MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Direction générale
de l'armement

GUIDE SDI SECNUM
N°2217

RÉFÉRENTIEL DE MATURITÉ CYBER NIVEAU « FONDAMENTAL »

2ème édition
(Les dates précises d'approbation et de publication sont accessibles dans SysMan)

Document entretenu par DGA/SSDI

L'édition en vigueur de ce document est celle accessible dans SysMan,
avec les informations complémentaires de sa fiche documentaire dématérialisée.
S'assurer de la validité et de la complétude de toute copie avant usage.

Rédaction	Jean-Pierre LEBEE	DGA/SSDI/DOCS	Adjoint Industrie et International
Vérification	Sylvie ULMANN	DGA/SSDI/DOCS	Animatrice du sous domaine SDI SecNum
Vérification	Stéphane GUILBERT	DGA/SSDI/DOCS	Responsable du sous-domaine SDI SecNum
Vérification	Nathalie BOUCHEZ	DGA/SSDI/AD	Animatrice et Responsable déléguée du domaine SDI
Approbation	Laurence GABOULEAUD	DGA/SSDI/D	Responsable du domaine SDI

POSITIONNEMENT DANS **L'ENVIRONNEMENT DGA**

Directions (entités) d'application :	Industriels de Défense
Activité du domaine de performance :	SDI
Pôles/métiers :	Maitrise des risques courants/Sécurité de défense et de l'information (MRC / SDI)
Systèmes de management :	ISO 9001

ÉVOLUTIONS

Nature des évolutions :	Mise sous la charte DGA actualisée et enregistrement qualité
Documents abrogés par cette édition :	

DÉCLINAISON

Autorisation de déclinaison :	☐	Le cas échéant, précisions du périmètre de déclinaison :

TABLE DES MATIÈRES

ANNEXE

GUIDE

Objet : Référentiel de maturité cyber niveau « fondamental »

1. OBJET DU DOCUMENT

Ce référentiel de maturité a été élaboré au sein d'un groupe de travail piloté par la DGA et réunissant des grands industriels de la Défense.

Il s'appuie sur différents documents de l'ANSSI (guide d'hygiène, 13 questions pour les TPE/PME, …) et vise à assurer par construction des équivalences avec des référentiels internationaux (CMMC notamment).

Il vise à assurer un niveau minimal de sécurité, permettant de contrer des attaques basiques. Il ne garantit donc pas l'entreprise qui l'applique contre toutes les menaces cyber.

2. CHAMP D'APPLICATION

Ce premier niveau de maîtrise du risque cyber vise à couvrir non seulement la confidentialité mais aussi la continuité d'activité les risques de propagation d'attaques via la supply chain.

Ces exigences concernent les SI utilisés pour la réalisation des contrats identifiés par le donneur d'ordre comme concourant à des activités de défense et notamment ceux qui ne sont pas soumis à une réglementation. Les contrats traitant d'informations protégées (DR) ou classifiées (S ou TS) sont en effet soumis à des textes réglementaires spécifiques, précisés dans les plans contractuels de sécurité ou les clauses des contrats. D'autres données comme par exemple les données à caractère personnel[1] font elles aussi l'objet de réglementations spécifiques.

Les informations sensibles ou les données sensibles de l'entreprise dont il est question dans ce document sont celles dont la connaissance, la modification ou la destruction par un tiers hostile permet de nuire à l'entreprise, ses clients ou ses fournisseurs ; comme par exemple des informations commerciales ou financières, des informations techniques précises, des secrets industriels, des données sensibles identifiées comme telles par des clients (dites données confiées), des logiciels livrés aux clients, etc.

3. SIGLES ET ABRÉVIATIONS

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations
CMMC	Cybersecurity Maturity Model Certification
CSIRT	Computer Security Incident Response Team
DIAG	Diagnostic cyber
DR	Diffusion Restreinte (niveau de protection)
DRSD	Direction du Renseignement et de la Sécurité de la Défense
ETI	Entreprise de Taille Intermédiaire
FAR	Federal Acquisition Rules
GICAN	Groupement des Industries de Construction et Activités Navales
GIFAS	Groupement des Industries Françaises Aéronautiques et Spatiales
GICAT	Groupement des Industries françaises de défense et de sécurité terrestres et aéroterrestres
MinArm	Ministère des Armées
NIST	National Institute of Standards and Technology
NP	Non Protégé
PME	Petite et Moyenne entreprise
PSSI	Politique de Sécurité des Systèmes d'Information
S	Secret (niveau de classification)

[1] https://www.cnil.fr/fr/reglement-europeen-protection-donnees

SDI	Sécurité de défense et de l'information
SecNum	Sécurité du Numérique
SI	Système d'Informations
TPE	Très Petite Entreprise
TS	Très Secret (niveau de classification)

4. UTILISATION DE CE REFERENTIEL

Ce référentiel doit être considéré comme un socle de base, permettant aux entreprises de commencer à traiter le risque cyber en mettant en place un premier niveau de protection de leurs activités et leurs actifs. Dans un environnement où les menaces sont toujours plus nombreuses, la montée en maturité cyber est un impératif majeur pour la continuité d'activité, voire la survie de la plupart des entreprises.

Ce référentiel peut être utilisé :

- De manière contractuelle, par un donneur d'ordre vers un de ses sous-traitants ou fournisseurs pour évaluer son niveau de maturité cyber.
- Dans le cadre d'un processus d'auto-évaluation par une entreprise souhaitant valoriser son niveau de maturité cyber auprès de ses donneurs d'ordres.

Il sera à terme utilisé dans le cadre d'un processus de certification de la maturité cyber.

Le référentiel de niveau fondamental a été conçu avec un souci de pragmatisme en proposant des mesures organisationnelles simples et des mesures techniques qui sont basées sur une configuration adaptée des systèmes d'exploitation (Windows, …) ou de logiciels très standards comme des anti-virus.

La mise en conformité à ces exigences ne demande donc pas d'investissements lourds en matériels ou logiciels spécialisés. Elle peut par contre demander des compétences techniques qui ne sont pas forcément disponibles dans toutes les entreprises. Il est dans ce cas possible de faire appel à un prestataire externe disposant de compétences cyber reconnues. On peut citer notamment les prestataires qualifiés par l'ANSSI[2], ceux identifiés par Aircyber de BoostAérospace ou le réseau des ExpertCyber[3] de Cybermalveillance qui peuvent être mobilisés pour ces travaux de sécurisation.

4.1 Exigences

Chaque exigence se présente sous la forme d'un tableau comprenant les éléments suivants :

- Référence ;
- Un libellé ;
- Un commentaire permettant de préciser le périmètre de l'exigence ;
- Les éléments de preuve devant être disponibles chez l'industriel en cas d'audit ;
- Des éléments d'appréciation de la preuve si besoin.

4.2 Réponses aux exigences

L'entreprise devra réaliser une évaluation du niveau de maturité cyber de son SI par rapport aux règles du présent référentiel. Cette analyse devra identifier les écarts entre les mesures mises en place et ces règles. Elle devra aussi s'assurer que les éléments de preuve demandés sont bien disponibles et accessibles dans le cas d'un éventuel audit.

Il n'y a pas de formalisme particulier imposé pour les éléments de preuve. L'entreprise peut cependant les rassembler dans un document unique, constituant ainsi une première version d'une politique de sécurité des systèmes d'information (PSSI).

[2] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[3] https://www.cybermalveillance.gouv.fr/accompagnement

4.3 Traitement des écarts

En analysant ce référentiel, une entreprise peut identifier des écarts par rapport aux exigences. Deux cas principaux sont envisageables :

- L'entreprise n'a pas encore mis en place les moyens techniques ou organisationnels requis (par exemple, elle n'a pas désigné de point de contact cyber, elle n'a pas défini de règles de gestion de ces mots de passe, …). Dans ce cas, il est souhaitable que l'entreprise produise un plan d'action listant les actions proposées et les jalons calendaires associés pour atteindre le niveau demandé. La fourniture de ce plan d'action peut être rendue obligatoire par voie contractuelle ou dans le cadre d'un processus de certification.
- L'entreprise considère que l'exigence n'est pas applicable sur l'ensemble des systèmes concernés. Par exemple, l'authentification individuelle de chaque utilisateur peut poser des problèmes dans un environnement industriel où les postes sont partagés par plusieurs opérateurs ou sont associés à des processus continus. Dans ce cas il est demandé à l'entreprise de justifier pourquoi les exigences ne peuvent être atteintes sur certains systèmes et éventuellement les mesures additionnelles mises en place (par exemple le service RH peut identifier qui était présent sur un poste de travail sur une période donnée).

L'évaluation du niveau de maturité cyber d'un SI par rapport aux règles du présent référentiel comprend donc :

- L'ensemble des règles avec lesquelles l'entreprise est conforme.
- La justification de chaque exception aux règles du présent référentiel.
- Le cas échéant, un plan d'action, où pour chaque écart qu'elle identifie l'entreprise indique les actions mises en place pour le corriger. Ce plan d'action prévoit, au minimum, l'échéance et le responsable de la mise en œuvre de chaque action.

Une attestation formelle est réalisée par le dirigeant exécutif de l'entreprise ou par toute personne qu'il désigne, à partir de ces éléments.

4.4 Mise à jour de **l'évaluation du niveau de maturité cyber**

La durée de validité de l'attestation formelle ne peut excéder trois ans.

Le réexamen de l'évaluation du niveau de maturité cyber peut être demandé contractuellement ou imposé par un processus de certification.

Dans tous les cas, l'entreprise réexamine le niveau de maturité cyber du système au moins tous les ans ou lorsqu'un événement est de nature à modifier le contexte dans lequel cette déclaration a été établie (par exemple un changement majeur de l'architecture du système d'information, changement d'organisation, etc.). L'entreprise archive les versions successives des attestations.

5. INFOGERANCE

De nombreuses entreprises mettent en place des contrats de service au périmètre plus ou moins étendu pour assurer l'exploitation de leurs systèmes numériques (contrats d'infogérance). Cette sous-traitance ne dégage pas l'entreprise de ses responsabilités, par exemple en cas d'attaque cyber pouvant impacter ses clients. Par contre, en fonction de la nature des activités ou tâches sous-traitées, une partie des exigences de ce référentiel pourra être réalisée par l'infogérant.

L'entreprise devra donc définir des clauses de sécurité dans les contrats qui la lient avec ses prestataires et fournisseurs de produits ou services numériques. Ces clauses devront être adaptées à la nature de la prestation réalisée et préciser le niveau de responsabilité du prestataire.

L'entreprise est responsable de contrôler la conformité de la prestation aux présentes règles, et doit obtenir des assurances contractuelles de cette conformité. Ces informations pourront être intégrées dans l'analyse de conformité.

6. LES SERVICES CLOUD

L'entreprise peut utiliser des services cloud, pour des applications de type messagerie (gmail, outlook, …), bureautique (office 365, google docs, …), ou pour héberger ses données ou ses services.

Cette forme d'externalisation pose par contre plusieurs risques qui doivent être analysés. Par exemple elle entraine des problèmes de dépendance à un tiers (et peut entrainer des difficultés de réversibilité si l'entreprise souhaite changer de fournisseur ou internaliser certains services) mais aussi de protection des données. Les risques peuvent venir dans ce second cas d'une défaillance technique du fournisseur de service, d'actions liées à des lois d'extraterritorialité comme le CLOUD act américain, voire à des clauses contractuelles imposées par le fournisseur (analyse des données systématique pour rechercher des contenus illégaux dans les mails ou les volumes de stockage).

Le recours à des services de cloud doit donc être une décision réfléchie, intégrant le risque cyber mais aussi le risque sur la propriété intellectuelle ou le patrimoine scientifique et technique de l'entreprise. Le recours à des solutions certifiées SecNumcloud par l'ANSSI peut permettre de répondre à un certain nombre des risques précités. Comme pour le recours à l'infogérance, le choix d'utiliser des services cloud n'exonère pas l'entreprise de ses responsabilités en matières de cybersécurité.

D'un point de vue technique, la grande diversité des services proposés (SaaS, PaaS, IasS, …) et des options contractuelles ne permet pas de définir une façon unique de décliner le présent référentiel.

L'entreprise devra donc en fonction de son contrat, identifier ce qui relève de sa responsabilité et ce qui est contractuellement réalisé par son fournisseur. Pour prendre un exemple, le fait que des données sont hébergées dans un cloud ne signifie pas que celles-ci sont sauvegardées. Cette sauvegarde peut être à la charge de l'utilisateur selon le contrat choisi.

7. RESSOURCES

Il existe une multitude d'informations disponibles sur le sujet de la cybersécurité. Les liens ci-dessous renvoient principalement vers des sites de l'administration.

7.1 ANSSI

Le site de l'ANSSI (www.ssi.gouv.fr) permet d'accéder à un volume très large d'information :

- Un MOOC de sensibilisation : https://secnumacademie.gouv.fr/ ;
- Un ensemble de guides de bonnes pratiques : https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/, https://www.ssi.gouv.fr/entreprise/precautions-elementaires/ ;
- Des listes de produits ou de prestataires qualifiés ;
- Des liens vers des formations labellisées ;
- Les textes réglementaires applicables.

Les délégués de l'ANSSI en régions, en lien avec les structures et les autorités régionales existantes peuvent apporter un soutien pour prévenir les incidents et sensibiliser les acteurs locaux du public et du privé aux bonnes pratiques informatiques : https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/

Ces actions s'appuient notamment sur le réseau de CSIRT (Computer Security Incident Response Team) régionaux en cours de mise en place pour prodiguer de l'assistance en cas d'incident cyber ou du conseil : https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux/

7.2 Ministère des Armées

Le ministère des Armées via notamment la DGA propose un ensemble de dispositifs destinés aux PME et ETI (https://www.defense.gouv.fr/nos-enjeux/dispositifs-specifiques-aux-pme-eti-du-ministere-armees) et notamment le DIAG Cyber qui permet de subventionner jusqu'à 80% des prestations d'audit et de conseil en cybersécurité.

La DRSD (Direction du renseignement et de la sécurité de la défense) propose des séances de sensibilisation dans le cadre de ses missions de contre-ingérence économique ou cyber : https://www.drsd.defense.gouv.fr/nos-missions#H

6.3 Cyber malveillance

Le site Cybermalveillance (https://www.cybermalveillance.gouv.fr/) permet notamment d'accéder à des experts de proximité labellisés :
https://www.cybermalveillance.gouv.fr/accompagnement/accueil

7.3 Autres acteurs non étatiques

Le pôle d'excellence cyber, met à disposition un ensemble de liens et d'informations pratiques comme par exemple un guide pratique de sécurité numérique pour les PME/PMI, Collectivités et petites organisations : https://www.pole-excellence-cyber.org/presentation-du-pole/guide-de-securite/

Dans le secteur privé des groupements professionnels sectoriels comme le GICAT, le GIFAS ou le GICAN peuvent aussi proposer des dispositifs de soutien ou d'accompagnement.

8. EXIGENCES

Les exigences sont définies dans le document : 20230708_NP_Formulaire-SDI-SecNum-2216-Ed.07_Socle Commun automatisé.xls disponible sur le site internet suivant : www.armement.defense.gouv.fr/ rubrique sécurité et habilitation / Sécurité du numérique.

ANNEXE I - TRAÇABILITE AVEC CMMC LEVEL 1

catégorie	exigence	référentiel Défense
Access control	AC.1.001 AC.L1-3.1.1 *Authorized Access Control* Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 2 3.1.1	RefDef-Protect-F5 RefDef-Protect-F9
	AC.1.002 AC.L1-3.1.2 *Transaction & Function Control* Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 2 3.1.2	RefDef-Protect-F9 RefDef-Protect-F13
	AC.1.003 AC.L1-3.1.20 *External Connections* Verify and control/limit connections to and use of external information systems. • FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev 2 3.1.20	RefDef-Protect-F1
	AC.1.004 AC.L1-3.1.22 *Control Public Information* Control information posted or processed on publicly accessible information systems. • FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 Rev 2 3.1.22	RefDef-Gouv-F2
identification &authentification	IA.1.076 IA.L1-3.5.1 *Identification* Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev 2 3.5.1	RefDef-Protect-F9
	IA.1.077 IA.L1-3.5.2 *Authentication* Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev 2 3.5.2	RefDef-Protect-F9 RefDef-Protect-F10
Media protection	MP.1.118 MP.L1-3.8.3 *Media Disposal* Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. • FAR Clause 52.204-21 b.1.vii • NIST SP 800-171 Rev 2 3.8.3	RefDef-Gouv-F6
Physical protection	PE.1.131 PE.L1-3.10.1 *Limit Physical Access* Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. • FAR Clause 52.204-21 b.1.viii • NIST SP 800-171 Rev 2 3.10.1	RefDef-Protect-F11
	PE.1.132 PE.L1-3.10.3 *Escort Visitors* Escort visitors and monitor visitor activity. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.3	RefDef-Protect-F12
	PE.1.133 PE.L1-3.10.4 *Physical Access Logs* Maintain audit logs of physical access. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.4	RefDef-Protect-F11
	PE.1.134 PE.L1-3.10.5 *Manage Physical Access*	RefDef-Protect-F11

catégorie	exigence	référentiel Défense
	Control and manage physical access devices. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.5	
system & communication protection	SC.1.175 SC.L1-3.13.1 *Boundary Protection* Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. • FAR Clause 52.204-21 b.1.x • NIST SP 800-171 Rev 2 3.13.1	RefDef-Protect-F1
	SC.1.176 SC.L1-3.13.5 *Public-Access System Separation* Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. • FAR Clause 52.204-21 b.1.xi • NIST SP 800-171 Rev 2 3.13.5	RefDef-Protect-F1
System and Information integrity	SI.1.210 SI.L1-3.14.1 *Flaw Remediation* Identify, report, and correct information and information system flaws in a timely manner. • FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 Rev 2 3.14.1	RefDef-Protect-F6
	SI.1.211 SI.L1-3.14.2 *Malicious Code Protection* Provide protection from malicious code at appropriate locations within organizational information systems. • FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 Rev 2 3.14.2	RefDef-Protect-F7
	SI.1.212 SI.L1-3.14.4 *Update Malicious Code Protection* Update malicious code protection mechanisms when new releases are available. • FAR Clause 52.204-21 b.1.xiv • NIST SP 800-171 Rev 2 3.14.4	RefDef-Protect-F7
	SI.1.213 SI.L1-3.14.5 *System & File Scanning* Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. • FAR Clause 52.204-21 b.1.xv • NIST SP 800-171 Rev 2 3.14.5	RefDef-Protect-F7 RefDef-Protect-F8