RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2 – TRANSPOSITION NATIONALE

CONSULTATION DE L'ÉCOSYSTEME DES ACTEURS ÉCONOMIQUES

PHASE 3 : MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSECURITÉ

RÉFÉRENTIEL DE CYBERSECURITÉ POUR LES FUTURS ACTEURS ÉCONOMIQUES ASSUJETTIS À NIS 2

PUBLIC VISÉ :

Fédérations et associations professionnelles ainsi que leurs adhérents

INFORMATION ET AVERTISSEMENT

Ce document rédigé par l'ANSSI présente la synthèse des réflexions internes relatives à la transposition nationale des mesures de gestion des risques cyber requises par la directive NIS 2, dans sa version du 15 novembre 2023. Ce document est un outil de discussion transmis avec le futur écosystème des acteurs économiques régulés dans le cadre du processus de consultation avec les représentants de ces mêmes acteurs économiques. Il ne doit ni être rendu public ni communiqué à l'extérieur du cercle des consultations.

Des explications complémentaires seront données lors du webinaire organisé par l'ANSSI le 16 novembre 2023 avec les fédérations et associations professionnelles afin de préciser la menace cybercriminelle à laquelle il répond, expliquer les fondements juridique et technique ayant permis l'élaboration de ce référentiel et enfin expliquer son fonctionnement.

Les éléments présents dans ce document ne constituent ni une base normative ni des obligations à mettre en œuvre à ce jour.

TABLE DES MATIERES

INFORMATION ET AVERTISSEMENT 2

PRESENTATION GENERALE DU DISPOSITIF DE GESTION DES RISQUES CYBER 4

GLOSSAIRE 5

Objectif de sécurité 1. L'entité recense ses systèmes d'information 8

Objectif de sécurité 2. L'entité dispose d'un cadre de gouvernance de la sécurité numérique 10

Objectif de sécurité 3. l'entité essentielle met en œuvre une approche par les risques 12

Objectif de sécurité 4. L'entité maîtrise son écosystème 14

Objectif de sécurité 5. L'entité essentielle audite la sécurité de ses systèmes d'information réglementés 15

Objectif de sécurité 6. L'entité prend en compte la sécurité numérique dans la gestion de ses ressources humaines 16

Objectif de sécurité 7. L'entité maîtrise ses systèmes d'information réglementés 17

Objectif de sécurité 8. L'entité maîtrise les accès physiques à ses locaux 19

Objectif de sécurité 9. L'entité sécurise l'architecture de ses systèmes d'information réglementés 20

Objectif de sécurité 10. L'entité sécurise les accès distants à ses systèmes d'information réglementés 22

Objectif de sécurité 11. L'entité protège ses systèmes d'information réglementés contre les codes malveillants 23

Objectif de sécurité 12. L'entité essentielle sécurise la configuration des ressources de ses systèmes d'information réglementés 24

Objectif de sécurité 13. L'entité gère les identités et les accès des utilisateurs à ses systèmes d'information réglementés 25

Objectif de sécurité 14. L'entité maîtrise l'administration de ses systèmes d'information réglementés 27

Objectif de sécurité 15. L'entité essentielle réalise les actions d'administration depuis des ressources dédiées 29

Objectif de sécurité 16. L'entité essentielle supervise la sécurité de ses systèmes d'information réglementés 31

Objectif de sécurité 17. L'entité est en capacité de réagir aux incidents de sécurité 33

Objectif de sécurité 18. L'entité dispose de capacité de continuité et de reprise d'activité 35

Objectif de sécurité 19. L'entité est en capacité de réagir aux crises d'origine cyber 36

Objectif de sécurité 20. L'entité dispose de moyens pour vérifier le fonctionnement de ses capacités opérationnelles 38

TABLEAUX DE CORRESPONDANCE 40

PRESENTATION GENERALE DU DISPOSITIF DE GESTION DES RISQUES CYBER

Le présent document détaille l'ensemble des objectifs de sécurité qu'il conviendrait d'atteindre pour les entités essentielles et importantes dans la cadre de la future réglementation NIS2.

Chaque **objectif** de sécurité est accompagné :

- de **justifications** au regard de **risques** associés.
- des **mesures de sécurité** à mettre en œuvre pour atteindre l'objectif, appelées également **moyens acceptables de conformité**
- d'un tableau précisant si les moyens acceptables de conformité sont applicables aux EE et/ou aux EI.

Ci-après, quelques précisions complémentaires :

- **L'objectif de sécurité** est l'obligation à laquelle devrait se conformer l'entité.
  - Il répondrait à la question « Quoi ? ».
  - Son atteinte serait **obligatoire**.
  - Certains objectifs ne s'appliqueraient qu'aux entités essentielles
- **Les justifications et risques associés** sont communiqués uniquement à titre pédagogique
- **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 ?».

GLOSSAIRE

Mot	Définition
Action d'administration	Installation, suppression, modification ou consultation d'une configuration d'une ressource d'un système d'information réglementé susceptible de modifier le fonctionnement ou la sécurité de celui-ci.
Administrateur	Personne physique disposant de droits privilégiés sur un système d'information réglementé, 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 SI et fournissant des mécanismes d'identification et d'authentification. *Par exemple : MICROSOFT ACTIVE DIRECTORY, OPENLDAP.*
Authentification multifacteur	Authentification mettant en œuvre plusieurs facteurs d'authentification parmi les suivants : • 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.
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 fourniture d'un produit/service ou de la non réalisation d'une activité deviennent inacceptables. *En anglais : maximum tolerable period of disruption (MTPD)*
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.
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.

Mot	Définition
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.
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 réglementés. Ce mécanisme s'appuie au minimum sur un facteur d'authentification et peut mettre en œuvre une authentification multifacteur.
Perte de données maximale admissible (PDMA)	Point à partir duquel les informations utilisées par une activité ou un service doivent être restaurées afin de permettre son fonctionnement à la reprise. *En anglais : Recovery point objective (RPO)*
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.
Systèmes d'information tiers	Réseau ou système d'information 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.*
Ressource	Composant d'un système d'information pouvant être matériel (serveur, poste de travail, périphérique, disque) ou logiciel (machine virtuelle, conteneur, application, fichier, information). Dans le cadre de l'Objectif de sécurité 11, la notion de « ressources logicielles » renvoie également aux démons, services, paquets, bibliothèques, greffons et applications.
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, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données.
Système d'information d'administration	Système d'information qui concoure aux actions d'administration des systèmes d'information réglementés.
Système d'information réglementé (SIR)	Système d'information qui concourt aux activités et services de l'entité et pour lesquels 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 par les activités ou services de l'entité ; • L'altération des informations nécessaires aux activités ou services de l'entité.

Mot	Définition
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 réglementé.
Sous-système	Ensemble de composants d'un système d'information réglementés constitués pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIR ou encore pour isoler des ressources d'un SIR ayant un même besoin de sécurité.

OBJECTIF DE SÉCURITÉ 1. L'ENTITE RECENSE SES SYSTEMES D'INFORMATION

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) Le recensement des systèmes d'information réglementés consiste, pour l'entité, en :

- La réalisation d'une cartographie des activités et des services de l'entité et des systèmes les supportant ;
- L'exclusion, si l'entité le décide, des systèmes d'information qui ne sont porteurs d'aucun risque impactant les activités ou les services fournis par l'entité.

Les systèmes d'information qui ne sont pas exclus sont désignés dans la suite du document « *systèmes d'information réglementés* » (ou SIR).

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) La directive NIS 2, s'agissant des mesures de sécurité obligatoires, vise 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[1] traitées par les activités ou services de l'entité ;
- L'altération des informations nécessaires aux activités ou services de l'entité.

MOYENS ACCEPTABLES DE CONFORMITE

		EI	EE
(a)	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 une entité importante ou essentielle (*par exemple : une entité devenue entité essentielle car elle exploite un oléoduc liste, en plus des activités et services participant à l'exploitation de l'oléoduc, toutes 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 ; ○ liste les systèmes d'information les supportant.	Oui	Oui

[1] Est entendu dans le présent texte comme informations sensibles au minimum toute information relative à un secret protégé par la loi (*par exemple : secret médical, propriété intellectuelle, secret bancaire*), à l'exception du secret de la défense nationale, ainsi que les données à caractère personnel sensibles au sens du RGPD. Cette notion peut être élargie à ce que l'entité considère, dans le cadre de ses activités ou des services qu'elle fournit, comme sensible.

		EI	EE
(b)	L'entité peut, au cas par cas et en le justifiant, exclure des systèmes d'information, parmi ceux listés en (a), pour lesquels il n'existe aucun besoin en disponibilité, en intégrité, en confidentialité ou en authenticité dont la non-satisfaction serait susceptible d'entraîner au moins un des risques suivants : • La dégradation ou l'interruption des activités ou services de l'entité ; • La divulgation à des personnes non autorisées d'informations sensibles traitées par les activités ou services de l'entité ; • L'altération des informations nécessaires aux activités ou services de l'entité.	Oui	Oui
(c)	Les systèmes d'information exclus conformément au (c) sont distingués des autres systèmes d'information dans la liste prévue au (a). La justification de l'exclusion doit figurer dans cette liste.	Oui	Oui
(d)	L'entité valide et réexamine annuellement, ou en tant que de besoin notamment en cas de mise en service d'un nouveau système d'information, la pertinence des exclusions prévues en (c).	Oui	Oui

OBJECTIF DE SÉCURITÉ 2. L'ENTITE DISPOSE D'UN CADRE DE GOUVERNANCE DE LA SECURITE NUMERIQUE

DESCRIPTION DE L'OBJECTIF DE SÉCURITE

(quoi, en quoi consiste l'objectif) Placé sous la responsabilité du dirigeant exécutif de l'entité, le cadre de gouvernance de la sécurité numérique consiste en la mise en place, au sein de l'entité :

- D'une organisation claire en termes de rôles et de responsabilités ;
- D'une politique de sécurité des systèmes d'information et des politiques :
  - D'usage du chiffrement,
  - De contrôle d'accès physique et logique,
  - De revue de l'application des mesures de sécurité mises en œuvre,
  - De maintien en condition de sécurité prévues par l'article 21.2 de NIS 2 ;
- De processus de gestion de la conformité.

L'entité communique à l'Agence nationale de la sécurité des systèmes d'information les coordonnées du point de contact, au sein de l'entité, pour les sujets relatifs à la sécurité numérique ainsi que la mise à jour de ces coordonnées.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Ce 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 affecter la réalisation de ses activités ou la fourniture de ses services.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

La mise en place d'un système de management de la sécurité de l'information (SMSI) conforme aux exigences prévues dans la norme ISO/CEI 27001:2022 et dont le domaine d'application couvre au minimum les systèmes d'information réglementés permet d'apporter une présomption de conformité à cet objectif.

ROLES ET RESPONSABILITES

		EI	EE
(a)	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 réglementés aux présentes mesures.	Oui	Oui
(b)	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.	**Non**	Oui
(c)	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*).	Oui	Oui

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION

		EI	EE
(a)	L'entité définit et met en œuvre une politique de sécurité des systèmes d'information (PSSI).	Oui	Oui
(b)	Cette PSSI comprend : • 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 réglementés dont il est responsable ; • L'engagement du dirigeant exécutif de l'entité à assurer la conformité aux exigences légales et réglementaires et en particulier celles définies dans la transposition nationale de la directive NIS 2.	Oui	Oui
(c)	Le dirigeant exécutif de l'entité approuve la PSSI.	Oui	Oui
(d)	La PSSI est revue annuellement et mise à jour lorsque nécessaire, notamment en cas d'évolutions majeures du contexte métier, technique ou organisationnel intervenues après son approbation.	Oui	Oui
(e)	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.	Oui	Oui
(f)	En particulier, et conformément à la directive NIS 2, l'entité définit et met en œuvre 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 maintien en condition de sécurité.	Oui	Oui

GESTION DE LA CONFORMITE

		EI	EE
(a)	Pour chaque système d'information réglementé, l'entité réalise et maintient à jour une analyse de la conformité du système d'information réglementé vis-à-vis des présentes mesures. L'analyse de la conformité identifie les écarts entre les mesures mises en œuvre par l'entité, les présentes mesures et les objectifs fixés par la réglementation.	Oui	Oui
(b)	L'entité établit, met en œuvre et suit dans la durée un plan d'action pour corriger ces écarts et atteindre les objectifs fixés par la réglementation. Ce plan d'action prévoit, au minimum, une échéance et un responsable pour la réalisation de chaque action.	Oui	Oui
(c)	En cas de recours à une ou plusieurs alternatives prévues dans les présentes mesures, l'entité les renseigne dans l'analyse de la conformité avec les justifications associées.	Oui	Oui
(d)	L'entité est capable de démontrer à tout moment l'atteinte des objectifs fixés par la réglementation, notamment en cas de contrôle. L'atteinte des objectifs fixés par la réglementation est présumée lorsque l'entité respecte les présentes mesures. Dans le cas contraire, elle est en capacité de fournir les éléments nécessaires pour démontrer l'atteinte des objectifs fixés par la réglementation.	Oui	Oui

OBJECTIF DE SÉCURITÉ 3. L'ENTITE ESSENTIELLE MET EN ŒUVRE UNE APPROCHE PAR LES RISQUES

DESCRIPTION DE L'OBJECTIF DE SÉCURITE

(quoi, en quoi consiste l'objectif) l'approche par les risques est placée sous la responsabilité du dirigeant exécutif de l'entité et permet à ce dernier :

- De prendre connaissance et de suivre dans le temps :
  - Les risques numériques pesant sur ses systèmes d'information réglementés,
  - Les mesures de sécurité mises en œuvre ou planifiées pour maîtriser ces risques ;
- D'accepter les risques résiduels.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) L'atteinte de cet objectif permet à une entité essentielle de maîtriser les risques numériques pesant sur ces systèmes d'information réglementés 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*).

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

La mise en place d'un système de management de la sécurité des systèmes d'information (SMSI) conforme aux exigences prévues dans la norme ISO/CEI 27001:2022 et dont le domaine d'application couvre au minimum les systèmes d'information réglementés permet d'apporter une présomption de conformité à cet objectif.

Le recours à un prestataire d'accompagnement et de conseil en sécurité (PACS), qualifié 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[2], pour la réalisation de l'analyse de risques dont le périmètre de la prestation couvre au minimum les systèmes d'information réglementés et le suivi par l'entité du plan d'amélioration continue de la sécurité issue de la prestation permettent d'apporter une présomption de conformité à cet objectif.

		EI	EE
(a)	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 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 (cf. Objectif de sécurité 2) 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

[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)

		EI	EE
(b)	L'entité s'assure que chaque système d'information réglementé 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 réglementés supportant cette activité ou ce service. Cette analyse de risques s'appuie sur les éléments issus : • De la PSSI (cf. Objectif de sécurité 2) ; • De la maîtrise de l'écosystème (cf. Objectif de sécurité 4) ; • De la maîtrise du système d'information réglementé (cf. Objectif de sécurité 7) ; • De l'approche par conformité (cf. section Objectif de sécurité 3) ; • Des audits (cf. Objectif de sécurité 5).	**Non**	Oui
(c)	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 et un responsable pour la réalisation de chaque action.	**Non**	Oui
(d)	L'entité réexamine de l'analyse de risques au minimum tous les 3 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 4. L'ENTITE MAITRISE SON ECOSYSTEME

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La maîtrise de l'écosystème consiste, pour l'entité, en la mise en place :

- D'une cartographie des prestataires et fournisseurs informatiques intervenant dans la réalisation des activités ou la fourniture des services de l'entité ;
- De processus visant à prendre en compte la sécurité numérique dans la relation contractuelle avec ces prestataires et fournisseurs.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 réglementés de l'entité.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Note : *a priori (à confirmer dans le cadre des travaux en cours), les moyens acceptables de conformité (ou mesures de sécurité) devraient être portés au niveau infra-règlementaire (par exemple un référentiel autonome). Une accroche réglementaire sera toutefois nécessaire pour prévoir la présomption de conformité aux objectifs en cas de respect des mesures de ce référentiel.*

CARTOGRAPHIE DE L'ECOSYSTEME

		EI	EE
(a)	L'entité définit et maintient à jour une cartographie de l'écosystème dans lequel ses systèmes d'information réglementés 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 ; • La liste des interconnexions avec les systèmes d'information réglementés de l'entité.	Oui	Oui
(b)	L'entité renseigne les coordonnées d'au moins un point de contact pour chaque entrée figurant dans la cartographie de l'écosystème.	Oui	Oui

SECURITE NUMERIQUE DANS LES CONTRATS AVEC LES PRESTATAIRES ET FOURNISSEURS INFORMATIQUES

		EI	EE
(a)	En cas de recours à un prestataire, l'entité s'assure de la conformité de la prestation aux exigences de la directive NIS 2, et dispose des assurances contractuelles de cette conformité. La vérification de la conformité peut s'appuyer sur des audits dont les conditions sont précisées par les moyens acceptables de conformité (b), (d) et (e) relatifs à l'audit (cf. Objectif de sécurité 5).	Oui	Oui

OBJECTIF DE SÉCURITÉ 5. L'ENTITE ESSENTIELLE AUDITE LA SECURITE DE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF

(quoi, en quoi consiste l'objectif) L'entité essentielle audite à intervalle planifié ses systèmes d'information réglementés. Ces audits permettent à l'entité essentielle :

- De vérifier l'atteinte des objectifs fixés par la réglementation ;
- D'évaluer l'exposition de ses systèmes d'information réglementés aux menaces cyber via la vérification de la présence de vulnérabilités sur ces deniers.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Les audits de sécurité permettent de vérifier la conformité des systèmes d'information réglementés aux objectifs fixés par la réglementation ainsi que d'évaluer le niveau de sécurité du système d'information réglementé. En l'absence d'audit, des vulnérabilités peuvent être présentes sur les systèmes d'information réglementés qui, si elles venaient à être exploitées, peuvent entraîner la dégradation ou l'interruption des activités ou des services fournis par l'entité essentielle.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire d'audit en sécurité des systèmes d'information (PASSI), qualifié 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], dont le périmètre de la prestation couvre les systèmes d'information réglementés et l'application des mesures correctives issues de la prestation permettent d'apporter une présomption de conformité à cet objectif.

		EI	EE
(a)	L'entité définit et met en œuvre un programme d'audit et s'assure que l'ensemble de ses systèmes d'information réglementés font l'objet d'un audit au moins tous les trois ans.	**Non**	Oui

(b)	L'audit de sécurité permet :
	• 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

(c)	L'audit de sécurité comprend un test d'intrusion (couvrant au minimum les interfaces exposées à des SI 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
(d)	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
(e)	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 et un responsable pour la réalisation de chaque action.	**Non**	Oui

[3] 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)

OBJECTIF DE SÉCURITÉ 6. L'ENTITE PREND EN COMPTE LA SECURITE NUMERIQUE DANS LA GESTION DE SES RESSOURCES HUMAINES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La prise en compte de la sécurité numérique dans la gestion des ressources humaines consiste, pour l'entité, en :

- La sensibilisation des utilisateurs, ainsi que la formation pour les fonctions les plus critiques, à la sécurité numérique ;
- La mise en place de processus prenant en compte la sécurité numérique dès l'arrivée d'un nouveau personnel et jusqu'à son départ de l'entité.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Par l'atteinte de cet objectif, les utilisateurs sont responsabilisés à l'usage des systèmes d'information réglementés de l'entité. En l'absence d'une telle responsabilisation, les utilisateurs peuvent être à l'origine de comportements dangereux du point de vue de la sécurité numérique (*par exemple : connexion d'un support amovible infecté sur un système d'information réglementé 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.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

		EI	EE
(a)	L'entité définit et met en œuvre une charte d'usage des systèmes d'information, applicable au minimum aux systèmes d'information réglementés, et la rend opposable à chacun des utilisateurs de ces systèmes d'information.	Oui	Oui
(b)	L'entité définit et met en œuvre un programme de sensibilisation à la sécurité numérique de l'ensemble des utilisateurs des systèmes d'information réglementés.	Oui	Oui
(c)	L'entité prévoit des clauses de sécurité dans les contrats de travail.	**Non**	Oui
(d)	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 réglementés. Ce processus prévoit : • La prise de connaissance par le personnel des règles de sécurité en vigueur lors de son 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 accès logiques aux SI et physiques aux locaux et salles.	Oui	Oui
(e)	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 7. L'ENTITE MAITRISE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SÉCURITE

(quoi, en quoi consiste l'objectif) La maîtrise des systèmes d'information réglementés consiste, pour l'entité, en la mise en place :

- D'une ou plusieurs cartographie(s) de ses systèmes d'information réglementés suffisamment détaillée(s) pour faciliter le maintien en condition opérationnelle et de sécurité et améliorer la réactivité de l'entité en cas d'incident de sécurité affectant ces systèmes d'information ;
- De processus de maintien en condition opérationnelle et de sécurité de ses systèmes d'information réglementés incluant notamment la veille sur les vulnérabilités diffusées par l'ANSSI, les fournisseurs et fabricants de produits, les prestataires mandatés ou les CSIRT.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) La ou les cartographie(s) permet(tent) à l'entité de faciliter le maintien en condition opérationnelle et de sécurité des systèmes d'information réglementés 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 de réduire les conséquences de l'incident. L'absence de cartographie expose l'entité au maintien de ressources vulnérables sur ses systèmes d'information réglementés 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 réglementés 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 réglementés qui, si elles venaient à être exploitées, peuvent entraîner la dégradation ou l'interruption des activités ou des services fournis par l'entité.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

CARTOGRAPHIE DES SYSTEMES D'INFORMATION REGLEMENTES

		EI	EE
(a)	L'entité élabore et maintient à jour une cartographie de ses systèmes d'information réglementés dont le niveau de détail est suffisant pour lui permettre : ○ d'assurer le maintien en condition opérationnel 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 dans un délai raisonnable 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*).	**Non**	Oui

MAINTIEN EN CONDITION OPERATIONNELLE ET DE SECURITE

		EI	EE
(a)	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 réglementés.	**Non**	Oui
(b)	L'entité maintient à jour des bases de connaissances des outils de protection contre les codes malveillants (*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*[4]).	Oui	Oui
(c)	L'entité met en œuvre une veille sur les vulnérabilités, les correctifs de sécurité et des mesures d'atténuation préconisées susceptibles de concerner les ressources de ses systèmes d'information réglementés (SIR), 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 matière de cyber sécurité tels que le CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) ou les CSIRT.	Oui	Oui
(d)	L'entité installe sans délai les correctifs de sécurité sur les ressources exposées à des réseaux 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
(e)	L'entité essentielle planifie et installe sur l'ensemble de ses ressources les correctifs de sécurité.	**Non**	Oui
(f)	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.	Oui	Oui
(g)	L'entité installe et maintient à jour les ressources logicielles de ses SIR, y compris les logiciels embarqués, dans des versions supportées par leurs fournisseurs ou leurs fabricants et comportant les mises à jour de sécurité.	Oui	Oui
(h)	L'entité vérifie que toute nouvelle version est téléchargée depuis les ressources mises à disposition par les éditeurs ou les fournisseurs.	Oui	Oui
(i)	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
(j)	L'entité définit et met en œuvre des mécanismes permettant de prendre connaissance, dans les meilleurs délais, des alertes émises par l'Agence nationale de sécurité des systèmes d'information, les éditeurs de produits utilisés par l'entité ou le prestataire mandaté par l'entité.	Oui	Oui
(k)	L'entité s'assure de la mise en œuvre d'une procédure pour traiter ces alertes et le cas échéant appliquer les mesures préconisées.	Oui	Oui

[4] *Endpoint Detection and Response*

OBJECTIF DE SÉCURITÉ 8. L'ENTITE MAITRISE LES ACCES PHYSIQUES A SES LOCAUX

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La maîtrise des accès physiques consiste, pour l'entité, en la mise en place de mécanismes de contrôle d'accès, la mise en œuvre de processus de gestion des droits d'accès et de gestion des visiteurs.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Par l'atteinte de cet objectif, l'entité s'assure que seules les personnes autorisées (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 réglementé par la connexion de supports amovibles infectés.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

		EI	EE
(a)	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.	Oui	Oui
(b)	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
(c)	L'entité s'assure du contrôle des accès aux locaux, aux salles serveurs et aux locaux techniques.	**Non**	Oui
(d)	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
(e)	L'entité s'assure que les personnes externes accédant aux locaux techniques et salles serveurs de l'entité sont accompagnées.	Oui	Oui

OBJECTIF DE SÉCURITÉ 9. L'ENTITE SECURISE L'ARCHITECTURE DE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF

(quoi, en quoi consiste l'objectif) La sécurisation de l'architecture des systèmes d'information consiste, pour l'entité, en :

- L'identification des besoins d'exposition et d'interconnexion des activités et services fournis par l'entité à de réseaux tiers ;
- Le filtrage des communications entrantes et sortantes de ses systèmes d'information réglementés, en particulier les flux dont l'origine, le transit ou la destination est un système d'information tiers.

Pour les entités essentielles, cela consiste également cloisonner les systèmes d'information réglementés en zones de sécurité cohérentes et le contrôle des points d'entrée et de sortie des systèmes d'information réglementés pour les utilisateurs, les prestataires et les fournisseurs.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 réglementés. 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 à des systèmes d'information réglementés depuis la compromission de systèmes d'information non réglementés*). La réalisation des activités de l'entité ou la fourniture de ses services peuvent être dégradées voire interrompues.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

CLOISONNEMENT

		EI	EE
(a)	L'entité cloisonne physiquement ou logiquement l'ensemble de ses systèmes d'information réglementés vis-à-vis des autres systèmes d'information (*les systèmes d'information non réglementés et systèmes d'information tiers*).	Oui	Oui
(b)	L'entité cloisonne physiquement ou logiquement chaque système d'information réglementé vis-à-vis des autres systèmes d'information (*les autres systèmes d'information réglementés, les systèmes d'information non réglementés et systèmes d'information tiers*).	**Non**	Oui
(c)	L'entité mène des réflexions, pour chaque système d'information réglementé, 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
(d)	Les sous-systèmes identifiés à la mesure (b) sont cloisonnés entre eux physiquement ou logiquement.	**Non**	Oui
(e)	L'entité met en œuvre au moins un sous-système "passerelle sortante" permettant : • aux ressources des SIR d'accéder aux SI tiers; • d'authentifier, de filtrer et de tracer les accès aux SI tiers *(par exemple : un serveur mandataire)*.	**Non**	Oui
(f)	L'entité met en œuvre au moins un sous-système "passerelle entrante" permettant : • d'exposer des ressources des SIR aux SI tiers;	**Non**	Oui

	• de filtrer et de tracer les accès depuis des SI tiers *(par exemple : un serveur mandataire inverse ou un relai)*		
(g)	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 réglementés et les autres systèmes d'information.	Oui	Oui
(h)	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 réglementé et les autres systèmes d'information, ou entre les sous-systèmes du système d'information réglementé.	**Non**	Oui

FILTRAGE DES COMMUNICATIONS

		EI	**EE**
(a)	L'entité définit et documente les communications nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle de sécurité circulant entre l'ensemble des systèmes d'information réglementés et les autres systèmes d'information.	Oui	Oui
(b)	L'entité définit et documente les communications nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle de sécurité circulant entre chaque système d'information réglementé et les autres systèmes d'information, ou entre les sous-systèmes du système d'information réglementé.	**Non**	Oui
(c)	L'entité met en œuvre, au niveau des interconnexions, les règles de filtrage pour n'autoriser que les communications identifiées à la mesure (a) ou (b). Les autres communications sont bloquées par défaut.	Oui	Oui
(d)	Au minimum, les communications entre les systèmes d'information réglementés de l'entité et les SI tiers sont filtrés par un ou des pares-feux dédiés à cet usage. (*par exemple : une entité mettant en œuvre un pare-feu pour filtrer les communications entre ses systèmes d'information (réglementés ou non) d'une part et les SI tiers d'autre part est une solution acceptable*)	Oui	Oui
(e)	L'entité effectue annuellement une revue de la mise en œuvre technique des règles de filtrage mentionnées à la mesure (c).	Oui	Oui

OBJECTIF DE SÉCURITÉ 10. L'ENTITE SECURISE LES ACCES DISTANTS A SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La sécurisation des accès distants consiste, pour l'entité, en la mise en place :

- De mécanismes d'identification et d'authentification des personnes accédant aux systèmes d'information réglementés de l'entité depuis des SI tiers (*par exemple : internet ou le système d'information d'un prestataire*) ;
- De mécanismes de sécurisation du canal de communication, des points d'entrée et de sortie et des d'accès aux systèmes d'information réglementés depuis des systèmes d'information tiers.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 SIR *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.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

		EI	EE
(a)	L'entité protège les accès à ses systèmes d'information réglementés (SIR) effectués à travers un système d'information tiers au moyen de mécanismes de chiffrement conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information.	Oui	Oui
(b)	De plus, lorsque les accès visés à la mesure (a) sont effectués par l'entité ou un prestataire qu'elle a mandaté à cet effet, l'entité protège les accès aux SIR par un mécanisme d'authentification conforme aux mesures de l'Objectif de sécurité 13.	Oui	Oui
(c)	Pour les accès visés à la mesure (b), le mécanisme d'authentification s'appuie sur une authentification multifacteur reposant au moins sur un facteur de connaissance.	**Non**	Oui
(d)	Lorsque des raisons techniques ou opérationnelles ne permettent pas la mise en œuvre d'une authentification multifacteur, l'entité met en œuvre des mesures permettant de réduire le risque associé.	**Non**	Oui
(e)	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 au SIR 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 préconisé par l'Agence nationale de la sécurité des systèmes d'information.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 11. L'ENTITE PROTEGE SES SYSTEMES D'INFORMATION REGLEMENTES CONTRE LES CODES MALVEILLANTS

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La protection contre les codes malveillants consiste, pour l'entité, en l'installation ou l'activation de solutions de protection contre les codes malveillants sur les ressources de ses systèmes d'informations réglementés.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) L'atteinte de cet objectif permet à l'entité de se protéger des codes malveillants qui pourraient être introduits sur ses systèmes d'information réglementés (*par exemple : par la mise en œuvre ou l'activation d'un antivirus*).

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

		EI	EE
(a)	Seules les ressources matérielles de l'entité, de ses personnels ou de ses prestataires clairement identifiées et participant à la réalisation des activités ou la fourniture des services de l'entité ou au maintien en condition opérationnelle et de sécurité se connectent aux systèmes d'information réglementés.	Oui	Oui
(b)	Seules les ressources matérielles dont l'entité, ou le prestataire qu'elle a mandaté, assure la gestion et participant à la réalisation des activités ou la fourniture des services de l'entité ou au maintien en condition opérationnelle et de sécurité se connectent aux systèmes d'information réglementés.	**Non**	Oui
(c)	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 (a) sur ses systèmes d'information réglementés.	Oui	Oui
(d)	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 (b) sur ses systèmes d'information réglementés.	**Non**	Oui
(e)	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 réglementés.	Oui	Oui
(f)	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 (comme par exemple les supports amovibles, la messagerie ou la navigation web), disposent de mécanismes de protection contre les risques d'exécution de codes malveillants.	Oui	Oui
(g)	L'entité procède à l'analyse des données provenant de sources externes lors de leur réception, pour y rechercher des codes malveillants.	Oui	Oui

OBJECTIF DE SÉCURITÉ 12. L'ENTITE ESSENTIELLE SECURISE LA CONFIGURATION DES RESSOURCES DE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La sécurisation de la configuration consiste, pour l'entité, en la mise en place de configurations durcies sur les ressources de ses systèmes d'information réglementés.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) En l'absence d'un tel objectif, un attaquant est capable 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 réglementé, 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 l'entité, la divulgation ou l'altération d'informations sensibles.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

		EI	EE
(a)	Seules les ressources logicielles nécessaires à la réalisation des activités et services de l'entité ou au maintien en condition opérationnelle ou de sécurité sont installées ou conservées sur les systèmes d'information réglementés.	**Non**	Oui
(b)	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
(c)	L'entité configure les ressources de ses SIR de manière sécurisée et 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
(d)	L'entité effectue annuellement une revue de configuration des ressources de ses SIR pour vérifier l'application des mesures précédentes. Il est recommandé que cette revue s'appuie sur un ou des outils automatisés.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 13. L'ENTITE GERE LES IDENTITES ET LES ACCES DES UTILISATEURS A SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La gestion des identités et des accès consiste, pour l'entité, en la mise en place :

- De mécanismes d'identification et d'authentification des utilisateurs des systèmes d'information réglementés ainsi que des processus automatiques ;
- De processus de gestion des droits d'accès permettant l'accès aux ressources mises à disposition qu'aux utilisateurs et processus automatiques authentifiés et justifiant d'un besoin opérationnel.

JUSTIFICATION ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) L'atteinte de cet objectif permet à l'entité de maîtriser les utilisateurs accédant à ses systèmes d'information réglementés, que ces derniers soient internes ou externes à l'entité (*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. L'atteinte de cet objectif permet également à l'entité de maîtriser les accès afin que ces 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 ou encore interrompe les activités ou services de l'entité reposant sur ce système d'information.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

IDENTIFICATION

		EI	EE
(a)	Les utilisateurs et les processus automatiques accédant aux ressources des systèmes d'information réglementés (SIR) de l'entité importante ou essentielle disposent de comptes individuels. Les utilisateurs peuvent, le cas échéant, disposer de plusieurs comptes individuels.	Oui	Oui
(b)	L'emploi d'un compte individuel du SIR est réservé à l'utilisateur ou au processus automatique auquel ce compte a été attribué.	Oui	Oui
(c)	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.	Oui	Oui
(d)	Lorsqu'un SIR 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.	Oui	Oui
(e)	L'entité désactive sans délai les comptes qui ne sont plus nécessaires.	Oui	Oui

AUTHENTIFICATION

		EI	EE
(a)	L'entité protège les accès des utilisateurs et processus automatiques aux ressources de ses systèmes d'information réglementés (SIR) au moyen d'un mécanisme d'authentification (*par exemple : un mécanisme d'authentification mono- ou multi-facteur*) impliquant au moins un élément secret (*par exemple : un facteur de connaissance tel qu'un mot de passe*).	Oui	Oui
(b)	L'entité définit, conformément à sa politique de contrôle d'accès physique et logique, les règles de gestion des facteurs d'authentification mis en œuvre dans ses SIR.	Oui	Oui
(c)	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
(d)	L'élément secret d'un compte partagé est renouvelé à chaque retrait d'un utilisateur de ce compte.	Oui	Oui
(e)	L'élément secret d'un compte n'est connu, accessible en clair ou modifiable que des utilisateurs qui en ont la responsabilité.	Oui	Oui
(f)	Les facteurs d'authentification sont conformes à l'état de l'art préconisé par l'Agence nationale de la 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
(g)	L'entité modifie sans délai l'élément secret associé à un compte désactivé.	**Non**	Oui
(h)	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
(i)	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'ACCES

		EI	EE
(a)	L'entité n'attribue des droits qu'aux utilisateurs et processus automatiques authentifiés.	Oui	Oui
(b)	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
(c)	Pour chaque ressource du SIR, 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
(d)	L'entité effectue périodiquement, au moins annuellement, une revue des droits d'accès. Cette revue doit notamment vérifier le respect de la présente mesure et, le cas échéant, corriger les anomalies.	Oui	Oui

OBJECTIF DE SÉCURITÉ 14. L'ENTITE MAITRISE L'ADMINISTRATION DE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La maîtrise de l'administration des systèmes d'information réglementés consiste, pour l'entité ou le prestataire mandaté pour réaliser cette activité, en la mise en œuvre de comptes d'administration dédiés à cet usage est utilisé par les personnes autorisées. Cela consiste également en la sécurisation de l'administration des annuaires qui représente le cœur de confiance des systèmes d'information réglementés de l'entité.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 :

- De désactiver des mesures de sécurité mise en place par l'entité complexifiant les capacités de l'entité à détecter les activités malveillantes sur ses systèmes d'information réglementés ; 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 (réglementés ou non) 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.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

COMPTES D'ADMINISTRATION

Le recours à un prestataire d'administration et de maintenance sécurisée (PAMS), qualifié 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], dont le périmètre de la prestation couvre au minimum les systèmes d'information réglementés permet à l'entité de bénéficier d'une présomption de conformité à cet objectif.

[5] 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)

		EI	EE
(a)	Les actions d'administration sur les systèmes d'information réglementés sont effectuées au moyen de comptes d'administration dédiés à cet usage.	Oui	Oui
(b)	Les comptes d'administration ne sont utilisés que par des administrateurs ou des personnes autorisées.	Oui	Oui
(c)	Les comptes d'administration sont des comptes qui respectent les mesures relatives à l'identification (cf. Objectif de sécurité 13).	Oui	Oui
(d)	Un compte d'administration est utilisé exclusivement pour se connecter à un système d'information d'administration, ou à une ressource pour effectuer des actions d'administration.	Oui	Oui
(e)	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	Oui	Oui
(f)	L'octroi de privilèges administrateur à un compte utilisateur est interdit.	Oui	Oui
(g)	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 spécifique à l'administration.	Oui	Oui
(h)	L'entité met également en œuvre des mesures permettant d'assurer la traçabilité des actions d'administration réalisées.	Oui	Oui
(i)	L'entité établit et tient à jour la liste des comptes d'administration de ses SIR.	Oui	Oui
(j)	L'attribution des droits aux comptes d'administration est limitée aux droits nécessaires aux actions d'administration de ce compte, sur les seuls périmètres techniques et fonctionnels qu'il administre. 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.	Oui	Oui
(k)	Les administrateurs ne réutilisent pas les éléments secrets entre comptes d'administration, ou entre un compte d'administration et un compte utilisateur.	Oui	Oui
(l)	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.	Oui	Oui

SECURITE DES ANNUAIRES

		EI	EE
(a)	La sécurité des systèmes d'information réglementés (SIR) de l'entité repose en grande partie sur la sécurité du ou des annuaires gérant les utilisateurs ou les ressources des SIR. L'ensemble des ressources regroupant ces annuaires, les ressources matérielles et logicielles hébergeant ces annuaires ou permettant de prendre le contrôle de ces annuaires est désigné par « cœur de confiance ».	Oui	Oui
(b)	Les actions d'administration du cœur de confiance sont réalisées *via* des comptes d'administration dédiés exclusivement à cet usage.	Oui	Oui
(c)	Les actions d'administration du cœur de confiance sont réalisées *via* des ressources dédiées exclusivement à cet usage.	Oui	Oui
(d)	Les connexions externes au cœur de confiance, à destination des ressources d'administration du cœur de confiance sont interdites par un dispositif de filtrage sur les ressources d'administration.	Oui	Oui
(e)	L'entité effectue annuellement une revue de la configuration des annuaires gérant les utilisateurs ou les ressources de ses SIR, afin d'identifier tout élément inutile ou anormal. Il est recommandé que cette revue s'appuie sur un outil automatisé.	Oui	Oui

OBJECTIF DE SÉCURITÉ 15. L'ENTITE ESSENTIELLE REALISE LES ACTIONS D'ADMINISTRATION DEPUIS DES RESSOURCES DEDIEES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) Cet objectif consiste, pour l'entité, en la mise en place d'un système d'information dédié à l'administration des systèmes d'information réglementés avec des ressources dédiées à ces actions et maîtrisées par l'entité ou le prestataire qu'elle a mandaté.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) L'atteinte de cet objectif permet à l'entité de s'assurer que les ressources utilisées pour l'administration de ces systèmes d'information réglementés 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 :

- De désactiver des mesures de sécurité mise en place par l'entité complexifiant les capacités de l'entité à détecter les activités malveillantes sur ses systèmes d'information réglementés ; 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.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire d'administration et de maintenance sécurisée (PAMS), qualifié 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[6], dont le périmètre de la prestation couvre au minimum les systèmes d'information réglementés permet à l'entité de bénéficier d'une présomption de conformité à cet objectif.

		EI	EE
(a)	Les actions d'administration sur les systèmes d'information réglementés sont effectuées au moyen d'un système d'information d'administration.	**Non**	Oui
(b)	Les ressources des systèmes d'information d'administration sont gérées et configurées par l'entité ou le prestataire qu'elle a mandaté pour réaliser les actions d'administration.	**Non**	Oui
(c)	Les ressources matérielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des actions d'administration.	**Non**	Oui
(d)	Le système d'exploitation utilisé pour effectuer des actions d'administration est utilisé exclusivement pour réaliser des actions d'administration.	**Non**	Oui
(e)	La connexion des administrateurs à un système d'information d'administration s'effectue au moyen d'un système d'exploitation utilisé exclusivement pour des actions d'administration.	**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)

		EI	EE
(f)	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.	**Non**	Oui
(g)	Les systèmes d'information d'administration sont connectés aux ressources du SIR 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
(h)	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.	**Non**	Oui
(i)	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 celui préconisé par l'Agence nationale de la sécurité des systèmes d'information.	**Non**	Oui
(j)	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 préconisées par l'Agence nationale de la sécurité des systèmes d'information.	**Non**	Oui
(k)	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 16. L'ENTITE ESSENTIELLE SUPERVISE LA SECURITE DE SES SYSTEMES D'INFORMATION REGLEMENTES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La supervision de sécurité consiste, pour l'entité essentielle, en la mise en place de moyens de journalisation, de détection et d'analyse des événements de sécurité sur ses systèmes d'information réglementés.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 réglementés. 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 l'entité*).

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire de détection des incidents de sécurité (PDIS), qualifié 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[7], dont le périmètre de la prestation couvre au minimum les systèmes d'information réglementés permet d'apporter une présomption de conformité à cet objectif.

		EI	EE
(a)	L'entité essentielle élabore, tient à jour et met en œuvre, conformément à sa politique de sécurité des systèmes d'information, une procédure de détection des incidents de sécurité susceptibles d'affecter ses systèmes d'information réglementés (SIR).	**Non**	Oui
(b)	Cette procédure prévoit des mesures organisationnelles et techniques destinées à détecter les incidents de sécurité. Les mesures organisationnelles comprennent les modalités : • De collecte des journaux nécessaires à la détection ; • D'exploitation des dispositifs de détection ; • D'analyse des événements de sécurité ; • D'amélioration des techniques de détection dans le temps. Les mesures techniques précisent notamment la nature et le positionnement des dispositifs de détection.	**Non**	Oui
(c)	Pour chacun de ses SIR, l'entité essentielle configure les ressources suivantes afin qu'ils journalisent des évènements de sécurité : • Les serveurs applicatifs ; • Les serveurs d'infrastructure ; • Les équipements de sécurité ; • Les équipements réseau ; • Les postes de travail des administrateurs ;	**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)

		EI	EE
	• Les stations d'ingénierie, les postes de maintenance et les consoles de programmation des systèmes industriels et des systèmes de sûreté des personnes et des installations. Les évènements de sécurité issus de ces ressources incluent au moins les évènements liés : • À l'authentification des utilisateurs ; • À la gestion des comptes et des droits d'accès ; • À l'accès aux ressources ; • Aux modifications des règles de sécurité du SIR ; • Au fonctionnement du SIR. Les journaux et événements de sécurité sont configurés de façon à ne pas enregistrer des champs supposés inclure des mots de passe ou autres éléments secrets d'authentification, en clair ou sous forme d'empreinte cryptographique.		
(d)	L'entité met en œuvre des dispositifs de détection analysant notamment l'ensemble des communications entre les SIR et les systèmes d'information tiers. L'entité essentielle veille à ce que l'installation et l'exploitation de ces dispositifs de détection n'affectent pas la sécurité et le fonctionnement de ses SIR. L'entité essentielle s'assure que les événements de sécurité issus des journaux et des dispositifs de détections sont horodatés au moyen de sources de temps synchronisées.	**Non**	Oui
(e)	L'entité essentielle enregistre et centralise les événements de sécurité issus des journaux et des dispositifs de détection de ses SIR dans un système de corrélation et d'analyse. Le système d'analyse conserve les événements de sécurité sur une durée d'au moins six mois, notamment pour permettre une exploitation à postériori. Le système d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection des incidents de sécurité.	**Non**	Oui
(f)	Dans le cas particulier d'un SIR en charge du transit de communications pour le compte de tiers (par exemple l'appairage pour l'échange de trafic internet), l'entité essentielle ne met en œuvre des dispositifs de détection que pour les flux de données autres que ceux correspondant aux flux des tiers.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 17. L'ENTITE EST EN CAPACITE DE REAGIR AUX INCIDENTS DE SECURITE

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La capacité de réagir aux incidents de sécurité consiste, pour l'entité, en la mise en place d'une organisation, de processus et d'outils adaptés à la gestion de ce type d'événements.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Cet objectif permet à l'entité de se préparer, de s'organiser pour faire face à des événements adverses 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.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire d'assistance et de conseil en sécurité (PACS), qualifié 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], 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.

		EI	EE
(a)	Le dirigeant exécutif de l'entité désigne un ou plusieurs points de contact sur les sujets relatifs à la sécurité numérique. L'entité communique à l'Agence nationale de la sécurité des systèmes d'information et, le cas échéant, aux autorités nationales compétentes les coordonnées de ces points de contact et leurs mises à jour.	Oui	Oui
(b)	Le dirigeant exécutif de l'entité essentielle 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 réglementés.	**Non**	Oui
(c)	Le dirigeant exécutif de l'entité s'assure de la notification des incidents qui ont ou sont susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ses activités et de ces services *via* le guichet mis à sa disposition par l'Agence nationale de la sécurité des systèmes d'information.	Oui	Oui
(d)	Le dirigeant exécutif de 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 ou fournisseurs contractant avec l'entité essentielle.	**Non**	Oui
(e)	Le dirigeant exécutif de l'entité essentielle 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.	**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)

		EI	EE
(f)	Le dirigeant exécutif de l'entité essentielle 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
(g)	Après chaque incident majeur, le dirigeant exécutif de l'entité essentielle s'assure 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.	**Non**	Oui
(h)	L'entité conserve les relevés techniques produits 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	Oui
(i)	Un système d'information spécifique doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système est cloisonné vis-à-vis du système d'information réglementé concerné par l'incident.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 18. L'ENTITE DISPOSE DE CAPACITE DE CONTINUITE ET DE REPRISE D'ACTIVITE

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La capacité de continuité et de reprise d'activité consiste, pour l'entité, en la mise en place :

- de mécanismes de sauvegarde et de restauration opérationnels et testés régulièrement ;
- de plans de continuité et de reprise d'activité.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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*).

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Note : *a priori (à confirmer dans le cadre des travaux en cours), les moyens acceptables de conformité (ou mesures de sécurité) devraient être portés au niveau infra-règlementaire (par exemple un référentiel autonome). Une accroche réglementaire sera toutefois nécessaire pour prévoir la présomption de conformité aux objectifs en cas de respect des mesures de ce référentiel*

		EI	EE
(a)	L'entité définit et met en œuvre des procédures de sauvegarde et de restauration de ses systèmes d'information réglementés (SIR) et des données qu'ils manipulent.	Oui	Oui
(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
(c)	L'entité s'assure que le processus de sauvegardes est testé au minimum une fois par an. Ces tests visent notamment à vérifier la bonne réalisation des sauvegardes et leur bonne restauration.	Oui	Oui
(d)	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
(e)	L'entité, pour chacun de ses activités et services, définit et documente la durée maximale d'interruption admissible (DMIA) et la perte de données maximale admissible (PDMA).	**Non**	Oui
(f)	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 avec la durée maximale d'interruption admissible et la perte de données maximale admissible.	**Non**	Oui
(g)	L'identification de ces mesures de continuité s'appuie notamment : • Sur la cartographie de l'écosystème (cf. Objectif de sécurité 4) ; • 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 19. L'ENTITE EST EN CAPACITE DE REAGIR AUX CRISES D'ORIGINE CYBER

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La capacité de réagir aux crises d'origine cyber consiste, pour l'entité, en la mise en place d'une organisation, de processus et d'outils adaptés à la gestion de ce type d'événements.

JUSTIFICATIONS ET RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) Cet objectif permet à l'entité de se préparer, de s'organiser pour faire face à des événements adverses 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 des activités et services fournis par l'entité.

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire d'assistance et de conseil en sécurité (PACS), qualifié 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[9], 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.

		EI	EE
(a)	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 les systèmes d'information réglementés.	Oui	Oui
(b)	L'entité s'assure du maintien à jour d'une liste des personnes mobilisables dans la gestion de la crise sur les sujets relatifs à la sécurité numérique ainsi que leurs coordonnées.	Oui	Oui
(c)	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. Ces informations sont tenues à la disposition des autorités nationales compétentes et en particulier de l'Agence nationale de la sécurité des systèmes d'information.	Oui	Oui
(d)	L'entité s'assure de la définition et de la mise en œuvre des mécanismes 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
(e)	L'entité essentielle s'assure de la définition 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
(f)	L'entité essentielle s'assure de la définition 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'Agence nationale de la sécurité des systèmes d'information.	**Non**	Oui

[9] 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)

(g)	L'entité essentielle 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 réglementés 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
(h)	L'entité essentielle 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
(i)	L'entité essentielle s'assure de la disponibilité de moyens de communication de secours en temps de crise lorsque les moyens de communication habituels sont indisponibles.	**Non**	Oui

OBJECTIF DE SÉCURITÉ 20. L'ENTITE DISPOSE DE MOYENS POUR VERIFIER LE FONCTIONNEMENT DE SES CAPACITES OPERATIONNELLES

DESCRIPTION DE L'OBJECTIF DE SECURITE

(quoi, en quoi consiste l'objectif) La vérification des capacités opérationnelles consiste, pour l'entité, en la mise en place d'exercices et d'entraînements à intervalles planifiés pour tester la préparation de l'entité en cas d'incident de sécurité ou de crises d'origine cyber.

JUSTIFICATIONS / RISQUES ASSOCIES

(pourquoi, la finalité = justification et risques adressés) 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 de crises 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*).

MOYENS ACCEPTABLES DE CONFORMITE / MESURES DE SECURITE

Le recours à un prestataire d'assistance et de conseil en sécurité (PACS), qualifié 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[10], 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.

		EI	EE
(a)	L'entité s'assure de la sensibilisation et de l'entraînement des personnes mobilisables dans le dispositif de gestion des crises d'origine cyber.	Oui	Oui
(b)	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 exigés dans les présentes règles à entraîner et/ou à tester ; • Une liste d'exercices permettant d'entraîner ou de tester les capacités opérationnelles ; • 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.	**Non**	Oui
(c)	Cette stratégie d'entraînement vise à tester les dispositifs mis en œuvre par l'entité essentielle 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
(d)	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.	**Non**	Oui

[10] 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)

	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.		

TABLEAUX DE CORRESPONDANCE

REPARTITION DES OBJECTIFS DANS LE MODELE GOUVERNANCE / PROTECTION / DEFENSE / RESILIENCE

Pilier	Objectif
Gouvernance	Objectif de sécurité 1 – L'entité recense ses systèmes d'information
	Objectif de sécurité 2 – L'entité dispose d'un cadre de gouvernance de la sécurité numérique
	Objectif de sécurité 3 – l'entité essentielle met en œuvre une approche par les risques
	Objectif de sécurité 4 – L'entité maîtrise son écosystème
	Objectif de sécurité 5 – L'entité essentielle audite la sécurité de ses systèmes d'information réglementés
	Objectif de sécurité 6 – L'entité prend en compte la sécurité numérique dans la gestion de ses ressources humaines
Protection	Objectif de sécurité 7 – L'entité maîtrise ses systèmes d'information réglementés
	Objectif de sécurité 8 – L'entité maîtrise les accès physiques à ses locaux
	Objectif de sécurité 9 – L'entité sécurise l'architecture de ses systèmes d'information réglementés
	Objectif de sécurité 10 – L'entité sécurise les accès distants à ses systèmes d'information réglementés
	Objectif de sécurité 11 – L'entité protège ses systèmes d'information réglementés contre les codes malveillants
	Objectif de sécurité 12 – L'entité essentielle sécurise la configuration des ressources de ses systèmes d'information réglementés
	Objectif de sécurité 13 – L'entité gère les identités et les accès des utilisateurs à ses systèmes d'information réglementés
	Objectif de sécurité 14 – L'entité maîtrise l'administration de ses systèmes d'information réglementés
Défense	Objectif de sécurité 15 – L'entité essentielle réalise les actions d'administration depuis des ressources dédiées
	Objectif de sécurité 16 – L'entité essentielle supervise la sécurité de ses systèmes d'information réglementés
	Objectif de sécurité 17 – L'entité est en capacité de réagir aux incidents de sécurité
Résilience	Objectif de sécurité 18 – L'entité dispose de capacité de continuité et de reprise d'activité
	Objectif de sécurité 19 – L'entité est en capacité de réagir aux crises d'origine cyber
	Objectif de sécurité 20 – L'entité dispose de moyens pour vérifier le fonctionnement de ses capacités opérationnelles

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 8
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 3
Art. 21.2.b : la gestion des incidents	Objectif de sécurité 16 Objectif de sécurité 17 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 18 Objectif de sécurité 19 Objectif de sécurité 20
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 4
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 7 Objectif de sécurité 9 Objectif de sécurité 10 Objectif de sécurité 11 Objectif de sécurité 12 Objectif de sécurité 13 Objectif de sécurité 14 Objectif de sécurité 15
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 2 Objectif de sécurité 5
Art. 21.2.g : les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité	Objectif de sécurité 6 Objectif de sécurité 20
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 9 Objectif de sécurité 10
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 4 Objectif de sécurité 7 Objectif de sécurité 13 Objectif de sécurité 14
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 10 Objectif de sécurité 13 Objectif de sécurité 19

CORRESPONDANCES MESURES NATIONALES – MESURES NIS 2

Mesures nationales	Mesures NIS 2
Objectif de sécurité 2 – L'entité recense ses systèmes d'information	Art. 21.2.i
Objectif de sécurité 2 – L'entité dispose 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 - l'entité essentielle met en œuvre une approche par les risques	Art. 21.2.a
Objectif de sécurité 4 – L'entité maîtrise son écosystème	Art. 21.2.d Art. 21.2.i
Objectif de sécurité 5 – L'entité essentielle audite la sécurité de ses systèmes d'information réglementés	Art. 21.2.f
Objectif de sécurité 6 – L'entité prend en compte la sécurité numérique dans la gestion de ses ressources humaines	Art. 21.2.g
Objectif de sécurité 7 – L'entité maîtrise ses systèmes d'information réglementés	Art. 21.2.e Art. 21.2.i
Objectif de sécurité 8 – L'entité maîtrise les accès physiques à ses locaux	Art. 21.2
Objectif de sécurité 9 – L'entité sécurise l'architecture de ses systèmes d'information réglementés	Art. 21.2.e Art. 21.2.h
Objectif de sécurité 10 – L'entité sécurise les accès distants à ses systèmes d'information réglementés	Art. 21.2.e Art. 21.2.h Art. 21.2.j
Objectif de sécurité 11 – L'entité protège ses systèmes d'information réglementés contre les codes malveillants	Art. 21.2.e
Objectif de sécurité 12 – L'entité essentielle sécurise la configuration des ressources de ses systèmes d'information réglementés	Art. 21.2.e
Objectif de sécurité 13 – L'entité gère les identités et les accès des utilisateurs à ses systèmes d'information réglementés	Art. 21.2.e Art. 21.2.i Art. 21.2.j
Objectif de sécurité 14 – L'entité maîtrise l'administration de ses systèmes d'information réglementés	Art. 21.2.e Art. 21.2.i
Objectif de sécurité 15 – L'entité essentielle réalise les actions d'administration depuis des ressources dédiées	Art. 21.2.e
Objectif de sécurité 16 – L'entité essentielle supervise la sécurité de ses systèmes d'information réglementés	Art. 21.2.b
Objectif de sécurité 17 – L'entité est en capacité de réagir aux incidents de sécurité	Art. 21.2.b
Objectif de sécurité 18 – L'entité dispose de capacité de continuité et de reprise d'activité	Art. 21.2.c
Objectif de sécurité 19 – L'entité est en capacité de réagir aux crises d'origine cyber	Art. 21.2.c Art. 21.2.j
Objectif de sécurité 20 – L'entité dispose de moyens pour vérifier le fonctionnement de ses capacités opérationnelles	Art. 21.2.b Art. 21.2.c Art. 21.2.g