RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2 – TRANSPOSITION NATIONALE

MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSECURITÉ

RECYF :

RÉFÉRENTIEL CYBER FRANCE

(ReCyf)

Version ~~2.~~42.5

VERSION DE TRAVAIL

TABLE DES MATIERES

PRESENTATION DU DOCUMENT

RECYF constitue le référentiel de cybersécurité mentionné au 6ème alinéa de l'article 14 du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (PJL). Il se compose d'objectifs de sécurité et, pour chacun d'eux, de moyens acceptables de conformité.

L'objectif de sécurité est l'obligation fixée par le décret pris en application de l'article 14 du PJL à laquelle doit se conformer l'entité.

- Il répond à la question « Quoi ? ».
- Son atteinte est **obligatoire**.
- Par défaut, les objectifs sont applicables aux entités importantes (EI), entités essentielles (EE) et aux opérateurs d'importance vitale sur leurs SI autres que leurs SIIV.
- En application du principe de proportionnalité, les objectifs 16 à 20 ne sont applicables qu'aux EE.

Les Moyens acceptables de conformité sont les mesures à mettre en œuvre proposées par l'ANSSI aux assujettis pour atteindre l'objectif.

- Ils répondent à la question « Comment ?».
- Ces moyens acceptables de conformité ne sont pas d'application obligatoire (sauf cas particuliers prévus à l'article 16 du PJL) mais permettent aux entités qui décideraient de les appliquer de pouvoir se prévaloir de leur mise en œuvre pour démontrer leur atteinte des objectifs de sécurité.
- En application du principe de proportionnalité, il est précisé pour chaque Moyen acceptable de conformité s'il concerne les EE et/ou les EI.

Ce référentiel précise les modalités selon lesquelles les entités importantes et essentielles peuvent se prévaloir auprès de l'autorité nationale de sécurité des systèmes d'information lors d'un contrôle du recours à des prestations qualifiées par l'Agence nationale de la sécurité des systèmes d'information ou à une certification à des normes internationales ou européennes précisées par l'autorité nationale de sécurité des systèmes d'information pour démontrer leur respect de tout ou partie d'un objectif de sécurité.

Enfin, des annexes détaillent les justifications associées à la mise en œuvre de chaque objectif au regard des risques associés et les correspondances entre ces objectifs et les dispositions pertinentes de la directive NIS2. Ces informations sont communiquées uniquement à des fins pédagogiques.

GLOSSAIRE

Mot	Définition
Action d'administration	Installation, suppression, modification ou consultation d'une configuration d'une ressource d'un système d'information susceptible de modifier le fonctionnement ou la sécurité de celui-ci.
Administrateur	Personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration ou de maintenance sur celui-ci, responsable d'un ou plusieurs domaines techniques.
Annuaire	Ressource logicielle centralisant des informations relatives aux utilisateurs, et parfois aux autres ressources d'un système d'information et fournissant des mécanismes d'identification et d'authentification. *Par exemple : MICROSOFT ACTIVE DIRECTORY, OPENLDAP.*
Authentification ~~multifacteurs~~multifacteur	Authentification mettant en œuvre plusieurs facteurs d'authentification ~~parmi les suivants~~appartenant à au moins deux des trois catégories suivantes : • Facteur de connaissance (*par exemple : un mot de passe*) ; • Facteur de possession (*par exemple : une application mobile*) ; • Facteur inhérent (*par exemple : l'empreinte digitale*).
Capacité opérationnelle	Ensemble des processus, ressources et outils disponibles pour permettre d'atteindre un objectif précis.
Code malveillant	Tout ou partie d'un programme ou d'un fichier permettant d'utiliser une ou plusieurs vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.
Cœur de confiance	Ensemble des ressources regroupant les annuaires, les ressources hébergeant ces annuaires ou permettant d'en prendre le contrôle.
Compte d'administration	Compte disposant de privilèges nécessaires aux actions d'administration. Il peut être partagé, individuel ou de service.
Dispositif de détection	Ensemble de ressources matérielles ou logicielles capables d'identifier des indicateurs de compromission et techniques d'attaques, sur des données brutes réseau ou système, pour générer des évènements de sécurité. *Par exemple : sondes réseau, solutions EDR.*
Durée maximale d'interruption admissible (DMIA)	Temps nécessaire pour que les impacts défavorables pouvant résulter de la non-~~/~~livraison ou fourniture d'un produit~~/~~ ou service ou de la non-réalisation d'une activité deviennent inacceptables. *En anglais: maximum tolerable period of disruption (MTPD)* *Source : ISO 22300:2025, 3.[illegible]*
Événement de sécurité	Occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une violation possible de la politique de sécurité des systèmes d'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité de l'information. *Source : ISO/IEC [illegible]000:2018, 3.30*

Mot	Définition
Facteur d'authentification	Élément utilisé pour réaliser l'authentification d'un utilisateur ou d'un processus automatique, sur la base d'une information mémorisée (facteur de connaissance), d'un élément physique stockant un secret (facteur de possession) ou d'une caractéristique liée à une personne (facteur inhérent).
Incident de sécurité	Événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles.
Indicateur de compromission	Combinaison d'informations techniques et contextuelles représentatives d'une manifestation ou d'une tentative de compromission, dont la présence peut être identifiée à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.
Information sensible	Les données à caractère personnel « sensibles » au sens du 1 de l'article 9 du Règlement (UE) 2016/679, les données d'une sensibilité particulière au titre de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, les données protégées au titre de l'article L. 151-1 du code de commerce ainsi que les données protégées au titre de la protection du patrimoine scientifique et technologique de la nation
Interconnexion	Ressource logicielle ou matérielle rendant possible le transfert d'information entre deux systèmes d'information ou entre deux sous-systèmes par une continuité de signaux électromagnétiques (*par exemple : câble réseau, diode optique*).
Mécanisme d'authentification	Mécanisme permettant d'authentifier un utilisateur ou un processus automatique préalablement à l'accès aux ressources des systèmes d'information. Ce mécanisme s'appuie au minimum sur un facteur d'authentification et peut mettre en œuvre une authentification ~~multifacteurs.~~multifacteur.
~~Perte~~Point de rétablissement de données ~~maximale admissible (PDMA~~(PRD)	Point à partir duquel les informations et données utilisées par une activité ~~ou un service doivent être~~sont restaurées afin de permettre ~~son~~un fonctionnement ~~à la~~en reprise. *En anglais: Recovery point objective (RPO)* *Source : ISO 22300:2025, 3.1.57*
Règle de filtrage	Instruction implémentée au sein d'un dispositif de filtrage (*par exemple : un pare-feu*) visant à autoriser ou interdire les flux de données en fonction : • De l'adresse IP source ou destination ; • Du protocole utilisé par le flux de données (*par exemple : TCP ou UDP*) ; • Des numéros de port source ou destination (*par exemple : TCP/23*) • De l'applicatif.
Réseau	Ensemble de ressources interconnectées permettant de communiquer au sein d'un ou plusieurs systèmes d'information
Réseau d'administration	Réseau dédié physiquement ou logiquement aux flux internes à ce réseau et les flux d'administration vers les systèmes d'information
Sécurité numérique	Actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces. (Article 2 1. du règlement 2019/881)

Mot	Définition
Sous-système	Ensemble de composants d'un système d'informations constitués pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un système d'information ou encore pour isoler des ressources d'un système d'information ayant un même besoin de sécurité.
Système d'analyse	Système d'information exploitant les événements de sécurité à la recherche d'indicateurs de compromission et de techniques d'attaques, dans le but d'identifier des incidents de sécurité.
Système d'information	Ensemble des infrastructures et services logiciels informatiques relevant de la responsabilité de l'entité, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données. Les ressources informatiques partagées ou mutualisées avec des tiers relevant du périmètre de responsabilité de l'entité, sont considérées comme faisant partie intégrante des systèmes d'information de l'entité et sont à ce titre pleinement assujetties aux obligations de la directive NIS 2.
Système d'information d'infrastructure	Système d'information généraliste utile aux activités ou aux services de l'entité, ou nécessaire au fonctionnement de plusieurs systèmes d'information de l'entité. *Par exemple : annuaire, messagerie, téléphonie, service de résolution de nom de domaine.* Un système d'information d'infrastructure peut être un système d'information.
Systèmes d'information tiers	Système d'information ou ressource informatique partagée ou mutualisée avec l'entité qui n'est pas sous la responsabilité de l'entité. *Point d'attention : lorsque l'entité externalise tout ou partie de son système d'information, ce dernier reste sous sa responsabilité. et n'est donc considéré comme un SI tiers au sens du présent référentiel.*
Utilisateur	Personnels de l'entité et prestataires agissant pour le compte de l'entité qui accèdent aux systèmes d'information.

OBJECTIFS DE SECURITE APPLICABLES AUX ENTITÉS IMPORTANTES ET ESSENTIELLES

GOUVERNANCE DES SYSTÈMES D'INFORMATION

OBJECTIF DE SÉCURITÉ 1. RECENSEMENT DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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 ;
1.2. La divulgation à des personnes non autorisées d'informations sensibles traitées par les activités ou services de l'entité ;
2.3. 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.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
1.1-EI/EE	L'entité liste l'ensemble de ses activités et services, y compris les activités et services qui ne correspondent pas aux critères pour lesquels l'entité ~~est devenue~~constitue une entité importante ou essentielle (*par exemple : une entité essentielle au titre d'une activité exploitation d'un oléoduc ~~liste~~doit lister, en plus des activités et services participant à l'exploitation de l'oléoduc, tous les services et les autres activités ~~et services~~ qu'elle fournit*). Pour chaque entrée de cette liste, l'entité : ○ identifie un responsable de l'activité ou du service (*par exemple le chef de service auquel est rattachée l'activité ou le service, un directeur métier, la direction générale~~, etc~~*) ; ○ liste les systèmes d'information les supportant.	Oui	Oui
1.2-EI/EE	L'entité précise dans la liste prévue au 1.1-EI/EE les systèmes d'information qui ne sont exposés à aucun des risques mentionnés à l'alinéa 2 de l'objectif de sécurité. L'entité renseigne les justifications de ces choix.	Oui	Oui
1.3-EI/EE	L'entité valide et réexamine annuellement~~, ou en~~ la liste prévue au 1.1-EI/EE, et en tant que de besoin, notamment en cas d'évolution des activités et services de l'entité ou en cas de mise en service d'un nouveau système d'information~~, la liste prévue au (a).~~	Oui	Oui

OBJECTIF DE SÉCURITÉ 2. MISE EN OEUVRE D'UN CADRE DE GOUVERNANCE DE LA SÉCURITÉ NUMÉRIQUE

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

Les entités [importantes et essentielles] :

- réalisent une analyse de leur conformité vis-à-vis des dispositions [pointer vers les dispositions du décret correspondant aux objectifs de sécurité],
- identifient les éventuels écarts existants par rapport aux objectifs de sécurité et,
- établissent et suivent dans la durée un plan d'action pour corriger chacun de ces écarts dans les meilleurs délais. Ce plan d'action est adapté à la structure de l'entité et à son environnement.

La responsabilité de ce plan d'action est déterminée au regard du cadre de gouvernance de la sécurité numérique mis en place.

Les entités essentielles établissent ce plan d'action en tenant compte de l'analyse de risques qu'elles sont tenues de réaliser en application de [l'objectif 16].

Ce plan d'action ne préjuge pas de l'appréciation du respect de ses obligations légales et règlementaires lors d'un contrôle par l'ANSSI.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~La~~Les entités importantes et essentielles peuvent se prévaloir lors d'un contrôle de la mise en place d'un système de management de la sécurité de l'information (SMSI) certifié conforme aux exigences prévues dans la norme ISO/CEI 27001:2022 ~~permet d'apporter une présomption~~pour démontrer le respect de ~~conformité à~~ cet objectif ~~pour~~sur les systèmes d'information couverts par la certification.

RÔLES ET RESPONSABILITÉS

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
2.A.1-EI/EE	Le dirigeant exécutif de l'entité est responsable de la sécurité numérique au sein de son entité et en particulier du suivi de la conformité des systèmes d'information aux présentes mesures.	Oui	Oui

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
2.A.2-EE	Il désigne au moins une personne qui le conseille et l'accompagne dans l'exercice de cette responsabilité. Cette personne est le point de contact privilégié de l'Agence nationale de la sécurité des systèmes d'information pour tous les sujets relatifs à la sécurité numérique (*notamment incidents de sécurité, communications de l'ANSSI sur les sujets relatifs aux entités essentielles*)	**Non**	Oui
2.A.3-EI/EE	L'entité définit et met en œuvre une organisation adaptée pour assurer sa sécurité numérique (*par exemple : la désignation d'un responsable de la sécurité numérique, l'établissement d'un RACI, la mise en place d'une comitologie*).	Oui	Oui

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
2.B.1-EI/EE	L'entité définit et met en œuvre une politique de sécurité des systèmes d'information (PSSI).	Oui	Oui
2.B.2-EI/EE	Cette PSSI comprend au moins : • L'organisation de la gouvernance de la sécurité numérique et notamment les rôles et les responsabilités du personnel interne et externe (*par exemple : prestataires, fournisseurs*) ; • Les orientations et objectifs stratégiques en matière de sécurité numérique déclinés de la stratégie globale de l'entité ; • L'engagement du dirigeant exécutif de l'entité à assurer la sécurité numérique des systèmes d'information dont il est responsable ; • L'engagement du dirigeant exécutif de l'entité à respecter les exigences légales et réglementaires et en particulier celles définies dans la transposition nationale de la directive NIS 2. • La PSSI tient également compte des exigences, procédures et spécificités propres au(x) secteur(s) dans lesquels l'entité exerce ses activités.	Oui	Oui
2.B.3-EI/EE	Le dirigeant exécutif de l'entité approuve la PSSI.	Oui	Oui
2.B.4-EI/EE	La PSSI est ~~à minima~~au minimum revue annuellement et mise à jour lorsque nécessaire, notamment en cas d'évolutions majeures de la menace, du contexte métier, technique ou organisationnel intervenues après son approbation.	Oui	Oui
2.B.5-EI/EE	L'entité décline, en tant que de besoin, la PSSI en politiques de sécurité relatives à des thèmes précis ~~et~~ permettant de couvrir tout ou partie des présentes mesures. En particulier, l'entité définit et met en œuvre, au minimum, des politiques de sécurité en matière : • D'usage du chiffrement ; • De contrôle d'accès physique et logique ; • De revue de l'application des mesures de sécurité mises en œuvre ; • De gestion des comptes.	Oui	Oui

GESTION DE LA CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
2.C.1-EI/EE	Pour chaque système d'information, l'entité réalise et maintient à jour une analyse de la conformité du système d'information vis-à-vis des ~~présentes~~ mesures du présent référentiel. L'analyse de la conformité identifie les éventuels écarts entre les mesures mises en œuvre par l'entité~~,~~ et les ~~présentes~~ mesures ~~et les objectifs fixés par~~prévues dans le présent référentiel. Cette analyse tient compte de la ~~réglementation~~PSSI de l'entité.	Oui	Oui
2.C.2-EI/EE	L'entité établit, met en œuvre et suit dans la durée un plan d'action ~~pour~~ adapté à la structure et à l'environnement dans lequel elle opère afin de corriger ces écarts ~~et atteindre~~dans les ~~objectifs fixés par la réglementation~~meilleurs délais. La responsabilité de ce plan d'action est déterminée au regard du cadre de gouvernance de la sécurité numérique mis en place. Ce plan d'action prévoit, au minimum, une échéance raisonnable au regard du besoin de sécurisation du système d'information et un responsable pour la réalisation de chaque action. Ce plan d'action ne préjuge pas de l'appréciation du respect de ses obligations légales et réglementaires lors d'un contrôle de l'ANSSI.	Oui	Oui
2.C.3-EI/EE	~~En cas de recours à une ou plusieurs alternatives prévues dans les présent référentiel, l'entité les renseigne dans l'analyse de la conformité avec les justifications associées.~~Lorsque l'entité n'est pas tenue de mettre en œuvre le référentiel mais qu'elle décide de l'appliquer pour démontrer sa conformité aux objectifs de sécurité, et qu'elle applique une ou plusieurs mesures alternatives aux moyens acceptables de conformité du référentiel, elle en précise les justifications dans son analyse de la conformité. L'ANSSI peut apprécier la pertinence de la mesure retenue pour satisfaire la mesure du référentiel non retenue lors d'un contrôle.	Oui	Oui

OBJECTIF DE SÉCURITÉ 3. MAÎTRISE DE L'ÉCOSYSTÈME

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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~~de droit ou de fait ainsi que le périmètre et la nature de la prestation ou du service fourni.

~~Ces~~Les entités [importantes ou essentielles] mettent en place des processus visant à s'assurer, notamment par la voie contractuelle~~, que leurs prestataires et fournisseurs~~ de la conformité des prestations informatiques ~~leur permettent de satisfaire à leurs~~dont elles bénéficient aux obligations ~~résultantes~~auxquelles l'entité est assujettie notamment en matière de ~~l'article 14~~gestion des risques qui menacent la sécurité de leurs réseaux et systèmes d'information et ~~du premier alinéa de l'article 17 [du PJL].~~de notification des incidents importants.

MOYENS ACCEPTABLES DE CONFORMITÉ

CARTOGRAPHIE DE L'ÉCOSYSTÈME

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
3.A.1-EI/EE	L'entité définit et maintient à jour une cartographie de l'écosystème dans lequel ses systèmes d'information sont mis en œuvre et contenant, au minimum, les informations suivantes : • La liste des prestataires et fournisseurs informatiques contribuant à la réalisation des activités ou des services de l'entité et avec lesquels il existe une relation ~~contractuelle~~de droit ou de fait (*par exemple : prestataire d'infogérance, matériels et services fournis par la maison mère à une filiale, fournisseur de matériel informatique)* • La liste des interconnexions avec les systèmes d'information de l'entité. (*Cette liste peut s'appuyer sur les démarches déjà réalisées par l'entité pour réaliser une telle liste. Par exemple, la déclaration de sous-traitance réalisée dans le cadre d'un contrat de la commande publique*).	Oui	Oui
3.A.2-EI/EE	L'entité renseigne et maintient à jour les coordonnées d'au moins un point de contact pour chaque entrée figurant dans la cartographie de l'écosystème.	Oui	Oui

SÉCURITÉ NUMÉRIQUE DANS LES CONTRATS AVEC LES PRESTATAIRES ET FOURNISSEURS INFORMATIQUES

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
3.B.1-EI/EE	En cas de recours à un prestataire ou à un fournisseur informatique, l'entité s'assure que ~~-~~la prestation ~~lui permet de satisfaire à ses~~est conforme aux obligations ~~légales~~auxquelles l'entité est assujettie, notamment en matière de gestion des risques qui menacent la sécurité de leurs réseaux et systèmes d'information et de notification des incidents importants et s'assure de disposer des assurances contractuelles de cette conformité (*par exemple : plan d'assurance sécurité, charte de télémaintenance, mise en place d'indicateurs de suivi de la conformité).*	Oui	Oui

3.B.2-EI/EE	L'entité vérifie périodiquement ~~que~~ la conformité de la prestation ~~lui permet de satisfaire à ses~~aux obligations ~~légales~~auxquelles l'entité est assujettie notamment en matière de gestion des risques qui menacent la sécurité de leurs réseaux et systèmes d'information et de notification des incidents importants. L'entité peut s'appuyer sur des audits dont les conditions sont précisées par les Moyens acceptables de conformité 17.2-EE, 17.4-EE et 17.5-EE relatifs à l'audit.	Oui	Oui

OBJECTIF DE SÉCURITÉ 4. INTÉGRATION DE LA SÉCURITÉ NUMÉRIQUE DANS LA GESTION DES RESSOURCES HUMAINES

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

Les entités [importantes ou essentielles] ~~intègrent la sécurité numérique dans la gestion de leurs ressources humaines en sensibilisant~~définissent les procédures visant à sensibiliser leurs utilisateurs, en particulier les dirigeants de l'entité, ~~et en formant~~ à la sécurité numérique ainsi qu'à former les personnes occupant des fonctions à responsabilités dans le domaine du numérique.

Ces entités ~~prennent en compte~~intègrent la sécurité numérique dans la gestion de leurs ressources humaines dès l'arrivée d'un nouveau personnel ~~et~~ jusqu'à son départ de l'entité.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
4.1-EI/EE	L'entité définit et met en œuvre une charte d'usage des systèmes d'information, et la rend opposable à chacun des utilisateurs de ces systèmes d'information. Cette charte peut prévoir des dispositions spécifiques pour les administrateurs. Cette charte peut également couvrir les systèmes d'information pour lesquels l'entité a décidé de ne pas appliquer les objectifs de sécurité.	Oui	Oui
4.2-EI/EE	L'entité définit et met en œuvre un programme de sensibilisation à la sécurité numérique de l'ensemble des utilisateurs. Ce programme doit comporter des actions tout au long de la présence des utilisateurs dans l'entité.	Oui	Oui
4.3-EE	L'entité prévoit des clauses de sécurité dans ~~les~~ses contrats de travail (*par exemple : clauses de confidentialité de nature à garantir la confidentialité des informations auxquelles les salariés ont accès au cours de leur contrat et à l'issu de celui-ci*).	**Non**	Oui
4.4-EI/EE	L'entité définit et met en œuvre un processus de gestion des arrivées, des départs et des changements de fonction des personnels et des tiers accédant aux systèmes d'information. Ce processus prévoit : • La prise de connaissance ~~par le personnel~~ des règles de sécurité en vigueur lors de ~~son~~leur arrivée ; • L'attribution des accès appropriés lors de ~~l'arrivée d'un personnel ;~~ leur arrivée ; • La mise à jour des accès lors d'un changement de fonction ; • Lors du départ ~~d'un personnel~~, la restitution de l'ensemble du matériel qui ~~lui~~ a été mis à disposition et la désactivation de l'ensemble ~~de ses~~des accès logiques aux systèmes d'information et physiques aux locaux et salles.	Oui	Oui
4.5-EI/EE	L'entité définit et met en œuvre, pour les fonctions assumant des responsabilités dans le domaine du numérique, un programme de formations dédiées à la sécurité numérique adapté à leurs responsabilités.	Oui	Oui

OBJECTIF DE SÉCURITÉ 5. MAÎTRISE DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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 ; et

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

CARTOGRAPHIE DES SYSTÈMES D'INFORMATION

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
5.A.1-EI/EE	L'entité élabore et maintient à jour au moins une cartographie de ses systèmes d'information dont le niveau de détail est suffisant pour lui permettre : ○ d'assurer le maintien en condition opérationnelles et de sécurité de ces systèmes (*par exemple : être capable d'identifier les ressources matérielles ou logicielles vulnérables suite à la publication d'un bulletin d'alerte*) ; ○ de pouvoir réagir sans retard injustifié à un incident de sécurité affectant ces systèmes d'information (*par exemple : être capable d'identifier les ressources matérielles ou logicielles affectées par un incident de sécurité et ainsi limiter les conséquences de l'incident*). Cette cartographie peut s'appuyer sur les recommandations de l'autorité nationale de sécurité des systèmes d'information en matière de cartographie.	Oui	Oui

MAINTIEN EN CONDITION OPÉRATIONNELLE ET DE SÉCURITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
5.B.1-EE	L'entité élabore, met en œuvre et maintient à jour une procédure de maintien en conditions opérationnelle et de sécurité des ressources matérielles et logicielles de ses systèmes d'information.	**Non**	Oui
5.B.2-EI/EE	L'entité maintient à jour les bases de connaissances des outils de protection contre les codes malveillants qu'elle utilise (*par exemple : la mise à jour de la base antivirale de l'antivirus, la mise à jour des signatures utilisées par la solution d'EDR*[1]).	Oui	Oui
5.B.3-EI/EE	L'entité met en œuvre une veille sur les vulnérabilités, les correctifs de sécurité et ~~des~~les mesures d'atténuation préconisées susceptibles de concerner les ressources de ses systèmes d'information, qui sont diffusées notamment par les fournisseurs ou les fabricants de ces ressources, par un prestataire mandaté ou par des centres de prévention et d'alerte en	Oui	Oui

[1] *Endpoint Detection and Response*

	matière de cyber sécurité tels que le CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) ou les CSIRT (centres de réponse aux incidents de sécurité informatique).		
5.B.4-EI/EE	L'entité met en œuvre, au regard de la nature de la vulnérabilité : • sans délai : les actions visant à l'installation~~, sans retard injustifié au regard de la nature de la vulnérabilité,~~ des correctifs de sécurité (*par exemple : le déploiement en environnement de test, ~~préprod~~pré-production et ~~prod~~production, mécanismes de rollback*)~~ ;~~ • sans retard injustifié : l'application effective des correctifs de sécurité après la réalisation des actions précédentes sur les ressources exposées à des systèmes d'information tiers (*par exemple : un serveur Web, un pare-feu exposé sur Internet, un serveur de messagerie*) et les postes de travail des utilisateurs.	Oui	Oui
5.B.5-EE	L'entité ~~essentielle~~ planifie et installe sur l'ensemble de ses ressources, y compris celles non exposées à des systèmes d'information tiers, les correctifs de sécurité.	**Non**	Oui
5.B.6-EI/EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas l'installation des correctifs de sécurité sur les ressources concernées, l'entité met en œuvre des mesures d'atténuation pour réduire les risques liés à l'utilisation d'une version comportant des vulnérabilités connues~~.~~ (*par exemple : isoler la ressource du reste du SI, mettre en place un contrôle d'accès renforcé*).	Oui	Oui
5.B.7-EI/EE	L'entité met en œuvre sans délai les actions visant à l'installation et le maintien à jour des ressources logicielles de ses systèmes d'information, y compris les logiciels embarqués, dans des versions bénéficiant d'un support par leurs fournisseurs ou leurs fabricants et comportant les mises à jour de sécurité.	Oui	Oui
5.B.8-EI/EE	L'entité vérifie que toute nouvelle version d'un logiciel est téléchargée depuis les ressources officielles mises à disposition par les éditeurs ou les fournisseurs.	Oui	Oui
5.B.9-EI/EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas l'installation d'une version supportée par le fournisseur ou l'éditeur, l'entité met en œuvre des mesures pour réduire les risques liés à l'utilisation d'une version obsolète.	Oui	Oui
~~*MCO_MCS.j*~~	~~L'entité définit et met en œuvre des mécanismes permettant de prendre connaissance, sans retard injustifié, des alertes émises par l'autorité nationale de sécurité des systèmes d'information, les éditeurs de produits utilisés par l'entité ou le prestataire mandaté par l'entité.~~	~~Oui~~	~~Oui~~
~~*MCO_MCS.k*~~	~~L'entité s'assure de la mise en œuvre d'une procédure pour traiter ces alertes et le cas échéant appliquer, sans retard injustifié, les mesures préconisées.~~	~~Oui~~	~~Oui~~

OBJECTIF DE SÉCURITÉ 6. MAÎTRISE DES ACCÈS PHYSIQUES AUX LOCAUX

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
6.1-EI/EE	L'entité met en place des mesures de sécurité permettant de limiter l'accès de personnes non autorisées à ses locaux, ses salles serveurs et ses locaux techniques (*par exemple : tenue d'un registre des visiteurs, badges d'accès, etc).*	Oui	Oui
6.2-EE	L'entité s'assure de la protection physique des locaux, salles serveurs et locaux techniques (*par exemple : vidéosurveillance, gardiennage, alarme*). Cette protection physique permet de prévenir, de surveiller et de réagir aux accès non autorisés à ces locaux.	**Non**	Oui
6.3-EE	L'entité s'assure que les droits d'accès physique sont attribués au regard du besoin strictement nécessaire à l'exécution des missions des personnes.	**Non**	Oui
6.4-EI/EE	L'entité s'assure que les personnes externes accédant aux locaux techniques et salles serveurs de l'entité sont accompagnées ou dûment autorisées.	Oui	Oui

OBJECTIF DE SÉCURITÉ 7. SÉCURISATION DE L'ARCHITECTURE DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF

Les entités [importantes ou essentielles] identifient les besoins d'exposition ~~et~~des services et interfaces de leurs systèmes d'information ainsi que les besoins 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~~communications entre ces zones de sécurité pour les utilisateurs, les prestataires et les fournisseurs.

MOYENS ACCEPTABLES DE CONFORMITÉ

CLOISONNEMENT

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
7.A.1-EI/EE	L'entité cloisonne physiquement et/ou logiquement l'ensemble de ses systèmes d'information vis-à-vis des autres systèmes d'information, y compris ~~les~~des systèmes d'information ~~sous sa responsabilité~~ pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité et les systèmes d'information tiers *(par exemple : cloisonnement logique par VLAN – réseau local virtuel - (réseau), par VM – machine virtuelle - (calcul) ou par volume (stockage))*.	Oui	Oui
7.A.2-EE	L'entité cloisonne physiquement et/ou logiquement chaque système d'information vis-à-vis des autres systèmes d'information, y compris ~~les~~des systèmes d'information ~~sous sa responsabilité~~ pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité et ~~les~~des systèmes d'information tiers (*par exemple : un système d'information est cloisonné logiquement des autres systèmes d'information de l'entité. Il est aussi cloisonné physiquement des systèmes d'information de l'entité pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité).*	**Non**	Oui
7.A.3-EE	L'entité mène des réflexions, pour chaque système d'information, sur la pertinence de définir des sous-systèmes. Lorsqu'elle n'identifie aucun sous-système, l'entité en apporte la justification. Un sous-système regroupe des ressources assurant des fonctionnalités similaires et ayant des niveaux de sensibilité, d'exposition et de sécurité homogènes.	**Non**	Oui
7.A.4-EE	Les sous-systèmes identifiés à la mesure 7.A.3-EE sont cloisonnés entre eux physiquement et/ou logiquement.	**Non**	Oui
7.A.5-EE	L'entité met en œuvre au moins un sous-système "passerelle sortante" permettant : • aux ressources de ses systèmes d'information d'accéder aux systèmes d'informations tiers ; • d'authentifier, de filtrer et de tracer les accès aux systèmes d'information tiers *(par exemple : un serveur mandataire)*.	**Non**	Oui
7.A.6-EE	L'entité met en œuvre au moins un sous-système "passerelle entrante" permettant : • d'exposer des ressources de ses systèmes d'information aux systèmes d'information tiers ;	**Non**	Oui

	• de filtrer et de tracer les accès depuis des systèmes d'information tiers *(par exemple : un serveur mandataire inverse ou un relai)*.		
7.A.7-EI/EE	Seules les interconnexions nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle ou de sécurité sont mises en œuvre entre l'ensemble des systèmes d'information et, d'une part les systèmes d'information tiers et, d'autre part les autres systèmes d'information sous la responsabilité de l'entité pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité ~~et les systèmes d'information tiers.~~.	Oui	Oui
7.A.8-EE	Seules les interconnexions nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle ou de sécurité sont mises en œuvre entre chaque système d'information et, d'une part les systèmes d'information tiers et, d'autre part les autres systèmes d'information sous la responsabilité de l'entité pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité ~~et les systèmes d'information tiers~~, ou entre les sous-systèmes du système d'information.	**Non**	Oui

FILTRAGE DES COMMUNICATIONS

		ATTENDU D'UNE EI	**ATTENDU D'UNE EE**
7.B.1-EI/EE	L'entité définit et documente les communications nécessaires : • à la réalisation de ses activités et services ; • au maintien en condition opérationnelle de sécurité circulant entre ~~l'ensemble des~~ les systèmes d'information et, d'une part les systèmes d'information tiers et, d'autre part les autres systèmes d'information ~~sous sa responsabilité~~ pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité ~~et les systèmes d'information tiers.~~ .	Oui	Oui
7.B.2-EE	L'entité définit et documente les communications nécessaires ~~:~~ ~~• à la réalisation de ses activités et services ;~~ au maintien en condition opérationnelle de sécurité circulant entre ~~chaque système d'information et les autres systèmes d'information sous sa responsabilité pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité et les systèmes d'information tiers ou entre~~ les sous-systèmes du système d'information.	**Non**	Oui
7.B.3-EI/EE	L'entité met en œuvre, au niveau des interconnexions, les règles de filtrage pour n'autoriser que les communications identifiées à la mesure 7.B.1-EI/EE ou 7.B.2-EE. Les autres communications sont bloquées par défaut.	Oui	Oui
7.B.4-EI/EE	~~Au~~L'entité filtre par un ou plusieurs pares-feux dédiés à cet usage, au minimum~~,~~ : • les communications entre les systèmes d'information de l'entité ~~et les autres systèmes d'information sous sa responsabilité~~ pour lesquels elle a décidé ~~de ne pas appliquer~~d'appliquer les objectifs ~~de sécurité~~ou non, d'une part ; et • les ~~systèmes d'information~~SI tiers ~~sont filtrés par un ou des pares-feux dédiés à cet usage~~d'autre part. *Par exemple : une entité mettant en œuvre un pare-feu pour filtrer les communications entre ses systèmes d'information (pour lesquels elle applique les objectifs de sécurité ou non) d'une part et les systèmes d'information tiers d'autre part est une solution acceptable.*	Oui	Oui
7.B.5-EI/EE	L'entité effectue annuellement une revue de la mise en œuvre technique des règles de filtrage mentionnées à la mesure 7.B.4-EI/EE.	Oui	Oui

OBJECTIF DE SÉCURITÉ 8. SÉCURISATION DES ACCÈS DISTANTS AUX SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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. Ces mécanismes sont conformes [~~aux exigences en matière d'identification (Objectif~~à l'Objectif de sécurité 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.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
8.1-EI/EE	L'entité protège les accès à ses systèmes d'information effectués à travers un système d'information tiers au moyen de mécanismes de chiffrement conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information *(par exemple : VPN TLS ou IPSec, protocoles applicatifs chiffrés comme TLS, SSH, etc.).*	Oui	Oui
8.2-EI/EE	~~De plus, lorsque~~Lorsque les accès visés à la mesure ~~(a)~~8.2-EI/EE sont effectués par ~~l'entité ou par toute personne~~les personnels et prestataires qu'elle a ~~autorisée~~autorisé, l'entité protège les accès aux systèmes d'information par un mécanisme d'authentification conforme aux mesures ~~de l'Objectif de sécurité 10.~~relatives à l'Authentification.	Oui	Oui
8.3-EE	Pour les accès visés à la mesure 8.2-EI/EE le mécanisme d'authentification est multifacteur et repose sur au moins un facteur de connaissance *(par exemple : authentification avec une carte à puce et un code PIN).*	**Non**	Oui
8.4-EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas la mise en œuvre d'une authentification ~~multifacteurs~~multifacteur, l'entité met en œuvre des mesures permettant de réduire le risque associé.	**Non**	Oui
8.5-EE	Les mémoires de masse (*par exemple : les « disques »*) des postes de travail et équipements mobiles permettant aux personnels et prestataires de l'entité d'accéder à distance aux systèmes d'information depuis un lieu qui n'est pas maîtrisé par l'entité, sont en permanence protégées par des mécanismes de chiffrement et d'authentification conformes à l'état de l'art tel que recommandé par l'autorité nationale de sécurité des systèmes d'information *(par exemple : disques chiffrés avec code PIN exigé pour le déchiffrement au démarrage).*	**Non**	Oui

OBJECTIF DE SÉCURITÉ 9. PROTECTION DES SYSTÈMES D'INFORMATION CONTRE LES CODES MALVEILLANTS

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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 ou dont elles ont confié la gestion et qui participent à la réalisation des activités ~~ou la fourniture de~~set services de l'entité ou au maintien en condition opérationnelle et de sécurité se connectent aux systèmes d'information.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
9.1-EI/EE	L'entité définit les ~~terminaux et~~ ressources matérielles ~~autorisés~~, en particulier les terminaux, autorisées à se connecter à ses systèmes d'information. *NB : Cette mesure autorise le AVEC (Apportez votre équipement de communication) ou BYOD en anglais.*	Oui	Oui
9.2-EE	Seules les ressources matérielles dont l'entité, ou le prestataire qu'elle a mandaté à cet effet, assure la gestion et qui participent à la réalisation des activités ou ~~à la fourniture~~ des services de l'entité ou au maintien en condition opérationnelle et de sécurité se connectent aux systèmes d'information. *NB : Cette mesure interdit le AVEC (Apportez votre équipement de communication) ou BYOD en anglais.*	**Non**	Oui
9.3-EI/EE	L'entité met en œuvre des mesures organisationnelles ou techniques visant à empêcher la connexion des ~~terminaux et des~~ ressources matérielles autres que celles identifiées à la mesure 9.1-EI/EE sur ses systèmes d'information.	Oui	Oui
9.4-EE	L'entité met en œuvre des mesures organisationnelles ou techniques visant à empêcher la connexion des ressources matérielles autres que celles identifiées à la mesure 9.2-EE sur ses systèmes d'information.	**Non**	Oui
9.5-EI/EE	Seuls les supports amovibles réinscriptibles nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle ou de sécurité se connectent à ses systèmes d'information~~.~~ *(par exemple : clefs USB ou disques dur amovibles).*	Oui	Oui
9.6-EI/EE	Les postes de travail, les serveurs et les équipements mobiles maîtrisés par l'entité, qui sont amenés à traiter de données provenant de sources externes (*par exemple les supports amovibles, la messagerie ou la navigation web*), à l'exception de données de mise à jour fournies par les éditeurs et dont l'authenticité et l'intégrité sont vérifiées, disposent de mécanismes de protection contre les risques d'exécution de codes malveillants (*par exemple : un antivirus ou un EDR).*	Oui	Oui
9.7-EI/EE	L'entité procède à l'analyse des données provenant de sources externes lors de leur réception, pour y rechercher des codes malveillants~~. (Par~~, à l'exception de données de mise à jour fournies par les éditeurs et dont l'authenticité et l'intégrité sont vérifiées *(par exemple : une passerelle mail analysant les pièces jointes avant distribution, un SAS de décontamination antivirale pour les clefs USB~~.)~~).*	Oui	Oui

OBJECTIF DE SÉCURITÉ 10. GESTION DES IDENTITÉS ET DES ACCÈS DES UTILISATEURS AUX SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

IDENTIFICATION

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
10.A.1-EI/EE	Les utilisateurs et les processus automatiques accédant aux ressources des systèmes d'information de l'entité disposent de comptes individuels. Les utilisateurs peuvent, le cas échéant, disposer de plusieurs comptes individuels.	Oui	Oui
10.A.2-EI/EE	L'emploi d'un compte individuel du système d'information est réservé à l'utilisateur ou au processus automatique auquel ce compte a été attribué.	Oui	Oui
10.A.3-EI/EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, l'entité met en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes (*par exemple : carnet de quart dans une salle de supervision, badgeuse à l'entrée de la salle*).	Oui	Oui
10.A.4-EI/EE	Lorsqu'un système d'information est utilisé pour diffuser de l'information au public, l'entité n'est pas tenue de créer de comptes pour l'accès du public à cette information (*par exemple : l'accès à un site vitrine ne nécessite pas d'authentifier les visiteurs alors que l'accès à l'intranet doit authentifier les utilisateurs).*	Oui	Oui
10.A.5-EI/EE	L'entité désactive les comptes qui ne sont plus nécessaires dans les délais prévus par sa politique de gestion des comptes (*par exemple : sous 7 jours*).	Oui	Oui
10.A.6-EI/EE	L'entité effectue périodiquement, au moins annuellement, une revue des comptes. Cette revue doit notamment vérifier le respect des présentes mesures relatives à l'identification et, le cas échéant, corriger les anomalies.	Oui	Oui

AUTHENTIFICATION

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
10.B.1-EI/EE	L'entité protège les accès des utilisateurs et processus automatiques aux ressources de ses systèmes d'information au moyen d'un mécanisme d'authentification impliquant au moins un élément secret (*par exemple : un mécanisme d'authentification mono-facteur tel qu'un mot de passe, ou multi-facteur, tel qu'une carte à puce avec code PIN*).	Oui	Oui
10.B.2-EI/EE	L'entité change les éléments secrets configurés par défaut, avant la mise en service d'une ressource. À cet effet, l'entité s'assure auprès du fabricant ou du fournisseur de la ressource qu'elle dispose des moyens et des droits permettant d'effectuer ces changements.	Oui	Oui
10.B.3-EI/EE	L'élément secret d'un compte partagé est renouvelé à chaque retrait d'un utilisateur de ce compte.	Oui	Oui

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
10.B.4-EI/EE	L'élément secret d'un compte n'est connu, que des utilisateurs autorisés à utiliser le compte (*par exemple : les mots de passe des comptes partagés peuvent être stockés dans un coffre-fort de mots de passe).*	Oui	Oui
10.B.5-EI/EE	Les facteurs d'authentification sont conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information en matière de complexité, en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de fréquence de renouvellement.	Oui	Oui
10.B.6-EI/EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas de modifier l'élément secret, l'entité met en œuvre un contrôle d'accès approprié à la ressource concernée ainsi que des mesures de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe.	Oui	Oui
10.B.7-EE	Dans le cadre de cette exception, l'entité met également en œuvre des mesures de sécurité permettant d'assurer la traçabilité des accès.	**Non**	Oui

DROITS D'ACCÈS

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
10.C.1-EI/EE	L'entité n'attribue des droits qu'aux utilisateurs et processus automatiques authentifiés.	Oui	Oui
10.C.2-EI/EE	Pour chaque utilisateur ou chaque processus automatique, l'entité n'attribue les droits d'accès qu'aux seules ressources nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle ou de sécurité.	Oui	Oui
10.C.3-EI/EE	Pour chaque ressource du système d'information, l'entité n'attribue les droits d'accès qu'aux seuls utilisateurs et processus automatiques justifiant d'un besoin au regard de leurs missions.	Oui	Oui
10.C.4-EI/EE	L'entité effectue périodiquement, au moins annuellement, une revue des droits d'accès. Cette revue doit notamment vérifier le respect ~~de la présente mesure~~des présentes mesures relatives au droit d'accès et, le cas échéant, corriger les anomalies.	Oui	Oui

OBJECTIF DE SÉCURITÉ 11. MAÎTRISE DE L'ADMINISTRATION DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

COMPTES D'ADMINISTRATION

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
11.A.1-EI/EE	Les actions d'administration sont effectuées exclusivement à partir de comptes d'administration~~,~~ et ~~inversement,~~ les comptes d'administration sont utilisés exclusivement pour les actions d'administration. *Par exemple : le compte d'administration d'un poste utilisateur est utilisé exclusivement pour l'administration de ce poste. L'utilisateur de ce poste dispose d'un compte bureautique non administrateur pour son utilisation quotidienne.*	Oui	Oui
11.A.2-EI/EE	Les comptes d'administration ne sont utilisés que par des administrateurs ou des personnes autorisées.	Oui	Oui
11.A.3-EI/EE	Les comptes d'administration respectent les mesures relatives à la gestion des identités et des accès des utilisateurs aux systèmes d'information.	Oui	Oui
11.A.4-EE	Un compte d'administration est utilisé exclusivement pour se connecter ~~à une ressource d'administration, ou à une ressource~~ aux ressources que ce compte administre pour effectuer des actions d'administration~~. (Par~~, ou à une ressource d'administration *(par exemple : ~~Le~~le compte administrateur d'un routeur est utilisé depuis un poste d'administration ou sur le routeur pour l'administrer).*	**Non**	Oui
11.A.5-EI/EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas d'effectuer des actions d'administration à partir d'un compte d'administration, l'entité met en œuvre des mesures permettant d'assurer le contrôle de ces actions d'administration et des mesures de réduction du risque lié à l'utilisation d'un compte non dédié à l'administration.	~~**Non**~~Oui	Oui
11.A.6-EE	L'entité établit et tient à jour la liste des comptes d'administration de ses systèmes d'information.	**Non**	Oui
11.A.7-EE	Lors de toute modification d'un compte d'administration (ajout, suppression, suspension ou modification des droits associés), l'entité vérifie que les droits d'accès aux ressources et fonctionnalités sont attribués en cohérence avec les besoins d'utilisation du compte. En particulier, afin de limiter la portée des droits individuels, ils sont attribués à chaque compte d'administration en les restreignant autant que possible au périmètre fonctionnel et technique de ce dernier. Pour ceci, il est recommandé d'octroyer les droits d'administration au travers des groupes dont les comptes d'administration sont membres.	**Non**	Oui

SÉCURITÉ DES ANNUAIRES

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
11.B.1-EI/EE	L'entité applique sans retard injustifié les correctifs de sécurité sur les annuaires gérant les utilisateurs ou les ressources de ses systèmes d'information.	Oui	Oui
11.B.2-EE	La sécurité des systèmes d'information de l'entité repose en grande partie sur la sécurité du ou des annuaires gérant les utilisateurs ou les ressources des systèmes d'information. L'ensemble des ressources regroupant ~~ces annuaires~~un annuaire, les ressources matérielles et logicielles hébergeant ~~ces annuaires~~cet annuaire ou permettant de prendre le contrôle de ~~ces annuaires~~cet annuaire (*les comptes, les hyperviseurs, les machines d'administration, etc.*) est désigné ~~par~~ « cœur de confiance » (*par exemple : Le Tier0 ~~pour les annuaires~~un annuaire AD DS constitue le cœur de confiance du système d'information).* ~~L'entité réalise les opérations d'identification.~~Pour chacun de ses annuaires, l'entité identifie les ressources constituant son cœur de confiance.	**Non**	Oui
11.B.3-EE	Les actions d'administration ~~du~~d'un cœur de confiance sont réalisées ~~via~~depuis des comptes d'administration dédiés ~~exclusivement à cet usage~~à l'administration de cœurs de confiance.	**Non**	Oui
11.B.4-EE	Les actions d'administration ~~du~~d'un cœur de confiance sont réalisées ~~via~~depuis des ressources dédiées exclusivement à ~~cet usage.~~l'administration de cœurs de confiance.	**Non**	Oui
11.B.5-EE	Les connexions externes ~~au~~à un cœur de confiance, à destination des ressources d'administration ~~du cœur~~de cœurs de confiance sont interdites par un dispositif de filtrage sur les ressources d'administration. ~~*Par*~~ *(par exemple : le filtrage peut être réalisé par le pare-feu local de la ressource d'administration du cœur de confiance~~.~~).*	**Non**	Oui
11.B.6-EE	L'entité effectue annuellement une revue de la configuration des annuaires gérant les utilisateurs ou les ressources de ses systèmes d'information, afin d'identifier tout élément inutile ou anormal. Il est recommandé que cette revue s'appuie sur un outil automatisé.	**Non**	Oui
11.B.7-EE	Lorsqu'elles existent, les recommandations de l'autorité nationale de sécurité des systèmes d'information relatives au cœur de confiance sont mises en œuvre (*par exemple : guide de sécurisation, guide de réponses à incidents, mémos techniques, recommandations issues des outils de revues de configurations).*	**Non**	Oui

OBJECTIF DE SÉCURITÉ 12. IDENTIFICATION ET RÉACTION AUX INCIDENTS DE SÉCURITÉ

RAPPEL DE L'OBJECTIF 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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités importantes et essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation ~~d'assistance~~d'accompagnement et de conseil en sécurité (PACS), qualifiée par l'Agence nationale de la sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[2], pour la préparation du dispositif de gestion des incidents et le suivi par l'entité du plan d'action issu de la prestation ~~permettent de bénéficier d'une présomption de conformité à l'objectif~~afin de démontrer leur respect de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
12.1-EE	L'entité s'assure de l'élaboration, du maintien à jour et de la mise en œuvre d'une procédure de traitement des incidents de sécurité affectant ses systèmes d'information.	**Non**	Oui
12.2-EE	L'entité s'assure de la mise en œuvre des outils permettant de collecter les signalements remontés, en particulier par les sources suivantes : • Les employés de l'entité essentielle ; • Les clients et les usagers des activités et services mis en œuvre par l'entité essentielle ; • Les prestataires ~~sou~~et les fournisseurs contractant avec l'entité essentielle.	**Non**	Oui
12.3-EI/EE	L'entité s'assure de la définition et de la mise en œuvre des mécanismes permettant d'analyser et de qualifier les événements remontés et d'identifier les incidents potentiels ou avérés.	Oui	Oui
12.4-EE	L'entité s'assure de la définition et de la mise en œuvre des mécanismes organisationnels et techniques permettant de réagir en cas d'incident et de limiter les conséquences sur la fourniture des services. Ces mécanismes sont repris, le cas échéant, dans la définition des plans de continuité et de reprise d'activité.	**Non**	Oui
12.5-EE	~~Après chaque incident majeur~~En complément des dispositions de l'article 17 de la loi XXX, l'entité ~~essentielle~~ s'assure, après chaque incident de sécurité, qu'une analyse des causes de l'incident a été réalisée. L'analyse des causes vise à définir et mettre en œuvre les mesures de sécurité permettant de limiter la vraisemblance d'un nouvel incident ou d'en réduire l'impact. L'entité conserve des preuves de cette analyse.	**Non**	Oui

[2] décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
12.6-EI/EE	L'entité conserve les relevés techniques ~~produits~~dont elle dispose (*par exemple : rapport d'analyse, alertes remontées par les outils de protection contre les codes malveillants*) ~~dans le cadre de la gestion des incidents~~ et pouvant être utilisés comme éléments de preuve en cas de judiciarisation. Ces relevés techniques sont conservés ~~hors ligne~~ pour une durée pertinente au regard de la protection des données à caractère personnel et en particulier la finalité du traitement.	~~Oui~~**Non**	Oui
12.7-EE	Les relevés techniques relatifs aux analyses des incidents sont ~~protégées~~protégés d'un incident qui les ~~rendant~~rendrait inexploitables (*par exemple : le stockage hors-ligne pour répondre à un incident de type rançongiciel*).	**Non**	Oui

OBJECTIF DE SÉCURITÉ 13. CONTINUITÉ ET REPRISE D'ACTIVITÉ

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
13.1-EI/EE	L'entité définit et met en œuvre des procédures de sauvegarde et de restauration de ses systèmes d'information et des ~~informations nécessaires à ces activités ou services.~~ données qu'ils manipulent.	Oui	Oui
~~*CONTINUITE_ACTIVITE.b*~~	~~Les mécanismes de sauvegarde sont dimensionnés pour répondre aux besoins de disponibilité associés aux différents services et aux différentes activités fournis par l'entité.~~	~~Oui~~	~~Oui~~
~~*CONTINUITE_ACTIVITE.c*~~*13.2-EI/EE*	L'entité s'assure que les processus de sauvegarde et de restauration sont testés au minimum une fois par an. Ces tests visent notamment à vérifier la bonne réalisation des sauvegardes et leur bonne restauration.	Oui	Oui
13.3-EI/EE	Les sauvegardes sont protégées d'un incident les rendant inexploitables (*par exemple : le stockage hors-ligne pour répondre à un incident de type rançongiciel*).	Oui	Oui
13.4-EE	L'entité, pour chacun de ses activités et services, définit et documente la durée maximale d'interruption admissible (DMIA) et ~~la perte~~le point de rétablissement des données ~~maximale admissible (PDMA~~(PRD).	**Non**	Oui
13.5-EI/EE	Les mécanismes de sauvegarde sont dimensionnés pour répondre aux besoins de disponibilité associés aux différents services et aux différentes activités fournis par l'entité.	Oui	Oui
13.6-EE	L'entité définit et met en œuvre un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) adaptés aux scénarios de crises d'origine cyber et ~~cohérent~~cohérents avec la durée maximale d'interruption admissible et ~~la perte~~le point de rétablissement des données ~~maximale admissible~~.	**Non**	Oui
~~*CONTINUITE_ACTIVITE.g*~~	~~L'entité essentielle s'assure que le plan de continuité d'activité (PCA) et le plan de reprise d'activité (PRA) sont testés au minium tous les trois ans.~~	~~**Non**~~	~~Oui~~
~~*CONTINUITE_ACTIVITE.h*~~*13.7-EE*	L'identification de ces mesures de continuité s'appuie notamment : • Sur la cartographie de l'écosystème ; • Sur la procédure de gestion des incidents pour détecter et réagir au plus tôt aux incidents ; • Sur la procédure de gestion des crises d'origine cyber pour permettre la reprise au plus tôt des services.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 14. RÉACTION AUX CRISES D'ORIGINE CYBER

RAPPEL DE L'OBJECTIF 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 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 informations relatives aux parties prenantes externes à l'entité pertinente dans la gestion de la crise.

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités importantes et essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation ~~d'assistance~~d'accompagnement et de conseil en sécurité (PACS), qualifiée par l'Agence nationale de la sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[3], pour la préparation du dispositif de gestion des crises d'origine cyber et le suivi par l'entité du plan d'action issu de la prestation ~~permettent de bénéficier d'une présomption de conformité à l'objectif~~pour démontrer leur respect de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
14.1-EI/EE	L'entité s'assure de la définition, du maintien à jour et de la mise en œuvre d'une procédure de gestion de crises en cas d'incident de sécurité ~~significatif~~ sur ses systèmes d'information nécessitant le passage en mode crise (*par exemple : pour les incidents importants au sens de l'article 17 du PIL*).	Oui	Oui
14.2-EI/EE	L'entité s'assure du maintien à jour d'une liste imprimée des personnes mobilisables dans la gestion de la crise sur les sujets relatifs à la sécurité numérique ainsi que leurs coordonnées.	Oui	Oui
14.3-EI/EE	L'entité s'assure que la liste des personnes mobilisables prévue au 14.2-EI/EE est accessible dans un format adapté à la nature de la crise (*par exemple, la liste doit être accessible au format papier si les systèmes d'information ne sont plus disponibles, et elle doit être accessible au format numérique si la version papier n'est pas accessible*).	Oui	Oui
14.4-EI/EE	L'entité s'assure du maintien à jour d'un annuaire des parties prenantes externes à l'entité pertinente dans la gestion de la crise en s'appuyant sur la cartographie de l'écosystème.	Oui	Oui
14.5-EE	L'entité s'assure de la mise en œuvre de retour d'expérience (RETEX) 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.	~~Non~~Oui	Oui
14.6-EE	L'entité s'assure de la définition, du maintien à jour et de la mise en œuvre des critères permettant d'activer et de désactiver le dispositif de gestion de crise prenant en compte les menaces cyber.	**Non**	Oui

[3] ~~décret~~Décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

14.7-EE	L'entité s'assure de la définition, du maintien à jour et de la mise en œuvre des procédures et des mécanismes de gestion de la crise adaptés à la menace cyber en s'appuyant sur les recommandations de l'autorité nationale de sécurité des systèmes d'information.	**Non**	Oui
14.8-EE	L'entité s'assure de la définition et de la mise en œuvre des mesures pour isoler, protéger et, le cas échéant, reconstruire les systèmes d'information concernés, activables en cas d'incident de sécurité ~~significatif~~. Ces mesures prennent en compte les infrastructures, applicatifs et services numériques externalisés à des prestataires et sont mises en place en cohérence avec les plans de continuité et de reprise d'activité.	**Non**	Oui
14.9-EE	L'entité s'assure de la définition d'une stratégie de communication adaptée aux crises d'origine cyber, incluant des scénarios de crise, le schéma d'organisation de la communication de crise, les outils de pilotage de la communication et des éléments de langage sur des sujets sensibles ou de crise. Cette stratégie prend en compte les scénarios de menaces cyber identifiés.	**Non**	Oui
14.10-EE	L'entité s'assure de la disponibilité de moyens de communication de secours, si possible, sécurisés en temps de crise lorsque les moyens de communication habituels sont indisponibles.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 15. EXERCICES, TESTS ET ENTRAINEMENTS

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités importantes et essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation ~~d'assistance~~d'accompagnement et de conseil en sécurité (PACS), qualifiée par l'Agence nationale de la sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[4], pour la réalisation d'exercices de crise d'origine cyber et le suivi par l'entité du plan d'action issu de la prestation ~~permettent de bénéficier d'une présomption de conformité à l'objectif~~pour démontrer leur respect de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
15.1-EI/EE	L'entité s'assure de la sensibilisation et de ~~l'entraînement des~~la mise en œuvre d'a minima un exercice sur table à une fréquence qu'elle définit pour les personnes mobilisables dans le dispositif de gestion des crises d'origine cyber.	Oui	Oui
15.2-EE	L'entité définit et met en œuvre une stratégie d'entraînement qui comporte, au minimum, les éléments suivants : • Une liste des acteurs amenés à participer aux différents dispositifs d'entraînement et d'exercice ; • Une liste d'exercices permettant d'entraîner ou de tester les capacités opérationnelles ; • Les objectifs visés par la stratégie ; • Les moyens de vérification ou d'évaluation d'atteinte de ces objectifs ; • Les scénarios de risques ou d'attaques à tester en priorité ; • La comitologie de suivi de la stratégie. Cette stratégie peut être mutualisée avec d'autres livrables ~~attendus~~.	**Non**	Oui
15.3-EE	Cette stratégie d'entraînement vise à tester les dispositifs mis en œuvre par l'entité en matière : • De gestion des alertes relatives aux incidents, aux vulnérabilités et menaces ; • De continuité et de reprise d'activité ; • De gestion des crises d'origine cyber.	**Non**	Oui
15.4-EE	L'entité décline cette stratégie dans la définition et la mise en œuvre d'un programme triennal d'entraînement et d'exercice. Ce programme précise notamment la fréquence de ces entraînements et exercices ainsi que leur nature et que leurs objectifs. Ce programme triennal doit permettre de tester les dispositifs de gestion des incidents, de gestion des crises d'origine cyber et de coopération avec l'écosystème et, le cas échéant, le volet cyber des plans de continuité et de reprise d'activité.	**Non**	Oui

[4] ~~décret~~Décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

OBJECTIFS DE SECURITE APPLICABLES AUX ENTITÉS ESSENTIELLES

GOUVERNANCE DES SYSTÈMES D'INFORMATION

OBJECTIF DE SÉCURITÉ 16. MISE EN ŒUVRE D'UNE APPROCHE PAR LES RISQUES

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~La~~Les entités essentielles peuvent se prévaloir lors d'un contrôle de la mise en place d'un système de management de la sécurité des systèmes d'information (SMSI) certifié conforme aux exigences prévues dans la norme ISO/CEI 27001:2022 ~~et dont~~pour démontrer le ~~domaine d'application couvre au minimum~~respect de cet objectif par les systèmes d'information ~~permet d'apporter une présomption de conformité à cet objectif~~couverts par la certification.

~~Le~~Les entités essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation d'accompagnement et de conseil en sécurité (PACS), qualifiée par l'Agence nationale de sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[5], pour la réalisation de l'analyse de risques et le suivi par l'entité du plan de traitement issu de la prestation ~~permet d'apporter une présomption de conformité à~~pour démontrer leur respect de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
16.1-EE	L'entité définit, met en œuvre et maintient à jour une gouvernance par les risques. Cette gouvernance vise à s'assurer que le risque numérique est pris en compte par le dirigeant exécutif de l'entité et les responsables d'activité ou de service de l'entité ~~identifiés conformément à l'objectif de sécurité 1~~au regard des rôles et responsabilités définis et que les moyens financiers, humains ou techniques adéquats sont alloués pour maîtriser ce risque. Cette gouvernance intègre les éléments issus de l'approche par la conformité et la complète par une approche par les risques, réalisée dans les conditions définies ci-après. Ces approches sont complémentaires et peuvent être mutualisées, notamment en termes de livrables attendus.	**Non**	Oui

[5] Décret En° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
16.2-EE	L'entité s'assure que chaque système d'information fait l'objet d'une analyse de risques. Cette exigence peut être satisfaite *via* la réalisation et le maintien à jour d'une analyse de risques pour chaque activité ou service qu'elle fournit, couvrant l'ensemble des systèmes d'information supportant cette activité ou ce service. Cette analyse de risques s'appuie sur les éléments issus : • De la PSSI et des spécificités sectorielles ; • De la maîtrise de l'écosystème ; • De la maîtrise du système d'information ; • De l'approche par conformité ; • Des audits. La méthode EBIOS RM peut être utilisée pour réaliser cette analyse de risques.	**Non**	Oui
16.3-EE	L'entité valide l'analyse de risques, accepte les risques résiduels et met en œuvre le plan d'action pour maîtriser ces risques. Le plan d'action prévoit, au minimum, une échéance raisonnable et un responsable pour la réalisation de chaque action.	**Non**	Oui
16.4-EE	L'entité réexamine l'analyse de risques au minimum tous les trois ans et en tant que de besoin, notamment en cas d'incident de sécurité ou d'évolutions majeures du contexte métier, technique ou organisationnel.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 17. AUDIT DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF

Les entités [essentielles] réalisent ou font réaliser à intervalles réguliers et 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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation d'audit en sécurité des systèmes d'information (PASSI), qualifiée par l'Agence nationale de la sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[6], dont le périmètre de la prestation couvre l'application des mesures correctives issues de la prestation ~~permettent d'apporter une présomption de conformité à~~pour démontrer leur respect de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
17.1-EE	L'entité définit et met en œuvre un programme d'audit de l'ensemble de ses systèmes d'information et s'assure que les audits associés à ce programme ainsi que leur profondeur et leur fréquence tiennent compte de tout ou partie de l'analyse de risque réalisée, de la criticité du système d'information au regard de son organisation et de l'exposition du système d'information aux risques numériques. Pour évaluer cette criticité et ce niveau d'exposition, l'entité peut s'appuyer sur les recommandations de l'autorité nationale de sécurité des systèmes d'information en matière de gestion des risques numériques.	**Non**	Oui
17.2-EE	L'audit de sécurité permet, de manière indépendante : • De vérifier, sur le périmètre défini, l'atteinte des objectifs fixés par la réglementation *via* ○ La conformité aux présentes mesures, ou ○ La mise en œuvre de mesures alternatives ; et • D'évaluer le niveau de sécurité du ou des systèmes d'information couverts au regard des menaces et des vulnérabilités connues.	**Non**	Oui
17.3-EE	Sans préjudice d'autres obligations légales et réglementaires, l'audit de sécurité comprend au minimum une activité parmi les suivantes : un test d'intrusion (couvrant au minimum les interfaces exposées à des systèmes sous la responsabilité de l'entité pour lesquels elle a décidé de ne pas appliquer les objectifs de sécurité ainsi qu'à des systèmes d'information tiers), un audit de configuration, un audit d'architecture, un audit organisationnel et physique et, lorsque cela est pertinent, un audit de code.	**Non**	Oui

[6] décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
17.4-EE	Le rapport de l'audit de sécurité présente : • Une synthèse de la conformité aux présentes mesures ou aux mesures définies par l'entité pour atteindre les objectifs fixés par la réglementation et du niveau de sécurité des systèmes d'information audités ; • Les constats de non-conformité et les vulnérabilités identifiées ; • Les recommandations pour y remédier.	**Non**	Oui
17.5-EE	L'entité définit et met en œuvre un plan d'action visant à corriger les non-conformités et les vulnérabilités identifiées. Ce plan d'action prévoit, au minimum, une échéance raisonnable et un responsable pour la réalisation de chaque action.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 18. SÉCURISATION DE LA CONFIGURATION DES RESSOURCES DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

Les entités [essentielles] limitent la surface d'attaque des composants de leurs systèmes d'information. Pour ce faire, elles 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 elles 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~~.~~.

MOYENS ACCEPTABLES DE CONFORMITÉ

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
18.1-EE	~~Seules~~L'entité n'installe et ne conserve sur ses systèmes d'information que les ressources logicielles nécessaires à la réalisation ~~des~~de ses activités et services ~~de l'entité~~ ou au maintien en condition opérationnelle ou de sécurité ~~sont installées ou conservées sur les~~de ses systèmes d'information~~.~~ ~~*Par*~~ *(par exemple : utilisation d'un modèle de configuration centralisé (master) contenant exclusivement les logiciels/services strictement nécessaires aux besoins métiers et d'administration~~.~~).*	**Non**	Oui
18.2-EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas de désactiver ou désinstaller une ressource logicielle, l'entité met en œuvre des mesures permettant de réduire le risque associé.	**Non**	Oui
18.3-EE	L'entité configure les ressources de ses systèmes d'information de manière sécurisée en s'appuyant sur les recommandations de l'éditeur de la fonctionnalité, du fabricant de la ressource ou de l'autorité nationale de sécurité des systèmes d'information.	**Non**	Oui
18.4-EE	L'entité effectue annuellement une revue de configuration des ressources de ses systèmes d'information pour vérifier l'application des mesures précédentes. Il est recommandé que cette revue s'appuie sur un ou des outils automatisés (*par exemple : scan de port et de vulnérabilité, revue (manuel ou automatique) des configurations des pares-feux par rapport aux matrices de flux).*	**Non**	Oui

OBJECTIF DE SÉCURITÉ 19. ADMINISTRATION DES SYSTÈMES D'INFORMATION DEPUIS DES RESSOURCES DÉDIÉES

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation d'administration et de maintenance sécurisée (PAMS), qualifiée par l'Agence nationale de sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[7], ~~permet à l'entité de bénéficier d'une présomption de conformité aux exigences b, c, d, e, f, g, j, k et l~~pour démontrer leur respect des mesures 19.2-EE, 19.3-EE, 19.4-EE, 19.5-EE, 19.6-EE, 19.7-EE, 19.10-EE, 19.11-EE, 19.12-EE de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
19.1-EE	Les actions d'administration sont effectuées au moyen d'un réseau d'administration dédié.	**Non**	Oui
19.2-EE	Les ressources des réseaux d'administration sont gérées et configurées par l'entité ou par le prestataire qu'elle a mandaté pour réaliser les actions d'administration.	**Non**	Oui
19.3-EE	Les ressources matérielles des réseaux d'administration sont utilisées exclusivement pour réaliser des actions d'administration.	**Non**	Oui
19.4-EE	Le poste physique utilisé pour effectuer des actions d'administration est utilisé exclusivement pour réaliser des actions d'administration.	**Non**	Oui
19.5-EE	La connexion des administrateurs à un réseau d'administration s'effectue au moyen d'un poste physique utilisé exclusivement pour des actions d'administration.	**Non**	Oui
19.6-EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas de dédier le poste de travail physique de l'administrateur pour les actions d'administration, l'entité met en œuvre des mesures de durcissement et de cloisonnement du système d'exploitation du poste de travail permettant d'isoler le système d'exploitation utilisé pour les actions d'administration du système d'exploitation utilisé pour les autres actions. Ces mesures sont conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information, y compris les recommandations alternatives.	**Non**	Oui
19.7-EE	Les réseaux d'administration sont connectés aux ressources du système d'information à administrer au travers d'une liaison réseau physique utilisée exclusivement pour les actions d'administration. Ces ressources sont administrées au travers de leur interface d'administration physique.	**Non**	Oui

[7] décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
19.8-EE	Les modalités de cloisonnement et de filtrage du réseau d'administration respectent les modalités de cloisonnement et ~~l~~de filtrage mis en œuvre entre et au sein des systèmes d'information *(par exemple : deux machines ne pouvant pas communiquer au travers des systèmes d'information ne peuvent pas communiquer au travers du réseau d'administration).*	**Non**	Oui
19.9-EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas d'administrer une ressource au travers d'une liaison réseau physique ou de son interface d'administration physique, l'entité met en œuvre des mesures de réduction du risque telles que des mesures de sécurité logique. Ces mesures sont conformes aux recommandations de l'autorité nationale de sécurité des systèmes d'information y compris les recommandations alternatives.	**Non**	Oui
19.10-EE	Les communications associées à des actions d'administration sont protégées par des mécanismes de chiffrement et d'authentification conformes à l'état de l'art tel que recommandé par l'autorité nationale de sécurité des systèmes d'information (*par exemple : en utilisant des protocoles sécurisés garantissant l'authentification de l'administrateur, l'intégrité et la confidentialité des messages).*	**Non**	Oui
19.11-EE	Les communications associées à des actions d'administration qui transitent sur des réseaux non dédiés à ces communications sont cloisonnées au moyen de mécanismes de chiffrement et d'authentification conformes aux mesures recommandées par l'autorité nationale de sécurité des systèmes d'information *(par exemple : au travers de tunnels VPN*).	**Non**	Oui
19.12-EE	Lorsque des raisons techniques ou opérationnelles ne permettent pas de recourir à des mécanismes de chiffrement ou d'authentification de ces communications, l'entité met en œuvre des mesures permettant de protéger la confidentialité et l'intégrité de ces flux et de renforcer le contrôle et la traçabilité des actions d'administration.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 20. SUPERVISION DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RAPPEL DE L'OBJECTIF DE SÉCURITÉ

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 évènements de sécurité, sans retard injustifié et au maximum sous ~~24h ouvrés.~~24 heures ;

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, notamment en matière de protection des données à caractère personnel.

MOYENS ACCEPTABLES DE CONFORMITÉ

~~Le~~Les entités essentielles peuvent se prévaloir lors d'un contrôle du recours à une prestation de détection des incidents de sécurité (PDIS), qualifiée par l'Agence nationale de la sécurité des systèmes d'information en application de l'article 10 du décret n° 2015-350 du 27 mars 2015 modifié[8], ~~permet d'apporter une présomption de conformité aux exigences~~pour démontrer leur respect des mesures a, c et e de cet objectif.

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
20.1-EE	L'entité s'assure 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 évènements de sécurité, sans retard injustifié et au maximum sous 24h ouvrés (*Par exemple : l'ensemble des évènements de sécurité issus de l'EDR*).	**Non**	Oui
20.2-EE	L'entité élabore et met en œuvre une démarche d'amélioration continue de son activité de supervision de sécurité, afin d'améliorer la couverture des scénarios de menaces identifiés à l'occasion de l'analyse de risque ~~(cf Objectif~~prévue à l'objectif de sécurité 16~~),~~, et l'efficacité de la supervision de sécurité, en accord avec les dispositions prévues 20.1-EE (*par exemple : augmentation des sources de collecte, amélioration des processus de traitements, augmentation des capacités de traitement, centralisation des journaux et des évènements de sécurité, mise en place*	**Non**	Oui

[8] décret n° 2015-350 du 27 mars 2015 modifié relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. (legifrance.gouv.fr)

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
	de corrélation, prise en compte de scénarios de menace supplémentaires).		
20.3-EE	L'entité ou le prestataire qu'elle a mandaté à cet effet maîtrise l'architecture et la configuration du système d'information supportant l'activité de supervision de sécurité (*par exemple : Le système peut être composé d'une ou plusieurs des chaînes suivantes : collecte, analyse, investigation, signalement).*	**Non**	Oui
20.4-EE	En lien avec la démarche d'amélioration continue, l'entité collecte les ~~journaux~~données de supervision et les évènements de sécurité utiles à la détection des scénarios principaux de menaces, conformément à la disposition prévue en 20.1-EE. Les journaux et évènements reflètent, la variété des activités du système d'information associées (*par exemple : réseau, système, applicatif, utilisateur).*	**Non**	Oui
20.5-EE	L'entité s'assure que les données de supervision et 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 (*par exemple : le règlement général sur la protection des données à caractère personnel).*	**Non**	Oui
20.6-EE	Les données de supervision et les événements de sécurité sont protégés d'un incident les rendant inexploitables (*par exemple : le stockage hors-ligne pour répondre à un incident de type rançongiciel).*	**Non**	Oui

JUSTIFICATIONS ET RISQUES ASSOCIES

Objectif de sécurité 1 : Recensement des SI	La directive NIS 2, prévoit la mise en œuvre des mesures de sécurité à l'ensemble des systèmes d'information de l'entité utilisés dans le cadre de ses activités et services. Pourtant si un incident de sécurité affecte certains de ces systèmes d'information, cela ne remettrait pas nécessairement en cause les activités ou les services de l'entité (*par exemple : le site du comité d'entreprise ou le site d'actualité interne de l'entité*). L'atteinte de cet objectif permettra aux entités importantes ou essentielles de concentrer leurs efforts sur les systèmes d'information pour lesquels un incident de sécurité pourrait entraîner : • La dégradation ou l'interruption des activités ou services de l'entité ; • La divulgation à des personnes non autorisées d'informations sensibles traitées pour les activités ou services de l'entité ; • L'altération des informations nécessaires aux activités ou services de l'entité.
Objectif de sécurité 2 : Mise en œuvre d'un cadre de gouvernance de la sécurité numérique	La mise en œuvre d'un cadre de gouvernance de la sécurité numérique permet l'allocation de ressources financières, techniques et humaines, adaptées aux besoins de l'entité en matière de sécurité numérique au regard de la menace à laquelle elle est exposée. L'atteinte de cet objectif permet à l'entité de piloter efficacement la sécurité numérique dans toutes ses dimensions, au bon niveau et dans la durée, en responsabilisant les rôles de décision et en mobilisant l'ensemble des parties prenantes concernées, afin de réduire l'exposition de l'entité à la menace d'origine cyber et pouvant, par exemple, affecter la réalisation des activités ou ~~la fourniture~~ des services de l'entité.
Objectif de sécurité 3 : Maîtrise de l'écosystème	La cartographie de l'écosystème et la prise en compte de la sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques permettent à l'entité de limiter les incidents de sécurité dont l'origine est la compromission de la chaîne de sous-traitance. En l'absence d'une telle mesure, l'entité s'expose à des attaques dont l'origine est la compromission d'un de ses prestataires ou fournisseurs informatiques, en particulier lorsque ces derniers sont interconnectés aux systèmes d'information de l'entité.
Objectif de sécurité 4 : Prise en compte de la sécurité numérique dans la gestion des ressources humaines	Par l'atteinte de cet objectif, les utilisateurs sont responsabilisés à l'usage des systèmes d'information de l'entité. En l'absence d'une telle responsabilisation, les utilisateurs peuvent adopter des comportements dangereux du point de vue de la sécurité numérique (*par exemple : connexion d'un support amovible infecté sur un système d'information de l'entité*) pouvant être à l'origine d'incident de sécurité entraînant une dégradation ou une interruption des activités ou des services fournis par l'entité.
Objectif de sécurité 5 : Maîtrise des SI	La ou les cartographie(s) permet(tent) à l'entité de faciliter le maintien en condition opérationnelle et de sécurité des systèmes d'information par l'identification rapide, en cas de publication d'une alerte de sécurité, des ressources affectées. La ou les cartographie(s) permet(tent) également à l'entité de pouvoir réagir rapidement en cas d'incident de sécurité par l'identification des ressources

	affectées et la mise en œuvre de mesures permettant de limiter la propagation de l'incident et d'en réduire les conséquences. L'absence de cartographie expose l'entité au maintien de ressources vulnérables sur ses systèmes d'information et, par conséquent, à l'exploitation de ces vulnérabilités pouvant entraîner la dégradation ou l'interruption des activités ou des services fournis par l'entité. Le processus de maintien en condition opérationnelle et de sécurité permet à l'entité de s'assurer que les ressources de ses systèmes d'information sont à jour et maintenues par l'éditeur ou le fournisseur. En l'absence d'un tel processus, des vulnérabilités peuvent être présentes sur les systèmes d'information qui, si elles venaient à être exploitées, pourraient, par exemple, entraîner la dégradation ou l'interruption des activités ou des services fournis par l'entité.
Objectif de sécurité 6 : Maîtrise des accès physiques aux locaux	Par l'atteinte de cet objectif, l'entité s'assure que seules les personnes autorisées (*par exemple : personnels de l'entité, prestataires ou visiteurs*) ont accès à ses locaux, ses salles serveurs ou ses locaux techniques. En l'absence d'un tel objectif, l'entité s'expose à ce que des personnes non autorisées et potentiellement malveillantes s'introduisent dans ses locaux pouvant entraîner, par exemple, le vol d'information sensible ou l'introduction de codes malveillants dans un système d'information par la connexion de supports amovibles infectés.
Objectif de sécurité 7 : Sécurisation de l'architecture des SI	Par l'atteinte de cet objectif, l'entité réduit son exposition à la menace d'origine cyber. En l'absence d'un tel objectif, l'entité augmente son exposition à la menace d'origine cyber facilitant la compromission de ses systèmes d'information. Les conséquences de cette compromission peuvent être aggravées par les possibilités de l'attaquant à étendre son attaque à d'autres systèmes d'information (*par exemple : latéralisation entre les systèmes d'information*), causant une dégradation voire une interruption des activités de l'entité ou de la fourniture de ses services.
Objectif de sécurité 8 : Sécurisation des accès distants aux SI	L'atteinte de cet objectif doit permettre à l'entité de concilier les besoins opérationnels nécessitant une forte interconnexion (*par exemple : interconnexion avec un fournisseur, pratique du télétravail et du nomadisme*) sans remettre en cause la sécurité des informations, des activités et ~~des~~ services de l'entité. En l'absence d'un tel objectif, l'entité s'expose, par exemple, à des vols de secrets d'authentification et à des accès illégitimes à ses systèmes d'information *via* les accès distants légitimes des personnels de l'entité, des processus automatiques ou des prestataires de l'entité, pouvant entraîner la dégradation voire l'interruption des activités ou services qu'elle fournit ou encore la divulgation d'informations sensibles.
Objectif de sécurité 9 : Protection des SI contre les codes malveillants	L'atteinte de cet objectif permet à l'entité de se protéger des codes malveillants qui pourraient être introduits sur ses systèmes d'information (*par exemple : par la mise en œuvre ou l'activation d'un antivirus*).
Objectif de sécurité 10 : Gestion des identités et des accès des	L'atteinte de cet objectif permet à l'entité de maîtriser les utilisateurs accédant à ses systèmes d'information, que ces derniers soient internes ou externes (*par exemple : les prestataires*), ainsi que les processus automatiques (*par exemple : les agents de supervision ou de sauvegarde*) *via* des mécanismes d'identification et d'authentification à l'état de l'art.

utilisateurs aux SI	L'atteinte de cet objectif permet également à l'entité de maîtriser les accès afin que les utilisateurs n'accèdent qu'aux seules ressources utiles pour l'accomplissement de leurs missions. En l'absence d'un tel objectif, l'entité s'expose à ce qu'un attaquant, profitant de l'absence de mécanismes d'authentification ou mécanismes d'authentification faibles (*par exemple : mots de passe pas suffisamment robustes*) usurpe l'identité d'un utilisateur légitime du système d'information, accède à celui-ci et exfiltre des informations sensibles, dégrade ou encore interrompe les activités ou services de l'entité reposant sur ce système d'information.
Objectif de sécurité 11 : Maîtrise de l'administration des SI	L'administration des systèmes d'information est une activité indispensable pour le maintien en condition opérationnelle et de sécurité de ces systèmes. De plus cette activité est extrêmement sensible, car elle permet d'avoir des droits étendus sur les ressources administrées. Cette capacité est extrêmement recherchée par les attaquants dans le déroulement de leurs attaques. L'atteinte de cet objectif permet à l'entité de s'assurer que les droits d'administration sont délivrés aux seuls personnels dont c'est la responsabilité et uniquement lorsqu'ils se sont authentifiés. Il permet également que les ressources utilisées pour les actions d'administration sur le cœur de confiance soient maîtrisées par l'entité. En l'absence d'un tel objectif, l'entité s'expose à ce qu'un attaquant usurpe l'identité d'une personne disposant des droits d'administration ou exploite une vulnérabilité d'une ressource d'administration exposée lui permettant, par exemple, de désactiver des mesures de sécurité mise en place par l'entité complexifiant, les capacités de celle-ci à détecter les activités malveillantes sur ses systèmes d'information ou d'introduire et d'exécuter des codes malveillants sur le système d'information, avec pour conséquence la dégradation ou l'interruption des activités ou des services fournis par l'entité. Lorsque l'attaquant dispose des droits d'administration sur le cœur de confiance, il est considéré que les systèmes d'information de l'entité liés à ce cœur de confiance sont totalement compromis avec des conséquences pour l'entité pouvant aller jusqu'à la nécessité de reconstruire tout ou partie de ses systèmes d'information.
Objectif de sécurité 12 : Identification et réaction aux incidents de sécurité	Cet objectif permet à l'entité de se préparer et de s'organiser pour faire face à des événements pouvant impacter la réalisation de ses activités ou la fourniture des services qu'elle fournit et de revenir rapidement à la normale limitant ainsi les conséquences pour l'entité. En l'absence d'un tel objectif, l'entité peut ne pas être en mesure de gérer les incidents de sécurité se traduisant par une aggravation des conséquences liées à ces incidents (*par exemple : allongement de la durée de résolution et de retour à la normale*) notamment sur les utilisateurs et les usagers en cas de dégradation ou d'interruption des activités et services fournis par l'entité.
Objectif de sécurité 13 : Continuité et reprise d'activité	Pour l'atteinte de cet objectif, l'entité s'assure de disposer de moyens lui permettant, suite à un incident de sécurité, de maintenir ses activités ou ses services dans un mode dégradé et de faciliter le retour à la normale. En l'absence d'un tel objectif, le manque de préparation de l'entité combiné éventuellement à l'inefficacité des outils disponibles (*par exemple : échec de la restauration des sauvegardes, échec de la bascule sur un site de secours*) permet à l'incident de prendre de l'ampleur et d'aggraver ses conséquences jusqu'à ces dernières soient perceptibles des utilisateurs ou usagers (*par exemple : dégradation ou interruption des activités ou services fournis par l'entité*).

Objectif de sécurité 14 : Réaction aux crises d'origine cyber	Cet objectif permet à l'entité de se préparer et de s'organiser pour faire face à des événements pouvant impacter les activités ou les services qu'elle fournit et de revenir rapidement à la normale limitant ainsi les conséquences pour l'entité. En l'absence d'un tel objectif, l'entité peut ne pas être en capacité de gérer les crises d'origine cyber se traduisant par une aggravation des conséquences liés à ces crises (*par exemple : allongement de la durée de résolution et de retour à la normale*) notamment sur les utilisateurs et les usagers en cas de dégradation ou d'interruption de ses activités et services.
Objectif de sécurité 15 : Exercices, tests et entraînements	L'atteinte de cet objectif permet à l'entité d'être familière avec les processus et mécanismes qu'elle met en œuvre pour accroître sa réactivité et améliorer sa gestion des incidents de sécurité ou des crises d'origine cyber. En l'absence d'un tel objectif, l'entité n'est pas préparée à la survenance d'un incident de sécurité ou d'une crise d'origine cyber notamment par la méconnaissance des responsabilités des personnes impliquées dans la gestion de ces événements, des procédures et processus existants pour les gérer. De plus, les mécanismes techniques appuyant la gestion des incidents de sécurité ou les crises d'origines qui n'ont pas été testés peuvent dysfonctionner au moment de les utiliser (*par exemple : échec de la restauration des sauvegardes, échec d'une bascule sur un site de secours*).
Objectif de sécurité 16 : Mise en œuvre d'une approche par les risques	L'atteinte de cet objectif permet à une entité essentielle de maîtriser les risques numériques pesant sur ces systèmes d'information en tenant compte des contextes organisationnel et technique spécifiques à son entité. À défaut, l'entité essentielle ne peut pas s'adapter aux risques numériques liés à ses contextes organisationnel (*par exemple : le nomadisme ou le télétravail*) ou technique (*par exemple : le recours à l'informatique en nuage*).
Objectif de sécurité 17 : Audit de la sécurité des SI	Les audits de sécurité permettent de vérifier la conformité des systèmes d'information aux objectifs fixés par la réglementation ainsi que d'évaluer le niveau de sécurité du système d'information. En l'absence d'audit, des vulnérabilités peuvent être présentes sur les systèmes d'information qui, si elles venaient à être exploitées, pourraient entraîner la dégradation ou l'interruption des activités ou des services fournis par l'entité essentielle.
Objectif de sécurité 18 : Sécurisation de la configuration des ressources des SI	En l'absence d'un tel objectif, un attaquant est en mesure de compromettre un système d'information par l'exploitation de vulnérabilités sur les services non essentiels à l'activité ou au service fourni par l'entité, maintenus sur un système d'information, mais non supervisés. L'entité s'expose également à l'exécution de codes malveillants sur ses systèmes d'information. Ces deux scénarios peuvent entraîner la dégradation ou l'interruption des activités et ~~des~~ services ~~fournis par~~de l'entité, la divulgation ou l'altération d'informations sensibles.
Objectif de sécurité 19 : Administration des SI depuis des ressources dédiées	L'atteinte de cet objectif permet à l'entité de s'assurer que les ressources utilisées pour l'administration de ces systèmes d'information sont sous sa maîtrise et qu'elles sont dédiées à cet usage. En l'absence d'un tel objectif, un attaquant pourrait compromettre, *via* de l'hameçonnage, le poste de travail d'un administrateur utilisé pour des activités bureautiques (*par exemple : navigation Internet, messagerie*). Une fois le poste de travail compromis, l'attaquant usurpe l'identité d'une personne disposant des droits d'administration ou exploite une vulnérabilité d'une ressource d'administration exposée lui permettant, par exemple, de désactiver des mesures

	de sécurité mise en place par l'entité complexifiant les capacités celle-ci à détecter les activités malveillantes sur ses systèmes d'information ou d'introduire et d'exécuter des codes malveillants sur le système d'information, avec pour conséquence la dégradation ou l'interruption des activités ou des services fournis par l'entité.
Objectif de sécurité 20 : Supervision de la sécurité des SI	L'atteinte de cet objectif permet à l'entité essentielle de disposer de capacité lui permettant d'identifier les potentiels incidents de sécurité au plus tôt et ainsi permettre de réagir rapidement et d'en réduire les conséquences. En l'absence d'un tel objectif, l'entité essentielle n'est pas en mesure de détecter une éventuelle compromission de toute ou partie de ses systèmes d'information. L'attaquant a la possibilité d'étendre le périmètre de son attaque *via* la latéralisation sans être détecté et par conséquent d'aggraver les conséquences de celle-ci. C'est lorsque ces conséquences seront significatives et potentiellement perceptibles des utilisateurs et des usagers des services qu'elle fournit que l'entité aura la capacité de réagir (*par exemple : en cas de dégradation ou d'interruption des activités et services ~~fournis par~~de l'entité*).

TABLEAUX DE CORRESPONDANCE

RÉPARTITION DES OBJECTIFS DANS LE MODÈLE GOUVERNANCE / PROTECTION / DÉFENSE / RÉSILIENCE

Pilier	Objectif
Gouvernance	Objectif de sécurité 1 – Recensement des systèmes d'information
	Objectif de sécurité 2 - Mise en œuvre d'un cadre de gouvernance de la sécurité numérique
	Objectif de sécurité 3 – Maîtrise de l'écosystème
	Objectif de sécurité 4 – Intégration de la sécurité numérique dans la gestion des ressources humaines
	Objectif de sécurité 16 – Mise en œuvre d'une approche par les risques
	Objectif de sécurité 17 – Audit de la sécurité des systèmes d'information
	Objectif de sécurité 5 – Maîtrise des systèmes d'information
Protection	Objectif de sécurité 6 – Maitrise des accès physiques aux locaux
	Objectif de sécurité 7 – Sécurisation de l'architecture des systèmes d'information
	Objectif de sécurité 8 – Sécurisation des accès distants aux systèmes d'information
	Objectif de sécurité 9 – Protection des systèmes d'information contre les codes malveillants
	Objectif de sécurité 10 – Gestion des identités et des accès des utilisateurs aux systèmes d'information
	Objectif de sécurité 11 – Maîtrise de l'administration des systèmes d'information
	Objectif de sécurité 18 – Sécurisation de la configuration des ressources des systèmes d'information
	0 – Administration des systèmes d'information depuis des ressources dédiées
Défense	Objectif de sécurité 12 – Identification et réaction aux incidents de sécurité
	Objectif de sécurité 20 – Supervision de la sécurité des systèmes d'information
Résilience	Objectif de sécurité 13 – Continuité et reprise d'activité
	Objectif de sécurité 14 – Réaction aux crises d'origine cyber
	Objectif de sécurité 15 – Exercices, tests et entraînements

CORRESPONDANCE MESURES NIS 2 – MESURES NATIONALES

Mesures NIS 2	Objectifs
Art. 20 : Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités.	Objectif de sécurité 2
Art. 21.2 : Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents	Objectif de sécurité 6
Art. 21.2.a : les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information	Objectif de sécurité 2 Objectif de sécurité 16
Art. 21.2.b : la gestion des incidents	Objectif de sécurité 12 Objectif de sécurité 15 Objectif de sécurité 20
Art. 21.2.c : la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises	Objectif de sécurité 13 Objectif de sécurité 14 Objectif de sécurité 15
Art. 21.2.d : la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs	Objectif de sécurité 3
Art. 21.2.e : la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités	Objectif de sécurité 5 Objectif de sécurité 7 Objectif de sécurité 8 Objectif de sécurité 9 Objectif de sécurité 10 Objectif de sécurité 11 Objectif de sécurité 17 0
Art. 21.2.f : des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité	Objectif de sécurité 2Objectif de sécurité 2 Objectif de sécurité 17
Art. 21.2.g : les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité	Objectif de sécurité 4 Objectif de sécurité 15
Art. 21.2.h : des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement	Objectif de sécurité 2 Objectif de sécurité 7 Objectif de sécurité 8
Art. 21.2.i : la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs	Objectif de sécurité 1 Objectif de sécurité 2 Objectif de sécurité 3 Objectif de sécurité 5 Objectif de sécurité 10

	Objectif de sécurité 11
Art. 21.2.j : l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins	Objectif de sécurité 8 Objectif de sécurité 10 Objectif de sécurité 14

CORRESPONDANCES MESURES NATIONALES – MESURES NIS 2

Mesures nationales	Mesures NIS 2
Objectif de sécurité 1 - Recensement des systèmes d'information	Art. 21.2.i
Objectif de sécurité 2 - Mise en œuvre d'un cadre de gouvernance de la sécurité numérique	Art. 20 Art. 21.2.a Art. 21.2.f Art. 21.2.h Art. 21.2.i
Objectif de sécurité 3 – Maîtrise de l'écosystème	Art. 21.2.d Art. 21.2.i
Objectif de sécurité 4 – Intégration de la sécurité numérique dans la gestion des ressources humaines	Art. 21.2.g
Objectif de sécurité 5 – Maîtrise des systèmes d'information	Art. 21.2.e Art. 21.2.i
Objectif de sécurité 6- Maîtrise des accès physiques aux locaux	Art. 21.2
Objectif de sécurité 7 – Sécurisation de l'architecture des systèmes d'information	Art. 21.2.e Art. 21.2.h
Objectif de sécurité 8 – Sécurisation des accès distants aux systèmes d'information	Art. 21.2.e Art. 21.2.h Art. 21.2.j
Objectif de sécurité 9 – Protection des systèmes d'information contre les codes malveillants	Art. 21.2.e
Objectif de sécurité 10 – Gestion des identités et des accès des utilisateurs aux systèmes d'information	Art. 21.2.e Art. 21.2.i Art. 21.2.j
Objectif de sécurité 11 – Maîtrise de l'administration des systèmes d'information	Art. 21.2.e Art. 21.2.i
Objectif de sécurité 12 – Identification et réaction aux incidents de sécurité	Art. 21.2.b
Objectif de sécurité 13 – Continuité et reprise d'activité	Art. 21.2.c
Objectif de sécurité 14 – Réaction aux crises d'origine cyber	Art. 21.2.c Art. 21.2.j
Objectif de sécurité 15 - Exercices, tests et entrainements	Art. 21.2.b Art. 21.2.c Art. 21.2.g
Objectif de sécurité 16 - Mise en œuvre d'une approche par les risques	Art. 21.2.a

Objectif de sécurité 17 - Audit de la sécurité des systèmes d'information	Art. 21.2.f
Objectif de sécurité 18 – Sécurisation de la configuration des ressources des systèmes d'information	Art. 21.2.e
0 – Administration des systèmes d'information depuis des ressources dédiées	Art. 21.2.e
Objectif de sécurité 20 – Supervision de la sécurité des systèmes d'information	Art. 21.2.b