Objectifs de sécurité NIS2 - France (Source : ANSSI, Dcument de travail version 2.4)	Détails de mise en place	Analyse du GT «Ecoconception & Cybersécurité»	Synthèse
Objectifs de sécurité applicables aux entités importantes et essentielles			
1. Recensement des systèmes d'information	*Les entités [importantes ou essentielles] réalisent et maintiennent à jour une liste de l'ensemble de leurs activités et services ainsi que des systèmes d'information y contribuant.* *Ces entités sont tenues d'appliquer les [objectifs de sécurité] sur l'ensemble de leurs systèmes d'information, à l'exception de ceux pour lesquels elles justifient, sur la base d'une analyse de risques, qu'ils ne sont pas exposés à l'un des risques suivants :* *1. La dégradation ou l'interruption, directe ou indirecte, des activités ou services de l'entité ;* *2. La divulgation à des personnes non autorisées d'informations sensibles traitées par les activités ou services de l'entité ;* *3. L'altération des informations nécessaires aux activités ou services de l'entité.* *La mise en œuvre de mesures de sécurité sur ces systèmes d'information ne permet pas de justifier qu'ils ne sont exposés à aucun des risques précités.* *Pour ces systèmes d'information, le choix de ne pas appliquer les objectifs de sécurité ainsi que sa justification au regard des critères précédents doivent apparaître explicitement dans la liste mentionnée au premier alinéa.*	**Il s'agit d'une synergie :** - Avoir un listing des services et une base de données (CMDB) permettant de faire le lien vers le hardware est une synergie avec la sécurité / sustainability / coût / maintenabilité / qualité. Ces outils sont encore peu implémentés. - Connaitre l'état de référence et maitriser les systèmes d'information actifs au sein de l'entité encourage le décommissionnement des actifs inutiles.	Synergie
2. Mise en oeuvre d'un cadre de gouvernance de la sécurité numérique	*Les entités [importantes et essentielles] définissent un cadre de gouvernance de la sécurité numérique placé sous la responsabilité du dirigeant exécutif.* *Le cadre de gouvernance de la sécurité numérique consiste en la mise en place, au sein des entités [importantes et essentielles] :* *1. D'une organisation ;* *2. De rôles et responsabilités en matière de sécurité numérique ;* *3. De processus de gestion de la conformité ;* *4. D'une politique de sécurité des systèmes d'information et des politiques comprenant au minimum des dispositions en matière d'usage du chiffrement, de contrôle d'accès physique et logique et de revue de l'application des mesures de sécurité mises en œuvre.*	**Il s'agit d'une synergie :** - La clarification des rôles et responsabilité permettra de mieux interfacer les deux enjeux ; - Les mesures de prévention préconisées, comme limiter les accès aux seules personnes le justifiant, permet de réduire l'exposition à des risques d'attaques qui auraient un impact environnemental significatif ; - La gouvernance étant au cœur des cadres RSE et durabilité, la synergie peut s'étendre à la liaison et à l'intégration de la RSE/ durabilité organisationnelle de l'entité dans celle de la sécurité (tout comme dans celle de la DSI, et autres départements).	Synergie
3. Maitrise de l'écosystème	*Les entités [importantes ou essentielles] réalisent et maintiennent à jour une liste des prestataires et fournisseurs informatiques intervenant dans la réalisation de leurs activités ou dans la fourniture de leurs services et avec lesquels il existe une relation contractuelle ainsi que le périmètre et la nature de la prestation ou du service fourni.* *Ces entités mettent en place des processus visant à s'assurer, notamment par voie contractuelle, que leurs prestataires et fournisseurs informatiques leur permettent de satisfaire à leurs obligations résultantes de l'article 14 et du premier alinéa de l'article 17 [du PJL].*	**Il s'agit d'une synergie :** - Si l'approche par les risques est intégrée au plus haut niveau de l'organisation, elle permet un échange entre les acteurs de la cybersécurité et du numérique responsable. Ceci est nécessaire à l'identification de synergies et à l'anticipation des problèmes d'approvisionnement, permettant de préparer des plans de continuité d'activité (ou DRP) et de dépasser les éventuelles divergences sur l'obsolescence. - l'objectif permet d'adresser la chaine de valeur de l'organisation (80% de l'impact climatique d'une DSI ou d'une ESN est lié à sa chaine de valeur amont (scope 3 amont)). Il y a une opportunité de solliciter ses fournisseurs à la fois sur le plan de la sécurité informatique et de ses impacts environnementaux, et de collecter ou de mettre à jour des informations, de favoriser la mise en oeuvre de plans d'actions cohérents.	Synergie
4. Intégration de la sécurité numérique dans la gestion de ses ressources humaines	*Les entités [importantes ou essentielles] intègrent la sécurité numérique dans la gestion de leurs ressources humaines en sensibilisant leurs utilisateurs, en particulier les dirigeants de l'entité, et en formant à la sécurité numérique les personnes occupant des fonctions à responsabilités dans le domaine du numérique.* *Ces entités prennent en compte la sécurité numérique dès l'arrivée d'un nouveau personnel et jusqu'à son départ de l'entité.*	**Il s'agit d'une opportunité de synergie :** - La sensibilisation et la formation sont des élements clés pour développer une culture partagée sur ces enjeux au sein de l'entreprise, tout en donnant du sens à l'approche «secure-and-sustainable-by-design». L'objectif permet de responsabiliser les utilisateurs finaux pour leur montrer qu'ils ont un rôle à jouer. - Embarquer les équipes cyber, UX (dont acessibilité) et éconception dans les process de développement des services numériques permet de garantir des systèmes plus pérennes et mieux acceptés par les usagés.	Opportunité de synergie
5. Maîtrise des systèmes d'information	*Les entités [importantes ou essentielles] disposent d'au moins une cartographie de leurs systèmes d'information suffisamment détaillée pour faciliter :* *1° Le maintien en condition opérationnelle et de sécurité de leurs systèmes d'information ;* *2° L'amélioration de la réactivité de ces entités en cas d'incident de sécurité affectant leurs systèmes d'information.* *Ces entités définissent et mettent en œuvre un processus de maintien en condition opérationnelle et de sécurité de leurs systèmes d'information visant à appliquer les correctifs de sécurité liés à des vulnérabilités affectant ces systèmes et ainsi à limiter l'exposition des entités aux risques numériques résultant de ces vulnérabilités.*	Il s'agit d'une synergie : - avoir un listing des services et une base de données (CMDB) permettant de faire le lien vers le hardware est une synergie avec la sécurité / sustainability / coût / maintenabilité / qualité. - Comme précédemment expliqué, la dimension préventive permet de limiter les impacts environnementaux qui seraient induits par une interruption de service.	Synergie
6. Maîtrise des accès physiques aux locaux	*Les entités [importantes ou essentielles] mettent en place des mécanismes de contrôle d'accès et de gestion des droits d'accès ainsi que des processus de gestion des visiteurs afin de s'assurer que seules les personnes autorisées ont accès à leurs locaux et en particulier aux locaux techniques ou contenant des serveurs de données.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - L'impact réel lié aux systèmes de sécurité physiques à déployer est à évaluer (impact environnemental du système de surveillance (caméra, stockage, capteurs/détecteurs et autres IoT, etc.) et de contrôle d'accès), en limitant les accès et les visites au juste nécessaire. - Les visites de centre informatique sont aussi un outil de sensibilisation à la matérialité du numérique. - Cet objectif permet de réduire les risques d'interruption de service qui auraient un impact environnemental certain.	Synergie et divergence
7. Sécurisation de l'architecture des systèmes d'information	*Les entités [importantes ou essentielles] identifient les besoins d'exposition et d'interconnexion de leurs activités et services fournis à des systèmes d'information tiers.* *Ces entités filtrent les communications entrantes et sortantes de leurs systèmes d'information, en particulier les flux dont l'origine, le transit ou la destination est un système d'information tiers.* *Les entités [essentielles] cloisonnent leurs systèmes d'information en zones de sécurité cohérentes et contrôlent les points d'entrée et de sortie des systèmes d'information pour les utilisateurs, les prestataires et les fournisseurs.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - L'objectif amène à avoir des réseaux indépendants, avec un impact environnemental significatif. - Si les outils d'identification des flux (ex : proxy), ont un impact environnemantal lié aux matériels nécessaires à leur fabrication / utilisation, ils permettent aussi de savoir quels flux circulent sur le réseau (observabilité) et d'établir des clés de répartition sur les différents usages (utile pour les ACV) de moyens communs (réseaux). Ils permettent aussi de limiter les flux. - Cet objectif va encourager une rationnalisation des interconnexions des flux de données, ce qui va dans le sens de la sobriété.	Synergie et divergence
8. Sécurisation des accès distants aux systèmes d'information	*Les entités [importantes ou essentielles] mettent en place :* *1. Des mécanismes d'identification et d'authentification des personnes et processus automatiques accédant à leurs systèmes d'information depuis des systèmes d'information tiers conformes [aux exigences en matière d'identification (Objectif 10)];* *2. Des mécanismes de sécurisation du canal de communication, des points d'entrée et de sortie et des accès à leurs systèmes d'information depuis des systèmes d'information tiers.*	**Il s'agit d'une synergie :** - A condition de mettre ces listes à jour et de limiter le nombre d'utilisateurs au strict nécessaire ; - Cet objectif permet également une réduction des risques de cyberattaques, qui auraient un impact environnemental certain. Un point de vigilance est toutefois à mettre en exergue (pour raison cyber et environnement). Il convient de ne pas mutliplier les systèmes d'authentification et de préférer un système mutualisé et maîtrisé.	Synergie
9. Protection des systèmes d'information contre codes malveillants	*Les entités [importantes ou essentielles] mettent en œuvre des mécanismes de protection contre les codes malveillants sur les ressources de leurs systèmes d'information.* *Les entités [essentielles] s'assurent que seules les ressources matérielles que ces entités, ou toute personne qu'elles ont mandatée à cet effet, gèrent et qui participent à la réalisation des activités ou la fourniture des services de l'entité ou au maintien en condition opérationnelle et de sécurité se connectent aux systèmes d'information.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - Des moyens nécessaires sont déployés (antivirus, process dans les chaines CICD) avec des impacts associés, mais ne pas le déployer exposerait à des risques qui auraient un coût potentiellement bien supérieur. - Un point de vigilance est à mentionner : il convient d'être vigilant à ce que les solutions mises en œuvre ne se mettent pas en conflit ou n'amènent pas à inhiber des agents, pour des questions de performance. Il y a donc une synergie à se poser la question des justes moyens.	Synergie et divergence
10. Gestion des identités et des accès des utilisateurs aux systèmes d'information	*Les entités [importantes ou essentielles] mettent en œuvre :* *1. Des mécanismes d'identification et d'authentification des utilisateurs et des processus automatiques de leurs systèmes d'information ;* *2. Des processus de gestion des droits permettant notamment l'attribution des droits d'accès aux ressources en fonction du besoin opérationnel des utilisateurs et des processus automatiques, la révocation des droits en cas de changement d'affectation des utilisateurs et la désactivation du compte utilisateur en cas de départ de l'entité.*	**Il s'agit d'une synergie :** - A condtion de mettre ces listes à jour et de limiter le nombre d'utilisateurs au strict nécessaire ; - Cet objectif permet également une réduction des risques de cyberattaques, qui auraient un impact environnemental certain. Un point de vigilance est toutefois à mettre en exergue (pour raison cyber et environnement). Il convient de ne pas mutliplier les systèmes d'authentification et de préférer un système mutualisé et maîtrisé.	Synergie
11. Maîtrise de l'administration des systèmes d'information	*Les entités [importantes ou essentielles], ou toute personne qu'elles ont mandatée pour réaliser les activités d'administration, disposent de comptes d'administration exclusivement dédiés à cet usage et utilisés par les seules personnes autorisées.* *Les entités [essentielles] s'assurent de la sécurisation de l'administration de leurs annuaires en s'appuyant sur les recommandations de l'autorité nationale de sécurité des systèmes d'information.*	**Il s'agit d'une synergie :** - A condtion de mettre ces listes à jour et de limiter le nombre d'utilisateurs au strict nécessaire ; - L'objectif limite les droits d'installation de composants qui consommeraient des ressources et pourraient engendrer des réductions de performance et une obsolescence prématurée.	Synergie
12. Identification et réaction aux incidents de sécurité	*Les entités [importantes ou essentielles] mettent en œuvre une organisation, des processus et des outils adaptés pour se préparer et réagir à des événements de sécurité susceptibles d'affecter la réalisation de leurs activités ou la fourniture de leurs services.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - Un état de crise coûte très cher et a des impacts environnementaux certains, mais nécessite des moyens spécifiques (ex : cellule de crise dédiée, avec une salle et des équipements informatiques).	Synergie et divergence
13. Continuité et reprise d'activité	*Les entités [importantes ou essentielles] mettent en œuvre des mécanismes de sauvegarde et de restauration des informations nécessaires à leurs activités ou services, opérationnels et les testent au minimum une fois par an.* *Les entités [essentielles] définissent et maintiennent à jour des plans de continuité et de reprise d'activité adaptés aux besoins de leurs activités et de la fourniture de leurs services.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - La continuité est envisagée avec une disponibilité d'outils réduite (cf : crise dans les hopitaux / retour papier). - Il incite également à travailler un DRP (Disaster Recovery Plan) et avoir une approche plus long-termiste. - En revanche, il oblige à avoir deux systèmes en parallèle ce qui multiplie les coûts envrionnementaux. - Les plans de continuité et de reprise d'activité doivent exister même en dehors de la cybersécurité, pour les grands groupes et en particulier les OIV. Cet objectif doit générer des questionnements sur la résilience, ou la robustesse, de l'organisation.	Synergie et divergence
14. Réaction aux crises d'origine cyber	*Les entités [importantes ou essentielles] mettent en œuvre une organisation, des processus et des outils adaptés pour se préparer et réagir à des crises d'origine cyber et tiennent ces informations à la disposition des autorités nationales compétentes et en particulier de l'autorité nationale de sécurité des systèmes d'information.* *Les [entités essentielles] mettent en œuvre des retours d'expérience permettant d'identifier les axes d'amélioration et les mesures associées à mettre en œuvre suite à un entraînement, un exercice ou une crise réelle.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - L'objectif oblige à avoir des cellules de gestion de crise qui anticipent les risques et sont aptes à y répondre ; - Un état de crise coûte très cher et a des impacts environnementaux certains, mais nécessite des moyens spécifiques (ex : cellule de crise dédiée, avec une salle et des équipements informatiques).	Synergie et divergence
15. Exercices, tests et entrainements	*Les entités [importantes ou essentielles] réalisent des exercices, tests et entraînements à intervalles réguliers pour vérifier la capacité de leur organisation, de leurs processus, de leurs outils et de leur préparation à faire face aux incidents de sécurité et aux crises d'origine cyber.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - Cet objectif génère des impacts environnementaux, mais ne pas le déployer expose à des risques dont l'impact environnemental serait supérieur ; - L'étude de cas réels permet d'identifier les moyens qui sont réellement utilisés et ceux qui ne le sont pas. Il s'agit d'une synergie sur la logique de démarche d'amélioration continue, nourrie par le retour d'expérience.	Synergie et divergence
Objectifs de sécurité applicables aux entités essentielles			
16. L'entité essentielle met en œuvre une approche par les risques	*Les entités [essentielles] mettent en œuvre une approche par les risques placée sous la responsabilité du dirigeant exécutif et leur permettant :* *1. de prendre connaissance et de suivre l'évolution des risques pesant sur leurs systèmes d'information ;* *2. de définir et suivre la mise en œuvre des mesures de sécurité pour maîtriser ces risques ;* *3. d'accepter les risques résiduels.*	**Il s'agit d'une synergie :** - L'objectif favorise une approche construite au juste besoin de séurité ; ceci limite les coûts et la mise en œuvre de moyens qui auraient un fort impact environnemental. - Les standards environnementaux ISO 14001 imposent de s'interfacer avec les systèmes de gestion des risques de l'organisation. Une approche commune est donc une opportunité d'échange et de partage des points de vue. - Des risques environnementaux, liés à l'adapatation (limitation des ressources en eau, en électricité, risques thermiques, risques de catastrophes naturelles), sont à anticiper car pouvant occasionner des interruptions de services. Des solutions peuvent être anticipées.	Synergie
17. Audit de la sécurité des systèmes d'information	*Les entités [essentielles] réalisent ou font réaliser à intervalles planifiés des audits de sécurité de leurs systèmes d'information.* *Ces audits doivent permettre de vérifier l'atteinte des objectifs [de sécurité] et d'évaluer le niveau de sécurité de leurs systèmes d'information.*	**Il s'agit d'une synergie :** - la démarche est comparable à l'amélioration continue dans les Systèmes de Management Environnementaux (SME) certifiés ISO 14001. Par exemple : les audits permettant de vérifier l'avancement des améliorations à apporter constatées lors de revues préscédentes, ou que les objectifs définis dans la politique sont atteints, sont des démarches similaires. - Le préventif a un coût environnemental, mais qui reste moindre par rapport au curatif en cas d'interruption des services.	Synergie
18. Sécurisation de la configuration des ressources des systèmes d'information	*Les entités [essentielles] s'assurent que seules les ressources logicielles nécessaires à la réalisation de leurs activités et la fourniture de leurs services ou au maintien en condition opérationnelle ou de sécurité sont installées ou conservées sur leurs systèmes d'information et configurent les ressources de leurs systèmes d'information de manière sécurisée en s'appuyant sur les recommandations de l'autorité nationale de sécurité des systèmes d'information, de l'éditeur de la fonctionnalité ou du fabricant de la ressource..*	**Il s'agit d'une synergie majeure :** - Cet objectif présente une opportunité de promouvoir des pratiques ambitieuses, avec des supports sur le long terme (10 ans ou plus ; cf. open source et systèmes d'exploitations durcis) ; - En appliquant un principe de minimisation, on réduit les consommations. Il s'agit d'une opportunité de maintenir des systèmes très sécurisés avec un impact faible, de réduire considérablement les impacts qu'induiraient des attaques réussies.	Synergie
19. Administration des systèmes d'information depuis des ressources dédiées	*Les entités [essentielles] mettent en place pour l'administration de leurs systèmes d'information :* *1° des postes d'administrations maîtrisés par l'entité ou toute personne qu'elle a mandatée pour réaliser cette activité et qui sont conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information ;* *2° une sécurisation et un cloisonnement des flux dédiés à cette activité, qui s'appuient sur les recommandations de l'autorité nationale de sécurité des systèmes d'information.*	**Il s'agit d'une synergie avec divergences potentielles :** - La mise en place de ressources dédiées génère des impacts environnementaux. Par exemple les employés d'ESN peuvent avoir un poste bureautique dédié pour chacun de leurs clients (avec des matérisations différentes), mais il existe des moyens pour éviter cette multiplication de PC (solutions déployés au sein de CS group par exemple). - Il existe aussi des synergies sur le fait que certains de ces outils sont indispensables à une démarche numérique responsable. Par exemple, avoir une CMDB à jour, des outils d'observabilité pour connaitre les ressources physiques dédiées à un service (vCPU, vRAM). Les logs peuvent être aussi très utiles pour identifier le nombre d'utilisateurs réels et le comparer à ceux déclarés.	Synergie et risque de divergence
20. Supervision de la sécurité des systèmes d'information	*Les entités [essentielles] :* *1° s'assurent que les équipes en charge de l'activité de supervision de sécurité dimensionnent et opèrent le système d'information supportant l'activité de supervision de sécurité en adéquation avec leur capacité opérationnelle, afin de prendre en compte les journaux et les événements de sécurité, sans retard injustifié et au maximum sous 24h ouvrés.* *2° élaborent et mettent en œuvre une démarche d'amélioration continue de leur activité de supervision de sécurité, afin d'améliorer la couverture des scénarios de menaces identifiés à l'occasion de l'analyse de risque prévue à l'[objectif de sécurité 16] du présent décret, et l'efficacité de la supervision de sécurité ;* *3° s'assurent que les événements de sécurité et les journaux sont conservés pour une durée d'au moins trois mois sans préjudice d'autres obligations légales et réglementaires.*	**Il s'agit à la fois d'une synergie et d'une divergence :** - Ne pas avoir de SOC / de système de supervision représente un risque de coûts environnementaux largement supérieurs en cas de cybermalveilleance. - Les logs occpuent des espaces mémoires significatifs, mais ils sont aussi des outils d'observabilité très utiles (ex : ils permettent de connaitre le nombre réel d'utilisateur, via l'authentification. Ils peuvent aussi être une source d'évaluation des ressources physiques utilisées. - Un point de vigilance est à mentionner : il s'agit de définir une durée de vie des logs et filtrer les évènements significatifs qui méritent d'être enregistrés.	Synergie et divergence