-vous de former des éducateurs, indépendamment de leur domaine, aux questions de sécurité de l'information et de protection de la vie privée? Par exemple, concernant la sécurité en ligne, la protection des données à caractère personnel, le harcèlement en ligne.	1	Encouragez-vous ou financez-vous des cours et des plans de formation consacrés à la cybersécurité pour les employés des agences pour l'emploi des États membres?	1	Faites-vous la promotion active de l'ajout de cours sur la sécurité de l'information dans l'enseignement supérieur, non seulement pour les étudiants en informatique mais aussi pour toute autre spécialité professionnelle? Par exemple, des cours adaptés aux besoins de cette profession.	1	Les institutions universitaires participent-elles à des discussions de premier plan dans le domaine de l'éducation et de la recherche en matière de cybersécurité à l'échelle internationale?	0
	4	-		-		Avez-vous des cours de cybersécurité et/ou un programme d'études spécialisé pour les niveaux 5 à 8 du CEC (cadre européen des certifications)?	1	Évaluez-vous régulièrement le déficit de compétences (pénurie de travailleurs qualifiés en cybersécurité) dans le domaine de la sécurité de l'information?	1	-	
	5	-		-		Encouragez-vous et/ou soutenez-vous les initiatives visant à inclure des cours sur la sécurité sur	1	Favorisez-vous la mise en réseau et le partage d'information entre les institutions universitaires, tant	1		

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
						l'internet dans l'enseignement primaire et secondaire?		à l'échelle nationale qu'internationale?			
7 - Renforcer les programmes de formation et d'enseignement	6	-		-		Financez-vous ou offrez-vous gratuitement des formations de base sur la cybersécurité à l'intention des citoyens?	0	Impliquez-vous le secteur privé, sous quelque forme que ce soit, dans des initiatives de formation à la cybersécurité? Par exemple, conception et organisation de cours, de stages, de détachements, etc.	1	-	
	7	-		-		Organisez-vous annuellement des événements en lien avec la sécurité de l'information (par exemple, des concours de hacking ou des hackathons)?	0	Déployez-vous des mécanismes de financement pour encourager l'obtention de diplômes en cybersécurité? Par exemple, des bourses d'études, un stage garanti, des emplois garantis dans un secteur spécifique ou des postes dans le secteur public.	0	-	
8 – Encourager la R&D	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous réalisé des études ou des analyses pour identifier les priorités de la R&D en matière de cybersécurité?	1	Disposez-vous d'un processus visant à définir les priorités de la R&D (par exemple, les sujets émergents pour la dissuasion, la protection, la détection et l'adaptation face aux nouveaux types de cyberattaques)?	1	Existe-t-il un plan pour relier les initiatives de R&D à l'économie réelle?	1	Les initiatives de R&D en matière de cybersécurité sont-elles conformes aux objectifs stratégiques pertinents, par exemple le MNU, H2020, Digital Europe, la stratégie de cybersécurité de l'UE?	1	À l'échelle nationale, assurez-vous une coopération avec des initiatives internationales de R&D liées à la cybersécurité?	1
	2	-		Le secteur privé participe-t-il à l'établissement des priorités en matière de R&D?	1	Existe-t-il des projets nationaux liés à la cybersécurité?	1	Existe-t-il un système d'évaluation des initiatives de R&D?	1	Les priorités de R&D sont-elles alignées sur la réglementation actuelle ou à venir (à l'échelle nationale)?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
8 – Encourager la R&D	3	-		Le monde universitaire participe-t-il à l'établissement des priorités en matière de R&D?	1	Disposez-vous d'écosystèmes locaux/régionaux de jeunes entreprises et d'autres canaux de mise en réseau (par exemple, parcs technologiques, pôles d'innovation, événements/plates-formes de mise en réseau) pour favoriser l'innovation (y compris pour les jeunes entreprises actives dans le domaine de la cybersécurité)?	1	Existe-t-il des accords de coopération avec les universités et d'autres établissements de recherche?	1	Participez-vous à des discussions de premier plan sur un ou plusieurs sujets de pointe en matière de R&D à l'échelle internationale?	0
	4	-		Existe-t-il des initiatives nationales de R&D liées à la cybersécurité?	0	Note-t-on des investissements dans des programmes de R&D en matière de cybersécurité dans les universités et le secteur privé?	1	Existe-t-il un organisme institutionnel reconnu qui supervise les activités de R&D en matière de cybersécurité?	0	-	
	5	-		-		Disposez-vous de chaires de recherche industrielle dans les universités permettant de faire le lien entre les sujets de recherche et les besoins du marché?	1	-		-	
	6	-		-		Disposez-vous de programmes de financement de la R&D dédiés à la cybersécurité?	0	-		-	
9 – Inciter le secteur privé à investir dans des mesures de sécurité	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Existe-t-il une politique sectorielle ou une volonté politique d'encourager le développement du secteur de la cybersécurité?	1	Le secteur privé participe-t-il à la mise au point d'incitations?	1	Existe-t-il des incitations économiques/réglementaires ou d'autres types d'incitations pour promouvoir les investissements dans la cybersécurité?	1	Y a-t-il des acteurs privés qui réagissent aux incitations en investissant dans des mesures de sécurité? Par exemple, des investisseurs spécialisés dans la cybersécurité et des investisseurs non spécialisés.	1	Concentrez-vous les incitations sur les sujets de cybersécurité en fonction des dernières évolutions de la menace?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
9 – Inciter le secteur privé à investir dans des mesures de sécurité	2	-		Avez-vous identifié des sujets spécifiques à développer en matière de cybersécurité? Par exemple, la cryptographie, la protection de la vie privée, une nouvelle forme d'authentification, l'IA pour la cybersécurité, etc.	0	Apportez-vous un soutien (par exemple, des incitations fiscales) aux jeunes entreprises et PME du secteur de la cybersécurité?	1	Incitez-vous le secteur privé à se concentrer sur la sécurité des technologies de pointe? Par exemple, la 5G, l'intelligence artificielle, l'IdO, l'informatique quantique, etc.	1	-	
	3	-		-		Offrez-vous des incitations fiscales ou d'autres motivations financières aux investisseurs du secteur privé pour les investissements dans les jeunes entreprises du domaine de la cybersécurité?	1	-		-	
	4	-		-		Facilitez-vous l'accès des jeunes entreprises et des PME du domaine de la cybersécurité aux procédures de passation de marchés publics?	0	-		-	
	5	-		-		Y a-t-il un budget disponible pour fournir des incitations au secteur privé?	0	-		-	
10 – Améliorer la cybersécurité de la chaîne d'approvisionnement	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous réalisé une étude sur les bonnes pratiques de sécurité pour la gestion de la chaîne d'approvisionnement utilisées par les services d'achat dans divers segments de l'industrie et/ou dans le secteur public?	1	Effectuez-vous des évaluations de la cybersécurité dans l'ensemble de la chaîne d'approvisionnement des services et produits TIC dans les secteurs critiques [tels qu'identifiés dans l'annexe II de la directive SRI (2016/1148)]?	1	Utilisez-vous un système de certification de la sécurité pour les produits et services basés sur les TIC? Par exemple, SOG-IS ARM en Europe (Comité consultatif pour les actions à mener dans le domaine de la sécurité des systèmes d'information, accord	1	Avez-vous mis en place un processus de mise à jour des évaluations de la cybersécurité de la chaîne d'approvisionnement des services et produits TIC dans les secteurs critiques [tels qu'identifiés dans l'annexe II de la directive SRI (2016/1148)]?	1	Disposez-vous de dispositifs de détection au niveau des éléments clés de la chaîne d'approvisionnement permettant de détecter les signes précoces de compromission? Par exemple, des contrôles de sécurité au niveau des FAI, des dispositifs de	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
						de reconnaissance mutuelle), Arrangement de reconnaissance des critères communs (ARCC), initiatives nationales, initiatives sectorielles, etc.				surveillance de la sécurité dans les principaux composants de l'infrastructure, etc.	
	2	-		Appliquez-vous des normes dans les politiques d'achat des administrations publiques pour garantir que les fournisseurs de produits ou de services TIC répondent aux exigences de base en matière de sécurité de l'information? Par exemple, ISO/IEC 27001 et 27002, ISO/IEC 27036, etc.	1	Faites-vous activement la promotion des meilleures pratiques en matière de sécurité et de protection de la vie privée dès la conception lors du développement des produits et services TIC? Par exemple, cycle de vie du développement de logiciels sécurisés, cycle de vie de l'IdO.	1	Avez-vous mis en place un processus de détection des maillons faibles de la cybersécurité dans la chaîne d'approvisionnement des secteurs critiques [tels qu'identifiés dans l'annexe II de la directive SRI (2016/1148)]?	1	-	
	3	-		-		Élaborez-vous et fournissez-vous un catalogue centralisé contenant des informations détaillées sur les normes existantes en matière de sécurité de l'information et de protection de la vie privée qui sont évolutives pour les PME et applicables par celles-ci?	1	Avez-vous mis en place des mécanismes pour garantir que les produits et services TIC indispensables pour les OSE sont cyberrésilients (c'est-à-dire que la disponibilité et la sécurité sont maintenues en cas de cyberincident)? Par exemple, par des tests, des évaluations régulières, la détection des éléments compromis, etc.	1	-	
10 – Améliorer la cybersécurité de la chaîne d'approvisionnement	4	-				Participez-vous activement à la conception d'un cadre de certification de l'UE pour les produits, services et processus numériques des TIC, tel qu'établi dans le règlement de l'Union européenne sur la cybersécurité (2019/881)? Par exemple, participation au Groupe européen de certification de cybersécurité (GECC), promotion des normes et procédures techniques pour la sécurité des produits/services TIC.	0	Encouragez-vous le développement de systèmes de certification destinés aux PME pour favoriser l'adoption de normes en matière de sécurité de l'information et de protection de la vie privée?	0	-	
	5	-		-		Offrez-vous des incitations aux PME pour qu'elles adoptent des normes de sécurité et de protection de la vie privée?	0	Avez-vous mis en place des dispositions pour encourager les grandes entreprises à renforcer la cybersécurité des petites entreprises dans leurs chaînes d'approvisionnement? Par	0	-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
								exemple, une plate-forme, des formations, des campagnes de sensibilisation, etc. dédiées à la cybersécurité.			
	6	-		-		Encouragez-vous les éditeurs de logiciels à soutenir les PME en garantissant des configurations par défaut sécurisées dans les produits destinés aux petites entreprises?	0	-		-	

4.1.3 Groupe nº 3: Cadre juridique et réglementaire

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
11 – Protéger l'infrastructure d'information critique, les OSE et les FSN	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Est-il généralement admis que les opérateurs d'IIC contribuent à la sécurité nationale?	1	Disposez-vous d'une méthodologie pour identifier les services essentiels?	1	Avez-vous mis en œuvre la directive SRI (2016/1148)?	1	Avez-vous une procédure de mise à jour du registre des risques?	1	Créez-vous et mettez-vous à jour des rapports sur le paysage de la menace?	1
	2	-		Avez-vous une méthodologie d'identification des IIC?	1	Avez-vous mis en œuvre la directive ICE (2008/114) concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection?	1	Avez-vous d'autres mécanismes en place pour apprécier si les mesures techniques et organisationnelles mises en œuvre par les OSE sont appropriées pour gérer les risques relatifs à la sécurité des réseaux et des systèmes d'information? Par exemple, des audits réguliers de la cybersécurité, un cadre national pour la mise en œuvre de mesures standard, des outils techniques fournis par le gouvernement tels que des dispositifs de détection ou une révision de la configuration spécifique du système, etc.	1	En fonction des dernières évolutions du paysage de la menace, êtes-vous en mesure d'intégrer un nouveau secteur dans votre plan d'action PIIC?	1
	3	-		Disposez-vous d'une méthodologie pour identifier les OSE?	1	Disposez-vous d'un registre national des OSE identifiés par secteur critique?	1	Révisez-vous et mettez-vous à jour en conséquence la liste des OSE identifiés au moins tous les deux ans?	1	En fonction des dernières évolutions dans le paysage de la menace, êtes-vous en mesure d'adapter de nouvelles exigences dans votre plan d'action PIIC?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
11 – Protéger l'infrastructure d'information critique, les OSE et les FSN	4	-		Disposez-vous d'une méthodologie pour identifier les fournisseurs de services numériques?	1	Disposez-vous d'un registre national des fournisseurs de services numériques identifiés?	1	Avez-vous d'autres mécanismes en place pour apprécier si les mesures techniques et organisationnelles mises en œuvre par les fournisseurs de services numériques sont appropriées pour gérer les risques relatifs à la sécurité des réseaux et des systèmes d'information? Par exemple, des audits réguliers de la cybersécurité, un cadre national pour la mise en œuvre de mesures standard, des outils techniques fournis par le gouvernement tels que des dispositifs de détection ou une révision de la configuration spécifique du système, etc.	1	-	
	5	-		Disposez-vous d'une ou de plusieurs autorités nationales chargées de superviser la protection des infrastructures d'information critiques et la sécurité des réseaux et des systèmes d'information? Par exemple, tel que requis dans la directive SRI (2016/1148).	1	Disposez-vous d'un registre national des risques identifiés ou connus?	1	Révisez-vous et mettez-vous à jour en conséquence la liste des fournisseurs de services numériques identifiés au moins tous les deux ans?	1	-	
	6	-		Élaborez-vous des plans de protection sectoriels spécifiques? Par exemple, incluant des mesures de base en matière de cybersécurité (obligations ou lignes directrices).	0	Disposez-vous d'une méthodologie pour inventorier les dépendances de l'IIC?	1	Utilisez-vous un système de certification de la sécurité (national ou international) pour aider les OSE et les fournisseurs de services numériques à identifier les produits TIC sécurisés? Par exemple, SOG-IS ARM en Europe, initiatives nationales, etc.	1	-	
	7	-		-		Déployez-vous des pratiques de gestion des risques pour identifier, quantifier et gérer les risques liés aux IIC à l'échelle nationale?	1	Utilisez-vous un système de certification de la sécurité ou une procédure de qualification pour évaluer les fournisseurs de services travaillant avec les OSE? Par exemple, les fournisseurs de services dans le domaine de la détection des incidents, de la réponse aux incidents, des audits	1	-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
								de cybersécurité, des services cloud, des cartes à puce, etc.			
	8	-		-		Vous engagez-vous dans un processus de consultation pour identifier les dépendances transfrontalières?	1	Avez-vous mis en place des mécanismes pour mesurer le degré de conformité des OSE et des fournisseurs de services numériques par rapport aux mesures de base en matière de cybersécurité?	0	-	
	9					Disposez-vous d'un point de contact unique chargé de coordonner les questions liées à la sécurité des réseaux et des systèmes d'information à l'échelle nationale, ainsi que la coopération transfrontalière à l'échelle de l'Union?	1	Avez-vous pris des dispositions pour assurer la continuité des services fournis par les infrastructures d'information critiques? Par exemple, l'anticipation des crises, les procédures de reconstruction des systèmes d'information critiques, la continuité des activités sans informatique, les procédures de sauvegarde par isolement physique, etc.	0		
11 – Protéger l'infrastructure d'information critique, les OSE et les FSN	10					Définissez-vous des mesures de base en matière de cybersécurité (obligations ou lignes directrices) pour les fournisseurs de services numériques et tous les secteurs identifiés dans l'annexe II de la directive SRI (2016/1148)?	1				
	11	-		-		Fournissez-vous des outils ou des méthodologies de détection des cyberincidents?	1	-		-	
	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
12 – Lutter contre la cybercriminalité	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
12 – Lutter contre la cybercriminalité	1	Avez-vous réalisé une étude pour identifier les besoins en matière d'application de la loi (base juridique, ressources, compétences, etc.) pour lutter efficacement contre la cybercriminalité?	1	Votre cadre juridique national est-il pleinement conforme au cadre juridique européen pertinent, y compris la directive 2013/40/UE relative aux attaques contre les systèmes d'information? Par exemple, en matière d'accès illégal aux systèmes d'information, d'atteinte illégale à l'intégrité d'un système ou de données, d'interception illégale, d'outils utilisés pour commettre des infractions, etc.	1	Disposez-vous d'unités dédiées à la lutte contre la cybercriminalité dans les parquets?	1	Recueillez-vous des statistiques conformément aux dispositions de l'article 14, paragraphe 1, de la directive 2013/40/UE (directive relative aux attaques contre les systèmes d'information)?	1	Disposez-vous d'une formation interinstitutionnelle ou d'ateliers de formation pour les AR, les juges, les procureurs et les CSIRT nationaux/gouvernementaux à l'échelle nationale et/ou multilatérale?	1
	2	Avez-vous réalisé une étude pour identifier les besoins des procureurs et des juges (base juridique, ressources, compétences, etc.) pour lutter efficacement contre la cybercriminalité?	1	Avez-vous des dispositions légales concernant le vol d'identité en ligne et le vol de données personnelles?	1	Disposez-vous d'un budget dédié aux unités de lutte contre la cybercriminalité?	1	Recueillez-vous des statistiques distinctes sur la cybercriminalité? Par exemple, des statistiques opérationnelles, des statistiques sur les tendances de la cybercriminalité, des statistiques sur les produits de la cybercriminalité et les dommages causés, etc.	1	Participez-vous à des actions coordonnées à l'échelle internationale pour mettre fin aux activités criminelles? Par exemple, l'infiltration de forums de piratage, de groupes de cybercriminalité organisés, de marchés du dark web, et le démantèlement de réseaux de machines zombies, etc.	1
	3	Votre pays a-t-il signé la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe?	1	Avez-vous des dispositions légales concernant les atteintes au droit d'auteur et à la propriété intellectuelle en ligne?	1	Avez-vous créé un organisme central/une entité centrale pour coordonner les activités dans le domaine de la lutte contre la cybercriminalité?	1	Évaluez-vous l'adéquation de la formation donnée au personnel des AR, aux magistrats et au personnel des CSIRT nationaux pour lutter contre la cybercriminalité?	1	Y a-t-il une séparation claire des tâches entre les CSIRT, les AR et le pouvoir judiciaire (procureurs et juges) lorsqu'ils coopèrent dans la lutte contre la cybercriminalité?	1
	4			Avez-vous pris des dispositions légales concernant le harcèlement en ligne?	1	Avez-vous mis en place des mécanismes de coopération entre les institutions nationales pertinentes impliquées dans la lutte contre la cybercriminalité, y compris les CSIRT nationaux des forces de l'ordre?	1	Effectuez-vous des évaluations régulières pour vous assurer que vous disposez de ressources suffisantes (effectifs, budget et outils) dédiées aux unités de lutte contre la cybercriminalité au sein des AR?	1	Votre cadre réglementaire facilite-t-il la coopération entre les CSIRT/les forces de l'ordre et le pouvoir judiciaire (procureurs et juges)?	1
	5			Avez-vous pris des dispositions légales concernant la fraude informatique? Par exemple, le respect des dispositions de la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe.	1	Coopérez-vous et partagez-vous les informations avec d'autres États membres dans le domaine de la lutte contre la cybercriminalité?	1	Effectuez-vous des évaluations régulières pour vous assurer que vous disposez de ressources suffisantes (effectifs, budget et outils) dédiées aux unités de lutte contre la cybercriminalité au sein des autorités judiciaires?	1	Participez-vous à l'élaboration et à la maintenance d'outils et de méthodologies, de formulaires et de procédures standardisés à partager avec les parties prenantes de l'UE (AR, CSIRT, ENISA, EC3 d'Europol, etc.)?	1
	6	-		Avez-vous pris des dispositions légales concernant la protection	1	Coopérez-vous et partagez-vous les informations avec les agences	1	Disposez-vous d'unités de tribunaux spécialisées ou de juges	1	Avez-vous mis en place des mécanismes avancés pour	0

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
				de l'enfance en ligne? Par exemple, le respect des dispositions de la directive 2011/93/UE et de la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe.		européennes (par exemple, EC3 d'Europol, Eurojust, ENISA) dans le domaine de la lutte contre la cybercriminalité?		spécialisés pour traiter les affaires de cybercriminalité?		dissuader les individus de se laisser attirer par la cybercriminalité ou d'y participer?	
	7	-		Avez-vous identifié un point de contact national opérationnel pour échanger des informations et répondre aux demandes d'informations urgentes des autres États membres concernant les infractions spécifiées dans la directive 2013/40/UE (directive relative aux attaques contre les systèmes d'information)?	1	Disposez-vous des outils adéquats pour lutter contre la cybercriminalité? Par exemple, taxonomie et classification de la cybercriminalité, outils de collecte de preuves électroniques, outils d'investigation informatique, plates-formes de partage de confiance, etc.	1	Avez-vous pris des dispositions dédiées au soutien et à l'assistance aux victimes de la cybercriminalité (utilisateurs généraux, PME, grandes entreprises)?	1	Votre pays utilise-t-il le plan d'action et/ou le Law Enforcement Emergency Response Protocol (LE ERP) de l'UE pour réagir efficacement en cas de cyberincidents de grande envergure?	0
	8			Votre agence répressive dispose-t-elle d'une unité spécialisée dans la cybercriminalité?	1	Disposez-vous de procédures opérationnelles permanentes pour traiter les preuves électroniques?	1	Avez-vous établi un cadre interinstitutionnel et des mécanismes de coopération entre toutes les parties prenantes pertinentes (par exemple, les AR, les CSIRT nationaux, les communautés judiciaires), y compris le secteur privé (par exemple, les opérateurs de services essentiels, les fournisseurs de services) le cas échéant, pour répondre aux cyberattaques?	1	-	
	9			Avez-vous désigné, conformément à l'art. 35 de la Convention de Budapest, un point de contact joignable 24 heures sur 24, 7 ours sur 7?	1	Votre pays participe-t-il aux formations proposées et/ou soutenues par les agences européennes (par exemple, Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Votre cadre réglementaire facilite-t-il la coopération entre les CSIRT et les forces de l'ordre?	1	-	
12 – Lutter contre la cybercriminalité	10	-		Avez-vous désigné un point de contact national opérationnel 24 heures sur 24 et 7 jours sur 7 pour le Law Enforcement Emergency Response Protocol (LE ERP) de l'UE afin de répondre aux cyberattaques majeures?	1	Votre pays envisage-t-il d'adopter le 2e protocole additionnel à la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe?	0	Avez-vous mis en place des mécanismes (par exemple, des outils, des procédures) pour faciliter l'échange d'informations et la coopération entre les CSIRT/les forces de l'ordre et éventuellement le pouvoir judiciaire (procureurs et juges) dans le domaine de la lutte contre la cybercriminalité?	1	-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
	11			Proposez-vous régulièrement des formations spécialisées aux parties prenantes impliquées dans la lutte contre la cybercriminalité (AR, pouvoir judiciaire, CSIRT)? Par exemple, des sessions de formation sur le dépôt d'une plainte et la poursuite des infractions facilitées par les TIC, des formations sur la collecte de preuves électroniques et la garantie de l'intégrité tout au long de la chaîne de possession, et des formations en investigation informatique, entre autres.	1						
	12			Votre pays a-t-il adhéré à/ratifié la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe?	1			-	-	-	
	13	-		Votre pays a-t-il signé et ratifié le protocole additionnel (visant à considérer comme criminels les actes de nature raciste et xénophobe commis par le biais de systèmes informatiques) à la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe?	0	-	-	-		-	
13 – Mettre en place des mécanismes de signalement des incidents	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Disposez-vous de mécanismes informels de partage	1	Disposez-vous d'un système de notification des incidents pour	1	Disposez-vous d'un système de notification des incidents	1	Disposez-vous d'une procédure harmonisée pour les systèmes de	1	Créez-vous un rapport annuel sur les incidents?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
		d'informations sur les incidents de cybersécurité entre les organisations privées et les autorités nationales?		tous les secteurs visés à l'annexe II de la directive SRI?		obligatoire qui fonctionne dans la pratique?		notification des incidents sectoriels?			
	2	-		Avez-vous mis en œuvre les obligations de notification pour les fournisseurs de services de télécommunication conformément à l'article 40 de la directive (UE 2018/1972)? La directive exige des États membres qu'ils veillent à ce que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public notifient sans retard indu à l'autorité compétente tout incident de sécurité ayant eu un impact significatif sur le fonctionnement des réseaux ou des services.	1	Existe-t-il un mécanisme de coordination/coopération pour les obligations de notification des incidents conformément au RGPD, à la directive SRI, à l'article 40 (ex-art. 13 *bis*) et à l'eIDAS?	1	Disposez-vous d'un système de notification des incidents pour les secteurs non visés par la directive SRI?	1	L'entité qui reçoit les rapports d'incident a-t-elle l'habitude de rédiger des rapports sur le paysage de la cybersécurité ou prépare-t-elle d'autres types d'analyses?	1
13 – Mettre en place des mécanismes de signalement des incidents	3	-		Avez-vous mis en œuvre les obligations de notification pour les prestataires de services de confiance conformément à l'article 19 du règlement eIDAS [(UE) nº 910/2014]? L'article 19 exige, entre autres, que les prestataires de services de confiance notifient à l'organe de contrôle les incidents/infractions importants.	1	Disposez-vous des outils adéquats pour assurer la confidentialité et l'intégrité des informations partagées par les différents canaux de notification?	1	Mesurez-vous l'efficacité des procédures de notification des incidents? Par exemple, indicateurs sur les incidents qui ont été notifiés par les canaux appropriés, timing du rapport d'incident.	1	-	
	4	-		Avez-vous mis en œuvre les obligations de notification pour les fournisseurs de services numériques conformément à l'article 16 de la directive SRI? L'article 16 exige que les fournisseurs de services numériques notifient sans retard indu à l'autorité compétente ou au CSIRT national tout incident ayant un impact substantiel sur la fourniture d'un service visé à	1	Avez-vous une plate-forme/un outil pour faciliter le processus de notification?	0	Avez-vous une taxonomie commune à l'échelle nationale pour la classification des incidents et les catégories de causes profondes?	0	-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
				l'annexe III qu'ils offrent au sein de l'Union.							
14 – Renforcer la protection de la vie privée et des données	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous réalisé des études ou des analyses pour identifier les domaines d'amélioration afin de mieux protéger le droit à la vie privée des citoyens?	1	L'autorité nationale chargée de la protection des données est-elle impliquée dans les domaines liés à la cybersécurité (par exemple, élaboration de nouvelles lois et réglementations en matière de cybersécurité, définition de mesures de sécurité minimales)?	1	Faites-vous la promotion des meilleures pratiques en matière de mesures de sécurité et de protection des données dès la conception à l'intention du secteur public et/ou privé?	1	Effectuez-vous des évaluations régulières pour vous assurer que vous disposez de ressources suffisantes (effectifs, budget et outils) dédiées à l'autorité chargée de la protection des données?	1	Avez-vous mis en place des mécanismes pour suivre les dernières évolutions technologiques afin d'adapter les lignes directrices et les dispositions/obligations légales pertinentes?	1
	2	Avez-vous développé une base juridique à l'échelle nationale pour faire appliquer le règlement général sur la protection des données (règlement UE nº 2016/679)? Par exemple, assurer la maintenance du règlement ou introduire des dispositions ou des limitations plus spécifiques aux règles du RGPD.	0	-		Organisez-vous des programmes de sensibilisation et de formation autour de ce sujet?	1	Encouragez-vous les organisations et les entreprises à se faire certifier selon la norme ISO/CEI 27701:2019 sur le système de management de la protection de la vie privée (PIMS)?	1	Participez-vous activement à des initiatives de R&D concernant les technologies de protection de la vie privée (PET) ou en faites-vous la promotion?	0
	3	-		-		Coordonnez-vous les procédures de notification des incidents avec l'APD?	1	-		-	
	4	-		-		Encouragez-vous et soutenez-vous le développement de normes techniques sur la sécurité de l'information et la protection de la vie privée? Sont-elles spécifiquement adaptées aux petites et moyennes entreprises (PME)?	0	-		-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
	5	-		-		Fournissez-vous des lignes directrices pratiques et évolutives pour aider les différents types de responsables du traitement des données à respecter les exigences et obligations légales en matière de vie privée et de protection des données?	0	-		-	

4.1.4 Groupe nº 4: Coopération

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
15 – Établir un partenariat public-privé (PPP)	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Est-il généralement admis que les PPP contribuent à augmenter le niveau de cybersécurité dans le pays par différents moyens? Par exemple, en partageant les intérêts dans la croissance de l'industrie de la cybersécurité, en coopérant à la mise en place d'un cadre réglementaire pertinent en matière de cybersécurité, en favorisant la R&D, etc.	1	Avez-vous un plan d'action national pour la mise en place de PPP?	1	Avez-vous établi des partenariats public-privé nationaux?	1	Avez-vous établi des PPP intersectoriels?	1	En fonction des dernières évolutions technologiques et réglementaires, êtes-vous en mesure d'adapter ou de créer des PPP?	1
	2	-		Établissez-vous une base juridique ou contractuelle (lois spécifiques, accords de confidentialité, propriété intellectuelle) dans le cadre des PPP?	1	Avez-vous établi des PPP spécifiques à certains secteurs?	1	Dans les PPP établis, vous concentrez-vous également sur la coopération public-public et privé-privé?	1		
	3	-		-		Fournissez-vous un financement pour la mise en place de PPP?	1	Faites-vous la promotion des PPP auprès des petites et moyennes entreprises (PME)?	1	-	
	4	-		-		Les institutions publiques dirigent-elles l'ensemble des PPP? À savoir: un point de contact unique du secteur public dirige et coordonne les PPP, les organismes publics s'entendent à l'avance sur ce qu'ils veulent réaliser, les administrations publiques donnent des directives	1	Mesurez-vous les résultats des PPP?	1	-	

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
						claires sur leurs besoins et limitations au secteur privé, etc.					
	5	-		-		Êtes-vous membre du partenariat public-privé contractuel (PPPc) de l'Organisation européenne pour la cybersécurité (ECSO)?	0	-		-	
	6	-		-		Avez-vous un ou plusieurs PPP qui travaillent sur les activités du CSIRT?	0	-		-	
15 – Établir un partenariat public-privé (PPP)	7					Avez-vous un ou plusieurs PPP qui travaillent sur les questions de protection des infrastructures d'information critiques?	0				
	8	-		-		Avez-vous un ou plusieurs PPP qui travaillent à la sensibilisation à la cybersécurité et au développement des compétences?	0	-		-	
	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
16 – Institutionnaliser la coopération entre les organismes publics	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Disposez-vous de canaux de coopération informels entre les organismes publics?	1	Avez-vous un programme national de coopération axé sur la cybersécurité? Par exemple, des comités consultatifs, des groupes de pilotage, des forums, des conseils, des cybercentres ou des groupes de réunion d'experts.	1	Les autorités publiques participent-elles au programme de coopération?	1	Assurez-vous que des canaux de coopération dédiés à la cybersécurité existent au moins entre les organismes publics suivants: services de renseignements, forces de l'ordre nationales, autorités judiciaires, acteurs gouvernementaux, CSIRT national et armée?	1	Les organismes publics disposent-ils d'un minimum d'informations uniformes sur les dernières évolutions du paysage de la menace et d'une conscience situationnelle en matière de cybersécurité?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
	2	-		-		Avez-vous mis en place des plates-formes de coopération pour l'échange d'informations?	1	Mesurez-vous les succès et les limites des différents programmes de coopération pour favoriser une coopération efficace?	1	-	
16 – Institutionnaliser la coopération entre les organismes publics	3	-		-		Avez-vous défini le périmètre des plates-formes de coopération (par exemple, les tâches et les responsabilités, le nombre de domaines d'intervention)?	1	-		-	
	4	-		-		Organisez-vous des réunions annuelles?	1	-		-	
	5	-		-		Disposez-vous de mécanismes de coopération entre les autorités compétentes à travers les régions géographiques? Par exemple, un réseau de correspondants de sécurité par région, un responsable de la cybersécurité dans les chambres économiques régionales, etc.	1	-		-	
17 – S'engager dans la coopération internationale (pas seulement avec les États membres de l'UE)	a	Couvrez-vous l'objectif dans votre SNCS actuelle ou prévoyez-vous de le couvrir dans la prochaine édition?	1	Existe-t-il des pratiques ou des activités informelles qui contribuent à atteindre l'objectif de manière non coordonnée?	1	Avez-vous un plan d'action formellement défini et documenté?	1	Examinez-vous votre plan d'action afin de tester sa performance en lien avec l'objectif?	1	Avez-vous mis en place des mécanismes pour garantir l'adaptation dynamique du plan d'action aux évolutions de l'environnement?	1
	b			Avez-vous défini les résultats escomptés, les principes directeurs ou les activités clés de votre plan d'action?	1	Avez-vous un plan d'action décrivant clairement l'affectation des ressources et la gouvernance?	1	Examinez-vous votre plan d'action afin de vous assurer qu'il est correctement optimisé et que des priorités adéquates sont établies par rapport à l'objectif?	1		
	c			Le cas échéant, votre plan d'action est-il mis en œuvre et a-t-il déjà donné des résultats de portée limitée?	0						
	1	Avez-vous une stratégie d'engagement international?	1	Avez-vous des accords de coopération avec d'autres pays (bilatéraux, multilatéraux) ou des partenaires dans d'autres pays? Par exemple, partage d'information, renforcement des capacités, assistance, etc.	1	Échangez-vous des informations au niveau stratégique? Par exemple, politique de haut niveau, perception des risques...	1	Les organismes publics nationaux de cybersécurité de votre pays sont-ils impliqués dans des programmes de coopération internationale?	1	Dirigez-vous des discussions sur un ou plusieurs sujets dans le cadre d'accords multilatéraux?	1

Objectif de la SNCS	#	Niveau 1	B	Niveau 2	B	Niveau 3	B	Niveau 4	B	Niveau 5	B
17 – S'engager dans la coopération internationale (pas seulement avec les États membres de l'UE)	2	Disposez-vous de canaux de coopération informels avec d'autres pays?	1	Disposez-vous d'un point de contact unique pouvant exercer une fonction de liaison pour assurer la coopération transfrontalière avec les autorités des États membres (groupe de coopération, réseau des CSIRT, etc.)?	1	Échangez-vous des informations au niveau tactique? Par exemple, bulletin des acteurs de la menace, les ISAC, les TTP, etc.	1	Évaluez-vous régulièrement les résultats des initiatives de coopération internationale?	1	Dirigez-vous des discussions sur un ou plusieurs sujets dans le cadre de traités ou de conventions internationaux?	1
	3	Les dirigeants publics ont-ils fait part de leur intention de s'engager dans la coopération internationale dans le domaine de la cybersécurité?	1	Disposez-vous de personnel qui se consacre à la cybersécurité et qui participe à la coopération internationale?	1	Échangez-vous des informations au niveau opérationnel? Par exemple, coordination des informations opérationnelles, incidents en cours, indicateurs de compromission, etc.	1	-		Dirigez-vous des discussions ou des négociations sur un ou plusieurs sujets au sein de groupes d'experts internationaux? Par exemple, Commission mondiale sur la stabilité du cyberespace (GCSC), groupe de coopération SRI de l'ENISA, Groupe d'experts gouvernementaux (GGE) des Nations unies sur la sécurité de l'information, etc.	1
	4	-		-		Participez-vous à des exercices de cybersécurité internationaux?	1	-		-	
	5	-		-		Participez-vous à des initiatives internationales de renforcement des capacités? Par exemple, formations, développement des compétences, rédaction de procédures standard, etc.	0	-		-	
	6	-		-		Avez-vous établi des accords d'assistance mutuelle avec d'autres pays? Par exemple, activités des AR, procédures judiciaires, mise en commun des capacités de réponse aux incidents, partage des actifs de cybersécurité, etc.	0	-		-	
	7	-		-		Avez-vous signé ou ratifié des traités ou conventions internationaux dans le domaine de la cybersécurité? Par exemple, le Code de conduite international pour la sécurité de l'information et la Convention sur la cybercriminalité.	0	-		-	

4.2 COMMENT UTILISER LE CADRE?

Cette section vise à fournir aux États membres des orientations et des recommandations pour déployer le cadre et remplir le questionnaire. Les recommandations énumérées ci-dessous sont principalement issues des commentaires recueillis lors des entretiens avec les représentants des États membres:

- **Anticipez les activités de coordination pour recueillir les données et les consolider.** La plupart des États membres s'accordent à dire que la réalisation d'un tel exercice d'autoévaluation devrait prendre environ 15 jours-personnes. Afin de réaliser l'autoévaluation, il faudra solliciter un large éventail de parties prenantes. Il est donc recommandé de prévoir du temps pour la phase de préparation afin d'identifier toutes les parties prenantes pertinentes au sein des organismes gouvernementaux, des agences publiques et du secteur privé.
- **Identifiez un organisme central chargé de réaliser l'autoévaluation à l'échelle nationale.** Étant donné que la collecte de données pour tous les indicateurs du CECN peut impliquer de nombreuses parties prenantes, il est recommandé d'avoir un organisme central ou une agence centrale qui se charge de réaliser l'autoévaluation ainsi que d'assurer la liaison entre et la coordination avec toutes les parties prenantes pertinentes.
- **Utilisez l'exercice d'évaluation comme un moyen de partager et de communiquer sur les sujets de cybersécurité.** Les enseignements tirés par les États membres ont montré que les discussions (qu'elles prennent la forme d'entretiens individuels ou d'ateliers collectifs) sont une bonne occasion de favoriser le dialogue autour des thèmes de la cybersécurité et de partager les points de vue communs et les domaines d'amélioration. En plus de mettre en lumière les principales réalisations, le partage des résultats peut également contribuer à promouvoir les thèmes liés à la cybersécurité.
- **Utilisez la SNCS comme cadre pour sélectionner les objectifs soumis à l'évaluation.** Les 17 objectifs qui composent le CECN ont été construits sur la base des objectifs communément couverts par les États membres dans leur SNCS. Les objectifs couverts dans le cadre de la SNCS doivent être utilisés pour déterminer la portée de l'évaluation. Toutefois, la SNCS ne doit pas limiter l'évaluation. La SNCS se concentrant naturellement sur les priorités, certains domaines y sont donc délibérément omis. Cela n'implique cependant pas qu'une capacité donnée ne soit pas présente. Par exemple, dans le cas où un objectif spécifique est omis de la SNCS, mais où le pays dispose de capacités de cybersécurité liées à cet objectif, l'évaluation de cet objectif peut avoir lieu.
- **Lorsque la portée de la SNCS évolue, assurez-vous que l'interprétation du score reste cohérente avec l'évolution de la SNCS.** Le cycle de vie de la SNCS s'étend sur plusieurs années. Généralement, les SNCS des États membres sont mises en œuvre avec une feuille de route portant sur trois à cinq ans, et le champ des thématiques couvertes varie entre deux éditions successives de la SNCS. Sachant cela, un soin particulier doit être apporté lors de la présentation des résultats de l'autoévaluation entre deux éditions de la SNCS: des changements de portée peuvent en effet avoir un impact sur le score de maturité final. Il est recommandé de comparer les scores sur l'ensemble des objectifs stratégiques d'une année à l'autre (donc de comparer les scores généraux globaux).

Rappel sur le mécanisme des scores – exemple concernant le taux de couverture
Le mécanisme des scores comprend deux niveaux de scores:
(i) **un taux de couverture général global** basé sur la liste complète des objectifs stratégiques présents dans le cadre d'autoévaluation; et
(ii) **un taux de couverture spécifique global** basé sur des objectifs stratégiques sélectionnés par l'État membre (correspondant généralement aux objectifs présents dans la SNCS du pays concerné).

De par sa conception (cf. section 3.1 sur le mécanisme des scores), le taux de couverture spécifique global sera égal ou supérieur au taux de couverture général global, car ce dernier peut inclure des objectifs qui ne sont pas couverts par l'État membre, ce qui réduit son score. Lorsqu'un État membre ajoute un nouvel objectif, le taux de couverture global augmente (c'est-à-dire que davantage d'indicateurs de maturité sont couverts), tandis que la maturité spécifique globale peut diminuer (dans le cas où l'objectif ajouté est à un stade initial et a donc un faible niveau de maturité).

- **Lorsque vous remplissez le questionnaire d'autoévaluation, gardez à l'esprit que l'objectif premier est de soutenir les États membres dans le renforcement des capacités en matière de cybersécurité.** Par conséquent, lorsque vous remplissez l'autoévaluation, même s'il peut parfois être difficile de répondre à la question de manière catégorique, il est recommandé de choisir la réponse la plus généralement acceptée. Si, par exemple, la réponse à une question est OUI sur un certain champ d'application mais NON sur un autre, les États membres doivent garder à l'esprit qu'une réponse négative nécessite une action: soit un plan de remédiation, soit un plan d'action sur un domaine d'amélioration devant être pris en compte dans les développements futurs.

5. PROCHAINES ÉTAPES

5.1 AMÉLIORATIONS À VENIR

Au cours des entretiens avec les représentants des États membres et pendant la phase de recherche documentaire, les recommandations suivantes visant à améliorer le cadre actuel d'évaluation des capacités nationales ont également été identifiées comme des évolutions futures potentielles:

- **Développer le mécanisme des scores pour permettre une plus grande précision.** Par exemple, un pourcentage de couverture pourrait être introduit au lieu de la réponse binaire OUI/NON afin de prendre en compte la complexité de la consolidation des capacités à l'échelle nationale. Dans un premier temps, une approche simple avec des réponses OUI/NON a été choisie.
- **Introduire des mesures quantitatives pour évaluer l'efficacité des SNCS des États membres.** En effet, le cadre d'évaluation des capacités nationales se concentre sur la mesure du niveau de maturité des capacités de cybersécurité des États membres. Cette approche pourrait être complétée par des mesures permettant d'évaluer l'efficacité des activités et des plans d'action mis en œuvre par les États membres pour renforcer ces capacités. Il ne semblait pas réaliste de mettre au point de tels indicateurs d'efficacité au stade actuel, étant donné le peu de retour d'information du terrain, la difficulté à trouver des indicateurs significatifs faisant le lien entre les résultats et la mise en œuvre de la SNCS, et la difficulté de concevoir des indicateurs réalistes pouvant être rassemblés par la suite. Cependant, cela reste un sujet sur lequel nous devrons travailler à l'avenir.
- **Passer d'un exercice d'autoévaluation à une approche d'évaluation.** Une évolution future potentielle du cadre pourrait être le passage à une approche d'évaluation afin d'évaluer la maturité des capacités de cybersécurité des États membres de manière plus cohérente. Le fait de confier l'évaluation à une tierce partie pourrait en effet permettre de réduire au maximum les biais potentiels.

ANNEXE A – VUE D'ENSEMBLE DES RÉSULTATS DE LA RECHERCHE DOCUMENTAIRE

L'Annexe A fournit un résumé des travaux antérieurs de l'ENISA sur les SNCS et un examen des modèles de maturité pertinents mis à la disposition du public en matière de capacités de cybersécurité. Les hypothèses suivantes sont prises en compte pour la sélection et l'examen des modèles:

- Tous les modèles ne sont pas basés sur une méthodologie de recherche rigoureuse;
- La structure et les résultats des modèles ne sont pas toujours expliqués en détail avec des liens clairs entre les différents éléments caractérisant chaque modèle;
- Certains modèles ne donnent pas de détails sur le processus de développement, la structure et la méthode d'évaluation;
- Les autres modèles et outils que nous avons trouvés ne donnent aucun détail concernant la structure et le contenu et ne sont donc pas répertoriés; et
- La sélection des modèles à examiner est basée sur la couverture géographique. L'accent sera principalement mis sur les modèles de maturité évaluant les capacités de cybersécurité construits pour mesurer la performance des pays européens. Cependant, il est important d'étendre la couverture géographique pour analyser les bonnes pratiques en matière d'élaboration de modèles de maturité dans le monde entier.

Cet examen systématique des modèles de maturité pertinents mis à la disposition du public en matière de capacités de cybersécurité a été réalisé en utilisant un cadre d'analyse sur mesure basé sur la méthodologie définie par Becker pour le développement des modèles de maturité[22]. Les éléments suivants ont été analysés pour chaque modèle de maturité existant:

- **Nom du modèle de maturité:** le nom du modèle de maturité et les principales références;
- **Institution à l'origine du modèle:** l'institution, publique ou privée, chargée de la mise au point du modèle;
- **Objectif général et cible:** la portée globale du modèle et la ou les cibles visées;
- **Nombre de niveaux et définition de ceux-ci:** le nombre de niveaux de maturité dans le modèle et leur description générale;
- **Nombre d'attributs et nom des attributs:** le nombre et le nom des attributs utilisés dans le modèle de maturité. L'analyse des attributs poursuit un objectif triple:
  - Décomposer le modèle de maturité en sections facilement compréhensibles;
  - Rassembler plusieurs attributs en groupes d'attributs répondant au même objectif; et
  - Fournir différents points de vue sur le sujet du niveau de maturité.
- **Méthode d'évaluation:** la méthode d'évaluation du modèle de maturité;

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application,» Business & Information Systems Engineering, vol. 1, nº 3, pp. 213–222, Juin 2009.

- **Représentation des résultats:** définir la méthode de visualisation des résultats du modèle de maturité. La logique qui sous-tend cette étape est que les modèles de maturité ne fonctionnent généralement pas s'ils sont trop complexes et que, par conséquent, le mode de représentation doit répondre à des besoins pratiques.

Travaux antérieurs sur les SNCS

En 2012, les premiers efforts de l'ENISA ont débouché sur la publication de deux documents au sujet des SNCS. Tout d'abord, le «Practical guide on the development and execution phase of NCSS»[23] propose un ensemble d'actions concrètes pour la mise en œuvre efficace d'une SNCS et présente le cycle de vie d'une SNCS en quatre phases: développement, exécution, évaluation et maintenance de la stratégie. Ensuite, un document intitulé «Setting the course for national efforts to strengthen security in cyberspace»[24] décrit l'état des stratégies de cybersécurité au sein de l'UE et au-delà en 2012 et propose aux États membres d'identifier les thèmes communs et les différences entre leurs SNCS.

Le premier cadre de l'ENISA pour l'évaluation de la SNCS d'un État membre a été publié en 2014[25]. Ce cadre contient des recommandations et des bonnes pratiques, ainsi qu'un ensemble d'outils de renforcement des capacités pour évaluer une SNCS (par exemple, les objectifs identifiés, les intrants, les résultats, les indicateurs clés de performance, etc.). Ces outils sont adaptés aux différents besoins des pays, qui en sont à différents niveaux de maturité dans leur planification stratégique. Toujours en 2014, l'ENISA a publié l'«Online NCSS Interactive Map»[26], qui permet aux utilisateurs de consulter rapidement les SNCS de tous les États membres et des pays de l'AELE, y compris leurs objectifs stratégiques et les bons exemples de mise en œuvre. Conçue dans un premier temps comme un répertoire des SNCS (2014), cette carte a été actualisée avec des exemples de mise en œuvre en 2018 et, depuis 2019, elle sert de *pôle d'information* pour centraliser les données fournies par les États membres sur leurs efforts de renforcement de la cybersécurité nationale.

Publié en 2016, le «NCSS Good Practice Guide»[27] identifie 15 objectifs stratégiques. Ce guide analyse également l'état d'avancement de la mise en œuvre de la SNCS de chaque État membre et identifie les diverses problématiques et lacunes de cette mise en œuvre.

En 2018, l'ENISA a ensuite publié le «National Cybersecurity Strategies Evaluation Tool»[28]: un outil d'autoévaluation interactif pour aider les États membres à évaluer leurs priorités et objectifs stratégiques en lien avec leur SNCS. Grâce à un ensemble de questions simples, cet outil fournit aux États membres des recommandations spécifiques pour la mise en œuvre de chaque objectif. Enfin, les «Good practices in innovation on Cybersecurity under the NCSS»[29] publiées en 2019 présentent le sujet de l'innovation en matière de cybersécurité dans le cadre des SNCS. Le document expose les problématiques et les bonnes pratiques dans les différentes

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, actualisée en 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Ce document est une mise à jour du guide de 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

dimensions de l'innovation, tels que perçues par les experts, afin d'aider à rédiger les futurs objectifs stratégiques innovants.

A.1 Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC)

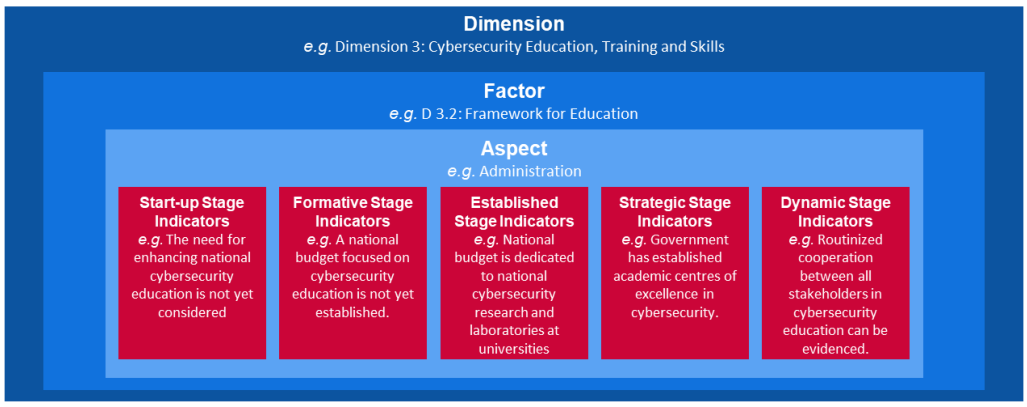
Le Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC) a été mis au point par le Centre de capacité de la cybersécurité mondiale (Capacity Centre), qui fait partie de l'Oxford Martin School au sein de l'Université d'Oxford. L'objectif du Capacity Centre est d'accroître l'échelle et l'efficacité du renforcement des capacités en matière de cybersécurité, tant au Royaume-Uni qu'ailleurs dans le monde, par le déploiement du Modèle de maturité des capacités en matière de cybersécurité (MMC). Le MMC s'adresse directement aux pays qui souhaitent accroître leur capacité nationale en matière de cybersécurité. Initialement déployé en 2014, le MMC a été révisé en 2016 suite à son utilisation dans l'examen de 11 capacités nationales de cybersécurité.

Attributs/Dimensions

Selon le MMC, la capacité de cybersécurité comprend **cinq dimensions**, qui représentent les groupes des capacités en matière de cybersécurité. Chaque groupe constitue un angle d'approche, d'étude et de compréhension différent des capacités en matière de cybersécurité. Dans les cinq dimensions, les **facteurs** décrivent les détails de la possession des capacités de cybersécurité. Ces détails sont des éléments qui contribuent à l'amélioration de la maturité des capacités de cybersécurité dans chaque dimension. Pour chaque facteur, plusieurs **aspects** représentent différentes composantes du facteur. Les aspects traduisent une méthode organisationnelle qui consiste à diviser les indicateurs en plus petits groupes plus faciles à comprendre. Chaque aspect est ensuite évalué au moyen d'**indicateurs** pour décrire les étapes, les actions ou les composantes qui indiquent un stade de maturité spécifique (défini dans la section suivante) dans un aspect, un facteur et une dimension distincts.

La figure ci-dessous montre la structure qui régit ces termes.

Figure 4: Exemple d'indicateurs du MMC



Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills

Factor
e.g. D 3.2: Framework for Education

Aspect
e.g. Administration

Dimension
p. ex. dimension 3: éducation, formation et compétences en matière de cybersécurité

Facteur
p. ex. D 3.2: cadre pour l'éducation

Aspect
p. ex. administration

Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Indicateurs de la phase de démarrage p. ex. le besoin de renforcer l'éducation nationale en matière de cybersécurité n'a pas encore été pris en considération
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Indicateurs de la phase de formation p. ex. un budget national axé sur l'éducation à la cybersécurité n'a pas encore été établi
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Indicateurs de la phase d'établissement p. ex. un budget national est consacré à la recherche nationale sur la cybersécurité et aux laboratoires des universités
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Indicateurs de la phase stratégique p. ex. le gouvernement a établi des centres d'excellence universitaires en matière de cybersécurité
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Indicateurs de la phase dynamique p. ex. on constate une coopération systématique entre toutes les parties prenantes de l'éducation à la cybersécurité

Les cinq dimensions sont détaillées ci-dessous:

i Concevoir la politique et la stratégie de cybersécurité (6 facteurs);
ii Encourager une culture de la cybersécurité responsable au sein de la société (5 facteurs);
iii Développer les connaissances en matière de cybersécurité (3 facteurs);
iv Créer des cadres juridiques et réglementaires efficaces (3 facteurs); et
v Maîtriser les risques au moyen de normes, d'organisations et de technologies (7 facteurs).

Niveaux de maturité

Le MMC utilise **cinq niveaux de maturité** pour déterminer dans quelle mesure un pays a progressé par rapport à un certain facteur/aspect des capacités de cybersécurité. Ces niveaux servent d'aperçu des capacités de cybersécurité existantes:

- **Démarrage**: à ce stade, soit il n'existe aucune maturité en matière de cybersécurité, soit elle en est à ses premiers balbutiements. Il se peut que des discussions initiales aient été entamées sur le renforcement des capacités de cybersécurité, mais aucune mesure concrète n'a été prise. Dans cette phase, on constate l'absence de preuves observables;
- **Formation**: certaines caractéristiques des aspects ont commencé à se développer et à être formulées, mais il se peut qu'elles restent ponctuelles, désorganisées, mal définies, ou qu'elles soient simplement «nouvelles». En revanche, la preuve de cette activité peut clairement être apportée;
- **Établissement**: les éléments de l'aspect sont en place et fonctionnent. Il n'y a cependant pas de réflexion approfondie quant à l'allocation relative des ressources. Peu de décisions de compromis ont été prises en ce qui concerne l'investissement «relatif» dans les divers éléments de l'aspect. L'aspect est toutefois fonctionnel et défini;
- **Stratégique**: des choix ont été faits quant aux parties de l'aspect qui sont importantes et moins importantes pour l'organisation ou le pays en question. La phase stratégique implique que ces choix ont été faits, en fonction des circonstances propres au pays ou à l'organisation; et
- **Dynamique**: dans cette phase, il existe des mécanismes clairs permettant de modifier la stratégie en fonction des circonstances du moment, comme la technologie de l'environnement de la menace, un conflit mondial ou un changement important dans un domaine de préoccupation (par exemple, la cybercriminalité ou la protection de la vie privée). Les organisations dynamiques ont développé des méthodes permettant de

modifier rapidement les stratégies. Cette phase se caractérise par une prise de décision rapide, la réaffectation des ressources et une attention constante portée à l'évolution de l'environnement.

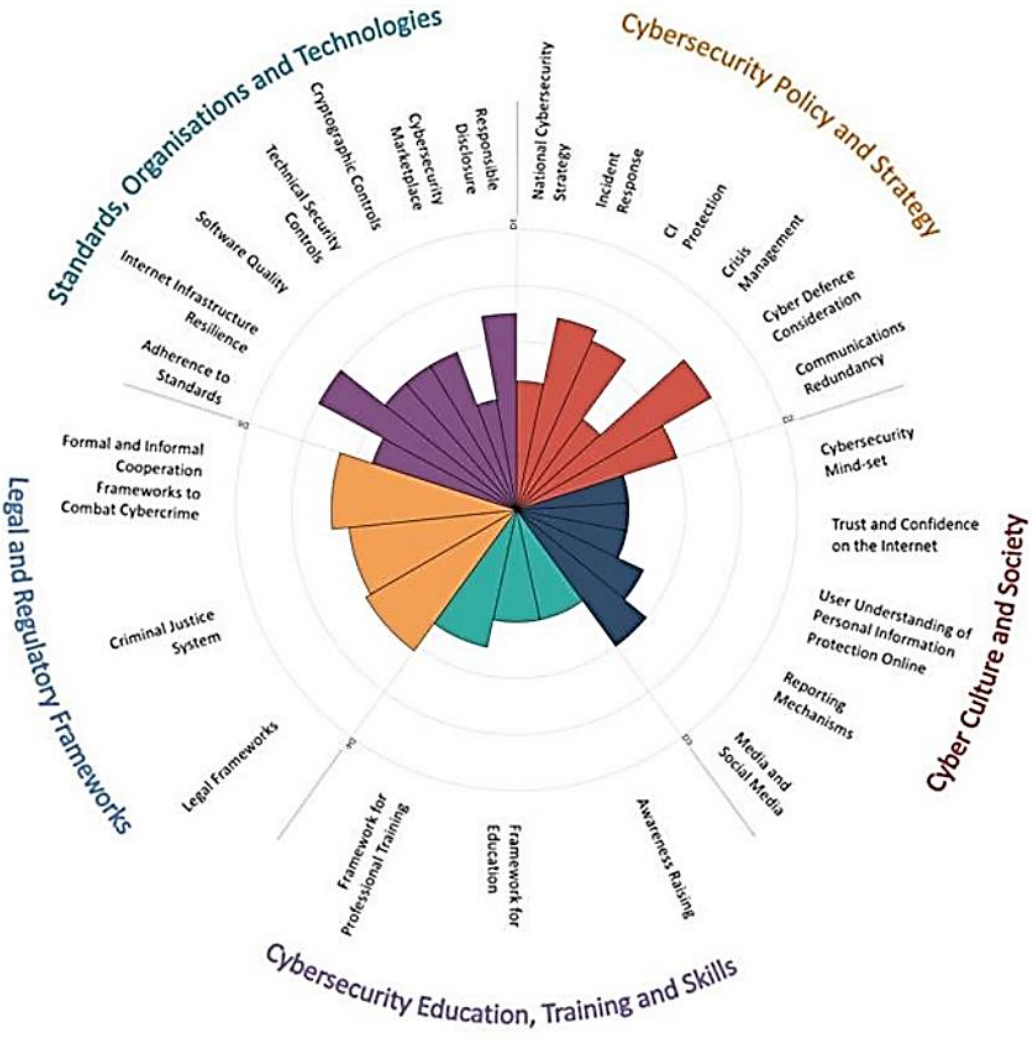
Méthode d'évaluation

Puisque le Capacity Centre n'a pas une compréhension approfondie et détaillée de chaque contexte national dans lequel le modèle est déployé, il travaille avec des organisations internationales ainsi que des ministères ou des organisations hôtes dans le pays concerné pour examiner la maturité des capacités de cybersécurité. Afin d'évaluer le niveau de maturité des cinq dimensions incluses dans le MMC, le Capacity Centre et l'organisation hôte rencontrent les parties prenantes nationales concernées des secteurs public et privé pendant deux ou trois jours et forment ainsi des groupes de discussion afin d'aborder les dimensions du MMC. Chaque dimension est abordée par au moins deux groupes de parties prenantes différents. Ce travail permet de récolter les données préliminaires qui serviront ensuite pour l'évaluation.

Mode de représentation des résultats

Le MMC fournit un aperçu du niveau de maturité de chaque pays au moyen d'un radar à cinq sections, une pour chaque dimension. Chaque dimension représente un cinquième du graphique, les cinq stades de maturité de chaque facteur s'étendant vers l'extérieur à partir du centre du graphique. Comme vous le voyez ci-dessous, la phase de démarrage est la plus proche du centre, tandis que la phase dynamique se situe au périmètre.

Figure 5 MMC: vue d'ensemble des résultats



Standards, Organisations and Technologies	Normes, organisations et technologies
Legal Regulatory Frameworks	Cadres juridique et réglementaire
Cybersecurity Education, Training and Skills	Éducation, formation et compétences en matière de cybersécurité
Cybersecurity Policy and Strategy	Politique et stratégie de cybersécurité
Cyber Culture and Society	Cyberculture et société
Responsible Disclosure	Divulgation responsable
Cybersecurity market place	Marché de la cybersécurité
Cryptographic Controls	Contrôles cryptographiques
Technical Security Controls	Contrôles de sécurité techniques
Software Quality	Qualité des logiciels
Internet Infrastructure Resilience	Résilience de l'infrastructure internet
Adherence to Standards	Respect des normes
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Cadres de coopération formels et informels pour lutter contre la cybercriminalité
Criminal Justice System	Système de justice pénale
Legal Frameworks	Cadres juridiques
Framework for Professional Training	Cadre pour la formation professionnelle
Framework for Education	Cadre pour l'éducation
Awareness Raising	Sensibilisation
Media and Social Medai	Médias et médias sociaux
Reporting Mechanisms	Mécanismes de signalement
User Understanding of Personal Information Protection Online	Compréhension par les utilisateurs de la protection des données personnelles en ligne
Trust and Confidence on the Internet	Confiance sur l'internet
Cybersecurity Mind-set	Esprit de la cybersécurité
Communications Redundancy	Redondance des communications

Cyber Defence Consideration	Prise en compte de la cyberdéfense
Crisis Management	Gestion de crise
CI Protection	Protection des IC
Incident Response	Réponse aux incidents
National Cybersecurity Strategy	Stratégie nationale de cybersécurité

Centre de capacité de la cybersécurité mondiale, Oxford Martin School, Université d'Oxford, 2017

A.2 Modèle de maturité des capacités en matière de cybersécurité (C2M2)

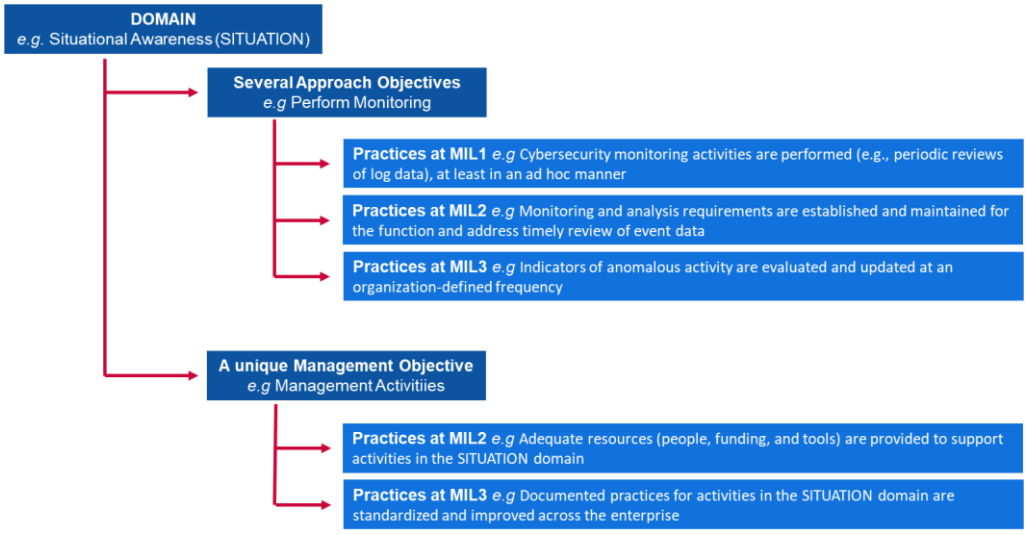
Le Modèle de maturité des capacités en matière de cybersécurité (C2M2) a été mis au point par le département américain de l'énergie en collaboration avec des experts des secteurs privé et public. L'objectif est d'aider les organisations de tous les secteurs, de tous types et de toutes tailles à évaluer leur programme de cybersécurité, à l'améliorer et à renforcer leur résilience opérationnelle. Le C2M2 se concentre sur la mise en œuvre et la gestion des pratiques de cybersécurité associées aux actifs liés à l'information, aux technologies de l'information (TI) et à la technologie opérationnelle (TO) ainsi qu'aux environnements dans lesquels ils évoluent. Le C2M2 définit les modèles de maturité comme suit: «un ensemble de caractéristiques, d'attributs, d'indicateurs ou de schémas types qui représentent les capacités et les progrès dans une discipline définie». Initialement déployé en 2014, le C2M2 a été révisé en 2019.

Attributs/Dimensions

Le C2M2 se penche sur **dix domaines**, qui sont le fruit du regroupement logique des pratiques de cybersécurité. Chaque ensemble de pratiques représente les activités qu'une organisation peut mettre en œuvre pour établir et faire évoluer les capacités dans le domaine. Chaque domaine est ensuite associé à un **objectif de gestion unique** et à **plusieurs objectifs d'approche**. Dans le cadre des objectifs tant d'approche que de gestion, **plusieurs pratiques** sont détaillées pour décrire les activités institutionnalisées.

La relation entre ces notions est résumée ci-dessous:

Figure 6: Exemple d'indicateur du C2M2



Domain eg Situational Awareness (SITUATION)	**Domaine** p. ex. conscience situationnelle (SITUATION)
Several Approaches Objectives e.g. Perform Monitoring	**Plusieurs objectifs d'approche** p. ex. effectuer un suivi
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Pratiques niveau 1 de l'indicateur de maturité (MIL1)** p. ex. des activités de suivi de la cybersécurité sont en place (p. ex. examens

périodiques des données de journal), au moins de manière ponctuelle

Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data

Pratiques MIL2 p. ex. les exigences en matière de suivi et d'analyse sont établies et font l'objet d'une maintenance pour la fonction; elles prévoient l'examen en temps voulu des données d'événement

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency

Pratiques MIL3 p. ex. les indicateurs d'activité anormale sont évalués et mis à jour à une fréquence déterminée par l'organisation

A unique Management Objectve e.g. Management Activities

Un objectif de gestion unique p. ex. activités de gestion

Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain

Pratiques MIL2 p. ex. des ressources adéquates (personnes, financement et outils) sont fournies pour soutenir les activités dans le domaine de la SITUATION

Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise

Pratiques MIL3 p. ex. des pratiques documentées pour les activités dans le domaine de la situation sont normalisées et améliorées dans toute l'entreprise

Les dix domaines sont détaillés ci-dessous:

i Gestion des risques (RISQUES);
ii Gestion des actifs, des changements et de la configuration (ACTIFS);
iii Gestion de l'identité et de l'accès (ACCÈS);
iv Gestion de la menace et des vulnérabilités (MENACE);
v Conscience situationnelle (SITUATION);
vi Réponse aux événements et incidents (RÉPONSE);
vii Gestion de la chaîne d'approvisionnement et des dépendances externes (DÉPENDANCES);
viii Gestion de la main-d'œuvre (MAIN-D'ŒUVRE);
ix Architecture de cybersécurité (ARCHITECTURE); et
x Gestion du programme de cybersécurité (PROGRAMME).

Niveaux de maturité

Le C2M2 utilise **quatre niveaux de maturité** (les «Maturity Indicator Levels, abrégés MIL) pour donner une double description de la progression de la maturité: progression de l'approche et progression de la gestion. Les MIL vont de MIL0 à MIL3 et sont destinés à être appliqués indépendamment à chaque domaine.

- **MIL0**: aucune pratique en place.
- **MIL1**: les premières pratiques sont en place, mais il se peut qu'elles restent ponctuelles.
- **MIL2**: caractéristiques de la gestion:
  - les pratiques sont documentées;
  - des ressources adéquates sont fournies pour soutenir le processus;
  - le personnel qui exécute les pratiques a les compétences et les connaissances appropriées; et
  - la responsabilité et l'autorité pour l'exécution des pratiques sont attribuées.

  Caractéristique de l'approche:
  - Les pratiques sont plus complètes ou plus avancées qu'au niveau MIL1.
- **MIL3**: caractéristiques de la gestion:
  - les activités sont guidées par des politiques (ou d'autres directives organisationnelles);
  - des objectifs de performance pour les activités du domaine sont établis et font l'objet d'un suivi pour contrôler les réalisations; et
  - les pratiques documentées pour les activités du domaine sont normalisées et améliorées dans toute l'entreprise.

  Caractéristique de l'approche:
  - les pratiques sont plus complètes ou plus avancées qu'au niveau MIL2.

Méthode d'évaluation

Le C2M2 est conçu pour être utilisé avec une **méthodologie d'autoévaluation** et une boîte à outils (disponible sur demande) pour permettre à une organisation de mesurer et d'améliorer son programme de cybersécurité. L'autoévaluation à l'aide de la boîte à outils prend une

journée, mais la boîte à outils peut être adaptée pour un effort d'évaluation plus rigoureux. De plus, le C2M2 peut être utilisé pour guider le développement d'un nouveau programme de cybersécurité.

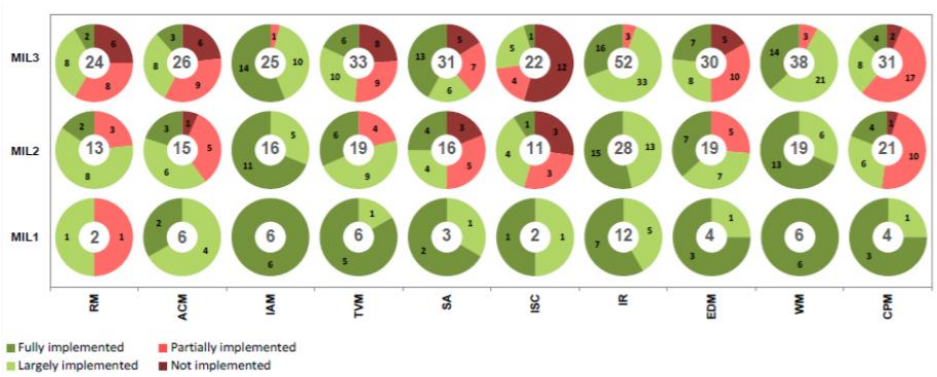
Le contenu du modèle est présenté à un haut niveau d'abstraction afin de pouvoir être interprété par des organisations de types, structures, tailles et secteurs d'activité divers. Une large utilisation de ce modèle par un secteur permet de procéder à l'évaluation comparative des capacités de cybersécurité dans ce secteur.

Mode de représentation des résultats

Le C2M2 fournit un rapport de notation d'évaluation généré à partir des résultats de l'enquête. Le rapport propose deux représentations des résultats: la vue Objectif, qui montre les réponses aux questions sur les pratiques pour chaque domaine et ses objectifs, et la vue Domaine, qui montre les réponses pour tous les domaines et les MIL. Les deux vues sont basées sur un système de représentation par graphiques circulaires («camemberts»), un par réponse, et un mécanisme des scores avec code couleur vert/rouge. Comme le montre la Figure 7, les secteurs rouges dans un graphique circulaire indiquent le nombre de questions de l'enquête pour lesquelles la réponse est «Non mis en œuvre» (rouge foncé) ou «Partiellement mis en œuvre» (rouge clair). Les secteurs verts indiquent le nombre de questions pour lesquelles la réponse est «Largement mis en œuvre» (vert clair) ou «Totalement mis en œuvre» (vert foncé).

La Figure 7 ci-dessous est un exemple de carte des scores à l'issue d'une évaluation de la maturité. Sur l'axe X, on trouve les dix domaines du C2M2, et sur l'axe Y, les niveaux de maturité (MIL). En regardant le domaine de la gestion des risques (GR) sur la carte des scores, on trouve trois graphiques circulaires, un pour chaque niveau de maturité, MIL1, MIL2 et MIL3. Pour le domaine GR, la carte des scores souligne qu'il y a deux éléments à évaluer pour atteindre le premier niveau de maturité, MIL1. Dans ce cas, un élément s'est vu attribuer le score «Largement mis en œuvre», tandis que l'autre est «Partiellement mis en œuvre». Pour le deuxième niveau de maturité, MIL2, le modèle prévoit l'évaluation de 13 éléments. Deux de ces 13 éléments appartiennent au premier niveau, MIL1, et 11 autres appartiennent au deuxième niveau, MIL2. Le même raisonnement s'applique au troisième niveau, MIL3.

Figure 7: C2M2 – exemple de la vue Domaine



Fully implemented	Totalement mis en œuvre
Largely implemented	Largement mis en œuvre
Partially implemented	Partiellement mis en œuvre
Not implemented	Non mis en œuvre
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	GR
ACM	GACC
IAM	GIA
TVM	GMV
SA	CS
ISC	ICA
IR	RI

EDM	GDE
WM	GM
CPM	GPC

Source: Département américain de l'énergie, Bureau de la fourniture d'électricité et de la fiabilité énergétique, 2015.

A.3 Cadre pour l'amélioration de la cybersécurité des infrastructures critiques

Le cadre pour l'amélioration de la cybersécurité des infrastructures critiques a été conçu au sein de l'Institut national des normes et des technologies (NIST). Il se concentre sur l'orientation des activités de cybersécurité et la gestion des risques au sein d'une organisation. Il s'adresse à tous les types d'organisations, quels que soient leur taille et leur degré de risque ou de sophistication en matière de cybersécurité. Dans la mesure où il s'agit d'un cadre et non d'un modèle, il est construit différemment des modèles analysés précédemment.

Le cadre se compose de trois parties: le noyau, les tranches de mise en œuvre et les profils:

- Le **noyau du cadre** est un ensemble d'activités liées à la cybersécurité, de résultats souhaités et de références applicables qui sont communs à tous les secteurs des infrastructures critiques. Ces éléments sont similaires aux attributs ou dimensions que l'on trouve dans les modèles de maturité des capacités de cybersécurité.
- Les **tranches de mise en œuvre** fournissent du contexte quant à la manière dont une organisation envisage le risque lié à la cybersécurité et les processus en place pour gérer ce risque. Allant de partiel (tranche 1) à adaptatif (tranche 4), les tranches décrivent un degré croissant de rigueur et de sophistication dans les pratiques de gestion du risque lié à la cybersécurité. Les tranches ne représentent pas des niveaux de maturité, mais sont plutôt destinées à soutenir la prise de décision organisationnelle sur la façon de gérer le risque lié à la cybersécurité, ainsi que sur les dimensions de l'organisation qui sont plus prioritaires et qui pourraient bénéficier de ressources supplémentaires.
- Un **profil** représente les résultats basés sur les besoins de l'entreprise que cette dernière a sélectionnés parmi les catégories et sous-catégories du cadre. Le profil reflète l'adéquation des normes, lignes directrices et pratiques par rapport au noyau du cadre dans un scénario de mise en œuvre particulier. Les profils peuvent être utilisés pour identifier les possibilités d'amélioration de la posture de cybersécurité en comparant un profil «actuel» (l'état «as is») avec un profil «cible» (l'état «to be»).

Noyau du cadre

Le noyau du cadre se compose de cinq **fonctions**. Considérées ensemble, ces fonctions fournissent une vision stratégique de haut niveau du cycle de vie de la gestion des risques de cybersécurité d'une organisation. Le noyau du cadre identifie ensuite les **catégories** et **sous-catégories** clés sous-jacentes pour chaque fonction et les associe à des références données à titre d'information telles que les normes, lignes directrices et pratiques existantes pour chaque sous-catégorie.

Les fonctions et catégories sont détaillées ci-dessous:

i **Identifier**: développer une compréhension organisationnelle sur la façon de gérer les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités.
   - Sous-catégories: gestion des actifs; environnement de l'entreprise; gouvernance; évaluation des risques; et stratégie de gestion des risques.

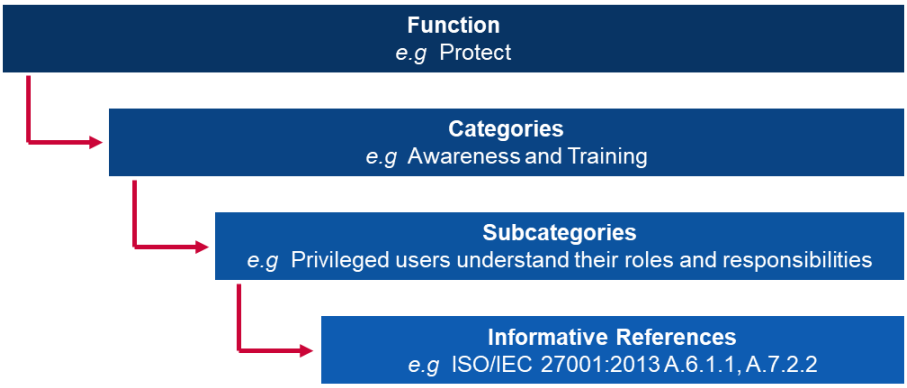
ii **Protéger**: élaborer et mettre en œuvre des mesures de protection appropriées pour assurer la fourniture des services essentiels.
   - Sous-catégories: gestion de l'identité et de l'accès; sensibilisation et formation; sécurité des données; processus et procédures de protection de l'information; maintenance; et technologie de protection.

iii **Détecter**: concevoir et mettre en œuvre des activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.
- Sous-catégories: anomalies et événements; surveillance continue de la sécurité; et processus de détection.

iv **Répondre**: concevoir et mettre en œuvre les activités appropriées pour prendre des mesures concernant un incident de cybersécurité détecté.
- Sous-catégories: planification de la réponse; communications; analyse; atténuation; et améliorations.

v **Rétablir**: concevoir et mettre en œuvre des activités appropriées pour la maintenance des plans de résilience et la restauration des capacités ou services qui auraient été altérés en raison d'un incident de cybersécurité.
- Sous-catégories: planification de la récupération; améliorations; et communications.

Figure 8: Exemple du Cadre pour l'amélioration de la cybersécurité des infrastructures critiques



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Fonction p. ex. protéger
Catégories p. ex. sensibilisation et formation
Sous-catégories p. ex. les utilisateurs privilégiés comprennent leurs rôles et responsabilités
Références données à titre d'information p. ex. ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Tranches

Le Cadre pour l'amélioration de la cybersécurité des infrastructures critiques repose sur **quatre tranches**, chacune d'elles étant définie selon trois axes: le processus de gestion des risques, le programme de gestion intégrée des risques et la participation externe. Les tranches ne doivent pas être considérées comme des niveaux de maturité mais comme un cadre permettant aux organisations de contextualiser leur vision du risque de cybersécurité et des processus mis en place pour gérer ce risque.

- **Tranche 1: partialité**
  - **Processus de gestion des risques**: les pratiques organisationnelles de gestion du risque de cybersécurité ne sont pas formalisées et le risque est géré de manière ponctuelle et parfois réactive;
  - **Programme de gestion intégrée des risques**: il y a une sensibilisation limitée au risque de cybersécurité à l'échelle de l'organisation. L'organisation met en œuvre la gestion du risque de cybersécurité de manière irrégulière, au cas par cas, et il se peut qu'elle ne dispose pas de processus permettant le partage des informations de cybersécurité en son sein;
  - **Participation externe**: l'organisation n'a pas conscience de son rôle au sein de l'écosystème plus large vis-à-vis des entités dont elle dépend ou des entités qui dépendent d'elle. L'organisation n'est généralement pas consciente des risques

cybernétiques liés à la chaîne d'approvisionnement des produits et services qu'elle fournit et utilise;

- **Tranche 2: conscience du risque**
  - **Processus de gestion des risques**: les pratiques de gestion des risques sont approuvées par la direction mais ne sont peut-être pas établies comme une politique à l'échelle de toute l'organisation;
  - **Programme de gestion intégrée des risques**: il existe une prise de conscience du risque de cybersécurité à l'échelle de l'organisation, mais aucune approche de gestion du risque de cybersécurité n'a été établie pour toute l'organisation. L'évaluation des risques cybernétiques liés aux actifs organisationnels et externes a lieu mais n'est généralement pas répétable ou récurrente;
  - **Participation externe**: en général, l'organisation a conscience de son rôle au sein de l'écosystème plus large vis-à-vis soit des entités dont elle dépend, soit des entités qui dépendent d'elle, mais pas des deux. De plus, l'organisation est consciente des risques cybernétiques liés à la chaîne d'approvisionnement des produits et services qu'elle fournit et utilise, mais elle n'agit pas de manière cohérente ou formelle face à ces risques;
- **Tranche 3: répétabilité**
  - **Processus de gestion des risques**: les pratiques de gestion des risques de l'organisation sont officiellement approuvées et exprimées sous forme de politique. Les pratiques organisationnelles de cybersécurité sont régulièrement mises à jour sur la base de l'application de processus de gestion des risques aux changements des exigences de l'entreprise ou de la mission et en fonction de l'évolution de la menace et du paysage technologique;
  - **Programme de gestion intégrée des risques**: il existe une approche à l'échelle de l'organisation pour gérer le risque de cybersécurité. Des politiques, processus et procédures tenant compte des risques sont définis, mis en œuvre comme prévu et réexaminés. Les cadres supérieurs veillent à ce que la cybersécurité soit prise en compte dans toutes les activités de l'organisation;
  - **Participation externe**: l'organisation a conscience de son rôle, des entités dont elle dépend et des entités qui dépendent d'elle dans l'écosystème plus large et elle est susceptible de contribuer à une meilleure compréhension des risques au sein de la communauté. L'organisation est consciente des risques cybernétiques liés à la chaîne d'approvisionnement des produits et services qu'elle fournit et utilise;
- **Tranche 4: adaptabilité**
  - **Processus de gestion des risques**: l'organisation adapte ses pratiques de cybersécurité en fonction des activités de cybersécurité antérieures et actuelles, y compris les enseignements tirés et les indicateurs prédictifs;
  - **Programme de gestion intégrée des risques**: il existe une approche à l'échelle de l'organisation pour gérer le risque de cybersécurité. Cette approche se base sur des politiques, processus et procédures tenant compte des risques pour faire face aux événements potentiels de cybersécurité; et
  - **Participation externe**: l'organisation a conscience de son rôle, des entités dont elle dépend et des entités qui dépendent d'elle dans l'écosystème plus large et elle est susceptible de contribuer à une meilleure compréhension des risques au sein de la communauté.

Méthode d'évaluation

Le Cadre pour l'amélioration de la cybersécurité des infrastructures critiques est destiné aux organisations pour leur permettre d'autoévaluer leurs risques afin de rendre leur approche et leurs investissements en matière de cybersécurité plus rationnels, efficaces et précieux. Pour examiner l'efficacité des investissements, une organisation doit d'abord avoir une compréhension claire de ses objectifs et de la relation entre ces objectifs et les résultats de la cybersécurité. Les résultats de la cybersécurité du noyau du cadre soutiennent l'autoévaluation de l'efficacité des investissements et des activités de cybersécurité.

A.4 Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2)

Le Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2) a été mis au point par la faculté de droit de l'Université du Qatar en 2018. Le Q-C2M2 s'appuie sur divers modèles existants pour élaborer une méthodologie d'évaluation complète visant à améliorer le cadre de cybersécurité du Qatar.

Attributs/Dimensions

Le Q-C2M2 adopte l'approche du cadre de l'Institut national des normes et des technologies (NIST), qui utilise cinq fonctions de base comme principaux domaines du modèle. Les cinq fonctions de base sont applicables dans le contexte qatari car elles sont communes à tous les secteurs d'infrastructures critiques, un élément important du cadre de cybersécurité qatari. Le Q-C2M2 est basé sur **cinq domaines**. Chaque domaine est ensuite divisé en plusieurs **sous-domaines** pour couvrir toute la gamme de maturité des capacités de cybersécurité.

Les cinq domaines sont détaillés ci-dessous:

i. Le **domaine «comprendre»** inclut quatre sous-domaines: cybergouvernance, actifs, risques et formation;
ii. Les sous-domaines du **domaine «sécuriser»** comprennent la sécurité des données, la sécurité technologique, la sécurité du contrôle d'accès, la sécurité des communications et la sécurité du personnel;
iii. Le **domaine «exposer»** comprend les sous-domaines suivants: surveillance, gestion des incidents, détection, analyse et exposition;
iv. Le **domaine «répondre»** comprend la planification de la réponse, l'atténuation et la communication de la réponse; et
v. Le **domaine «durabiliser»** comprend la planification de la récupération, la gestion de la continuité, l'amélioration et les dépendances externes.

Niveaux de maturité

Le Q-C2M2 utilise **cinq niveaux de maturité** mesurant la maturité des capacités d'une entité étatique ou d'une organisation non étatique au niveau de la fonction de base. Ces niveaux visent à évaluer la maturité dans les cinq domaines détaillés dans la section précédente.

- **Initiation**: emploie des pratiques et des processus de cybersécurité ponctuels dans certains des domaines;
- **Mise en œuvre**: des politiques ont été adoptées pour la mise en œuvre de toutes les activités de cybersécurité dans les domaines, le but étant de finaliser la mise en œuvre à un moment donné;
- **Développement**: des politiques et des pratiques ont été mises en œuvre pour développer et améliorer les activités de cybersécurité dans les domaines, le but étant de suggérer de nouvelles activités à mettre en œuvre;
- **Adaptabilité**: les activités de cybersécurité sont revisitées et réexaminées, et des pratiques sont adoptées sur la base des indicateurs prédictifs dérivés d'expériences et de mesures antérieures; et
- **Souplesse**: poursuite de la phase d'adaptation, en mettant l'accent sur la souplesse et la rapidité lors de la mise en œuvre des activités dans les domaines.

Méthode d'évaluation

Le Q-C2M2 est à un stade précoce de recherche et n'est pas encore prêt pour la mise en œuvre. C'est un cadre qui pourrait être utilisé pour déployer un modèle d'évaluation détaillé pour les organisations qataries à l'avenir.

A.5 Certification du modèle de maturité de la cybersécurité (CMMC)

La Certification du modèle de maturité de la cybersécurité (CMMC) a été développée par le Département américain de la défense (DoD) en collaboration avec l'Université Carnegie Mellon

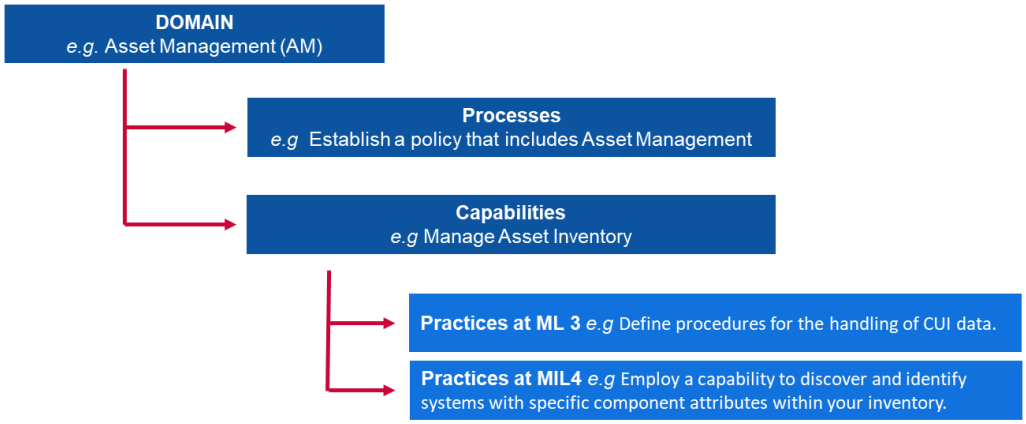
et le laboratoire de physique appliquée de l'Université Johns Hopkins. L'objectif principal du DoD dans la conception de ce modèle est de protéger les informations du secteur de la base industrielle de la défense (DIB). Les informations ciblées par le CMMC sont classées soit comme «Informations sous contrats fédéraux», informations fournies par ou générées pour le gouvernement dans le cadre d'un contrat et non destinées à être divulguées au public, soit comme «Informations non classifiées contrôlées», informations qui nécessitent des contrôles de sauvegarde ou de diffusion conformément aux lois, règlements et politiques gouvernementales. Le CMMC mesure la maturité de la cybersécurité et fournit les meilleures pratiques ainsi qu'un élément de certification pour assurer la mise en œuvre des pratiques associées à chaque niveau de maturité. La dernière version du CMMC a été publiée en 2020.

Attributs/Dimensions

Le CMMC examine **17 domaines** représentant des groupes de processus et de capacités de cybersécurité. Chaque domaine est ensuite subdivisé en plusieurs **processus** qui sont similaires d'un domaine à l'autre; et il comprend une à plusieurs **capacités** réparties sur cinq niveaux de maturité. Les capacités (ou aptitudes) sont ensuite détaillées en **pratiques** pour chaque niveau de maturité pertinent.

La relation entre ces notions s'articule comme suit:

Figure 9: Exemple d'indicateurs du CMMC



DOMAIN e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 e.g Define procedures for the handling of CUI data
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory

DOMAINE p. ex. gestion des actifs (GA)
Processus
p. ex. établir une politique qui comprend la gestion des actifs
Capacités
p. ex. gérer l'inventaire des actifs
Pratiques MIL3 p. ex. définir des procédures pour le traitement des données issues des «Informations non classifiées contrôlées»
Pratiques MIL4 p. ex. utiliser sa capacité pour découvrir et identifier les systèmes ayant des attributs de composants spécifiques au sein de l'inventaire

Les 17 domaines sont détaillés ci-dessous:

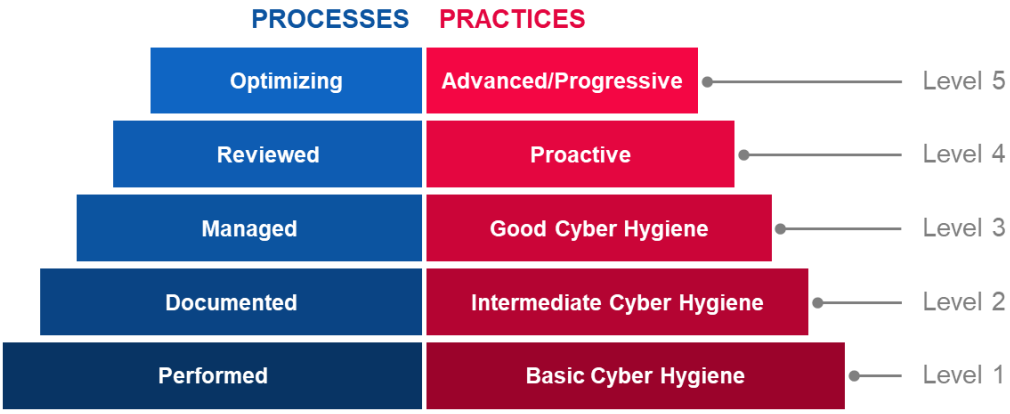
i Contrôle de l'accès (CA);
ii Gestion des actifs (GA);
iii Audit et responsabilité (AR);
iv Sensibilisation et formation (SF);
v Gestion de la configuration (GC);
vi Identification et authentification (IA);
vii Réponse aux incidents (RI);
viii Maintenance (MA);
ix Protection des médias (PM);

x Sécurité du personnel (SP);
xi Protection physique (PP);
xii Récupération (RE);
xiii Gestion des risques (GR);
xiv Évaluation de la sûreté (ES);
xv Conscience situationnelle (CS);
xvi Protection du système et des communications (PS); et
xvii Intégrité du système et des informations (IS).

Niveaux de maturité

Le CMMC utilise **cinq niveaux de maturité** définis en fonction des processus et des pratiques. Afin d'atteindre un certain niveau de maturité dans le CMMC, une organisation doit remplir les conditions préalables des processus et pratiques du niveau en question. Cela implique également la validation des conditions préalables de tous les niveaux inférieurs.

Figure 10: Niveaux de maturité du CMMC



PROCESSES	PROCESSUS
Optimizing	Optimisé
Reviewed	Réexaminé
Managed	Géré
Documented	Documenté
	Réalisé
PRACTICES	PRATIQUES
Advanced/Progressive	Avancé/Progressif
Proactive	Proactif
Good Cyber Hygiene	Bonne hygiène cybernétique
Intermediate Cyber Hygiene	Hygiène cybernétique intermédiaire
Basic Cyber Hygiene	Hygiène cybernétique de base
Level 5	Niveau 5
Level 4	Niveau 4
Level 3	Niveau 3
Level 2	Niveau 2
Level 1	Niveau 1

- **Niveau 1**
  - **Processus – Réalisé**: l'organisation est seulement capable de mettre en œuvre ces pratiques de manière ponctuelle et peut se baser sur la documentation ou non. La maturité du processus n'est pas évaluée pour le niveau 1;
  - **Pratiques – Hygiène cybernétique de base**: le niveau 1 se concentre sur la protection des «Informations sous contrats fédéraux» et comprend uniquement les pratiques qui correspondent aux exigences de protection de base;
- **Niveau 2**
  - **Processus – Documenté**: le niveau 2 exige qu'une organisation établisse et documente des pratiques et des politiques pour guider la mise en œuvre de ses

efforts en lien avec le CMMC. La documentation des pratiques permet leur répétabilité. Les organisations développent des capacités matures en documentant leurs processus, puis en les mettant en pratique tels qu'ils sont documentés;
- **Pratiques – Hygiène cybernétique intermédiaire**: le niveau 2 sert de niveau de progression intermédiaire entre le niveau 1 et le niveau 3 et consiste en un sous-ensemble des exigences de sécurité spécifiées dans NIST SP 800-171 complété par des pratiques provenant d'autres normes et références;

- **Niveau 3**
  - **Processus – Géré**: le niveau 3 exige qu'une organisation établisse un plan démontrant la gestion des activités pour la mise en œuvre de la pratique, qu'elle assure la maintenance de ce plan et qu'elle lui attribue les ressources nécessaires. Le plan peut comprendre des informations sur les missions, les objectifs, les plans de projet, les ressources, la formation requise et la participation des parties prenantes concernées;
  - **Pratiques – Bonne hygiène cybernétique**: le niveau 3 se concentre sur la protection des «Informations non classifiées contrôlées» et englobe toutes les exigences de sécurité spécifiées dans NIST SP 800-171 ainsi que des pratiques supplémentaires provenant d'autres normes et références visant à atténuer les menaces;
- **Niveau 4**
  - **Processus – Réexaminé**: le niveau 4 exige qu'une organisation réexamine ses pratiques et en mesure l'efficacité. À ce niveau, en plus de mesurer l'efficacité des pratiques, les organisations sont capables de prendre des mesures correctives si nécessaire et d'informer la direction supérieure de l'état de la situation ou des problèmes qui se présentent de façon récurrente;
  - **Pratiques – Proactif**: le niveau 4 se concentre sur la protection des «Informations non classifiées contrôlées» et englobe un sous-ensemble des exigences de sécurité renforcées. Ces pratiques renforcent les capacités de détection et de réponse d'une organisation pour faire face à l'évolution des tactiques, techniques et procédures et s'y adapter;
- **Niveau 5**
  - **Processus – Optimisé**: le niveau 5 exige qu'une organisation normalise et optimise la mise en œuvre des processus dans l'ensemble de l'organisation; et
  - **Pratiques – Avancé/Progressif**: le niveau 5 se concentre sur la protection des «Informations non classifiées contrôlées». Les pratiques supplémentaires augmentent la profondeur et la sophistication des capacités de cybersécurité.

Méthode d'évaluation

Le CMMC est un modèle relativement récent, finalisé au cours du premier trimestre 2020. À ce jour, il n'a été déployé dans aucune organisation. Néanmoins, les contractants du DoD s'attendent à faire appel à des examinateurs tiers certifiés pour effectuer des audits. Le DoD attend de ses contractants qu'ils mettent en œuvre les meilleures pratiques pour favoriser la cybersécurité et la protection des informations sensibles.

A.6 Modèle de maturité de la cybersécurité communautaire (MMCSC)

Le Modèle de maturité de la cybersécurité communautaire (MMCSC) a été mis au point par le Centre for Infrastructure Assurance and Security de l'Université du Texas. L'objectif du MMCSC est de mieux définir les méthodes permettant de déterminer l'état actuel de la cyberpréparation d'une communauté et de fournir une feuille de route à suivre par les communautés dans leurs efforts de préparation. Les communautés ciblées par le MMCSC sont principalement les gouvernements locaux et les administrations d'États fédérés. Le MMCSC a été conçu en 2007.

Attributs/Dimensions

Les niveaux de maturité sont définis selon **six dimensions principales** qui couvrent les différents aspects de la cybersécurité au sein des communautés et des organisations. Ces dimensions sont clairement définies pour chaque niveau de maturité (vous trouverez le détail

des dimensions et des niveaux à la Figure 31: Résumé des dimensions **du MMCSC**). Les six dimensions sont:

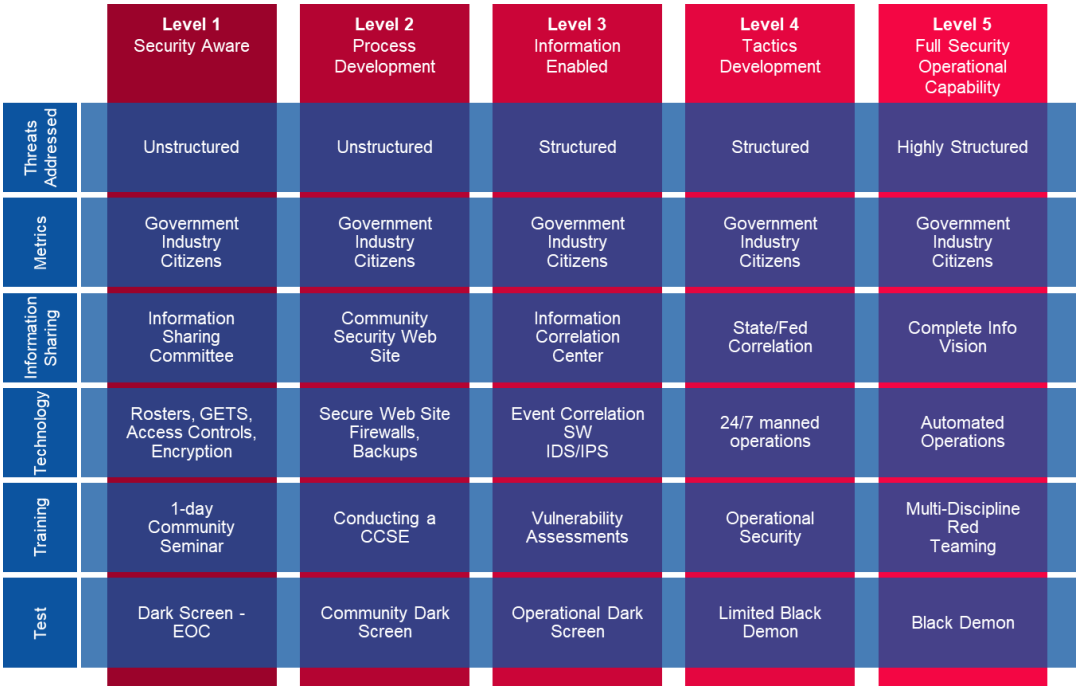
i Gestion des menaces;
ii Mesures;
iii Partage d'information;
iv Technologies;
v Formation; et
vi Test.

Niveaux de maturité

Le MMCSC repose sur **cinq niveaux de maturité** basés sur les principaux types de menaces et d'activités traités au niveau en question:

- **Niveau 1: Sensibilisation à la sécurité**
  Le thème principal des activités à ce niveau est de sensibiliser les individus et organisations aux menaces, problèmes et questions liés à la cybersécurité;
- **Niveau 2: Élaboration des processus**
  Ce niveau est conçu pour aider les communautés à établir et améliorer les processus de sécurité nécessaires pour traiter efficacement les problèmes de cybersécurité;
- **Niveau 3: Culture de l'information**
  Conçu pour améliorer les mécanismes de partage d'information au sein de la communauté afin de permettre à cette dernière de corréler efficacement des informations apparemment disparates;
- **Niveau 4: Élaboration des tactiques**
  Les éléments de ce niveau sont conçus pour élaborer des méthodes à la fois meilleures et plus proactives pour la détection des attaques et la réponse aux attaques; À ce niveau, la plupart des méthodes de prévention devraient être en place.
- **Niveau 5: Capacité opérationnelle de sécurité totale**
  Ce niveau renferme tous les éléments qui devraient être mis en place pour permettre à une organisation de se considérer comme pleinement préparée sur le plan opérationnel à faire face à tout type de cybermenace.

Figure 31: Résumé des dimensions du MMCSC par niveau



	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1
Security Aware
Level 2
Process Development
Level 3
Information Enabled
Level 4
Tactics Development
Level 5
Full Security Operational Capability
Threats Addressed
Metrics
Information sharing
Technology
Training
Test
Unstructured
Governement
Industry
Citizens
Information Sharing Committee
Rosters, GETS, Assess Controls, Encryption
1-dat Community Seminar
Dark Screen – EOC
Unstructured
Governement
Industry
Citizens
Community Security Web site
Secure Web Site Firewalls, Backups
Conudcting a CCSE
Community Dark Screen
Structured
Governement
Industry
Citizens
Information Correlation Center
Event Correlation SW IDS/IPS
Vulnerability Assessment
Operational Dark Screen

Niveau 1
Sensibilisation à la sécurité
Niveau 2
Élaboration des processus
Niveau 3
Culture de l'information
Niveau 4
Élaboration des tactiques
Niveau 5
Capacité opérationnelle de sécurité totale
Gestion des menaces
Mesures
Partage d'information
Technologies
Formation
Test
Non structuré
Gouvernement
Industrie
Citoyens
Comité de partage d'information
Tableaux, SEAOG, contrôles des accès, cryptage
Séminaire d'une journée pour la communauté
Dark Screen – EOC
Non structuré
Gouvernement
Industrie
Citoyens
Site web de la sécurité de la communauté
Pare-feu sur les sites web sécurisés, sauvegardes
Réaliser un ECSC
Dark Screen communautaire
Structuré
Gouvernement
Industrie
Citoyens
Centre de corrélation de l'information
Logiciel IDS/IPS pour la corrélation des événements
Évaluation de la vulnérabilité
Dark Screen opérationnel

Structured	Structuré
Governement	Gouvernement
Industry	Industrie
Citizens	Citoyens
State/Fed Correlation	Corrélation étatique/fédérale
24/7 manned operations	Opération 24/7 avec intervention humaine
Operational Security	Sécurité d'exploitation
Limited Black Demon	Black Demon limité
Highly Structured	Hautement structuré
Governement	Gouvernement
Industry	Industrie
Citizens	Citoyens
Complete Info Vision	Vision intégrale sur les informations
Automated Operations	Opérations automatisées
Multi-Discipline Red Teaming	Red teaming multidisciplinaire
Black Demon	Black Demon

Méthode d'évaluation

En tant que méthodologie d'évaluation, le MMCSC est destiné à être déployé par les communautés avec la contribution des agences répressives étatiques et fédérales. Il vise à aider la communauté à définir ce qui est le plus important, les cibles les plus probables et ce qui doit être protégé (et dans quelle mesure). Avec ces objectifs à l'esprit, des plans peuvent être élaborés pour amener chaque aspect de la communauté au niveau de maturité requis en matière de cybersécurité. L'intelligence spécifique générée par le MMCSC aide à définir les objectifs des différents tests et exercices pouvant être utilisés pour mesurer l'efficacité des programmes établis.

A.7 Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework (MMSI)

Le Modèle de maturité de la sécurité de l'information (MMSI) a été développé au sein de la faculté des sciences informatiques et de l'ingénierie de l'Université Roi Fahd du pétrole et des minéraux en Arabie saoudite. Le MMSI propose un nouveau modèle de maturité des capacités pour mesurer la mise en œuvre des mesures de cybersécurité. L'objectif du MMSI est de permettre aux organisations de mesurer les progrès de leur mise en œuvre au fil du temps en utilisant régulièrement le même outil de mesure afin de s'assurer que la posture de sécurité souhaitée est maintenue. Le MMSI a été conçu en 2017.

Attributs/Dimensions

Le MMSI s'appuie sur les domaines évalués existants du cadre NIST et ajoute une dimension sur l'évaluation de la conformité. Cela porte le modèle à **23 domaines évalués** pour la posture de sécurité d'une organisation. Les 23 domaines évalués sont:

i Gestion des actifs;
ii Environnement de l'entreprise;
iii Gouvernance;
iv Évaluation des risques;
v Stratégie de gestion des risques;
vi Évaluation de la conformité;
vii Contrôle de l'accès;
viii Sensibilisation et formation;
ix Sécurité des données;
x Processus et procédures de protection de l'information;
xi Maintenance;
xii Technologie de protection;
xiii Anomalies et événements;
xiv Surveillance continue de la sécurité;
xv Processus de détection;

xvi Planification de la réponse;
xvii Communication de la réponse;
xviii Analyse de la réponse;
xix Atténuation de la réponse;
xx Amélioration de la réponse;
xxi Planification de la récupération;
xxii Amélioration de la récupération; et
xxiii Communication de la récupération.

Niveaux de maturité

Le MMSI repose sur **cinq niveaux de maturité**, qui, malheureusement, ne sont pas détaillés dans la documentation disponible.

- **Niveau 1:** Processus réalisé;
- **Niveau 2:** Processus géré;
- **Niveau 3:** Processus établi;
- **Niveau 4:** Processus prévisible; et
- **Niveau 5:** Processus en cours d'optimisation.

Méthode d'évaluation

Le MMSI ne propose pas de méthodologie spécifique pour mener l'évaluation pour les organisations.

A.8 Modèle des capacités d'audit interne (MCAI) dans le secteur public

Le Modèle des capacités d'audit interne (MCAI) a été développé par la Fondation de recherche de l'Institut des auditeurs internes dans le but de renforcer les capacités et la défense des intérêts par l'autoévaluation dans le secteur public. Destiné aux professionnels de l'audit, le MCAI fournit un aperçu du modèle à proprement parler ainsi qu'un guide pour aider utiliser le modèle comme un outil d'autoévaluation.

Bien que le MCAI soit axé sur les capacités d'audit interne, plutôt que sur le renforcement des capacités en matière de cybersécurité, le modèle est conçu comme un outil d'autoévaluation de la maturité pour les entités du secteur public qui peut être appliqué globalement pour améliorer les processus et l'efficacité. Dans la mesure où le champ d'application n'est pas axé sur la cybersécurité, les attributs ne seront pas analysés. Le MCAI a été finalisé en 2009.

Niveaux de maturité

Le Modèle des capacités d'audit interne (MCAI) comprend **cinq niveaux de maturité**, chacun décrivant les caractéristiques et les capacités d'une activité d'audit interne au niveau en question. Les niveaux de capacité du modèle fournissent une feuille de route pour l'amélioration continue.

- **Niveau 1: Initial**
  Pas de capacités durables et répétables– dépend des efforts individuels
  - Ponctuel ou non structuré;
  - Audits ou contrôles uniques et isolés de documents et de transactions pour en vérifier l'exactitude et la conformité;
  - Les résultats dépendent des compétences de la personne qui occupe la fonction;
  - Aucune pratique professionnelle établie autre que celles fournies par les associations professionnelles;
  - Approbation du financement par la direction, le cas échéant;
  - Absence d'infrastructures;
  - Les auditeurs font généralement partie d'une unité organisationnelle de plus grande ampleur;
  - Les capacités institutionnelles ne sont pas développées.
- **Niveau 2: Infrastructures**
  Pratiques et procédures durables et répétables

- La question ou la problématique clé pour le niveau 2 consiste à savoir comment établir et maintenir la répétabilité des processus et donc assurer des capacités reproductibles;
- Des relations pour les rapports d'audit interne, des infrastructures administratives et de gestion, et des pratiques et processus professionnels sont mis en place (orientation, processus et procédures d'audit interne);
- La planification de l'audit se base principalement sur les priorités de la direction;
- On continue de s'appuyer essentiellement sur les aptitudes et compétences de personnes spécifiques;
- Conformité partielle aux normes.

▶ **Niveau 3: Intégration**

Pratiques professionnelles et de gestion appliquées uniformément;

- Les politiques, processus et procédures d'audit interne sont définis et documentés. Ils interagissent et se complètent, et sont intégrés dans l'infrastructure de l'organisation;
- La gestion de l'audit interne et les pratiques professionnelles sont bien établies et appliquées uniformément dans toute l'activité d'audit interne;
- L'audit interne commence à s'aligner sur les activités de l'organisation et les risques auxquels elle est confrontée;
- L'audit interne évolue, passant d'un simple audit interne traditionnel à l'intégration d'un membre de l'équipe à part entière et à la fourniture de conseils sur la performance et la gestion des risques;
- L'accent est mis sur la constitution d'équipes et les capacités de l'activité d'audit interne, ainsi que sur son indépendance et son objectivité;
- Conformité générale aux normes.

▶ **Niveau 4: Gestion**

Intègre les informations provenant de toute l'organisation pour améliorer la gouvernance et la gestion des risques;

- Correspondance entre l'audit interne et les attentes des principales parties prenantes;
- Des mesures de performance sont en place pour évaluer et surveiller les processus et résultats de l'audit interne;
- L'audit interne est reconnu comme apportant des contributions significatives à l'organisation;
- L'audit interne fait partie intégrante de la gouvernance et de la gestion des risques de l'organisation;
- L'audit interne est une unité fonctionnelle bien gérée;
- Les risques sont mesurés et gérés de manière quantitative;
- Les aptitudes et compétences requises sont en place avec une capacité de renouvellement et de partage des connaissances (au sein de l'audit interne et dans toute l'organisation).

▶ **Niveau 5: Optimisation**

Apprentissage à l'intérieur et à l'extérieur de l'organisation pour une amélioration continue;

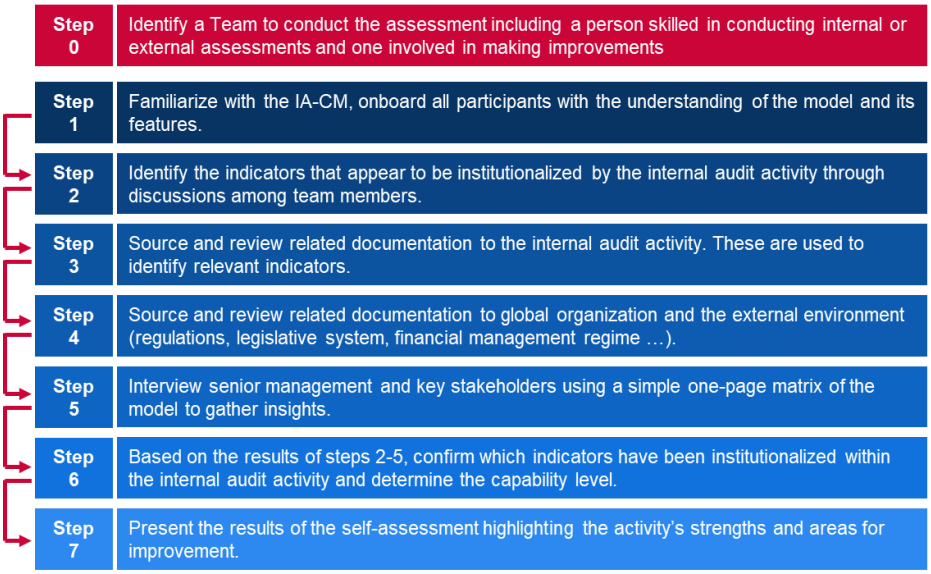
- L'audit interne est une organisation qui apprend, avec des améliorations et des innovations continues des processus;
- L'audit interne utilise les informations provenant de l'intérieur et de l'extérieur de l'organisation pour contribuer à l'atteinte des objectifs stratégiques;
- Performances de classe mondiale/recommandées/meilleures pratiques;
- L'audit interne est un élément incontournable de la structure de gouvernance de l'organisation;
- Compétences professionnelles et spécialisées de haut niveau;
- Les mesures des performances individuelles, des unités et de l'organisation sont entièrement intégrées afin
- d'améliorer les performances.

Méthode d'évaluation

Le Modèle des capacités d'audit interne est clairement conçu pour l'autoévaluation. Il s'accompagne d'étapes détaillées à suivre pour son utilisation et d'un jeu de diapositives à personnaliser. Avant de commencer l'autoévaluation, une équipe spécifique doit être identifiée, comprenant au minimum une personne qualifiée pour mener des évaluations internes ou

externes des audits internes et une personne impliquée dans l'introduction d'améliorations dans ce domaine.

Figure 12: Étapes de l'autoévaluation selon le MCAI



Step 0	Étape 0
Step 1	Étape 1
Step 2	Étape 2
Step 3	Étape 3
Step 4	Étape 4
Step 5	Étape 5
Step 6	Étape 6
Step 7	Étape 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Identifiez une équipe pour mener l'évaluation, y compris une personne qualifiée pour mener des évaluations internes ou externes et une autre pour apporter des améliorations.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Familiarisez-vous avec le MCAI, intégrez tous les participants en vous assurant qu'ils comprennent le modèle et ses caractéristiques.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Identifiez les indicateurs qui semblent être institutionnalisés par l'activité d'audit interne au travers de discussions entre les membres de l'équipe.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Recherchez et examinez la documentation relative à l'activité d'audit interne. Cela vous permettra d'identifier les indicateurs pertinents.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Recherchez et analysez la documentation relative à l'organisation globale et à l'environnement externe (réglementation, système législatif, régime de gestion financière, etc.).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Interrogez la direction générale et les principales parties prenantes en utilisant une simple matrice du modèle tenant sur une page afin de recueillir des informations.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Sur la base des résultats des étapes 2 à 5, confirmez les indicateurs qui ont été institutionnalisés au sein de l'activité d'audit interne et déterminez le niveau des capacités.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Présentez les résultats de l'autoévaluation en soulignant les points forts de l'activité et les domaines d'amélioration.

A.9 Indice mondial de la cybersécurité (IMCS)

L'Indice mondial de la cybersécurité (IMCS) est une initiative de l'Union internationale des télécommunications (UIT) qui vise à examiner l'engagement et la situation en matière de cybersécurité dans toutes les régions où l'UIT est active: Afrique, Amérique, Asie-Pacifique, CEI, Europe et monde arabe. Il met en avant les pays qui font preuve d'un grand engagement et dont les pratiques sont recommandables. L'objectif de l'IMCS est d'aider les pays à identifier

les domaines d'amélioration en matière de cybersécurité, ainsi que de les motiver à prendre des mesures pour améliorer leur classement, contribuant ainsi à élever le niveau général de la cybersécurité dans le monde.

L'IMCS étant un indice et non un modèle de maturité, il n'utilise pas des niveaux de maturité mais plutôt un score pour classer et comparer l'engagement en matière de cybersécurité des nations et des régions à l'échelle mondiale.

Attributs/Dimensions

L'Indice mondial de la cybersécurité (IMCS) se base sur les cinq piliers du Programme mondial de cybersécurité (GCA). Ces piliers forment les cinq sous-indices de l'IMCS. Chacun de ces piliers comprend un ensemble d'indicateurs. Les cinq piliers et les indicateurs sont les suivants:

i **Juridique**: mesures basées sur l'existence d'institutions et de cadres juridiques traitant de la cybersécurité et de la cybercriminalité.
- Législation en matière de cybercriminalité;
- Réglementation en matière de cybersécurité; et
- Endiguement/restriction de la législation en matière de courrier indésirable.

ii **Technique**: mesures basées sur l'existence d'institutions et de cadres techniques traitant de la cybersécurité.
- CERT/CIRT/CSIRT;
- Cadre de mise en œuvre des normes;
- Organisme de normalisation;
- Mécanismes et capacités techniques déployés pour faire face au courrier indésirable;
- Utilisation du cloud à des fins de cybersécurité; et
- Mécanismes de protection de l'enfance en ligne.

iii **Organisationnel**: mesures basées sur l'existence d'institutions de coordination des politiques et de stratégies de développement de la cybersécurité à l'échelle nationale.
- Stratégie nationale de cybersécurité;
- Agence responsable; et
- Cybersécurité.

iv **Renforcement des capacités**: mesures basées sur l'existence de programmes de recherche et de développement, de programmes éducatifs et de formation, de professionnels certifiés et d'agences du secteur public favorisant le renforcement des capacités.
- Campagnes de sensibilisation du public;
- Cadre de certification et d'accréditation des professionnels de la cybersécurité;
- Formations professionnelles en cybersécurité;
- Programmes éducatifs ou universitaires en cybersécurité;
- Programmes de R&D en cybersécurité; et
- Mécanismes d'incitation.

v **Coopération**: mesures basées sur l'existence de partenariats, de cadres de coopération et de réseaux de partage d'information.
- Accords bilatéraux;
- Accords multilatéraux;
- Participation à des forums/associations internationaux;
- Partenariats public-privé;
- Partenariats entre les agences et au sein de celles-ci; et
- Meilleures pratiques.

Méthode d'évaluation

L'IMCS est un outil d'autoévaluation construit sur la base d'une enquête[30] de questions binaires, précodées et ouvertes. L'utilisation de réponses binaires élimine tout risque d'évaluation basée sur l'opinion et tout biais éventuel à l'égard de certains types de réponses.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_French.pdf

Les réponses précodées permettent de gagner du temps et d'analyser les données avec plus de précision. De plus, une simple échelle dichotomique permet une évaluation plus rapide et plus complexe car elle n'exige pas de longues réponses, ce qui accélère et rationalise le processus de réponse et l'évaluation ultérieure. Le répondant doit seulement confirmer la présence ou l'absence de certaines solutions de cybersécurité préidentifiées. Un mécanisme d'enquête en ligne, utilisé pour recueillir les réponses et télécharger les supports pertinents, permet à un panel d'experts d'extraire les bonnes pratiques et un ensemble d'évaluations qualitatives thématiques.

Le processus global de l'IMCS est mis en œuvre comme suit:

- Une lettre d'invitation est envoyée à tous les participants, les informant de l'initiative et demandant un point focal chargé de collecter toutes les données pertinentes et de remplir le questionnaire de l'IMCS en ligne. Lors de l'enquête en ligne, le point focal convenu est officiellement invité par l'UIT à répondre au questionnaire;
- Collecte de données primaires (pour les pays qui ne répondent pas au questionnaire):
  - L'UIT élabore un premier projet de réponse au questionnaire sur la base de données accessibles au public et de recherches en ligne;
  - Le projet est envoyé aux points focaux pour examen;
  - Les points focaux précisent les réponses et renvoient ensuite le projet;
  - Le projet corrigé est envoyé à chaque point focal pour approbation finale; et
  - Le questionnaire validé est utilisé pour l'analyse, l'établissement du score et le classement.
- Collecte de données secondaires (pour les pays qui répondent au questionnaire):
  - L'UIT identifie les réponses manquantes, les documents d'appui, les liens, etc.;
  - Le point focal améliore la précision des réponses lorsque c'est nécessaire;
  - Le projet corrigé est envoyé à chaque point focal pour approbation finale; et
  - Le questionnaire validé est utilisé pour l'analyse, l'établissement du score et le classement.

A.10 L'Indice de cyberpuissance (ICP)

L'Indice de cyberpuissance (ICP) a été créé en 2011 par le programme de recherche de l'Economist Intelligence Unit sponsorisé par Booz Allen Hamilton. L'ICP est un «modèle quantitatif et qualitatif dynamique [...] qui mesure les attributs spécifiques du cyberenvironnement à travers quatre moteurs de la cyberpuissance: le cadre juridique et réglementaire, le contexte économique et social, l'infrastructure technologique et l'application industrielle, et qui examine les progrès numériques dans les industries clés»[31]. L'objectif de l'Indice de cyberpuissance est de comparer la capacité des pays du G20 à résister aux cyberattaques et à déployer l'infrastructure numérique nécessaire à une économie prospère et sûre. L'exercice de comparaison fourni par l'ICP se concentre sur 19 pays du G20 (à l'exclusion de l'UE). L'indice fournit ensuite un classement des pays pour chaque indicateur.

Attributs/Dimensions

L'Indice de cyberpuissance (ICP) est basé sur quatre moteurs de la cyberpuissance. Chaque catégorie est ensuite mesurée par de multiples indicateurs afin de donner un score spécifique à chaque pays. Les catégories et les piliers sont les suivants:

i **Cadre juridique et réglementaire**
  - Engagement du gouvernement en faveur du cyberdéveloppement
  - Politiques de cyberprotection
  - Cybercensure (ou absence de cybercensure)
  - Efficacité politique
  - Protection de la propriété intellectuelle

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

ii **Contexte économique et social**
- Niveaux d'éducation
- Compétences techniques
- Ouverture du commerce
- Degré d'innovation dans l'environnement des entreprises

iii **Infrastructure technologique**
- Accès aux technologies de l'information et de la communication
- Qualité des technologies de l'information et de la communication
- Caractère abordable des technologies de l'information et de la communication
- Dépenses dans les technologies de l'information
- Nombre de serveurs sécurisés

iv **Application industrielle**
- Réseaux intelligents
- Services de santé en ligne
- Commerce électronique
- Transport intelligent
- E-gouvernement

Méthode d'évaluation

L'ICP est un modèle de notation quantitative et qualitative. L'évaluation a été menée par l'Economist Intelligence Unit au moyen d'indicateurs quantitatifs provenant de sources statistiques disponibles et sur la base d'estimations lorsque les données manquaient. Les principales sources utilisées sont l'Economist Intelligence Unit, l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), l'Union internationale des télécommunications (UIT) et la Banque mondiale.

A.11 L'Indice de cyberpuissance (ICP)

Cette section résume les principales conclusions de l'analyse des modèles de maturité existants. Le Tableau 5: Vue d'ensemble des modèles **de maturité analysés** donne une vue d'ensemble des principales caractéristiques de chaque modèle selon le modèle de Becker modifié. Dans le Tableau 6 Comparaison des niveaux de **maturité**, vous trouverez les définitions de haut niveau des niveaux de maturité des modèles analysés. Le Tableau 7 fournit une vue d'ensemble des dimensions ou des attributs utilisés dans chaque modèle.

Tableau 5: Vue d'ensemble des modèles de maturité analysés

Nom du modèle	Institution à l'origine du modèle	Objectif	Cible	Nbre de niveaux	Nbre d'attributs	Méthode d'évaluation	Représentation des résultats
Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC)	Centre de capacité de la cybersécurité mondiale Université d'Oxford	Accroître l'échelle et l'efficacité du renforcement des capacités en matière de cybersécurité à l'échelle internationale	Pays	5	5 dimensions principales	Collaboration avec une organisation locale pour peaufiner le modèle avant de l'appliquer au contexte national	Radar à 5 sections
Modèle de maturité des capacités en matière de cybersécurité (C2M2)	Département américain de l'énergie (DoE)	Aider les organisations à évaluer et à améliorer leurs programmes de cybersécurité et à renforcer leur résilience opérationnelle	Organisations de tous les secteurs, de tous types et de toutes tailles	4	10 domaines clés	Méthodologie et outils d'autoévaluation	Tableau de bord avec graphiques circulaires
Cadre pour l'amélioration de la cybersécurité des infrastructures critiques	Institut national des normes et des technologies (NIST)	Cadre visant à orienter les activités de cybersécurité et la gestion des risques au sein des organisations	Organisations	s.o. (4 tranches)	5 fonctions principales	Autoévaluation	-
Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2)	Faculté de droit de l'Université du Qatar	Fournir un modèle pratique pouvant être utilisé pour comparer, mesurer et développer le cadre de cybersécurité du Qatar	Organisations qataries	5	5 domaines clés	-	-
Certification du modèle de maturité de la cybersécurité (CMMC)	Département américain de la défense (DoD)	Encourager les meilleures pratiques de cybersécurité pour protéger les informations	Organisations du secteur de la base industrielle de la défense (DIB)	5	17 domaines clés	Évaluation par des auditeurs tiers	-
Modèle de maturité de la cybersécurité communautaire (MMCSC)	Centre for Infrastructure Assurance and Security de l'Université du Texas	Déterminer l'état actuel de la cyberpréparation d'une communauté et fournir une feuille de route à suivre par les communautés dans leurs efforts de préparation	Communautés (gouvernements locaux ou administrations d'États fédérés)	5	6 dimensions principales	Évaluation au sein des communautés avec une contribution de l'État et des agences répressives fédérales	-
Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework (MMSI)	Faculté des sciences informatiques et de l'ingénierie Université Roi Fahd du pétrole et des minéraux en Arabie saoudite	Permettre aux organisations de mesurer leurs progrès de mise en œuvre au fil du temps pour s'assurer qu'elles conservent la posture de sécurité souhaitée	Organisations	5	23 domaines évalués	-	-
Modèle des capacités d'audit interne (MCAI) dans le secteur public	Fondation de recherche de l'Institut des auditeurs internes	Renforcer les capacités d'audit interne et la défense des intérêts par l'autoévaluation dans le secteur public	Organisations du secteur public	5	6 éléments	Autoévaluation	-
Indice mondial de la cybersécurité (IMCS)	Union internationale des télécommunications (UIT)	Examiner l'engagement et la situation en matière de cybersécurité, et aider les pays à identifier les domaines d'amélioration en matière de cybersécurité	Pays	s.o.	5 piliers	Autoévaluation	Tableau de classement

L'Indice de cyberpuissance (ICP)	L'Economist Intelligence Unit et Booz Allen Hamilton	Comparer la capacité des pays du G20 à résister aux cyberattaques et à déployer l'infrastructure numérique nécessaire à une économie prospère et sûre	Pays du G20	s.o.	4 catégories	Évaluation comparative par l'Economist Intelligence Unit	Tableau de classement

Tableau 6 Comparaison des niveaux de maturité

Modèle	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC)	**Démarrage** Soit il n'existe aucune maturité en matière de cybersécurité, soit elle en est à ses premiers balbutiements. Il se peut que des discussions initiales aient été entamées sur le renforcement des capacités de cybersécurité, mais aucune mesure concrète n'a été prise. Dans cette phase, on constate l'absence de preuves observables.	**Formation** Certaines caractéristiques des aspects ont commencé à se développer et à être formulées, mais il se peut qu'elles restent ponctuelles, désorganisées, mal définies, ou qu'elles soient simplement «nouvelles». En revanche, la preuve de cette activité peut clairement être apportée.	**Établissement** Les éléments de l'aspect sont en place et fonctionnent. Il n'y a cependant pas de réflexion approfondie quant à l'allocation relative des ressources. Peu de décisions de compromis ont été prises en ce qui concerne l'investissement «relatif» dans les divers éléments de l'aspect. L'aspect est toutefois fonctionnel et défini.	**Stratégique** Des choix ont été faits quant aux parties de l'aspect qui sont importantes et moins importantes pour l'organisation ou le pays en question. La phase stratégique implique que ces choix ont été faits, en fonction des circonstances propres au pays ou à l'organisation.	**Dynamique** Il existe des mécanismes clairs permettant de modifier la stratégie en fonction des circonstances du moment, comme la technologie de l'environnement de la menace, un conflit mondial ou un changement important dans un domaine de préoccupation (par exemple, la cybercriminalité ou la protection de la vie privée). Les organisations dynamiques ont développé des méthodes permettant de modifier rapidement les stratégies. Cette phase se caractérise par une prise de décision rapide, la réaffectation des ressources et une attention constante portée à l'évolution de l'environnement.
Modèle de maturité des capacités en matière de cybersécurité (C2M2)	**MIL0** Aucune pratique en place.	**MIL1** Les premières pratiques sont en place, mais il se peut qu'elles restent ponctuelles.	**MIL2** Caractéristiques de la gestion: Les pratiques sont documentées; Des ressources adéquates sont fournies pour soutenir le processus; Le personnel qui exécute les pratiques a les compétences et les connaissances appropriées; et La responsabilité et l'autorité pour l'exécution des pratiques sont attribuées. Caractéristique de l'approche: Les pratiques sont plus complètes ou plus avancées qu'au niveau MIL1.	**MIL3** Caractéristiques de la gestion: Les activités sont guidées par des politiques (ou d'autres directives organisationnelles); Des objectifs de performance pour les activités du domaine sont établis et font l'objet d'un suivi pour contrôler les réalisations; et Les pratiques documentées pour les activités du domaine sont normalisées et améliorées dans toute l'entreprise. Caractéristique de l'approche: Les pratiques sont plus complètes ou plus avancées qu'au niveau MIL2.	-

Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework (MMSI)	Processus réalisé	Processus géré	Processus établi	Processus prévisible	Processus en cours d'optimisation
Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2)	**Initiation** Emploie des pratiques et des processus de cybersécurité ponctuels dans certains des domaines.	**Développement** Des politiques et des pratiques ont été mises en œuvre pour développer et améliorer les activités de cybersécurité dans les domaines, le but étant de suggérer de nouvelles activités à mettre en œuvre.	**Mise en œuvre** Des politiques ont été adoptées pour la mise en œuvre de toutes les activités de cybersécurité dans les domaines, le but étant de finaliser la mise en œuvre à un moment donné.	**Adaptabilité** Les activités de cybersécurité sont revisitées et réexaminées, et des pratiques sont adoptées sur la base des indicateurs prédictifs dérivés d'expériences et de mesures antérieures.	**Souplesse** Poursuite de la phase d'adaptation, en mettant l'accent sur la souplesse et la rapidité lors de la mise en œuvre des activités dans les domaines.
Certification du modèle de maturité de la cybersécurité (CMMC)	**Processus: réalisé** L'organisation est seulement capable de mettre en œuvre les pratiques de manière ponctuelle et peut se baser sur la documentation ou non. La maturité du processus n'est dès lors pas évaluée pour le niveau 1. **Pratiques: hygiène cybernétique de base** Le niveau 1 se concentre sur la protection des «Informations sous contrats fédéraux» et comprend uniquement les pratiques qui correspondent aux exigences de protection de base.	**Processus: documenté** Le niveau 2 exige qu'une organisation établisse et documente des pratiques et des politiques pour guider la mise en œuvre de ses efforts en lien avec le CMMC. La documentation des pratiques permet leur répétabilité. Les organisations développent des capacités matures en documentant leurs processus, puis en les mettant en pratique tels qu'ils sont documentés. **Pratiques: hygiène cybernétique intermédiaire** Le niveau 2 sert de niveau de progression intermédiaire entre le niveau 1 et le niveau 3 et consiste en un sous-ensemble des exigences de sécurité spécifiées dans NIST SP 800-171 complété par des pratiques provenant d'autres normes et références.	**Processus: géré** Le niveau 3 exige qu'une organisation établisse un plan démontrant la gestion des activités pour la mise en œuvre de la pratique, qu'elle assure la maintenance de ce plan et qu'elle lui attribue les ressources nécessaires. Le plan peut comprendre des informations sur les missions, les objectifs, les plans de projet, les ressources, la formation requise et la participation des parties prenantes concernées. **Pratiques: bonne hygiène cybernétique** Le niveau 3 se concentre sur la protection des «Informations non classifiées contrôlées» et englobe toutes les exigences de sécurité spécifiées dans NIST SP 800-171 ainsi que des pratiques supplémentaires provenant d'autres normes et références visant à atténuer les menaces.	**Processus: réexaminé** Le niveau 4 exige qu'une organisation réexamine ses pratiques et en mesure l'efficacité. À ce niveau, en plus de mesurer l'efficacité des pratiques, les organisations sont capables de prendre des mesures correctives si nécessaire et d'informer la direction supérieure de l'état de la situation ou des problèmes qui se présentent de façon récurrente. **Pratiques: proactif** Le niveau 4 se concentre sur la protection des «Informations non classifiées contrôlées» et englobe un sous-ensemble des exigences de sécurité renforcées. Ces pratiques renforcent les capacités de détection et de réponse d'une organisation pour faire face à l'évolution des tactiques, techniques et procédures et s'y adapter.	**Processus: optimisé** Le niveau 5 exige qu'une organisation normalise et optimise la mise en œuvre des processus dans l'ensemble de l'organisation. **Pratiques: avancé/progressif** Le niveau 5 se concentre sur la protection des «Informations non classifiées contrôlées». Les pratiques supplémentaires augmentent la profondeur et la sophistication des capacités de cybersécurité.
Modèle de maturité de la cybersécurité communautaire (MMCSC)	**Sensibilisation à la sécurité** Le principal thème des activités à ce niveau est de sensibiliser les individus et organisations aux menaces, problèmes et questions liés à la cybersécurité.	**Élaboration des processus** Niveau conçu pour aider les communautés à établir et améliorer les processus de sécurité nécessaires pour traiter efficacement les problèmes de cybersécurité.	**Culture de l'information** Conçu pour améliorer les mécanismes de partage d'information au sein de la communauté afin de permettre à cette dernière de corréler efficacement des informations apparemment disparates.	**Élaboration des tactiques** Les éléments de ce niveau sont conçus pour élaborer des méthodes à la fois meilleures et plus proactives pour la détection des attaques et la réponse aux attaques. À ce niveau, la plupart	**Capacité opérationnelle de sécurité totale** Ce niveau renferme tous les éléments qui devraient être mis en place pour permettre à une organisation de se considérer comme pleinement préparée sur

				des méthodes de prévention devraient être en place.	le plan opérationnel à faire face à tout type de cybermenace.
Modèle des capacités d'audit interne (MCAI) dans le secteur public	**Initial** Pas de capacités durables et répétables – dépend des efforts individuels.	**Infrastructures** Pratiques et procédures durables et répétables.	**Intégration** Pratiques professionnelles et de gestion appliquées uniformément.	**Gestion** Intègre les informations provenant de toute l'organisation pour améliorer la gouvernance et la gestion des risques.	**Optimisation** Apprentissage à l'intérieur et à l'extérieur de l'organisation pour une amélioration continue.

Tableau 7: Comparaison des attributs/dimensions

	Modèle de maturité des capacités en matière de cybersécurité pour les nations (MMC)	Modèle de maturité des capacités en matière de cybersécurité (C2M2)	Modèle de maturité des capacités en matière de cybersécurité au Qatar (Q-C2M2)	Certification du modèle de maturité de la cybersécurité (CMMC)	Certification du modèle de maturité de la cybersécurité (CMMC)	Modèle de maturité de la sécurité de l'information pour le NIST Cybersecurity Framework (MMSI)	Cadre pour l'amélioration de la cybersécurité des infrastructures critiques	Indice mondial de la cybersécurité (IMCS)	L'Indice de cyberpuissance (ICP)
Niveaux	5 dimensions subdivisées en plusieurs facteurs, comprenant eux-mêmes de multiples aspects et indicateurs (Figure 4)	10 domaines comprenant un objectif de gestion unique et plusieurs objectifs d'approche (Figure 6)	5 domaines divisés en sous-domaines	17 domaines subdivisés en processus et comprenant une à plusieurs capacités, qui sont ensuite détaillées en pratiques (Figure 9)	6 dimensions principales	23 domaines évalués	5 fonctions avec catégories et sous-catégories clés sous-jacentes (Figure).	5 piliers comprenant plusieurs indicateurs	4 catégories comprenant plusieurs indicateurs
Attributs/Dimensions	i Concevoir la politique et la stratégie de cybersécurité; ii Encourager une culture de la cybersécurité responsable au sein de la société; iii Développer les connaissances en matière de cybersécurité; iv Créer des cadres juridiques et réglementaires efficaces; et v Maîtriser les risques au moyen de normes, d'organisations et de technologies.	i Gestion des risques; ii Gestion des actifs, des changements et de la configuration; iii Gestion de l'identité et de l'accès; iv Gestion de la menace et des vulnérabilités; v Conscience situationnelle; vi Réponse aux événements et incidents; vii Gestion de la chaîne d'approvisionnement et des dépendances externes; viii Gestion de la main-d'œuvre; ix Architecture de cybersécurité; x Gestion du programme de cybersécurité.	i Comprendre (cybergouvernance, actifs, risques et formation); ii Sécuriser (sécurité des données, sécurité technologique, sécurité du contrôle d'accès, sécurité des communications et sécurité du personnel); iii Exposer (surveillance, gestion des incidents, détection, analyse et exposition); iv Répondre (planification de la réponse, atténuation et communication de la réponse); v Durabiliser (planification de la récupération, gestion de la continuité,	i Contrôle de l'accès; ii Gestion des actifs; iii Audit et responsabilité; iv Sensibilisation et formation; v Gestion de la configuration; vi Identification et authentification; vii Réponse aux incidents; viii Maintenance; ix Protection des médias; x Sécurité du personnel; xi Protection physique; xii Récupération; xiii Gestion des risques; xiv Évaluation de la sûreté; xv Conscience situationnelle; xvi Protection du système et des communications;	i Gestion des menaces; ii Mesures; iii Partage d'information; iv Technologies; v Formation; vi Test.	i Gestion des actifs; ii Environnement de l'entreprise; iii Gouvernance; iv Évaluation des risques; v Stratégie de gestion des risques; vi Évaluation de la conformité; vii Contrôle de l'accès; viii Sensibilisation et formation; ix Sécurité des données; x Processus et procédures de protection de l'information; xi Maintenance; xii Technologie de protection; xiii Anomalies et événements; xiv Surveillance continue de la sécurité; xv Processus de détection;	i Identifier; ii Protéger; iii Détecter; iv Répondre; v Rétablir.	i Juridique; ii Technique; iii Organisationnel; iv Renforcement des capacités; v Coopération.	i Cadre juridique et réglementaire; ii Contexte économique et social; iii Infrastructure technologique; iv Application industrielle.

			amélioration et dépendances externes).	xvii	Intégrité du système et des informations.		xvi xvii xviii xix xx xxi xxii xxiii	Planification de la réponse; Communication de la réponse; Analyse de la réponse; Atténuation de la réponse; Amélioration de la réponse; Planification de la récupération; Amélioration de la récupération; Communication de la récupération.	

ANNEXE B – BIBLIOGRAPHIE DE LA RECHERCHE DOCUMENTAIRE

Almuhammadi, S. and Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», in Computer Science & Information Technology (CS & IT). Disponible à l'adresse: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Disponible à l'adresse: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf

Belgian Government (2012) Cyber Security Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Disponible à l'adresse: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) «Introduction to Return on Security Investment».

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Disponible à l'adresse: https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Disponible à l'adresse: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Council of Ministers (2019) Portuguese Official Journal, Series 1 — No. 108 - Resolution of the Council of Ministers No. 92/2019. Disponible à l'adresse: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity - Self-assessment Tool (pas de date). Disponible à l'adresse: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011) Specialised cybercrime units - Good practice study. Disponible à l'adresse: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (pas de date). Disponible à l'adresse: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (pas de date) «Welcome to the NCSS Training Tool».

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Disponible à l'adresse: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Disponible à l'adresse: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Disponible à l'adresse: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Cybersecurity Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Commission européenne (2012) Règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Disponible à l'adresse: https://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:52012PC0238&from=fr

European Network and Information Security Agency (2012) NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

European Network and Information Security Agency (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

European Network and Information Security Agency (2016) Guidelines for SMEs on the security of personal data processing.

European Network and Information Security Agency (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

European Union and Agency for Network and Information Security (2017) Handbook on security of personal data processing. Disponible à l'adresse: http://dx.publications.europa.eu/10.2824/569768

European Union and Agency for Network and Information Security (2014) *ENISA – CERT Inventory – Inventory of CERT teams and activities in Europe*. Disponible à l'adresse: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Disponible à l'adresse: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Federal Chancellery of the Republic of Austria (2013) Austrian Cyber Security Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Federal Ministry of the Interior (2011) Cyber Security Strategy for Germany. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Cabinet du Premier ministre français (2014) Stratégie nationale pour la sécurité du numérique. Disponible à l'adresse: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) «Evaluating Business Process Maturity Models», Journal of the Association for Information Systems. Disponible à l'adresse: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Government of Bulgaria (2015) National Cyber Security Strategy - Cyber-resistant Bulgaria 2020.

Government of Croatia (2015) The National Cyber Security Strategy of The Republic of Croatia. Disponible à l'adresse: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Government of Greece (2017) National Cyber Security Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Government of Hungary (2018) Strategy for the Security of Network and Information Systems. Disponible à l'adresse: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Government of Ireland (2019) National Cyber Security Strategy. Disponible à l'adresse: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Government of Spain (2019) National Cyber Security Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Institute of Internal Auditors (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

International Telecommunication Union (ITU) (2018) The Global Cybersecurity Index. Disponible à l'adresse: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunication Union (ITU) (2018) Guide to developing a national cybersecurity strategy. Disponible à l'adresse: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) «Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework», International Review of Law.

Latvian Government (2014) Cyber Security Strategy of Latvia. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministry for Competitiveness and Digital, Maritime and Services Economy (2016) Malta Cyber Security Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministry of Economic Affairs and Communications (2019) Cybersecurity Strategy – Republic of Estonia. Disponible à l'adresse: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministry of National Defence Republic of Lithuania (2018) National Cyber Security Strategy.

National Cyber Security Centre (2015) National Cyber Security Strategy of the Czech Republic. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cyber Security Strategies - Interactive Map (pas de date). Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

National Cybersecurity Strategies Evaluation Tool (2018). Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

Institut national des normes et des technologies (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Institut national des normes et des technologies. Disponible à l'adresse: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Object Management Group (2008) Business Process Maturity Model. Disponible à l'adresse: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, European Union and Joint Research Centre - European Commission (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Disponible à l'adresse: https://www.oecd.org/sdd/42495745.pdf

Office of the commissioner of Electronic Communications and Postal Regulations (2012) Cybersecurity Strategy of the Republic of Cyprus.

Journal officiel de l'Union européenne (2008) DIRECTIVE 2008/114/CE DU CONSEIL du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. Disponible à l'adresse: https://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32008L0114&from=fr

Organisation for Economic Co-operation and Development (OECD) (2012) Cybersecurity policy making at a turning point. Disponible à l'adresse: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) «National Cyber Security Strategies - Practical Guide on Development and Execution».

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.

Presidency of the Council of Ministers (2017) The Italian Cybersecurity Action Plan. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Disponible à l'adresse: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Romanian Government (2013) Cyber security strategy of Romania. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Disponible à l'adresse: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN

Secretariat of the Security Committee (2019) Finland's Cyber Security Strategy 2019. Disponible à l'adresse: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovakian Government (2015) Cyber Security Concept of the Slovak Republic. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Directive 2010/41/UE du Parlement européen et du Conseil du 7 juillet 2010.

Smith, R. (2016) «Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016», in Smith, R., Core EU Legislation. Londres: Macmillan Education. Disponible à l'adresse: https://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32016L1148&from=fr

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Swedish Government (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

The Danish Government - Ministry of Finance (2018) Danish Cyber and Information Security Strategy. Disponible à l'adresse: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

The Federal Council (2018) National strategy for the protection of Switzerland against cyber risks.

The Luxembourguish Government Council (2018) National Cybersecurity Strategy. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

The Netherlands Governement (2018) National Cyber Security Agenda. Disponible à l'adresse: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-

security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

The White House (2018) National Cyber Strategy of the United States of America. Disponible à l'adresse: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Trimintzios, P., et al. (2011) Cyber Europe Report. Disponible à l'adresse: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report.* Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Disponible à l'adresse: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021 (2016). Disponible à l'adresse: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

University of Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) «ITU National Cybersecurity Strategy Guide». Disponible à l'adresse: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

White, G. (2007) «The Community Cyber Security Maturity Model», in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

ANNEXE C – AUTRES OBJECTIFS ÉTUDIÉS

Les objectifs détaillés ci-dessous ont été étudiés dans le cadre de la phase de recherche documentaire et des entretiens menés par l'ENISA. Les objectifs suivants ne font pas partie du cadre d'évaluation des capacités nationales, mais ils mettent en lumière des sujets qui méritent d'être abordés. Chacun des sous-chapitres suivants explique pourquoi l'objectif n'a pas été retenu.

- Développer des stratégies de cybersécurité sectorielles spécifiques;
- Lutter contre les campagnes de désinformation;
- Sécuriser les technologies de pointe (5G, IA, informatique quantique, etc.);
- Assurer la souveraineté des données; et
- Fournir des incitations pour le développement du secteur de la cyberassurance.

Développer des stratégies de cybersécurité sectorielles spécifiques

L'adoption de stratégies sectorielles qui ciblent les interventions et les incitations sectorielles introduit assurément une capacité décentralisée plus forte. Cette approche convient particulièrement aux États membres dont les OSE doivent composer avec des cadres et des réglementations différents et où il existe de nombreuses dépendances en raison de la nature transversale de la cybersécurité. En effet, dans plusieurs États membres, il est courant de compter des dizaines d'autorités nationales et d'organismes de régulation qui connaissent les spécificités de chaque secteur et qui détiennent un mandat pour faire appliquer une réglementation spécifique à chaque secteur.

Le Danemark, par exemple, a lancé six stratégies ciblées sur les efforts en matière de cybersécurité et de sécurité de l'information dans les secteurs les plus critiques afin de développer une capacité décentralisée plus forte dans ces domaines. Chaque «unité sectorielle» contribuera à l'évaluation des menaces au niveau sectoriel, à la surveillance, aux exercices de préparation, à la mise en place de systèmes de sécurité, au partage des connaissances et aux instructions, entre autres. Les stratégies sectorielles couvrent les secteurs suivants:

- Énergie;
- Soins de santé;
- Transports;
- Télécommunications;
- Finances; et
- Maritime.

D'autres États membres ont exprimé leur intérêt à l'égard des stratégies de cybersécurité sectorielles spécifiques afin de refléter toutes les exigences réglementaires. Cependant, il convient de noter qu'un tel objectif pourrait ne pas convenir à tous les États membres en fonction de leur taille, de leurs politiques nationales et de leur maturité. La grande difficulté à s'assurer que le cadre puisse prendre en compte toutes les spécificités a conduit l'ENISA à ne pas inclure cet objectif dans le cadre.

Lutter contre les campagnes de désinformation

Les États membres intègrent la protection des principes fondamentaux tels que les droits de l'homme, la transparence et la confiance du public dans leurs stratégies nationales de cybersécurité. Cette démarche est cruciale, surtout lorsqu'on a affaire à une désinformation diffusée par les médias d'information traditionnels ou les plates-formes des médias sociaux. En outre, la cybersécurité est actuellement l'un des plus grands défis électoraux. En effet, des activités telles que la diffusion de fausses informations ou de propagande négative ont été observées dans divers pays à l'approche d'élections importantes. Cette menace est susceptible de nuire au processus démocratique de l'UE. À l'échelle européenne, la Commission a présenté un plan d'action[32] pour intensifier les efforts de lutte contre la désinformation en Europe: ce plan se concentre sur quatre domaines clés (détection, coopération, collaboration avec les plates-formes en ligne et sensibilisation) et sert à développer les capacités de l'UE et à renforcer la coopération entre les États membres.

Quatre des 19 pays interrogés ont fait part de leur intention d'aborder le problème de la désinformation et de la propagande dans leur SNCS.

Par exemple, la SNCS[33] française dispose ce qui suit: «Il appartient à l'État d'informer les citoyens sur les risques de manipulation et les techniques de propagande utilisées par des acteurs malveillants sur Internet. Après les attentats perpétrés contre la France en janvier 2015, le gouvernement a mis en place une plate-forme d'information sur les risques liés à la radicalisation islamiste via les réseaux de communications électroniques: "Stop-djihadisme.gouv.fr".» Cette approche pourrait être étendue pour répondre à d'autres phénomènes de propagande ou de déstabilisation.»

Autre exemple, la SNCS 2019-2024 de la Pologne[34] précise ceci: «contre les activités manipulatrices telles que les campagnes de désinformation, des actions systémiques sont nécessaires pour sensibiliser les citoyens à la nécessité de vérifier l'authenticité des informations et de réagir aux tentatives de déformation des informations».

Toutefois, lors des entretiens menés par l'ENISA, plusieurs États membres ont indiqué qu'ils n'abordaient pas le problème dans le cadre de leur SNCS comme une menace pour la cybersécurité, mais plutôt à un niveau sociétal plus large, par exemple, au travers d'initiatives politiques.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Sécuriser les technologies de pointe (5G, IA, informatique quantique, etc.)

Alors que la menace informatique continue de se renforcer, le développement de nouvelles technologies entraînera très probablement une augmentation de l'intensité et du nombre de cyberattaques et une diversification des méthodes, des moyens et des cibles utilisés par les acteurs de la menace. Toujours est-il que ces nouvelles solutions technologiques de pointe ont le potentiel de devenir les éléments constitutifs du marché numérique européen. Afin de protéger la dépendance numérique croissante des États membres et l'émergence de nouvelles technologies, des mesures d'incitation et des politiques à part entière devraient être mises en place pour soutenir le développement et le déploiement sûrs et fiables de ces technologies dans l'UE.

Au cours de la phase de recherche documentaire effectuée sur les SNCS des États membres, les technologies de pointe suivantes ont été citées comme présentant un intérêt pour les États membres: la 5G, l'IA, l'informatique quantique, la cryptographie, l'informatique de périphérie, les véhicules connectés et autonomes, les mégadonnées et les données intelligentes, la chaîne de blocs, la robotique et l'IdO.

Plus particulièrement, début 2020, la Commission européenne a publié une communication appelant les États membres à faire le nécessaire pour mettre en œuvre l'ensemble des mesures recommandées dans les conclusions de la boîte à outils sur la 5G[35]. Cette boîte à outils sur la 5G fait suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G adoptée par la Commission en 2019, qui plaidait en faveur d'une approche européenne unifiée en matière de sécurité des réseaux 5G[36].

Au cours des entretiens menés par l'ENISA, il a été souligné que ce sujet est davantage un sujet transversal abordé dans l'ensemble de la SNCS plutôt que comme un objectif spécifique en soi.

Assurer la souveraineté des données

D'une part, le cyberespace peut être considéré comme un formidable espace commun mondial, facilement accessible, offrant un haut degré de connectivité et capable de générer de grandes opportunités de croissance socioéconomique. D'autre part, le cyberespace se caractérise aussi par sa faible juridiction, la difficulté d'attribuer des actions, l'absence de frontières, et des systèmes interconnectés pouvant être poreux et dont les données peuvent être volées ou même accessibles à des gouvernements étrangers. Outre ces deux perspectives, l'écosystème numérique est marqué par la concentration des plates-formes et des infrastructures de services en ligne appartenant à un groupe très restreint d'acteurs. Tous les aspects susmentionnés amènent les États membres à promouvoir la souveraineté numérique. Atteindre la souveraineté numérique signifie que les citoyens et les entreprises sont en mesure de s'épanouir pleinement en utilisant des services numériques et des produits TIC fiables sans craindre pour leurs données personnelles, leurs actifs numériques, leur autonomie économique ou leur influence politique.

La souveraineté des données ou la souveraineté numérique est défendue par les États membres à l'échelle internationale et à l'échelle européenne. Bien que les États membres ne

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

semblent pas aborder la question directement dans leur SNCS en tant qu'objectif spécifique, soit ils l'abordent en tant que principe transversal, soit ils exposent leur intention de garantir la souveraineté numérique à l'échelle nationale dans des publications ad hoc en se concentrant sur les technologies clés. Par exemple, dans la revue stratégique de cyberdéfense française de 2018, il est indiqué que «la maîtrise des technologies suivantes est primordiale pour assurer la souveraineté numérique: chiffrement des communications, détection des cyberattaques, radios professionnelles mobiles, cloud computing et intelligence artificielle»[37].

À l'échelle européenne, les États membres participent activement à la définition de la stratégie européenne pour les données (COM/2020/66 final) et à l'élaboration du cadre de certification de l'UE pour les produits, services et processus numériques des TIC établi par le règlement de l'UE sur la cybersécurité (2019/881) afin de garantir l'autonomie numérique stratégique au niveau européen.

La phase d'entretiens avec les États membres a montré que le sujet de la souveraineté numérique est souvent considéré comme une question plus vaste, qui ne se limite pas à la cybersécurité. C'est ce qui explique que les États membres ne couvrent pas le sujet dans leur SNCS et, pour les rares qui le font, qu'ils ne le couvrent pas comme un objectif spécifique en soi.

Fournir des incitations pour le développement du secteur de la cyberassurance

L'état actuel du secteur de la cyberassurance montre que le marché mondial s'est incontestablement développé. Cependant, il n'en est qu'à ses débuts: il faut encore collecter des données et de nombreux précédents doivent encore être établis (par exemple, couverture du risque silencieux, cyberrisques systémiques, etc.). De plus, les pertes estimées cumulées des cyberattaques dans le monde entier sont d'un tout autre ordre de grandeur par rapport à la capacité de couverture actuelle du secteur de la cyberassurance (Document de travail du FMI – Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). Cependant, le développement du secteur de la cyberassurance peut certainement apporter des avantages et jeter les bases de mécanismes vertueux. En effet, les mécanismes de cyberassurance peuvent aider:

- À sensibiliser les entreprises aux cyberrisques;
- À évaluer l'exposition aux cyberrisques de manière quantitative;
- À améliorer la gestion des cyberrisques;
- À fournir un soutien aux organisations victimes de cyberattaques; et
- À couvrir les dommages (matériels ou non) induits par une cyberattaque.

Certains États membres ont commencé à travailler sur ce sujet. Par exemple:

- L'Estonie a adopté une approche «attentiste» dans sa SNCS: «Pour atténuer les cyberrisques dans le secteur privé en général, la demande et l'offre de services de cyberassurance en Estonie seront analysées et, sur cette base, des principes de coopération pour les parties liées seront convenus, y compris en ce qui concerne le partage d'information, la préparation de l'évaluation des risques, etc. Aujourd'hui, les fournisseurs de services de cyberassurance sont peu nombreux sur le marché estonien et il est nécessaire de commencer par déterminer qui offre quoi. La

[37] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

complexité de la protection d'assurance est souvent considérée comme une entrave au développement du marché de la cyberassurance.»

- Le Luxembourg soutient spécifiquement le développement du secteur de la cyberassurance dans sa SNCS: «Objectif 1: Création de nouveaux produits et services. Pour mutualiser les risques et encourager la victime d'un incident numérique cyber à recourir à l'aide d'un expert pour gérer cet incident et pour rétablir le système affecté par un acte malicieux, les compagnies d'assurance seront encouragées à créer des produits spécifiques dans le domaine de l'assurance cyber.»

Les réactions des personnes interrogées ont été très diverses sur ce sujet: certains États membres ont déclaré que la cyberassurance est récemment devenue un sujet de discussion, tandis que d'autres ont fait savoir que, bien que le sujet soit prometteur, le secteur n'est pas encore assez mature. Cependant, un grand nombre de personnes interrogées ont déclaré que le sujet n'est pas abordé dans le cadre de la SNCS, soit parce qu'il a été jugé trop spécifique, soit parce qu'il ne relève pas du champ d'application de la SNCS.

TP-02-21-253-FR-N

À propos de l'Agence européenne pour la cybersécurité

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations, consultez www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-483-1
DOI: 10.2824/46758