ÉCOCONCEPTION ET CYBERSÉCURITÉ :

GUIDE DE MISE EN APPLICATION

C4T

CYBER 4 TOMORROW

SOMMAIRE

Avant-propos

Souvent considérées comme des démarches aux logiques distinctes, la cybersécurité et l'écoconception peuvent pourtant se renforcer mutuellement. Si certaines exigences peuvent diverger et nécessitent des arbitrages, une analyse comparée des principales recommandations des deux domaines met en évidence de réelles synergies et des leviers d'action communs.

Le guide « Écoconception et cybersécurité : guide de mise en application » conçu par le GT « Écoconception & Cybersécurité » rattaché à l'initiative Cyber4Tomorrow[1] s'inscrit dans la continuité des travaux produits par la Mission interministérielle au numérique écoresponsable (MiNumEco)[2].

Réalisé par les professionnels de la cybersécurité et du Numérique Responsable, le présent document s'attache à cartographier les synergies et divergences liant cybersécurité et écoconception, en expliquant les critères et les arguments utilisés pour l'évaluation. Il propose également des pistes de réfléxions pour batir une cybersécurité plus durable.

Il est structuré autour de deux axes de lecture complémentaires :

- Premièrement, l'analyse des critères d'écoconception présentés dans le Référentiel Général d'Ecoconception des Services Numériques (RGESN)[3] à l'aune de bonnes pratiques de cybersécurité ;
- Deuxièmement, l'étude des contrôles de cybersécurité issus du référentiel de sécurité du National Institute of Standards and Technology (NIST)[4] du point de vue des impacts environnementaux.

En complément, une étude prospective des objectifs de sécurité issus de la transposition de la directive européenne Network and Information Security 2 (NIS2) dans le droit français[5], a été réalisée.

L'objectif de cette analyse est de favoriser la prise en compte conjointe de l'écoconception et des mesures de cybersécurité, en préservant un niveau de sécurité optimal des systèmes d'information.

La publication de ce document intervient dans un contexte marqué par la multiplication des signaux (réglementaires, normatifs, géopolitiques et environnementaux) encourageant le rapprochement des deux expertises. Ces premières réflexions entendent faciliter l'appropriation d'une approche « secure-and-sustainable-by-design » par les responsables de la sécurité des systèmes d'information (RSSI) et inspirer les organismes élaborant le cadre de protection face aux cyberattaques et de stabilité du cyberespace. Plus largement, elles visent à promouvoir cette approche comme fondement différenciant de la cybersécurité européenne.

[1] Cyber4Tomorrow (C4T) est une initiative co-portée par le Campus Cyber et Numeum qui vise à rassembler les professionnels de la cybersécurité pour construire un numérique de confiance. Disponible sur : https://cyber4tomorrow.fr/
[2] MiNUM ECO. (2022). Écoconception, cybersécurité et protection des données, quelles synergies ?. Disponible sur : https://ecoresponsable.numerique.gouv.fr/publications/ecoconception-securite/
[3] Référentiel général d'écoconception de services numériques (RGESN). (2024). Arcep, Arcom, en lien avec l'ADEME. Disponible sur : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/
[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. Disponible sur : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[5] ANSSI. (2026). NIS2 - Transposition nationale - Mesures de gestion des risques en matière de cybersécurité - RECYS : Référentiel Cyber France (ReCyF). Version 2.5 du 17/03/2026. Disponible sur : https://messervicescyber-ressources.cellar-c2.services.clever-cloud.com/20260317_NIS_V2_ReCyF_v2.5.pdf

Remerciements

Remerciements

L'initiative Cyber4Tomorrow et le Campus Cyber tiennent à remercier l'ensemble des contributrices et contributeurs du GT « Ecoconception & Cybersécurité » ayant travaillé sur le guide « Ecoconception et cyberséurité - Guide de mise en application » depuis le lancement des travaux, en avril 2025.

- **Les coordinateurs :** Emmanuel Laroche (Sopra Steria), Agnès Comte (Banque de France)

- **Les contributeurs actifs :** Nicolas Perrin (Banque de France), Corinne Rosaenz (Thales), Laurent Theringaud (Thales), Antoine Planquette (RATP), Yoann Bouchet (RATP), Cyril Sompairac (RATP), Renaud Heluin (RATP), Jérémie Jourdin (Advens), Marine Chabran Rodrigues (Wavestone), Skander Guetari (Capgemini), Christophe Acezat (Société Générale), Isabelle Berrien (Société Générale).

Les remerciements sont également adressés aux membres du Comité de relecture, composé comme suit :

- ADIRA : Pierre-Antoine Troubat
- AGIT : Emmanuelle Olivié-Paul
- CESIN : Loïs Samain
- Green IT : Auban Derreumaux, Laure Alfonsi
- INR : Vincent Courboulay
- IRIT : Romain Laborde

1. Introduction

1. Introduction

1.1 Contexte et enjeux

Recours croissant à l'intelligence artificielle, construction massive de centres de données... l'accélération technologique dont nous sommes témoins lance des défis de taille aux acteurs du numérique. Dans un contexte marqué par le dérèglement climatique, la raréfaction des ressources critiques et la densification des tensions géopolitiques, une question pourtant cruciale fait figure de grande absente : celle de la compréhension et de l'amélioration des impacts environnementaux[6] de la cybersécurité. En parallèle, les cyberattaques se multiplient et deviennent de plus en plus sophistiquées.[7] L'écoconception apparaît alors comme un précieux allié pour aider la cybersécurité à relever ces enjeux de sécurité, mais également pour évaluer, maîtriser et optimiser ses propres externalités environnementales (ex : émissions carbone, consommation d'eau, impacts sur la biodiversité, épuisement des ressources abiotiques...).

De même, les crises climatiques et géopolitiques induisent des évolutions progressives - mais durables - dans les pratiques de cybersécurité : gestion des risques redéfinie par la multiplication des catastrophes climatiques[8], évolutions réglementaires[9] ou normatives[10] appelant à une meilleure prise en compte de l'impact environnemental de la cybersécurité, tensions géopolitiques croissantes augmentant le risque aux dépendances aux infrastructures étrangères, souvent plus polluantes[11]... Au-delà d'apporter une réponse nécessaire à ces enjeux contemporains ces changements structurels appellent un sursaut stratégique collectif. Ils ouvrent la voie au développement d'un modèle numérique européen puissant, alliant nativement exigences de sécurité et optimisation de l'empreinte environnementale.

À rebours d'une opposition superficielle, la cybersécurité et le Numérique Responsable ne s'affrontent donc pas entre logique d'empilement et logique de suppression : ils convergent dans une même démarche de maîtrise des risques et d'adaptation durable de l'organisation à son environnement, à intégrer dès la conception des produits et services et dans la sécurisation des systèmes d'information. On parle d'une approche conjointe, mêlant au plus tôt « écoconception » et « cybersécurité ».

Le guide d'écoconception des services numériques, document AFNOR Spec 2201, définit l'écoconception comme une « approche méthodique qui prend en considération les aspects environnementaux du processus de conception et développement dans le but de réduire les impacts environnementaux négatifs tout au long du cycle de vie d'un produit. Appliquée aux services numériques, l'écoconception a pour objectif de réduire ou limiter les impacts environnementaux de ces services, de l'expression des besoins jusqu'à leur fin de vie. » [12]

[6] L'empreinte environnementale d'un produit ou service numérique est généralement calculée selon la méthode ACV multi-critères, cadrée par le standard européen "PEF" et reposant sur la norme ISO 14040/44.
[7] ANSSI. (2026). Panorama de la menace 2025. Disponible sur : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf
[8] World Economic Forum. (2026). Global Cybersecurity Outlook 2026. Disponible sur: https://www.metametris.com/media/262575e6-8a50-11ef-96d1-0242ac120013/043c44ca-f05f-11f0-93c2-def04981102a/0-wef-global-cybersecurity-outlook-2026.pdf
[9] LegiFrance. (2021). LOI n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France. Disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272
[10] ISO. (2024). ISO/IEC 27001:2022/Amd 1:2024. Disponible sur : https://www.iso.org/standard/88435.html
[11] Carbone 4. (2024). Bulletin numérique : Nuageux avec risque d'émissions cachées. Disponible sur : https://www.carbone4.com/article-numerique-cloud-emissions-cachees
[12] AFNOR. (2022). AFNOR Spe 2201. Disponible sur : https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2201/ecoconception-des-services-numeriques/fa203506/323315

La cybersécurité quant à elle, est définit par l'ANSSI comme un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles ». [13]

A date, l'un des rares textes mentionnant explicitement l'écoconception et la cybersécurité est le document « Écoconception, cybersécurité et protection des données, quelles synergies ? » produit en 2022 par MiNumEco, avec les contributions du Campus Cyber, de la Direction Interministérielle du Numérique, du Ministère de la Transition Écologique, de l'ANSSI, de la CNIL, de l'Université de Rennes, de l'Institut du Numérique Responsable et de la Banque de France. S'il démontre l'existence d'injonctions contradictoires entre objectifs environnementaux, cybersécurité et protection des données, qu'il ne s'agit pas de nier (ex : défense en profondeur, ressources spécifiques pour le chiffrement, exigences de disponibilité nécessitant des moyens redondants....), il identifie également des synergies (ex : nécessité d'être pensé dès la conception, minimisation des services développés et des surfaces d'attaques, connaissances et maîtrise du SI...) qu'il s'agit ici d'approfondir.
L'analyse proposée dans ce guide a également été entendue à l'impact environnemental des pratiques de cybersécurité existantes, majoritairement adoptées par les professionnels.

1.2 Objectifs du livrable

Ce présent document s'inscrit dans la continuité des travaux du rapport « Écoconception, cybersécurité et protection des données, quelles synergies ? » mentionné ci-dessus. Il approfondit ces conclusions de manière plus détaillée et opérationnelle, pour aider les RSSI à intégrer concrètement l'écoconception dans leurs pratiques quotidiennes. Pour ce faire, il a été décidé de les aborder sous un angle opérationnel, en les confrontant notamment aux bonnes pratiques éprouvées et reconnues en cybersécurité et en écoconception (cf. 2. Méthodologie adoptée).

L'ambition des résultats rassemblés ici est double :

- Fournir une nouvelle grille de lecture, construite à partir des exigences communes à des référentiels « cybersécurité » et « Numérique Responsable » reconnus, permettant d'éclairer les RSSI dans leurs choix et posant les bases d'une prise en compte de la dimension environnementale au sein des pratiques de cybersécurité ;

- Contribuer à l'émergence d'une approche « secure-and-sustainable-by-design » portée par l'initiative Cyber4Tomorrow, et déjà affichée par plusieurs grands groupes pour le développement de leurs services numériques.

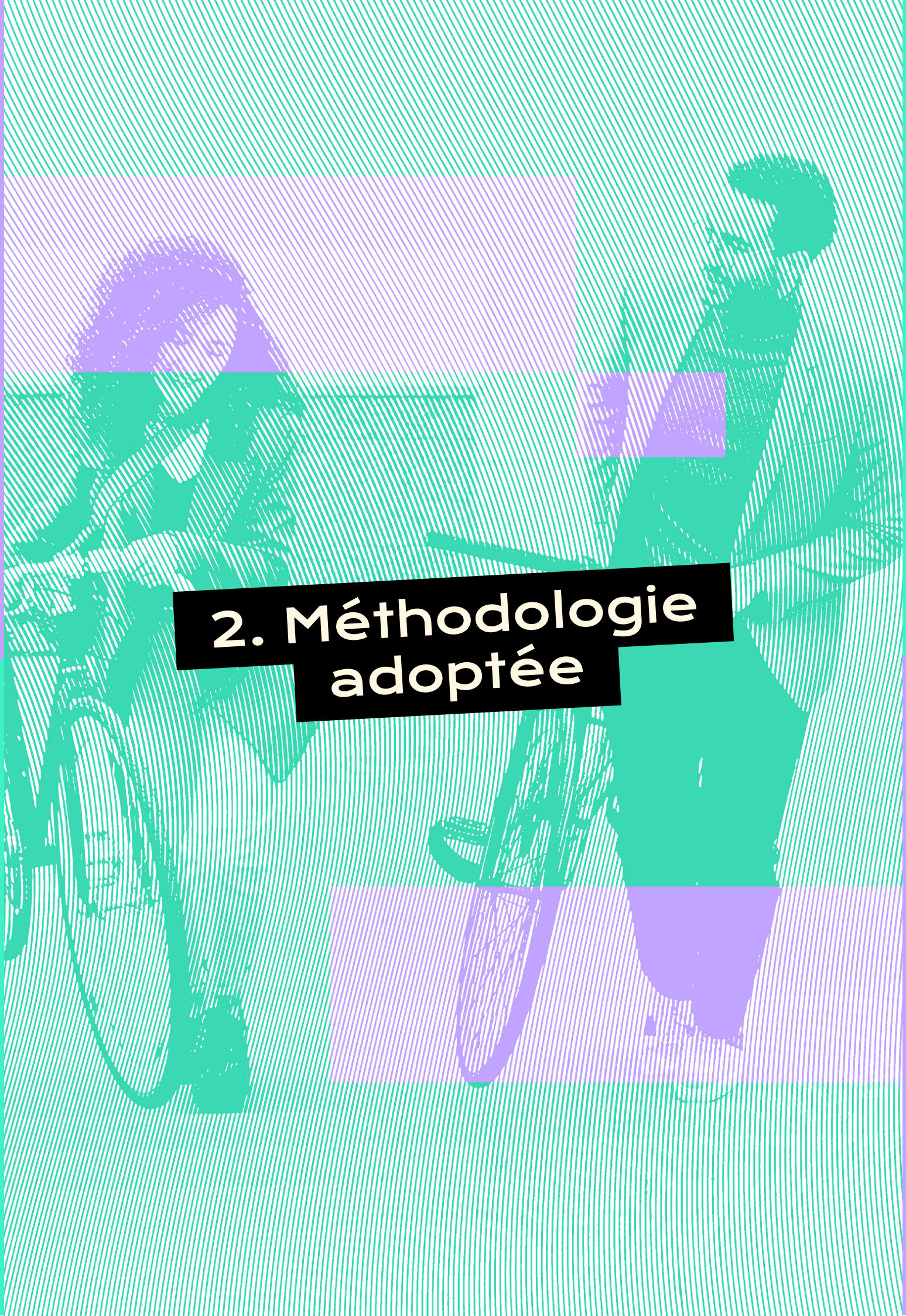
[13] ANSSI. (2026). CyberDico. Disponible sur : https://cyber.gouv.fr/cyberdico/

1.3 Cibles

Ce document s’adresse prioritairement aux responsables de la sécurité des systèmes d’information (RSSI) qui s’interrogent, envisagent ou souhaitent développer une approche « secure-and-sustainable-by-design », en prenant en compte exigences réglementaires et impacts environnementaux.

Il s’adresse également aux parties prenantes internes aux entreprises qui travaillent avec le département cybersécurité et qui souhaiteraient accompagner le développement de l’approche : product owner, personnel de la DSI, équipes en charge de la RSE, éditeurs, architectes et développeurs, spécialistes en UX/UI, responsables de la gestion des données. Il fournit aux chargés du Numérique Responsable et de l’écoconception des arguments positifs pour s’inscrire dans les processus de cybersécurité existants.

Enfin, les parties prenantes externes aux entreprises comme les organismes de réglementation ou les législateurs pourront elles aussi s'emparer des conclusions de ces travaux.



2. Méthodologie adoptée

2. Méthodologie adoptée

Pour construire ce guide, une méthodologie articulée autour de deux axes complémentaires a été retenue : l'étude de recommandations d'écoconception de services numériques à l'aune des enjeux de cybersécurité, et l'analyse de recommandations de cybersécurité au regard des externalités environnementales qu'elles génèrent.

Cette approche qualitative, permettant d'identifier efficacement les convergences et les divergences reliant les deux domaines, présente plusieurs avantages : en s'appuyant sur des référentiels existants et reconnus par les professionnels du secteur[14], il est possible de capitaliser sur un corpus de connaissances déjà produites (1) et de l'approfondir, de faciliter l'appropriation de ces recommandations en évitant une rupture brutale avec les pratiques déjà en place au sein des organisations (2), sans biaiser l'analyse « en faveur » de l'une ou de l'autre discipline.

L'approche quantitative a été exclue, car trop complexe à déployer à date ; celle-ci aurait nécessité de prendre en référence un système d'information et d'évaluer ses impacts environnementaux, avec et sans la mise en place des bonnes pratiques étudiées.

Une précision méthodologique importante doit être soulignée ici. Si les deux approches ont été retenues, la méthode employée pour l'étude des recommandations d'écoconception diffère de celle utilisée pour l'étude des recommandations de cybersécurité :

- **L'étude des recommandations d'écoconception a été menée via la recherche de synergies / divergences avec des enjeux de cybersécurité,** afin d'en identifier des axes de développement communs (cf. 2.1. De l'écoconception vers la cybersécurité). L'identification des synergies encourage la rapprochement des démarches de sécurité et d'écoconception, quand l'identification des divergences (ou risques de divergences) pousse à rechercher les solutions techniques les plus durables, sans dégrader le niveau de sécurité ;

- Le risque cyber n'étant pas traité de la même manière que l'écoconception dans la plupart des organisations, une approche adaptée aux pratiques des RSSI a été retenue pour l'étude des recommandations de cybersécurité. **Dans cette partie, l'objectif n'est pas de définir de potentielles synergies ou divergences avec les principes de l'écoconception, mais d'encourager le lecteur à questionner la nécessité du contrôle de cybersécurité en interrogeant sa valeur ajoutée.** L'utilité d'un contrôle dépend du contexte de chaque organisation ; l'approche retenue se veut donc pragmatique et flexible, afin que chaque RSSI puisse se l'approprier. In fine, il est proposé de réfléchir le déploiement des mesures de cybersécurité non plus pour se prémunir de l'entièreté des risques cyber (approche qui sous-entend l'application de toutes les recommandations de cybersécurité, mesures qui ne sont pas toujours nécessaires, alourdissent les budgets et dégradent d'autant plus les impacts environnementaux du système d'information), mais des risques qui pèsent réellement sur l'organisation (approche alignée sur le contexte et les besoins de l'organisation, et moins gourmande en ressources). Cette proposition exclut les contrôles de cybersécurité rendus obligatoires par des textes de lois et qui donc, doivent nécessairement être mis en place. (cf. 2.2 De la cybersécurité vers l'écoconception).

14 Le RGESN pour la partie "Écoconception" et le NIST et NIS 2 pour la partie "Cybersécurité". Ces choix sont justifiés ci-dessous.

15 ANSSI. (2026). NIS 2 – TRANSPOSITION NATIONALE MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSECURITÉ. RECYF : RÉFÉRENTIEL CYBER FRANCE (ReCyF). Disponible sur : https://messervicescyber-ressou[illegible]. services.clever-cloud.com/20260317_NIS_V2_ReCyF_v2.5.pdf

- **L'approche fondée sur la recherche de synergies et l'identification des divergences a également été retenue pour anticiper la mise en œuvre nationale de la directive européenne NIS2, via l'étude du référentiel « NIS2 »,** désormais ReCyF dans sa dernière version publiée par l'ANSSI, en mars 2026[15]. L'ambition est d'attirer l'attention sur les points de divergence possibles dans l'application des objectifs de sécurité présentés dans le document pour, in fine, encourager chaque organisation à appliquer les méthodes d'arbitrage présentées dans ce guide au référentiel cybersécurité qu'elle utilise.

2.1. De l'écoconception vers la cybersécurité

Cette première partie propose de répondre à la question suivante : « quelles conséquences les bonnes pratiques d'écoconception destinées à réduire les impacts environnementaux d'un service numérique peuvent avoir d'un point de vue cybersécurité ? »

Pour ce faire, la première étape a consisté à sélectionner un référentiel d'écoconception des services numériques parmi les différents déjà existants. Ce dernier devait répondre aux critères suivants : être opérationnel, reconnu et utilisé par les professionnels du secteur et référençant des bonnes pratiques qu'il était possible de considérer dans les contraintes de temps du groupe de travail. Le choix du panel d'experts s'est ainsi porté sur **la deuxième version du Référentiel général d'écoconception de services numériques (RGESN).**

i Le RGESN (Référentiel Général d'Écoconception de Services Numériques ; Version 2) est un cadre publié en 2024 par l'ARCOM / ARCEP qui définit des bonnes pratiques pour réduire l'impact environnemental des services numériques. Il fournit 78 critères mesurables et des recommandations opérationnelles pour écoconcevoir à toutes les étapes du cycle de vie : conception, développement, hébergement et exploitation. Son objectif est d'aider les organisations à créer des services numériques plus sobres, durables et responsables.

Chacune des 78 bonnes pratiques proposées par le référentiel a été étudiée à l'aune des questions suivantes :

- Cette bonne pratique entre-t-elle en synergie avec les enjeux de cybersécurité ? Est-elle neutre ? Ou au contraire, est-elle divergente ?
- Sur quels fondements la réponse a-t-elle été formulée ?
- Quelles limites ou quelles précautions doivent être respectées pour préserver la synergie lorsqu'elle existe ? Comment peut-on dépasser une éventuelle divergence ?

Chaque réponse, justifiée avec précision, a été formulée à l'issue d'échanges entre spécialistes de l'écoconception et experts de la cybersécurité.

Une analyse finale des résultats a ensuite été réalisée et présentée dans la partie « 3.1 Approche environnementale : l'analyse du RGESN » du présent rapport.

2.2. De la cybersécurité vers l'écoconception

Les questions traitées dans la seconde partie du document ont été formulées de la manière suivante : « quelles bonnes pratiques de cybersécurité ont de forts impacts environnementaux » et « quelles sont les bonnes pratiques de cybersécurité qui pourraient contribuer à réduire l'impact environnemental d'un service numérique ? » ; la réponse à la seconde question étant intrinsèquement liée à la première.

Pour cette seconde partie de l'étude, **le référentiel de sécurité du National Institute of Standards and Technology (NIST)** a été sélectionné.

i Le NIST a publié un cadre méthodologique en matière de cybersécurité reconnu à l'échelle internationale. Il comprend un ensemble de normes, de lignes directrices et de bonnes pratiques que les entreprises peuvent mettre en œuvre pour gérer de manière proactive les menaces cyber. Ces recommandations répondent à l'appellation « contrôles de sécurité ». Ces derniers sont classés en 5 grandes catégories, appelées « fonctions » : « IDENTIFY », « PROTECT », « DETECT », « RESPOND » et « RECOVER ».

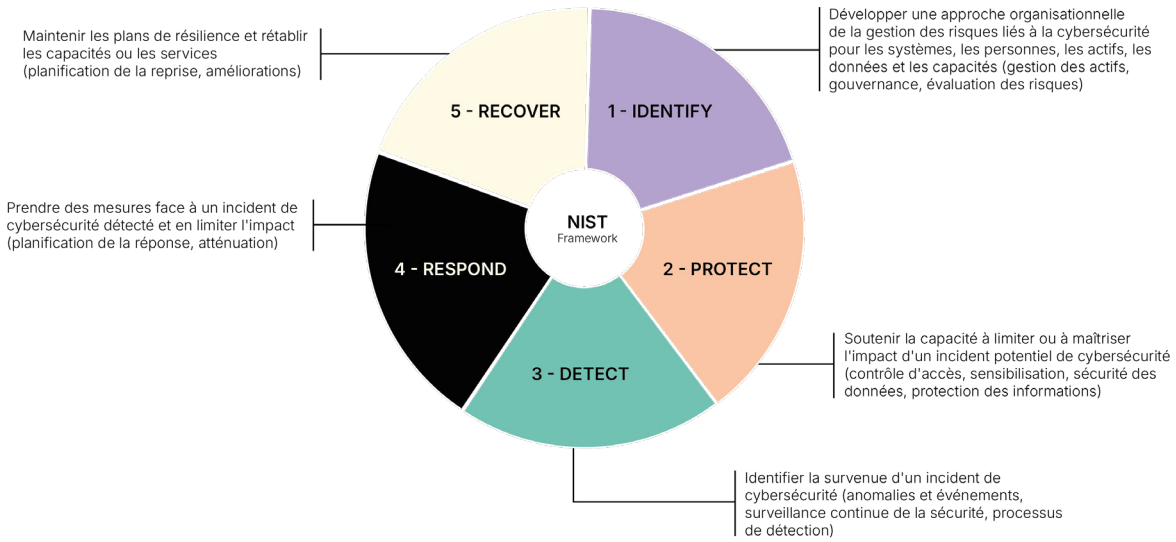


Figure 1 : Présentation des 5 fonctions du référentiel de sécurité du NIST

Plusieurs éléments expliquent ce choix. En 2022, la société Wavestone a réalisé une étude à l'origine de la Méthodologie CyberSustainability, une méthode de calcul de l'empreinte carbone cyber des organisations proposée par Cyber4Tomorrow[16]. Cette méthodologie de calcul est basée sur l'identification des 65 contrôles de sécurité les plus émissifs sur les 700 proposés[17] [18] par le référentiel du NIST.

[16] Cyber4Tomorrow. (2025). Déployer la méthodologie d'évaluation de l'empreinte carbone de la cybersécurité. Disponible sur : https://cyber4tomorrow.fr/actions/methodologie-evaluation-empreinte-carbone-cybersecurite/

[17] Wavestone. (2024). Comment réduire l'impact environnemental de la cybersécurité ?. Disponible sur : https://www.wavestone.com/fr/insight/cyber-sustainability-methodologie/

[18] Pour les réaliser ce filtrage, trois questions ont été formulées : ce contrôle nécessite-t-il l'utilisation d'un nombre important de terminaux ? (1) ; ce contrôle nécessite-t-il l'utilisation d'un nombre important de serveurs ? (2) ; ce contrôle nécessite-t-il l'utilisation d'un nombre important d'équipements réseau et de bande passante ? (3). S'il était possible de répondre "oui" à une ou plusieurs de ces trois questions, le contrôle a été comptabilisé comme "émissif".

Cet important travail a contribué à la sélection du référentiel du NIST comme cadre de référence pour la présente étude. Deux autres arguments ont également orienté ce choix : sa renommée auprès des professionnels du secteur, et son caractère très concret.

Dans la continuité des travaux menés dans le cadre de l'élaboration de la Méthodologie CyberSustainability, les 65 mesures de sécurité du NIST retenues ont donc été étudiées selon la méthode MoSCoW, une méthodologie d'arbitrage permettant d'identifier les besoins essentiels et de classer les priorités.

i Issue des méthodologies agiles, la Méthode MoSCoW a été formalisée dans les années 1990 pour fluidifier la gestion de projet. Elle permet de classifier les besoins ou les fonctionnalités selon leur importance, grâce à l'acronyme éponyme :

- **Must have** : Éléments indispensables, sans lesquels le projet échoue ;
- **Should have** : Éléments importants, à inclure si possible, mais négociables ;
- **Could have** : Éléments souhaitables, réalisables si le temps le permet ;
- **Won't have** : Éléments exclus pour ce projet, reportés ou abandonnés.

La méthode MoSCoW aide ainsi à définir les contrôles de sécurité « Must have », « Should have », « Could have » et « Won't have » propres à chaque organisation. Elle invite ainsi les RSSI à s'interroger sur la nécessité du contrôle (est-il négociable, négociable sous conditions de contexte ou non-négociable ?), ce questionnement permettant de définir un niveau de risque "acceptable" par chaque organisation - en fonction de la sensibilité des données exposées et de son contexte.

Une fois l'arbitrage réalisé, l'organisation peut alors supprimer, réduire, transférer ou accepter le contrôle de sécurité proposé par le cadre de référence. Le contrôle est alors implémenté lorsque que sa valeur ajoutée est attestée.

En adoptant une analyse par les risques - plutôt que par les contrôles, comme le préconisent les pratiques de cyber-résilience - cette méthodologie permet d'aligner précisément l'application des pratiques de sécurité sur le niveau de risque réel de l'organisation (contexte réglementaire...). En faisant évoluer les pratiques d'un statut de risque minimal à celui de risque optimal, la résilience opérationnelle et environnementale se trouve ainsi maximisée.

Les résultats de ces analyses sont présentés dans la partie « 3.2 Approche cybersécurité : l'analyse du référentiel du NIST ».

2.3. Etude prospective de la transposition de la directive européenne NIS2

La transposition de la directive européenne NIS2 a également été prise en compte dans le cadre de cette étude, à titre prospectif. L'objectif est d'identifier les synergies et divergences afin d'encourager à appliquer la méthode MoSCoW au référentiel de bonnes pratiques de cybersécurité utilisé par l'entreprise, pour limiter les impacts des exigences de sécurité.

> i La directive européenne NIS2 vise à assurer un niveau commun élevé de cybersécurité dans l'ensemble de l'Union Européenne en instaurant pour des milliers d'entités importantes et essentielles réparties dans 18 secteurs d'activités, une obligation de mettre en œuvre des mesures de gestion de risques et de notifier les incidents importants affectant leurs systèmes d'information. Sa transposition (en cours) en droit français prévoit 20 objectifs de sécurité que les entités importantes et essentielles sont tenues d'atteindre.

Contrairement au NIST dont l'application n'est pas exigée par la loi française, se conformer à la directive NIS2 sera obligatoire pour toutes les structures qui y sont soumises. Si elle est en cours de transposition en France, les 20 objectifs de sécurité que devront atteindre les futures « entités importantes et essentielles » ont été rendus publics et peuvent supporter une première analyse.

Ces 20 objectifs ont été passés en revue, en questionnant :

- Cet objectif de sécurité entre-t-il en synergie avec les enjeux d'écoconception ? Est-il neutre ? Ou au contraire, est-il divergent ?
- Sur quels fondements la réponse a-t-elle été formulée ?
- Quelles limites ou quelles précautions doivent être respectées pour préserver la synergie lorsqu'elle existe ? Comment peut-on dépasser une éventuelle divergence ?

Cette analyse pourra être approfondie lorsque le texte sera définitivement adopté par les autorités nationales, ouvrant la voie à de nouvelles propositions dans le respect du cadre législatif en vigueur.

3. Résultats

3. Résultats

Deux méthodologies de travail - chacune basées sur deux référentiels distincts - articulées dans une seule et même analyse croisée, permettent de prendre en considération les exigences et contraintes spécifiques aux métiers de la cybersécurité et du Numérique Responsable. Leurs apports sont complémentaires et convergent vers une approche commune, destinée à intégrer ces méthodologies et référentiels dès la conception des services numériques, depuis le développement de produits, services ou fonctionnalités de cybersécurité jusqu'à l'intégration des principes d'écoconception et de cybersécurité dans les services numériques. Elles permettent également aux RSSI de concevoir de manière optimisée la protection des systèmes d'information. Cette combinaison contribue à renforcer la résilience technique et opérationnelle, tout en limitant la consommation de ressources.

Les résultats approfondis des analyses sont à retrouvées dans les Annexes 1, 2 et 3.

3.1 Approche environnementale : l'analyse du RGESN

3.1.1. Résultats généraux

Parmi les 78 recommandations d'écoconception du RGESN, il apparait que 76 ne présentent aucune divergence avec les pratiques de cybersécurité communément admises et appliquées par les professionnels du secteur.

Seules 2 recommandations peuvent présenter un risque de divergence, risque qui est levé à condition de respecter des précautions précises :

- Une bonne pratique relative à la mise à l'échelle dynamique des ressources informatiques (Virtual CPU / Virtual RAM), car ces outils de mise à l'échelle peuvent être utilisés comme vecteurs lors d'attaques (Critère n°3.2 de la Famille « Architecture »). La divergence est levée, et son impact sur la cybersécurité est considéré comme neutre, si les outils utilisés font l'objet d'une validation par les équipes cybersécurité et si ces outils sont les seuls utilisables au sein de l'organisation ;
- Une bonne pratique qui ne présente pas de divergence, à condition de respecter un critère de vigilance : il s'agit de la mise en cache des contenus transférés (Critère n°6.2 de la Famille « Frontend »). Pratique à éviter pour les données sensibles, comme les données personnelles par exemple. Pour les données non sensibles, la réduction du flux réseau fait de cette bonne pratique une synergie sous condition.

Au final, 21 bonnes pratiques sont considérées comme neutres : elles n'ont aucun impact, ni positif, ni négatif, du point de vue de la cybersécurité.

A contrario, de réelles synergies sont identifiées :

- 47 bonnes pratiques constituent des synergies directes ;
- 10 bonnes pratiques constituent des synergies en respectant certaines conditions, précisées dans le tableau d'analyse joint en Annexe 1. La recommandation 6.2 mentionnée précédemment comme présentant un risque de divergence, entre dans cette catégorie, si les précautions mentionnées sont respectées.

Trois familles principales de synergies, résultant de ces bonnes pratiques, sont identifiées :

1 Des améliorations d'organisation et de processus.
27 bonnes pratiques sont répertoriées dans cette catégorie.
Mentionnons quelques recommandations majeures présentant des synergies :
- Privilégier des technologies interopérables et des architectures modulaires (ex : critère n°1.9 de la Famille « Stratégie ») ;
- Gérer les mises à jour sur toute la durée du service (ex : critère n°2.2 de la Famille « Spécification ») ;
- Adapter les niveaux de chiffrement au juste besoin (ex : critère n°1.7 de la Famille « Stratégie »).

2 Une réduction des quantités de données.
20 bonnes pratiques sont répertoriées dans cette catégorie.
Mentionnons quelques recommandations majeures présentant des synergies :
- Réduire les volumes de données transférés (ex : critère n°4.1 de la Famille « UX/UI » ;
- Favoriser l'observabilité du système d'information et en particulier du réseau ;
- Définir une politique des données et leur attribuer une durée de vie (ex : critère n°2.7 de la Famille « Spécifications ») ;
- Détruire les données obsolètes (ex : critère n°5.8 de la Famille « Content ») ;
- Limiter leur duplication aux cas le nécessitant strictement ;
- Maîtriser leur hébergement. Une famille « Hébergement » est dédiée au sujet.

3 La réduction de la surface d'attaque.
13 bonnes pratiques sont référencées dans cette catégorie.
Mentionnons quelques recommandations majeures présentant des synergies :
- Bien identifier les utilisateurs de chaque service ainsi que leur matériel (type d'équipements, âge, et système d'exploitation et mises à jour (ex : critère n°2.1 de la Famille « Spécifications ») ;
- Limiter le nombre d'utilisateurs au strict nécessaire et mettre à jour leurs listes (ex : critère n°1.2 de la famille « Stratégie ») ;
- Identifier les services numériques qui sont peu ou qui ne sont plus utilisés, puis les décommissionner dès que cela est possible. Il est à noter que les logs de cybersécurité peuvent être très utiles pour cela, parfois plus qu'une CMDB (ex : Critère n°2.7 de la Famille « Spécification »).

Parmi les 10 recommandations qui présentent des synergies sous réserve de respecter certaines conditions, il s'agit souvent de poser les questions qui permettent aussi de clarifier la situation pour des enjeux de cybersécurité.
Par exemple :
- Les services tiers utilisés ont-ils été qualifiés, tant sur le plan de la sécurité que sur le plan environnemental ?
- A-t-on sélectionné les composants d'interface les plus simples possible ?
- A-t-on embarqué dans sa démarche ses fournisseurs et autres parties prenantes ? En coopération avec les achats ?
- Le service numérique est-il utilisable en connexion bas débit ou hors connexion ?

3.1.2.Résultats affinés par familles

Parmi les 9 familles de bonnes pratiques du RGESN, certaines familles présentent plus de synergies que les autres. Le tableau ci-dessous classe ces familles dans l'ordre de celles présentant le plus de synergies, vers celles qui en présentent moins :

Famille (Nombre de bonnes pratiques du RGESN)	Synergies avérées	Synergies sous condition	Divergence potentielle nécessitant des précautions	Bonnes pratiques neutres
	Nombre (%)	Nombre (%)	Nombre (%)	Nombre (%)
Stratégie (10)	6 (60%)	1 (10%)		3 (30%)
Spécification (10)	2 (20%)	**8 (80%)**		
Architecture (7)	5 (71%)		1 (14%)	1 (14%)
UX/UI (15)	10 (67%)			5 (33%)
Contenus (8)	**8 (100%)**			
Front End (7)	**6 (86%)**	1 (14%)		
Back End (4)	2 (50%)			2 (50%)
Hébergement (10)	5 (50%)			5 (50%)
Algorithmie (7)	3 (43%)			4 (57%)
Total (78)	**47 (60%)**	**10 (13%)**	**1 (1%)**	**21 (27%)**

Tableau 1 : Analyse des familles du RGESN au regard des synergies / divergences avec les pratiques de cybersécurité

On constate que certaines familles sont riches en synergies marquées : les familles « Contenus » (ce qui couvre les données), « Front End », « Architecture » et « UX/UI ». Dans le cadre d'une démarche d'éco-conception des services numériques, il est donc possible de renforcer la priorité de ces bonnes pratiques, en soulignant ces synergies, voire de rapprocher cette démarche de celles engagées dans le cadre de la cybersécurité.

Aucune famille ne présente de divergence potentielle, à l'exception d'une bonne pratique dans la famille « Architecture ». Elle impose des précautions sur les mécanismes de mise à l'échelle automatique (scalability) des ressources informatiques. Il s'agit, comme mentionné précédemment, de ne pas utiliser n'importe quelle solution technique mais de la sélectionner sur des critères techniques précis de cybersécurité, tout en mettant en perspective son empreinte environnementale.

3.1.3. De fortes synergies identifiées

Le travail réalisé a permis d'identifier un potentiel de synergies fortes, qui permettent de systématiser des leviers d'action importants pour la cybersécurité et le Numérique Responsable. Il serait intéressant de faire travailler les équipes concernées de concert, en renforçant les bonnes pratiques communes. Mentionnons par exemple les revues de code et d'architecture, qui peuvent embarquer les revues d'écoconception, intégrées aux process de développement, processus agiles par exemple. Ceci matérialise une approche « secure-and-sustainable-by-design », approche avant-gardiste revendiquée par plusieurs grands groupes pour définir leur manière, actuelle ou à venir, de développer leurs services numériques.

Notons qu'il existe aussi une opportunité de valoriser les bénéfices de ces bonnes pratiques, en énergie, en euros et en CO2, mais aussi en robustesse (valeur stratégique) plus difficile à quantifier, en travaillant avec les équipes compétentes en Numérique Responsable.

3.2 Approche cybersécurité : l'analyse du référentiel du NIST

Tout comme il a été possible de questionner les conséquences des bonnes pratiques d'écoconception d'un point de vue « cybersécurité », il est possible de questionner les conséquences environnementales des bonnes pratiques de cybersécurité proposées par des référentiels techniques. Cette démarche a été menée par le groupe de travail à partir des 65 contrôles de sécurité les plus émissifs du référentiel de cybersécurité du NIST, reconnu et utilisé par les professionnels de ce secteur à l'échelle internationale (cf. 2. Méthodologie adoptée).

3.2.1. Répartition des impacts par fonctions

Sur les 700 contrôles de sécurité proposés par le référentiel du NIST, les 65 contrôles les plus émissifs ont été identifiés lors de la conception de la Méthodologie CyberSustainability. Ces 65 contrôles sont répartis de la manière suivante, suivant la nomenclature du NIST.

Fonction NIST	Contrôles	Pourcentage		**Contrôles à fort impact**	Pourcentage
DETECT (DE)	96	14%		13	20%
IDENTIFY (ID)	128	18%		12	18%
PROTECT (PR)	384	**55%**		38	58%
RECOVER (RC)	40	**6%**		1	2%
RESPOND (RS)	56	**8%**		1	2%
Total	**704**	**100%**		**65**	**100%**

Tableau 2 : Répartition des contrôles par fonctions et par impacts

La répartition des contrôles selon les fonctions NIST est globalement similaire à celle des contrôles ayant un fort impact environnemental. La fonction PROTECT domine dans les deux cas (55 % des points d'évaluation généraux contre 58 % pour l'impact environnemental), suivie de DETECT (14 % contre 20 %) et IDENTIFY (18 %).

Les leviers de réduction d'impact environnemental se concentrent principalement au sein de la fonction PROTECT, qui soutient la capacité à limiter ou contenir l'impact d'un événement potentiel via des domaines tels que le contrôle d'accès, la formation et la sensibilisation, la sécurité des données et la protection des informations, puis dans une moindre mesure au sein de DETECT et IDENTIFY. Par conséquent, les équipes en charge de la mise en œuvre de la protection devront être davantage mobilisées pour maximiser ces opportunités de réduction.

3.2.2. Management des risques optimisés

Le suivi du référentiel tend vers un niveau de risque très limité, voire nul. Il constitue un moyen de gérer au mieux les risques liés à la cybersécurité en adoptant une approche proactive. Toutefois, l'application stricte de ces bonnes pratiques, sans remise en question des risques potentiels — notamment pour celles à fort impact environnemental — doit être reconsidérée afin d'intégrer une dimension soutenable (d'un point de vue environnemental biensûr, mais aussi financier). Cette dernière vise à renforcer la résilience, la durabilité et la robustesse des systèmes.

En effet, un système non sécurisé n'est pas durable, mais un système ignorant les risques environnementaux ne l'est pas davantage. Si la cybersécurité et l'écoconception sont deux domaines aux objectifs distincts (le premier cherche à gérer les risques opérationnels liés aux attaques informatiques, tandis que le second œuvre à modérer, ou à diminuer, les impacts sur notre écosystème), il est possible d'intégrer ces deux dimensions dans le management des risques via la méthode MoSCoW.

i Rappel - Acronyme de la méthode MoSCoW :

- **Must have** : Éléments indispensables, sans lesquels le projet échoue ;
- **Should have** : Éléments importants, à inclure si possible, mais négociables ;
- **Could have** : Eléments souhaitables, réalisables si le temps le permet ;
- **Won't have** : Éléments exclus pour ce projet, reportés ou abandonnés.

Cette dernière a été appliquée aux 65 pratiques du référentiel NIST les plus impactantes sur le plan environnemental. L'objectif est d'encourager les RSSI à trouver, pour chaque pratique, le bon compromis permettant d'appliquer l'exigence NIST pour atteindre un niveau de risque qualifié « d'optimal ». Il s'agit d'aligner précisément l'application des mesures de sécurité sur le niveau de risque réel de l'organisation (contexte réglementaire, exposition, etc.) et de faire évoluer ces pratiques, d'une logique de risque minimal vers celle de risque optimal, maximisant ainsi la résilience opérationnelle et environnementale de l'organisation.

Pour ce faire, il est proposé au lecteur une démarche systématique de questionnement de ces 65 bonnes pratiques sur le risque acceptable. Pour facilier l'adoption de la démarche, une pré-analyse a été réalisée pour déterminer si le contrôle est : (1) négociable, (2) négociable sous conditions de contexte, (3) non-négociable selon les critères suivants :

Mise en œuvre du contrôle :
- Must have = Vital = non-négociable
- Should have = dans la mesure du possible = négociable sous conditions de contexte
- Could have = nice to have = négociable

Quelques éléments de compréhension sont à noter :
- Les contrôles classés comme « Won't have » ne sont pas applicables, et donc pas appliqués. Ils ont donc été exclus de la sélection ;
- Il est envisageable de se passer de certaines exigences dans des cas d'usages bien précis, spécifiques aux organisations. Dans ce cas, le niveau d'application peut être ramené au niveau le moins critique, à savoir « Could have » ;
- Les résultats des questions sont en adéquation avec la sensibilité de la donnée (Confidentialité, Intégrité, Disponibilité) et du respect de la réglementation européenne ou nationale (RSE, CSRD, LPM...) :
- Pour les contrôles le nécessitant, un niveau d'arbitrage (organisation/entreprise, DSI, métier, local, services numériques ou applicatif, etc.) est proposé pour valider les risques introduits : (1) suppression, (2) réduction, (3) acceptation ou (4) transfert au niveau d'arbitrage adéquat.

3.2.3. Analyse de la latitude pour une gestion optimisée des risques

Parmi les 65 contrôles de sécurité les plus impactants, 9 sont de nature organisationnelle. Leur mise en œuvre est principalement associée à des processus, des politiques et au renforcement de la gouvernance. A l'inverse, les 56 contrôles techniques restant mobilisent avant tout des solutions technologiques. Contrairement au référentiel général où la répartition entre les différentes typologies d'actions est équilibrée, cette sélection se distingue par une surreprésentation des contrôles techniques.

Qualification MoSCow	Contrôle	Technique	Organisationnel
Could	24	24	0
Must	20	13	7
Should	**21**	19	2
Total	**65**	**56**	**9**

Tableau 3 : Répartition des contrôles impactant par typologie

Sur les 65 contrôles, la série des questionnements permet de limiter l'impact environnemental des pratiques et, par extension, de répondre à la mise en œuvre des bonnes pratiques du RGESN.

Voici quelques exemples :
- Parmi les contrôles classés en « Must », l'exemple relatif à la collecte des logs est assez éloquent. Des réflexions peuvent être engagées pour gérer au mieux la volumétrie, le cycle de vie et la durée de rétention de la donnée. Ceci correspond à la bonne pratique n° 7.3 du RGESN (le service numérique met-il en place des durées de conservation sur les données et documents en vue de leur suppression ou archivage passé ce délai ?)

- Parmi les contrôles classés en « Must », 5 d'entre eux ont été identifiés comme des opportunités ; c'est à dire que leur mise en place permettrait de renforcer les bénéfices environnementaux. Par exemple : renforcer les infrastructures critiques et leur suivi peut permettre d'optimiser la configuration et la réduction de la surface d'attaque (réduction, suppression des composants inutiles, etc.)

- Autre exemple, pour le contrôle « Administration access to cloud consoles », classé dans les « Should ». Ce contrôle exige que l'accès soit effectué via un bastion pour assurer la traçabilité. Cependant, pour des SI soumis à moins de contraintes, d'autres mesures peuvent être implémentées. On imagine des mécanismes de sécurité plus faciles à appréhender en investissements, tant humains que financiers.

3.2.4 Priorisation des contrôles à optimiser

La matrice Excel fournie en Annexe 2 permettra d'identifier rapidement les contrôles à analyser pour optimiser la gestion des risques, en fonction des exigences d'écoconception, du niveau de priorité de l'organisation et des latitudes dont dispose le lecteur.

Pour guider la lecture de l'Annexe 2, le tableau ci-dessous résume l'analyse MoSCoW menée sur les contrôles de sécurité en fonction de l'intensité de leur impact environnemental.

Intensité des impacts *1 = faible* *4 = fort*	Nombre de contrôles
Total 1	**9**
Could	4
Must	3
Should	2
Total 2	**32**
Could	15
Must	7
Should	10
Total 3	**18**
Could	3
Must	7
Should	8
Total 4	**6**
Could	2
Must	3
Should	1
Total général	**65**

Tableau 4 : Classement des contrôles par intensité d'impact environnemental

De même, afin de faciliter l'appropriation de la méthode par le lecteur, deux exemples d'analyse qu'il est possible de mener à partir de l'Annexe 2 ont été développés ci-dessous. Elles concernent le contrôle « CLOUD 06-lvl4 » lié à la résilience des services cloud et le contrôle « ENDPT.14-lvl4 » relatif à la sécurité des postes de travail des administrateurs.

Résilience des services cloud

ID : CLOUD.06-lvl4 - Fonction du NIST : PROTECT - Classification MoSCoW : « Could »

Contrôle : « Quelle est la stratégie mise en place pour assurer la redondance en cas d'interruption du service ? »
Exigences : « Des capacités de redondance entre les centres de données situés dans différentes régions sont possibles et régulièrement testées ».

Questionnement proposé :
Que souhaite-t-on protéger ? Quel est l'évènement redouté ? Le type de redondance envisagé est-il intrarégional ? multirégional ? Ai-je des locaux dans différentes régions ? Quelles sont les ressources allouées à la mise en place et la maintenance de cette redondance ? La redondance aboutit-elle à se rapprocher des clients ?
Exemple : La réduction des flux réseau limite l'impact environnemental, le rapprochement physique améliore la performance du service numérique. Parmi les ressources nécessaires, quelles sont celles qui peuvent être optimisées et comment ?

Arbitrage du risque :
Au niveau départemental ? Au niveau des métiers, selon le domaine d'activité ?

Sécurité des postes de travail des administrateurs

ID : ENDPT.14-lvl4 - Fonction du NIST : PROTECT - Classification MoSCoW : « Could »

Contrôle : « Comment les postes de travail des administrateurs sont-ils gérés ? »
Exigences : « Des postes de travail dédiés (Privileged Access Workstation - PAW) sont mis en place »

Questionnement proposé :
Quelles sont les ressources allouées à la mise en place et la maintenance de cette redondance ?
Exemple : L'augmentation de poste physique alourdit l'impact environnemental. Parmi les ressources nécessaires, de quelle façon nous pouvons les optimiser ? En mutualisant ? En partageant ? En virtualisant ?
Quelles sont les typologies d'administration et quels sont les risques associés ?
Exemple : Administration fonctionnelle et administration opérationnelle – Éphémère versus Statique

Arbitrage du risque :
- Arbitrage local : administration au niveau de l'application pour l'administration fonctionnelle ;
- Arbitrage départemental : administration via des machines virtuelles ;
- Arbitrage global : administration opérationnelle via des postes physiques ;

L'optimisation risques / bénéfices vise à faire tendre au maximum vers de l'arbitrage local et de mutualiser l'usage des postes physiques, dans la mesure du possible.

Les questions à poser pour guider l'arbitrage sont dépendantes du contexte de l'organisation. Il convient aux RSSI et aux équipes de cybersécurité disposant des connaissances nécessaires à la prise de recul critique proposée par ce document, de formuler les questionnements qui mettront en perspective le référentiel avec les besoins de protection de la structure.

3.2.3 Etude prospective : la transposition de NIS2 et ses perspectives opérationnelles

Le référentiel « NIS2 », élaboré dans le cadre de la transposition en cours de la directive NIS2 en droit national français, fixe les objectifs de sécurité que devront atteindre les futures entités assujetties. Une version préliminaire de ce référentiel a été utilisée pour cette étude afin d'inviter à privilégier les solutions techniques les plus durables, sans compromis sur les exigences de sécurité en synergie et d'encourager à appliquer la méthode MoSCoW au référentiel de bonnes pratiques de cybersécurité utilisé par l'organisme / l'entreprise pour limiter les impacts des exigences ayant potentiellement des divergences.

L'analyse de 20 objectifs de sécurité, déclinés du cadre européen au niveau national, a permis d'identifier que :

- **10 objectifs sont évalués comme des synergies claires**, dont une synergie majeure liée à l'usage de configurations durcies, par exemple pour les systèmes d'exploitation qui peuvent être maintenus durant 10 ans ou plus, sans remplacement du matériel physique.

- **1 objectif est évalué comme une synergie avec un risque limité de divergence**. Cet objectif portant sur l'administration des systèmes depuis des ressources dédiées présente un risque de divergence évalué comme limité car il existe des solutions techniques maîtrisées pour limiter ces ressources, et parce que certains de ces outils sont nécessaires pour construire une approche « Numérique Responsable ». Par exemple, le fait d'avoir une CMDB permettant de connaître et de maîtriser son portefeuille d'applications ou des listes d'utilisateurs à jour et maintenues. Ce niveau de maîtrise sera aussi une clé pour permettre le décommissionnement des services peu ou pas utilisés, qui ont une empreinte conséquente et qui sont autant de vulnérabilités potentielles.

- **1 objectif a été évalué comme une opportunité de synergie.** Cet objectif portant sur l'intégration de la sécurité numérique dans la gestion de ses ressources humaines pourrait permettre de réaliser des actions de sensibilisations et des formations qui associent cybersécurité et Numérique Responsable. L'enjeu étant à la fois de sensibiliser sur des risques peu connus et mal maitrisés, de donner du sens aux démarches de transformation et de travailler sur la résilience de l'organisation, à court comme à moyen et long termes. Les 2 démarches impliquent l'adhésion de l'ensemble des métiers techniques et des utilisateurs, dans une approche transverse. Au-delà d'une vision des développements et du maintien en condition opérationnelle des services, qui promeut une approche « secure-and-sustainable-by-design », il s'agit aussi de travailler la maturité de la culture d'entreprise sur ces sujets.

- **8 objectifs ont été évalués comme à la fois des synergies et des divergences**. Synergies car ils poussent globalement à une sobriété d'usage et une limitation des flux, mais aussi divergences car ils nécessitent l'ajout de moyens spécifiques, vecteurs d'impacts. Dans tous les cas, ces objectifs sont des garanties pour éviter ou limiter les impacts économiques, sociaux et environnementaux qu'aurait un acte de malveillance réussi. Il n'est donc nullement envisagé d'aller à l'encontre de ces recommandations, mais plutôt d'encourager à quantifier les impacts, environnementaux en particulier, associés aux moyens déployés et d'intégrer des critères pour limiter ces impacts dans les cahiers des charges et les évaluations des offres qui y répondent, afin de sélectionner les solutions les plus durables. Plusieurs guides et méthodologies pour les achats Numériques Responsables permettent d'établir des grilles d'évaluation pour concrétiser la démarche et embarquer sa chaine de valeur, dont les fournisseurs.

- **Aucun objectif n'a été évalué comme une divergence absolue.**


4. Conclusion

4. Conclusion

La principale ambition de ce guide est de démontrer que l'écoconception et la cybersécurité ne poursuivent pas des objectifs contradictoires mais, au contraire, qu'il existe de réelles synergies entre ces disciplines. Plus encore, bien que n'ayant pas les mêmes objectifs, elles peuvent profiter de démarches ou de moyens communs pour les atteindre.

En effet, **l'analyse des 78 bonnes pratiques du RGESN menée dans la première partie de cette étude montre que la majorité des recommandations d'écoconception sont compatibles avec les pratiques de cybersécurité.** Si 21 bonnes pratiques sont estimées neutres du point de vue de la cybersécurité, 47 bonnes pratiques ont un impact positif direct et 10 apportent des bénéfices sous conditions. Ces synergies se regroupent en trois grands axes : l'amélioration des processus et de l'organisation, la réduction des volumes de données, et la diminution de la surface d'attaque. Concrètement, cela inclut des actions comme la gestion des mises à jour, la limitation des données, ou encore la suppression des services inutiles. Certaines familles de pratiques, comme les contenus, le front-end, l'architecture et l'UX/UI, concentrent particulièrement ces synergies.

De même, **l'étude menée sur les 65 contrôles de sécurité les plus émissifs du NIST via la méthode MoSCoW démontre qu'il est possible d'adapter les exigences de sécurité au niveau de risque réel d'une organisation, en passant d'une logique de gestion du « risque minimal » à celui du « risque optimal ».** Cette démarche permet de prioriser les contrôles selon leur niveau de nécessaire application (Must, Should, Could), en fonction du contexte, tout en intégrant les contraintes réglementaires et opérationnelles. Les résultats montrent qu'une partie des contrôles peut être ajustée pour réduire leur impact environnemental, en optimisant par exemple la gestion des logs ou en adaptant certains mécanismes de sécurité selon les besoins. Cette approche favorise une gestion plus fine des risques, combinant performance environnementale et résilience opérationnelle, tout en identifiant des opportunités d'optimisation et de priorisation des contrôles les plus impactants.

En s'appuyant sur l'analyse de référentiels connus et reconnus, ce document encourage ainsi les professionnels de la cybersécurité et du Numérique Responsable à coopérer pour répondre à l'enjeu de réduction des impacts environnementaux du numérique, tout en garantissant un niveau de sécurité optimal. Plus largement, **il s'illustre comme un support facilitant la compréhension et l'adoption d'une approche « secure-and-sustainable-by-design » par les organisations.**

En effet, les synergies démontrées par le présent document ouvrent la voie à la concrétisation des deux approches dans les mêmes processus opérationnels, lors des phases de conception et de développement, ou lors de l'utilisation et de la maintenance d'un service numérique, et ce jusqu'à son décommissionnement. Ce guide démontre également qu'il est possible de déployer des mesures de sécurité adaptées aux risques qui pèsent réellement sur le système d'information à défendre, évitant ainsi de multiplier les protections. Cet argument peut s'avérer particulièrement pertinent lorsqu'il est mis en perspective avec la multiplication et la complexité des cyberattaques.

Si les synergies entre les démarches de Numérique Responsable et de sécurisation des systèmes d'information sont avérées et démontrées par le présent guide, **il serait toutefois illusoire de croire qu'elles peuvent se substituer l'une à l'autre :**

- L'écoconception d'un service numérique, aussi rigoureuse soit-elle, ne garantit pas la sécurisation de ce service ;
- Inversement, la mise en place de processus de cybersécurité n'implique pas nécessairement la réduction des impacts environnementaux liés au déploiement et à l'usage de ce service.

Dans un souci de transparence, il semble important également de mentionner les éléments qui n'ont pas été intégrés dans cette analyse :

- **Certaines thématiques technologiques sont peu ou ne sont pas abordées dans ce document**. On pense notamment aux enjeux soulevés par l'Intelligence Artificielle, qui induit une forte augmentation des impacts environnementaux mais qui peut être utilisée pour l'analyse d'événements et la détection de menaces.

- **Les aspects sociaux du Numérique Responsable n'ont pas été pris en compte dans le cadre de cette étude**. Il s'agit d'un axe qui pourrait faire l'objet d'analyses complémentaires, en étudiant par exemple l'impact croisé des référentiels d'accessibilité.

- **L'approche développée dans ce document s'est centralisée sur les services numériques et leur écoconception, il serait intéressant d'analyser aussi les bonnes pratiques de Numérique Responsable liées aux équipements informatiques sous le prisme de la cybersécurité.** Parmi ces bonnes pratiques la question de l'augmentation de la durée de vie des équipements (terminaux, serveurs, équipements réseau) est un levier fort pour réduire les impacts, environnementaux et sociétaux, liés à leur fabrication et à leur fin de vie. L'obsolescence des équipements, liée à la fin du support sur les systèmes d'exploitation est un enjeu qui mériterait lui aussi d'être traité. D'autant que des solutions techniques souveraines peuvent être promues qui peuvent elles aussi être vectrices de synergie avec la cybersécurité ; mentionnons en particulier l'adoption de systèmes d'exploitation durcis et open source, très utilisés sur les applications critiques, et qui sont aptes à gérer certaines adhérences à des systèmes fermés. La question de la destruction systématique des disques durs, lorsque des solutions reconnues d'effacement des données existent, mériterait elle aussi d'être posée.

Le Groupe de travail « Écoconception et cybersécurité » de l'initiative Cyber4Tomorrow appelle de ses vœux la poursuite des travaux pour approfondir le croisement des deux expertises. Dans un contexte de mutation environnementale de notre écosystème planétaire, il est indispensable de prendre en considération les limites écologiques présentes et à venir. Plus qu'une nécessité, intégrer des exigences de sécurité et des exigences environnementales dès la conception des produits et services numériques et dans la sécurisation d'un système d'information peut s'avérer un élément différenciant pour les acteurs français et européens. Cet atout semble d'autant plus impactant dans un contexte international invitant à une meilleure maitrise de la souveraineté numérique à l'échelle de l'Union Européenne.

Sources bibliographiques et webo-graphiques

Les recommandations considérées dans ce guide ont été identifiées à partir des documents listés ci-dessous. Ils constituent une référence en termes de bibliographie et webographie relative aux enjeux de cybersécurité et d'écoconception des services numériques.

Documents en français

- **AFNOR**. (2022). Référentiel AFNOR pour l'écoconception des services numériques : AFNOR Spec 2201. Disponible sur : https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2201/ecoconception-des-services-numeriques/fa203506/323315

- **AFNOR**. (2024). Référentiel général pour l'IA frugale - Mesurer et réduire l'impact environnemental de l'IA : AFNOR Spec 2314. Disponible sur : https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2314/referentiel-general-pour-lia-frugale-mesurer-et-reduire-limpact-environneme/fa208976/421140

- **ANSSI**. (2026). CyberDico. Disponible sur : https://cyber.gouv.fr/cyberdico/

- **ANSSI**. (2026). NIS 2 – TRANSPOSITION NATIONALE MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSECURITÉ. RECYF : RÉFÉRENTIEL CYBER FRANCE (ReCyF). Disponible sur : https://messervicescyber-ressources.cellar-c2.services.clever-cloud.com/20260317_NIS_V2_ReCyF_v2.5.pdf

- **ANSSI**. (2026). Panorama de la menace 2025. Disponible sur : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf

- **ARCOM/ARCEP**. (2024). Référentiel général d'écoconception de services numériques (RGESN). Disponible sur : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

- **Carbone 4.** (2024). Bulletin numérique : Nuageux avec risque d'émissions cachées. Disponible sur : https://www.carbone4.com/article-numerique-cloud-emissions-cachees

- **Cyber4Tomorrow.** (2025). Présenter la méthodologie d'évaluation de l'empreinte carbone de la cybersécurité au sein de son organisation. Disponible sur : https://cyber4tomorrow.fr/actions/evaluation-empreinte-carbone-de-la-cybersecurite/

- **INR**. (2021). RIA31, le référentiel IA Ethique et Responsable. Disponible sur : https://institutnr.org/ria31-le-referentiel-ia-ethique-et-responsable

- **ISO**. (2024). ISO/IEC 27001:2022/Amd 1:2024Information security, cybersecurity and privacy protection — Information security management systems — RequirementsAmendment 1: Climate action changes. Disponible sur : https://www.iso.org/standard/88435.html

- **LegiFrance**. (2021). LOI n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France. Disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272

- **MiNUM ECO**. (2024). Référentiel Général d'Ecoconception des Services Numériques (RGESN). Disponible sur : https://ecoresponsable.numerique.gouv.fr/docs/2024/rgesn-mai2024/referentiel_general_ecoconception_des_services_numeriques_version_2024.pdf

- **Wavestone**. (2024). Comment réduire l'impact environnemental de la cybersécurité ? Disponible sur : https://www.wavestone.com/fr/insight/cyber-sustainability-methodologie/

Documents en anglais

- **NIST**. (2024). The NIST Cybersecurity Framework (CSF) 2.0. Disponible sur : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- **N. SUNDBERG**. (2022). Sustainable IT Playbook for Technology Leaders. O.REILLY.
- **World Economic Forum**. (2026). Global Cybersecurity Outlook 2026. Disponible sur: https://www.metametris.com/media/262575e6-8a50-11ef-96d1-0242ac120013/043c-44ca-f05f-11f0-93c2-def04981102a/0-wef-global-cybersecurity-outlook-2026.pdf

Glossaire

Les acronymes francophones et anglophones utilisés dans ce guide ont été listés ci-dessous.

- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information
- **CISO :** Chief Information Security Officer
- **CMDB** : Configuration Management Database
- **INR** : Institut du Numérique Responsable
- **MiNUM ECO** : Mission Interministèrielle Numérique Responsable
- **NIS2** : Network and Information Security 2
- **NIST** : National Institute of Standards and Technology
- **NR** : Numérique Responsable
- **RGESN** : Référentiel général d'écoconception de services numériques
- **RSSI** : Responsable de la Sécurité des Systèmes d'Information

ÉCOCONCEPTION ET CYBERSÉCURITÉ :

GUIDE DE MISE EN APPLICATION

C4T

CYBER 4 TOMORROW