Famille	N° Critère	Intitulé	Synergie	Divergence	Justification	Compléments et points de vigilance	Priorisation	Réduction surface attaque	Réduction flux Faveur détection	Organisationnel / process	Bénéfice financier
Stratégie	1.1	Le service numérique a-t-il été évalué favorablement en termes d'utilité en tenant compte de ses impacts environnementaux ?	Neutre	Non	L'utilité pour la transition écologique n'a pas d'impact pour la cybersécurité.						
	1.2	Le service numérique a-t-il défini ses cibles utilisatrices, les besoins métiers et les attentes réelles des utilisateurs-cibles ?	Oui	Non	Ce critère est cohérent avec le principe des moindres privilèges en cybersécurité.		P1	1			
	1.3	Le service numérique a-t-il au moins un référent identifié en écoconception numérique ?	Neutre	Non	La nomination d'un référent NR ne peut pas nuire à la cybersécurité.	Potentielle synergie, dans une approche «secure-and-sustainable-by-design» qui va induire de nommer et d'impliquer un référent NR et un référent cybersécurité.					
	1.4	Le service numérique réalise-t-il régulièrement des revues pour s'assurer du respect de sa démarche d'écoconception ?	Oui sous condition	Non	Ces revues sont une opportunité pour vérifier que les objectifs initiaux sont atteints (sur le plan de la sécurité, des impacts environnementaux et des performances) et de vérifier l'absence de régression lorsque le service est opérationnel. Il s'agit également d'une synergie garantissant la qualité des évolutions.	Il s'agit d'une synergie, à condition que les revues soient faites en même temps.	P1			1	
	1.5	Le service numérique s'est-il fixé des objectifs en matière de réduction ou de limitation de ses propres impacts environnementaux ?	Neutre	Non	Fixer des objectifs environnementaux ne doit pas amener à renoncer à des exigences de cybersécurité.	Il est important que cette bonne pratique soit neutre, pour ne pas amener à remettre en question la démarche d'écoconception.					
	1.6	Le service numérique collecte-t-il la donnée de façon responsable et raisonnée ?	Oui	Non	Il s'agit d'une synergie avec le principe de réduction de surface d'attaque : moins on conserve des données non-utilisées ou stockées sans raison, moins il y a de risques que ces données soient détournées.	Nota : des synergies potentielles existent si les indicateurs utilisés pour le numérique responsable permettent d'aider au décommissionnement des fonctions, des services métier ou techniques, ou des données qui ont peu d'usages (principes de minimisation d'exposition), mais ce point est traité avec la bonne pratique 2.7.	P1	1			1
	1.7	Le service numérique a-t-il recours à un niveau de chiffrement adapté à ses besoins ?	Oui	Non	Il s'agit d'une exigence commune à la cybersécurité et à l'écoconception, qui a aussi pour vertu de réduire les coûts.	Comme mentionné dans le RGESN, cette bonne pratique ne doit pas amener à descendre en dessous du niveau de chiffrement nécessaire. Des algorithmes de chiffrement peuvent être optimisés en termes de performance et de réduction d'empreinte environnementale.	P1			1	
	1.8	Le service numérique a-t-il mis en place des efforts d'open source ?	Oui	Non	L'open source peut être un facteur pour renforcer l'auditabilité et la transparence. L'open source est aussi un facteur d'indépendance et de souveraineté, car on réduit son niveau de dépendance en ayant accès au code.	Des contre-exemples peuvent exister si le nombre de personnes qui ont développé et qui maintiennent le produit est réduit. Il est préférable que le produit repose sur une communauté.	P2			1	
	1.9	Le service numérique a-t-il été conçu avec des technologies standard interopérables plutôt que des technologies spécifiques et fermées ?	Oui	Non	Il s'agit d'une synergie pour lutter contre l'obsolescence et maintenir les services dans la durée, à des coûts maitrisés. Cette bonne pratique apporte aussi la garantie de reposer sur des protocoles standardisés et éprouvés.	Il est souhaitable que les briques interopérables soient laussi standardisées, comme mentionné dans la bonne pratique du RGESN, pour garantir un degré de validation sur le plan de la cybersécurité.	P1			1	
	1.10	'Le service numérique repose-t-il sur des API documentées et ouvertes pour interagir avec le matériel ?	Oui	Non	Il s'agit d'une synergie pour lutter contre l'obsolescence et maintenir les équipements dans la durée, à des coûts maitrisés. Cette bonne pratique apporte aussi la garantie de faciliter les audits de sécurité: ce qui est documenté est plus facilement auditable	«Open source» ne signifie pas forcément «usage libre». D'un point de vue «cybersécurité», il peut être utile qu'un service soit ouvert mais pas libre.	P2				1
Spécification	2.1	Le service numérique a-t-il défini la liste des profils de matériels que les utilisateurs vont pouvoir employer pour y accéder ?	Oui	Non	Connaitre les matériels pouvant être compatibles (ou non) avec le service permet d'écarter des équipements qui ne seraient pas sûrs (ex : matériel doté de puces électroniques dont on ne connait pas la fonctionnalité).	Point de vigilance : sans support des fonctionnalités de cybersécurité, le matriel doit être exclu de la liste des équipements compatibles et autorisés. Ce point de vigilance est mentionné dans le RGESN (critère n° 3.4).	P1			1	
	2.2	Le service numérique a-t-il défini la liste des profils de matériels que les utilisateurs vont pouvoir employer pour y accéder ?	Oui	Non	Tant que les équipements peuvent réaliser leurs mises à jour de sécurité, garantir la compatibilité avec les anciens modèles est un moyen de limiter l'impact environnemental et financier de la cybersécurité.	Point de vigilance : sans support des fonctionnalités de cybersécurité, le matériel doit être exclu de la liste des équipements compatibles et autorisés. Ce point de vigilance est mentionné dans le RGESN (critère n° 3.4).	P2				1
	2.3	Le service numérique est-il utilisable via une connexion bas débit ou hors connexion ?	Oui sous condition	Non	Travailler hors connexion est une pratique sécurisée, sous réserve que les mises à jour de sécurité soient bien effectuées sur le terminal.	En connexion bas débit, se connecter à un VPN peut s'avérer impossible. En demandant de tester en bas débit, on se prive de l'utilisation de services qui nécessiteraient un degré de sécurisation exigeant la connexion VPN.	P3	1			
	2.4	Le service numérique est-il utilisable sur d'anciennes versions de système d'exploitation et de navigateurs web ?	Oui sous condition	Non	Cette exigence oblige une prise en compte de la version des systèmes d'exploitation, de leur âge et de la durée de la maintenance. Cela peut permettre d'anticiper dès l'apparition de vulnérabilités causées par absence de mises à jour, par exemple. Dans cette recommandation «ancien» ne signifie pas que les mises à jour de sécurité ne sont plus supportées.	Sous condition de bien s'assurer que les dernières mises à jour de sécurité ont été effectuées. Le degré de priorité élevé car cette pratique est importante pour augmenter la durée de vie des équipements, tout en maintenant le degré de cybersécurité.	P1			1	
	2.5	Le service numérique s'adapte-t-il à différents types de terminaux d'affichage ?	Oui sous condition	Non	Cette exigence permet de freiner l'obsolescence des équipements les moins puissants en n'affichant que la quantité d'information utile.	A condition d'éviter de dupliquer le service numérique avec une version spécifique pour chaque type de terminal.	P2				1
	2.6	Le service numérique a-t-il été conçu avec une revue de conception et une revue de code comprenant parmi ses objectifs la réduction des impacts environnementaux de chaque fonctionnalité ?	Oui sous condition	Non	Revue de code, revue d'architecture et validation des fonctionnalités, sont des mesures indispensables d'un point de vue «cybersécurité» ; il y a donc une synergie à réaliser en mettant en place des revues communes. Cela permet de limiter le nombre de fonctionnalités, limitant ainsi la surface d'attaque.	A condition de ne pas ségréger les revues par approche (revue «numérique responsable séparée de la revue «cybersécurité», par exemple) et d'être en mesure d'intégrer ces revues à des méthodologies type «Agile».	P1			1	
	2.7	Le service numérique a-t-il prévu une stratégie de maintenance et de décommissionnement ?	Oui sous condition	Non	Il s'agit d'une synergie compatible avec la réduction de surface d'attaque par arrêt des services (ou d'une partie de leurs fonctionnalités et suppression de leurs données qui ne sont plus ou sont sous-utilisées) ; il n'y a pas de service qui présente moins de risque que celui qui est arrêté. Publier le code source de services arrêtés peut être très utile à la communauté.	A condition d'avoir un plan de décommissionnement et des rendez-vous associés, tel que défini dans l'exigence. Un point de vigilance est à souligner sur la sauvegarde des logs (pour l'IA par exemple), la politique du «je garde tout au cas où» doit être supplantée par une politique de sélection des données utiles, pertinentes et valides.	P1			1	1
	2.8	Le service numérique impose-t-il à ses fournisseurs de garantir une démarche de réduction de leurs impacts environnementaux ?	Oui sous condition	Non	Il s'agit d'une opportunité pour utiliser les revues avec les fournisseurs pour demander des engagements, tant sur la partie cybersécurité que sur la réduction d'impacts environnementaux ; embarquer sa chaine de valeur est indispensable pour les 2 approches.	Sous réserve d'intégrer les 2 sujets aux mêmes revues et évaluations, et sous réserve que les services achats soient moteurs sur les 2 sujets (dans une démarche commune d'achats responsables).	P1			1	
	2.9	Le service numérique a-t-il pris en compte les impacts environnementaux des composants d'interface prêts à l'emploi utilisés ?	Oui sous condition	Non	Si des composants sont simples et si le transfert de données est limité, leur contrôle est facilité. Dans une approche KISS, les risques sont réduits. La réduction de surface d'attaque et simplifie également les audits.	Sous réserve que les composants ayant le moins d'impact qui soient sélectionnés.	P2	1		1	
	2.10	'Le service numérique a-t-il pris en compte les impacts environnementaux des services tiers utilisés lors de leur sélection ?	Oui sous condition	Non	Si les services tiers utilisés sont simples et éprouvés, et si le transfert de données est limité, leur contrôle est simplifié ; la réutilisation est une synergie.	Sous réserve que les composants ayant le moins d'impact qui soient sélectionnés.	P2			1	
Architecture	3.1	Le service numérique repose-t-il sur une architecture, des ressources ou des composants conçus pour réduire leurs propres impacts environnementaux ?	Neutre	Non	L'exigence d'évaluation des impacts des briques utilisées est sans corrélation directe avec les enjeux de cybersécurité.	En cybersécurité, les principes de récursion et de chaines de dépendance existent aussi.					
	3.2	Le service numérique fonctionne-t-il sur une architecture pouvant adapter la quantité de ressources utilisées à la consommation du service ?	Neutre	Possible	Les traitements resteront les mêmes, donc la réduction des ressources ne se traduira pas par une amélioration du niveau de sécurité.	La mise à l'échelle dynamique peut se traduire par un risque supérieur sur l'interruption ou la dégradation du service (ce qui concerne plus la résilience que la sécurité). Les algorithmes d'autoscaling évoluent fréquemment et leur prédictibilité peut faire défaut.					
	3.3	Le service numérique est-il en mesure de supporter l'évolution technique des protocoles ?	Oui	Non	La mise à jour des protocoles permet d'anticiper les futures menaces en cybersécurité (crypto-agilité, protocole d'authentification...)	Pouvoir changer les protocoles représente un intérêt convergent pour lutter contre l'obsolescence. Une limite est à relever : augmenter la taille des clés est parfois une solution retenue pour la partie cyber, ce qui peut engendrer un coût environnemental.	P1			1	1
	3.4	Le service numérique garantit-il la mise à disposition de mises à jour correctives pendant toute la durée de vie prévue des équipements et des logiciels liés au service ?	Oui	Non	Les mises à jour sont des pratiques fondamentales de cybersécurité ; s'assurer de la durée de disponibilité des mises à jour et du support associé va dans le sens de la sécurisation des systèmes dans la durée.	Il s'agit aussi d'un intérêt convergent pour lutter contre l'obsolescence.	P1			1	1
	3.5	Le service numérique propose-t-il d'installer des mises à jour correctives indépendamment des mises à jour évolutives de façon transparente ?	Oui	Non	Séparer mises à jour de sécurité et mises à jour fonctionnnelles permet d'avoir les mises à jour de sécurité plus rapidement, et de faciliter leur publication. Certaines nouvelles fonctionnalités ne sont pas utilisées et demandent des ressources supplémentaires qui vont contribuer à une baisse des performances et à une obsolescence perçue comme prématurée.	En pratique, la mise en œuvre peut être compliquée pour des raisons de coûts des tests de non-régression. Certains outils sont l'objet de mises à jour si fréquentes qu'il est courant de constater des absences de mises à jour qui exposent à des risques de cybersécurité. Séparer les mises à jour fonctionnelles et les mises à jour de sécurité permettrait de ralentir le nombre et la fréquence des mises à jour.	P3			1	1
	3.6	Le service numérique propose-t-il les mises à jour incrémentielles, afin de ne pas remplacer tout le code à chaque mise à jour ?	Oui	Non	La modularité, sous réserve qu'elle soit faite dans le respect des bonnes pratiques des métiers informatiques (architectes/développeurs), est un facteur limitant les régressions y compris en termes de sécurité.	En pratique, des complications pour des raisons de coûts des tests de non-régression purraient être redoutées, mais l'incrémentiel facilite aussi la recette ecar on a la garantie que seul le composant en question a été modifié	P2			1	
	3.7	Le service numérique optimise-t-il la sollicitation des environnements de développement, de préproduction ou de test en fonction de ses besoins ?	Oui	Non	En arrêtant les environnements non-utilisés (en particulier, ceux de développement), on réduit la surface d'attaque temporelle.	La représentativité des environnements de développement est parfois éloignée des environnements de production.	P2	1			
UX/UI	4.1	Le service numérique comporte-t-il uniquement des animations, vidéos et sons dont la lecture automatique est désactivée ?	Oui	Non	La réduction du flux de données diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent.		P3		1		
	4.2	Le service numérique affiche-t-il uniquement des contenus sans défilement infini ?	Oui	Non	La réduction du flux de données diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent.		P3		1		
	4.3	Le service numérique optimise-t-il le parcours de navigation pour chaque fonctionnalité principale ?	Oui	Non	La réduction du nombre de fonctionnalités réduit la surface d'attaque, et la réduction du temps passé sur le service réduit l'exposition. La simplification engendrée dans les pipelines CI/CD (chaines d'intégration et développement continues) réduit les vulnérabilités potentielles.		P2	1			
	4.4	Le service numérique permet-il à l'utilisateur de décider de l'activation d'un service tiers ?	Oui	Non	Les services tiers sont autant de failles potentielles ; limiter leur activation réduit donc la surface d'attaque.	Les pratiques de cyber contrôlent systématiquement les services tiers utilisés et limitent leur nombre au strict nécessaire, qu'ils soient activables ou lancés automatiquement. La cybersécurité encourage à pousser la bonne pratique jusqu'à la remise en question de l'utilisation du service tiers.	P2	1		1	
	4.5	Le service numérique utilise-t-il majoritairement des composants fonctionnels natifs du système d'exploitation, du navigateur ou du langage utilisé ?	Oui	Non	La bonne pratique réduit le nombre de contrôle de nouveaux composants fonctionnels et facilite les revues de cybersécurité.	Les composants fonctionnels natifs bénéficient déjà d'un support de maintenance cyber.	P1		1		
	4.6	Le service numérique utilise-t-il uniquement du contenu vidéo, audio et animé porteur d'informations ?	Oui	Non	La réduction du flux de données diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent.		P3		1		
	4.7	Le service numérique opte-t-il pour les choix les plus sobres entre le texte, l'image, l'audio ou la vidéo, selon les besoins utilisateurs ?	Oui	Non	La réduction du flux de données diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent.	Réduire les types de format (texte, son, vidéo...) permet de réduire le nombre de requête / instance.	P3		1		
	4.8	Le service numérique limite-t-il le nombre des polices de caractères téléchargées ?	Oui	Non	La bonne pratique réduit le nombre de contrôle de nouveaux composants fonctionnels et facilite les revues de cybersécurité.	Les polices de caractère peuvent paraitre anectodiques d'un point de vue «cybersécurité», or elles sont utilisées pour aider à la traçabilité ou à la detection de menaces (ex : phishing) car elles peuvent être la signature de certains pays à risque.	P3			1	
	4.9	Le service numérique limite-t-il les requêtes serveur lors de la saisie utilisateur ?	Oui	Non	La réduction du flux de données diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent. Contrôler et suivre dans le temps le nombre de requête «http» entre client et serveur, ainsi que l'absence de requête identique ou redondante, est nativement une bonne pratique de cybersécurité.	Réduire les appels à des API, scripts, librairies ou polices de caractères tiers présente un bénéfice direct d'un point de vue «cybersécurité».	P1		1	1	
	4.10	Le service numérique informe-t-il l'utilisateur du format de saisie attendu, en évitant les requêtes serveur inutiles pour la soumission d'un formulaire ?	Oui	Non	La réduction du nombre de requête entre client et serveur diminue les ressources informatiques nécessaires aux contrôles, et donc les facilitent.		P3		1		
	4.11	Le service numérique informe-t-il l'utilisateur, avant le transfert, des poids et formats de fichier attendus ?	Neutre	Non	La sensibilisation aux poids et formats des fichiers transférés n'empêche pas leur transfert. Les bénéfices sur les flux de données ne sont pas systématiques.						
	4.12	Le service numérique indique-t-il à l'utilisateur que l'utilisation d'une fonctionnalité a des impacts environnementaux importants ?	Neutre	Non	La sensibilisation aux impacts environnementaux n'empêche pas l'utilisation du service. Les bénéfices d'un point de vue cybersécurité ne sont pas systématiques.						
	4.13	Le service numérique limite-t-il le recours aux notifications, tout en laissant la possibilité à l'utilisateur de les désactiver ?	Oui	Non	Les notifications peuvent provoquer une séquence de phishing ; réduire leur nombre permet donc de réduire ce risque.		P3		1		
	4.14	Le service numérique évite-t-il le recours à des procédés manipulatoires dans son interface utilisateur ?	Neutre	Non	Les mécanismes de captation de l'attention ne se traduisent pas systématiquement par des menaces de cybersécurité, même si les intentions sont de manipuler l'utilisateur final à des fins malhonnêtes.				1		
	4.15	Le service numérique fournit-il à l'utilisateur un moyen de contrôle sur ses usages afin de suivre et de réduire les impacts environnementaux associés ?	Neutre	Non	La sensibilisation aux impacts environnementaux n'empêche pas l'utilisation du service.				1		
Content	5.1	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte de visualisation de chaque image ?	Oui	Non	Les préconisations fonctionnelles favorisent l'efficacité du service mais sont neutres sur les critères de confidentialité, d'intégrité et de disponibilité sur action malveillante. En revanche, la réduction du flux d'information favorise la détection d'actions malveillantes. Préciser les formats à utiliser en évitant les formats exotiques favorise la vérification et permet de définir des formats à utiliser qui intègrent des standards de sécurité du marché (reconnus en terme de robustesse et de maitrise des risques) pour l'analyse.		P2		1		
	5.2	Le service numérique propose-t-il des images dont le niveau de compression est adapté au contenu et au contexte de visualisation ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes.		P2		1		
	5.3	Le service numérique utilise-t-il, pour chaque vidéo, une définition adaptée au contenu et au contexte de visualisation ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes, et donc l'observation générale du service.		P1		1		
	5.4	Le service numérique propose-t-il des vidéos dont le mode de compression est efficace et adapté au contenu et au contexte de visualisation ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes.		P2		1		
	5.5	Le service numérique propose-t-il un mode « écoute seule » pour ses vidéos ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes, et donc l'observation générale du service.		P1		1		
	5.6	Le service numérique propose-t-il des contenus audios dont le mode de compression est adapté au contenu et au contexte d'écoute ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes.		P2		1		
	5.7	Le service numérique utilise-t-il un format de fichier adapté au contenu et au contexte d'utilisation pour chaque document ?	Oui	Non	Les préconisations fonctionnelles favorisent l'efficacité du service mais sont neutres sur les critères de confidentialité, d'intégrité et de disponibilité sur action malveillante. En revanche, la réduction du flux d'information favorise la détection d'actions malveillantes. Préciser les formats à utiliser en évitant les formats exotiques favorise la vérification et permet de définir des formats à utiliser qui intègrent des standards de sécurité du marché (reconnus en terme de robustesse et de maitrise des risques) pour l'analyse.		P2		1		
Front end	5.8	Le service numérique a-t-il une stratégie d'archivage et de suppression, automatique ou manuelle, des contenus obsolètes ou périmés ?	Oui	Non	Le critère va dans le sens de la réduction de surface d'attaque. Les données stagnantes et anciennes peuvent être une source de vulnérabilité (via des VM non gérées par exemple). Une donnée doit avoir une durée de vie et son traitement en fin de vie doit être défini.		P1	1		1	
	6.1	Le service numérique s'astreint-il à un poids maximum et une limite de requête par écran ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes. Cela contribue à la réduction de surface d'attaque et à la limitation au minimum des flux, pour répondre aux besoins stricts du service.	Point de vigilance : ceci ne doit pas se faire au détriment d'un éventuel chiffrement. Il est recommander de distinguer les types d'informations par service applicatif (avec un propre endpoint par service, par exemple).	P3	1	1		
	6.2	Le service numérique utilise-t-il des mécanismes de mise en cache pour la totalité des contenus transférés dont il a le contrôle ?	Oui sous condition	Non si des vigilances sont respectées	La réduction du flux d'information favorise la détection d'actions malveillantes. Cependant, les informations sensibles ne devraient pas être mises en cache. Le cache doit donc être autorisé par défaut, mais inhibé en cas de données identifiées comme sensibles.	Le stockage doit être sécurisé en cas de données sensibles (ex : chiffrement dans un container). Le stockage en navigateur n'est pas forcément préconisé d'un point de vue cybersécurité car la donnée est exposée. La bonne pratique proposée est d'avoir sur les terminaux 2 flux et 2 environnements virtuels séparés (pro / données privées).	P2		1		
	6.3	Le service numérique a-t-il mis en place des techniques de compression pour les ressources transférées dont il a le contrôle ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes.	Les mécanismes de compression doivent faire l'objet d'une validation par les services de cybersécurité. Attention à éviter de compresser les données sensibles, car les mécanismes de compresion peuvent favoriser la récupération de données.	P3		1		
	6.4	Le service numérique affiche-t-il majoritairement des images dont les dimensions d'origine correspondent aux dimensions du contexte d'affichage ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes.	Le traitement côté serveurs doit être optimisé afin d'éviter tout déni de service lié aux ressources de calculs nécessaires.	P2		1		
	6.5	Le service numérique évite-t-il de déclencher le chargement de ressources et de contenus inutilisés pour chaque fonctionnalité ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes et contribue directement à la réduction de la surface d'attaque.		P1		1		
	6.6	Le service numérique restreint-il l'usage des capteurs des terminaux utilisateurs au besoin du service ?	Oui	Non	La réduction du flux d'information favorise la détection d'actions malveillantes et contribue directement à la réduction de la surface d'attaque.		P2	1	1		
	6.7	Le service numérique héberge-t-il toutes les ressources statiques transférées dont il est l'émetteur sur un même domaine ?	Oui	Non	Limiter les domaines permet de simplifier les politiques CSP.	L'intérêt est évident à l'échelle d'une même entreprise. Lorsque le fournisseur de services adresse plusieurs clients externes, il peut être intéressant d'avoir des noms de domaines séparés par client. La dernière phrase est importante et doit être respectée : Les ressources statiques, hors services tiers, sont transférées via un seul nom de domaine à un instant « t ».	P3			1	
Back end	7.1	Le service numérique a-t-il recours à un système de cache serveur pour les données les plus utilisées ?	Neutre	Non	Pas d'amélioration ni de dégradation identifiée concernant la cybersécurité.	La solution de mise en cache doit être analysée d'un point de vue cybersécurité. La vérification d'intégrité est particulièrement importante.					
	7.2	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 ?	Oui	Non	Le critère va dans le sens de la réduction de surface d'attaque. Les données stagnantes et anciennes peuvent être une source de vulnérabilité (via des VM non gérées par exemple). Une donnée doit avoir une durée de vie et son traitement en fin de vie doit être défini.	Les données à caractère légal ou de certification doivent faire l'objet de procédure particulière.	P1	1		1	
	7.3	Le service numérique informe-t-il l'utilisateur d'un traitement en cours en arrière-plan ?	Oui	Non	Le critère pointe un intérêt commun entre cybersécurité et écoconception car cela permet de limiter les sources d'erreurs. La synergie est assez forte si on empêche également le rejeu tant que l'action est en cours, car elle limite la capacité d'un bot à utiliser cette fonctionnalité pour provoquer un déni de service.	Cette bonne pratique peut aller à l'encontre de développements hatifs, et encourage la qualité. Plusieurs solutions techniques sont possibles en backend, alors que ce point n'est souvent traité qu'en frontend.	P3			1	
	7.4	Le service numérique s'appuie-t-il sur un mécanisme de consensus qui minimise sa consommation de ressources ?	Neutre	Non	Il existe de multiples types de blockchains. Qu'elle soit basée sur du minage ou non ne présente pas de différence majeure en terme de sécurisation.	Eviter une blockchain si on peut l'éviter est une bonne pratique d'un point de vue «cybersécurité». Les blockchains les plus complexes sont les plus compliquées à sécuriser.					
Hébergement	8.1	Le service numérique utilise-t-il un hébergement ayant une démarche de réduction de son empreinte environnementale ?	Neutre	Non	Les consommations d'énergie, d'eau et de ressources participent à la résilience globale du service, mais ne sont pas directement liées aux enjeux de cybersécurité.						
	8.2	Le service numérique utilise-t-il un hébergement qui fournit une politique de gestion durable des équipements ?	Oui	Non	La sélection des équipements est une opportunité pour se questionner sur la maitrise des impacts environnementaux par les fabricants, ainsi que sur les risques cyber associés aux composants des équipements. La fin de vie est une opportunité pour gérer l'effacement des données, avec des opportunités de privilégier des méthodes non destructives et de réserver les méthodes destructives aux disques durs magnétiques les plus sensibles pour des OIV.	Certaines normes privilégiant la destruction physique (par exemple, le perçage du disque dur) devraient être remises en question compte tenu de l'évolution des technologies (SSD par exemple) et des méthodes d'effacement.	P2			1	
	8.3	Le service numérique utilise-t-il un hébergement dont le PUE (Power Usage Effectiveness) est minimisé ?	Neutre	Non	Le PUE est un indicateur qui n'est pas lié aux enjeux de cybersécurité mais plus un DC est sécurisé (TIER élevé), plus le PUE est dégradé.	Point de vigilance : le PUE ne doit pas pousser à dégrader le niveau de sécurité.					
	8.4	Le service numérique utilise-t-il un hébergement dont son WUE (Water Usage Effectiveness) est minimisé ?	Neutre	Non	Un WUE plus faible se traduit généralement par un PUE plus élevé. Ceci n'a pas d'impact sur la cybersécurité.						
	8.5	Le service numérique utilise-t-il un hébergement dont l'origine de consommation d'électricité est documentée et majoritairement d'origine renouvelable ?	Neutre	Non	L'origine de l'électricité (qui dans tous les cas provient en majorité du réseau national) n'affecte pas sa disponibilité (à date).						
	8.6	Le service numérique utilise-t-il un hébergement dont la localisation géographique est cohérente avec ses activités et qui minimise son empreinte environnementale ?	Oui	Non	La localisation du data centre est un point important en terme de souveraineté (à l'échelle nationale ou européenne) et de réglementation, par exemple sur les risques associés aux transferts de données.	Pour les offreurs de service, il est possible de constater une opposition entre la situation géographique des clients et la souveraineté sur les données / une localisation du data center sur une région en fourniture électrique bas carbone.	P1			1	
	8.7	Le service numérique utilise-t-il un hébergement qui traite efficacement la chaleur produite par les serveurs ?	Neutre	Non	Les systèmes de récupération de chaleur (ou de refroidissement naturel) sont transparents du point de vue «cybersécurité».						
	8.8	Le service numérique héberge-t-il de façon distincte les données « chaudes » et « froides » ?	Oui	Non	On constate un intérêt d'un point de vue «cybersécurité» et d'un point de vue «réduction des impacts environnementaux», à pouvoir arrêter ou mettre en veille les serveurs hébergeant des données froides.	Point de vigilance : la séparation des données pourrait amener à surdimensionner les ressources informatiques d'un côté ou de l'autre, ou des deux.	P1	1			
	8.9	Le service numérique duplique-t-il les données uniquement lorsque cela est nécessaire ?	Oui	Non	Ne dupliquer que le nécessaire permet de réduire la surface d'attaque.		P1	1			
	8.10	Le service numérique tient-il compte des contraintes externes pour minimiser l'impact environnemental des calculs et transferts de données asynchrones ?	Oui	Non	Lisser la charge de calcul permet d'optimiser les ressources et de limiter le nombre de serveurs et d'équipements réseau (dimensionné en pic), et donc de réduire la surface d'attaque.	Nota: on peut considérer qu'il est surprenant que cette bonne pratique soit classée dans la famille «hébergement», en considérant qu'elle relève plutôt de la conception du service numérique. Mais le RGESN estime que les responsable des l'hébèrgement sont ceux qui peuvent indiquer les périodes de moindre charge et encourager leur client à mieux les utiliser (par exemple via la tarification).	P3	1			
Algorithmie	9.1	Le service numérique a-t-il interrogé la nécessité d'une phase d'entraînement pour éviter un usage non justifié et déraisonné ?	Oui	Non	Certains modèles d'IA peuvent être influencés par des données biaisées ; limiter les entrainements et la quantité des données utilisées permet de réduire ce type de risques.	Sans phase d'apprentissage, les biais existant dans le modèle ne seront pas améliorés. Sans visibilité sur les données initiales d'entrainement, il est difficile de quantifier les bénéfices de nouveaux entrainements.	P3			1	
	9.2	Le service numérique utilise-t-il une phase d'apprentissage avec un niveau de complexité minimisé et proportionné à l'usage effectif du service ?	Neutre	Non	Ce critère n'engendre pas d'impact clair d'un point de vue «cybersécurité».						
	9.3	Le service numérique a-t-il mis en place des mécanismes visant à limiter la quantité d'entraînement nécessaire à son fonctionnement ?	Oui	Non	Certains modèles d'IA peuvent être influencés par des données biaisées ; limiter les entrainements et la quantité des données utilisées permet de réduire ce type de risques.	Sans phase d'apprentissage, les biais existant dans le modèle ne seront pas améliorés. Sans visibilité sur les données initiales d'entrainement, il est difficile de quantifier les bénéfices de nouveaux entrainements.	P3			1	1
	9.4	Le service numérique limite-il la quantité de données utilisées pour la phase d'apprentissage au strict nécessaire ?	Oui	Non	Certains modèles d'IA peuvent être influencés par des données biaisées ; limiter les entrainements et la quantité des données utilisées permet de réduire ce type de risques.	Sans phase d'apprentissage, les biais existant dans le modèle ne seront pas améliorés. Sans visibilité sur les données initiales d'entrainement, il est difficile de quantifier les bénéfices de nouveaux entrainements.	P3			1	
	9.5	Le service numérique optimise-t-il l'occurrence de mise à jour et de réentraînement des modèles en fonction de ses besoins et des cibles utilisatrices ?	Neutre	Non	Ce critère n'engendre pas d'impact clair d'un point de vue «cybersécurité».						
	9.6	Le service numérique utilise-t-il des techniques de compression pour les modèles utilisés lors de la phase d'entraînement ?	Neutre	Non	Ce critère n'engendre pas d'impact clair d'un point de vue «cybersécurité». La compression risque de dégrader la précision, mais seule la qualité du résultat est affectée.						
	9.7	Le service numérique utilise-t-il une stratégie d'inférence optimisée en termes de consommation de ressources et des cibles utilisatrices ?	Neutre	Non	Ce critère n'engendre pas d'impact clair d'un point de vue «cybersécurité».						