ADN 35

NIS 2, du texte à la mise en pratique, théorie et retour d'expérience

Mercredi 02 Juillet 2025

Partagez votre expérience :
@adnouest

Christian QUIVY

CGI

Directeur Conseil
Expert Cybersécurité

Clément DESDEVISES

NIJI

Digital Account Manager

Stéphane NORGEOT

CD35

Directeur des Systèmes
Numériques

Déroulé

9h30 | Présentation de la réglementation NIS2 - Retransmission depuis Nantes

Régis Dubrulle, Délégué régional sécurité numérique Pays de la Loire à l'ANSSI

10h00 | Mise en oeuvre de NIS2

Christian Quivy, CGI

10h20 | REX Analyse d'écart

Guillaume Mouty, NIJI ; Stéphane Norgeot, CD35 ; Clément Le Corre, CD35

11h00 | Fin

Mise en oeuvre de NIS 2

Christian Quivy

CGI

Directeur Conseil Expert Cybersécurité

Pour une entreprise conforme au GHI de l'ANSII

Différence : NIS 2 introduit des exigences plus larges et structurées, tout particulièrement en matière de gouvernance, de gestion de crise et réaction à incident, de pilotage de la cybersécurité, et de la chaîne d'approvisionnement.

Mise en conformité NIS 2 étape par étape (sur la base d'une évaluation des écarts / GHI) :

1. **renforcer sa gouvernance Cyber en impliquant le CoDir / DG** (exigence explicite du NIS 2), nommer un RSSI, définir les rôles et responsabilités, intégrer la gestion des risques et son pilotage ;
2. **gérer les risques cyber** en formalisant une démarche d'évaluation et gestion des risques (tracer les évaluations et actualisation) ;
3. **intégrer la supply-chain** à la cybersécurité et contractualiser les clauses de sécurité avec les prestataires stratégiques ;
4. **préparer et tester une procédure de gestions de crise** Cyber (détecter, répondre, notifier) et le plan de communication interne/externe sur incident
5. **former et sensibiliser** en continue tous les utilisateurs, y compris le CoDir ;
6. **assurer la continuité d'activité** en précisant les modalités de sauvegarde, de restauration et de continuité des activités critiques ;
7. **centraliser et formaliser** les politiques, processus, preuves d'application et tests menés (audit, contrôle, exercice…) pour prouver sa conformité.

Pour une entreprise certifiée ISO 27001:2022

Différence : ISO 27001 est une solide base à l'introduction du NIS 2 qui prévoit des exigences additionnelles sur la gouvernance, la notification d'incidents et les responsabilités.

Mise en conformité NIS 2 étape par étape (sur la base d'une évaluation des écarts / GHI) :

1. **Adapter sa gouvernance Cyber** pour formaliser l'implication du CoDir / DG (exigence du NIS 2)
2. **Mettre à jour la politique de notification d'incidents selon les délais du NIS 2** (préparer des scenarii, procédures et moyens d'alerte à l'autorité) ;
3. **Revoir et compléter les clauses de sécurité** dans les contrats fournisseurs stratégiques ;
4. **Tester et améliorer la gestion de crise et la communication** interne/externe sur incident majeur ;
5. **Mettre à jour le corpus documentaire** (preuves, procédures, plans de réponse).

Astuce pour se déclarer auprès de l'ANSSI

Point d'attention : des **écarts au GHI ou à l'ISO 27002:2022** sont possibles, il faut donc **évaluer leurs impacts sur la mise en conformité NIS 2**.

NIS 2 obligera à fournir diverses informations : **l'ANSSI évaluera votre investissement en cybersécurité.**

Anticiper les livrables suivants :

1. **roadmap stratégique de mise en conformité** (jalons, pilote, budget estimatif…) ;
2. **plan d'actions pluriannuel** et détaillé (priorité, remédiation, planning, responsabilités type RACI) ;
3. **tableau de bord** de suivi de la mise en conformité et rapport d'avancement ou d'étape qui intègre les parties prenantes.

Associer la direction et les métiers : **aligner la conformité NIS 2** aux métiers et aux enjeux de l'organisation, **faciliter l'acceptation** des nouvelles exigences.
Un écart de conformité est toujours possible s'il est justifié et acceptable (ne remet pas en cause les principes Cyber ou n'introduit pas une faille).

Synthèse des écarts NIS 2 / GHI

Exigence NIS 2	Réponse/Contrôle GHI ANSSI	Écart/Besoin complémentaire NIS 2
Gouvernance cybersécurité impliquant la direction	Recommandation GHI 1.3 : organiser une instance de pilotage	NIS 2 impose rôle formel du CODIR dans la gouvernance
Désignation formelle d'un RSSI/CISO	GHI 1.1 : nommer un responsable sécurité	Préciser rattachement hiérarchique au plus haut niveau décisionnel
Politique de cybersécurité documentée	GHI 1.2 : établir une politique de sécurité	Adapter la politique aux exigences de la directive européenne
Gestion des risques régulière	GHI 2.1 : réaliser une analyse de risques périodique	Inclure explicitement la chaîne d'approvisionnement et tiers critiques
Plan de gestion de crise et continuité d'activité cyber	GHI 5.1 : mettre en place PCA/PRA	Tester spécifiquement les scénarios cyber et notification interne/externe
Notification incidents majeurs aux autorités (24h/72h)	GHI 5.2 : signaler incidents graves à la DSI	Ajouter processus de notification directe à l'ANSSI/autorité compétente
Sécurité de la chaîne d'approvisionnement	GHI 3.3 : contrôler les fournisseurs	Contractualiser des clauses de cybersécurité obligatoires et audits tiers
Sensibilisation et formation continue	GHI 4.1 : formation initiale et recyclage annuel	Étendre la formation au CODIR et aux parties prenantes clés
Documentation et traçabilité des preuves de conformité	GHI 6.1 : conserver journaux et rapports d'audit	Formaliser un registre de conformité dédié NIS 2
Amélioration continue selon évolutions menaces	GHI 7.1 : mettre à jour périodiquement le référentiel	Intégrer retours d'incidents et exercices pour NIS 2

Synthèse des écarts NIS 2 / ISO 27001:2022

Exigence NIS 2	Réponse ou contrôle ISO 27001:2022	Écart ou réalisation complémentaire à prévoir
Gouvernance de la cybersécurité impliquant la direction	Leadership, context (clauses 5.1, 4.1, 4.2)	NIS 2 demande une implication plus directe
Désignation formelle d'un RSSI ou responsable cybersécurité	Clause 5.3, Annexe A.5.1	Préciser rôle, statut et rattachement à la direction
Politique de cybersécurité documentée	Clauses 5.2, 6.1.3, Annexe A.5.1	Généré par l'ISO 27001
Gestion des risques régulière	Clauses 6.1.2/6.1.3 – Annexe A.8.2	Renforcer la prise en compte de la chaîne d'approvisionnement
Plan de gestion de crise cybersécurité et de continuité d'activité	Annexe A.5.29/A.5.30, Clauses 8.2-8.3	Adapter aux scénarios cyber et exigences NIS 2 (test, notification)
Notification rapide (24h/72h) des incidents majeurs aux autorités	Clauses 16.1, 6.1.3, Annexe A.5.24	Adapter pour notification "autorité" et non seulement clients/fournisseurs
Sécurité de la chaîne d'approvisionnement et contractualisation	Annexe A.5.19, A.5.20	Clauses plus explicites à formaliser pour la NIS 2
Sensibilisation et formation	Annexe A.6.3, A.7.2	Élargir la cible pour inclure CODIR et responsables critiques
Surélévation reporting, tableau de bord, documentation de conformité	Clauses 9.1, 10.1, Annexe A.5.34/A.5.35	Renforcer la visibilité et le suivi des livrables NIS 2
Communication en gestion de crise	Annexe A.5.26, A.8.2, Clauses 7.4	Scénarios de gestion de crise cyber explicitement testés
Renforcement continu selon évolution des menaces	Clause 10.1, 10.2 (amélioration continue)	Alignement ISO 27001, formaliser la mise à jour NIS 2

Avez-vous des questions ?

REX Analyse d'écart NIS 2
NIJI - CD35

Guillaume MOUTY

NIJI

Consultant Cybersécurité - RSSI

Stéphane NORGEOT

CD35

Directeur des Systèmes Numériques chez Département d'Ille-et-Vilaine

Clément LE CORRE

CD35

Responsable de la Sécurité des Systèmes d'Information au Département d'Ille-et-Vilaine - RSSI

Directive NIS 2 : l'essentiel

Applicabilité

- → Partiellement applicable en 2024
- → 18 secteurs d'activité concernés (voir Annexe Directive) avec application de seuils (CA + Nombre collaborateurs)
- → Transposition nécessaire pour désigner les entités publiques concernées

Ambitions NIS2

- → Améliorer la résilience des entités publiques et privées implantées sur le territoire de l'UE
- → Assurer une uniformisation des législations et des pratiques entre Etats
- → Améliorer la coopération et la réactivité des Etats membres

Objectifs pour l'entité

- → Gouverner la sécurité de l'information de l'entité
- → Protéger ses ressources
- → Se défendre en cas d'attaque
- → Assurer la résilience des activités de l'entité

Directive NIS 2 : l'essentiel

Déployer une gouvernance sécurité à haut niveau

- Impliquer la direction (« dirigeant exécutif de l'entité »)
- Par défaut, un SIR couvre l'intégralité du SI de l'entité (avec possibilité d'exclusion)
- Se déclarer à l'ANSSI et mettre en place un mécanisme de déclaration des incidents

Mettre en place une logique d'amélioration continue

- Documenter
- Contrôler/mesurer
- Améliorer/mettre à jour les pratiques

Maîtriser son écosystème

- Écosystème interne : RH, moyens généraux…
- Écosystème externe avec répercussion des exigences sur les fournisseurs et les partenaires (à la charge de l'entité)

Assurer la conduite du changement

- Sensibiliser et former les collaborateurs et les dirigeants
- Accompagner les restrictions d'usages et les contraintes
- Saisir l'opportunité de réinterroger/simplifier les processus

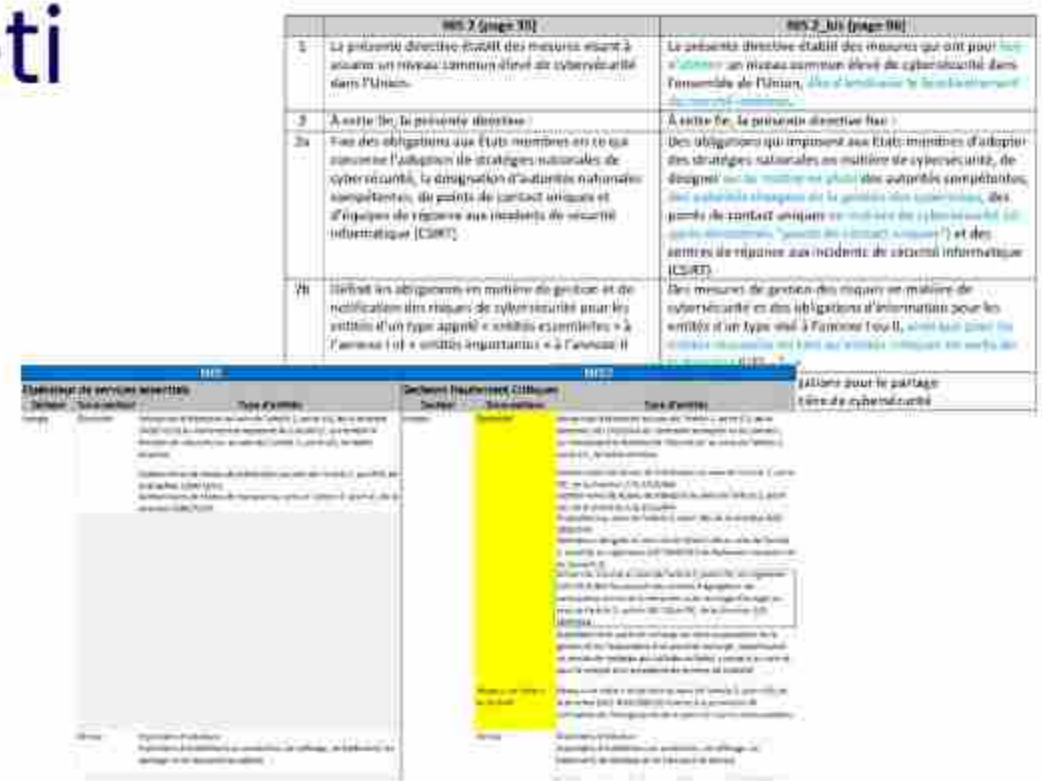
1 | Notre appropriation NIS 2

Réception par Imineti

Analyse du fond

Avant le vote de la commission analyse approfondie de la directive

- → Analyse comparative de NIS et NIS2 puis des évolutions du texte
- → Tableaux comparatifs des annexes, des sanctions et pouvoirs de contrôle
- → Elaboration d'une synthèse des actions à réaliser pour les entités



	NIS 2 (page 33)	NIS 2_bis (page 86)
1	La présente directive établit des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union.	La présente directive établit des mesures qui ont pour but d'assurer un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur.
2	À cette fin, la présente directive :	À cette fin, la présente directive fixe :
2a	Fixe des obligations aux États membres en ce qui concerne l'adoption de stratégies nationales de cybersécurité, la désignation d'autorités nationales compétentes, de points de contact uniques et d'équipes de réponse aux incidents de sécurité informatique (CSIRT) ;	Des obligations qui imposent aux États membres d'adopter des stratégies nationales en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité (ci-après dénommés "points de contact uniques") et des centres de réponse aux incidents de sécurité informatique (CSIRT) ;
2b	Définit les obligations en matière de gestion et de notification des risques de cybersécurité pour les entités d'un type appelé « entités essentielles » à l'annexe I et « entités importantes » à l'annexe II	Des mesures de gestion des risques en matière de cybersécurité et des obligations d'information pour les entités d'un type visé à l'annexe I ou II, ainsi que pour les entités recensées en tant qu'entités critiques en vertu de la directive (UE) [...] ;
		plations pour le partage tière de cybersécurité

Tableau des différences de pouvoir des autorités nationales (ex

	Entité essentielle (Art 32)	Entité importante (Art 33)
Surveillance	a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés	a) des inspections sur place et des contrôles à distance ou par, effectués par des professionnels formés
	b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou une autorité compétente	
		b) des audits de sécurité ciblés réalisés par un organisme indépendant ou une autorité compétente

Publication d'un premier article suivi d'intervention devant plusieurs groupes de travail ou rencontre IT Fin 2023

Construction d'une expertise

Comme toute procédure législative

- manque de visibilité et de précision
- nécessité de creuser et d'analyser les avis de tous les « experts »

Au début temporisation par manque de connaissances et d'exigences concrètes

Initiatives de l'ANSSI

- Organisation de groupes de travail par secteurs d'activité
- Communication des 20 objectifs
- 1ere mission à partir des objectifs transmis au CD35

Etudes des transpositions européennes

- Belgique
- Grèce

Elaboration d'une doctrine Imineti

- Clients cherchaient des réponses toutes faites et rapides et certains éditeurs proposaient des solutions et services mettant « en conformité »
- Attention à être clair avec les clients sur le caractère non définitif et sur les interprétations réalisées

Construction d'une offre pour les différentes entités

DEMARRAGE

APPLICABILITE DE LA DIRECTIVE

Objectifs :

- Identifier les activités concernées par la Directive
- Définir le périmètre du SIH

FORMATION/SENSIBILISATION

Objectifs :

- Former le responsable de la sécurité aux attentes de la directive
- Sensibiliser la Direction aux enjeux de NIS2
- Expliciter le rôle de la Direction dans la démarche

EVALUATION DES ECARTS DE CONFORMITE

Objectifs :

- Analyser l'écart entre les pratiques et les attendus de la Directive
- Etablir une feuille de route macro
- Identifier la charge nécessaire pour la mise en conformité

MISE EN CONFORMITÉ

ANIMATION

Objectifs :

- Coordonner les différents intervenants concernés
- Mesurer et rendre compte de l'avancement des travaux
- Structurer les étapes de la mise en conformité

FACTORIEL

Objectifs :

- Mobiliser l'ensemble des intervenants concernés
- Réaliser les actions structurantes créant un cadre propice à l'atteinte des objectifs

MISE EN CONFORMITE COMPLETE

Objectifs :

- Déléguer sa mise en conformité selon ses besoins
- Identifier ses forces et pallier ses faiblesses

INITIALISATION | Evaluation des écarts

Objectifs

- → Analyser l'écart entre les pratiques et les attendus de la Directive
- → Etablir une feuille de route macro
- → Identifier la charge nécessaire pour la mise en conformité

Méthodologie

1. Comprendre le contexte de l'entreprise et son organisation
2. Auditer les architectures et pratiques existantes
3. Évaluer le niveau de conformité via à vis de la directive
4. Etablir les chantiers à mener à travers une feuille de route

Prérequis

- Périmètre du SIR
- Interlocuteur SSI identifié

Nos savoirs faire

- Expertise d'audits organisationnels (NIS2, ISO 27001, HDS)
- Expertise d'audits d'architectures et de configurations (NIS2, Secnumcloud, HDS)

Livrables

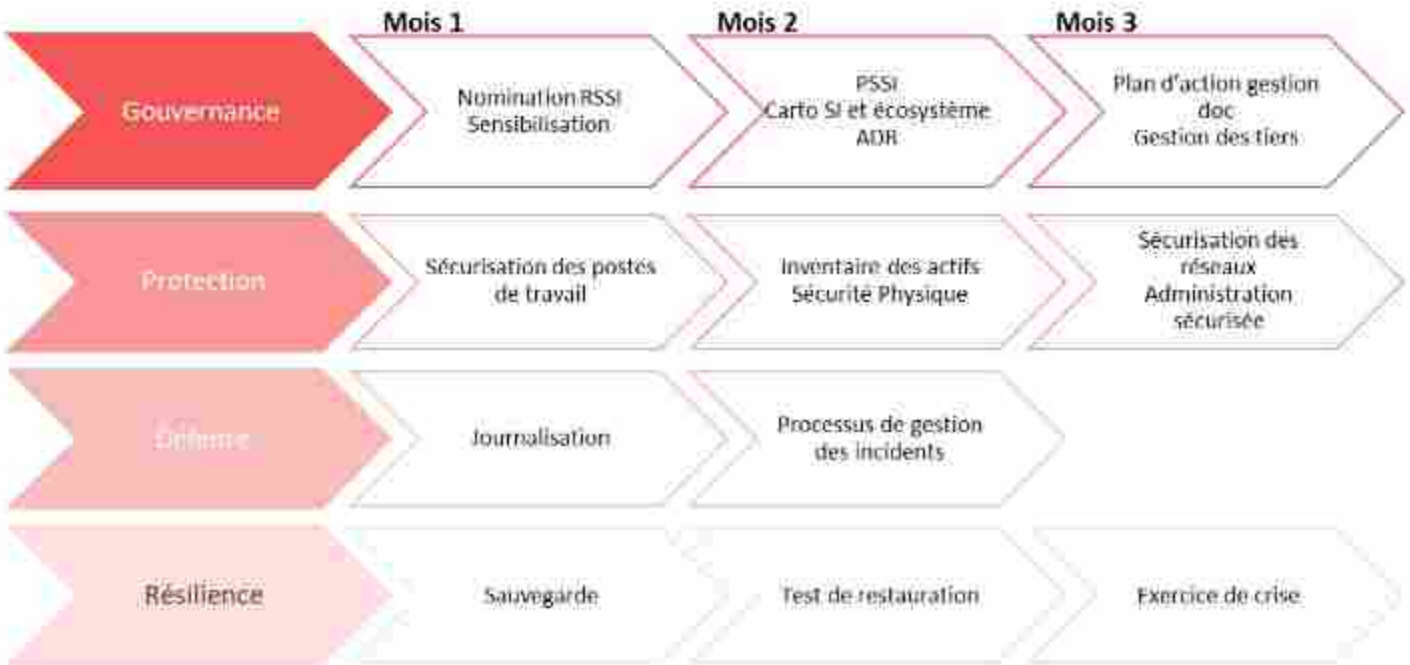
- Rapport d'écarts de conformité
- Feuille de route macro avec les charges associées

MISE EN CONFORMITÉ | Pack initial

Objectifs

➔ Mobiliser l'ensemble des intervenants concernés

➔ Réaliser les actions structurantes créant un cadre propice à l'atteinte des objectifs



Prérequis

- Périmètre du SIR validé

Nos savoirs faire

- Accompagnement du RSSI dans la réalisation des actions
- Animation d'ateliers de co-construction
- Rédaction des documents
- Déploiement des solutions techniques

Livrables

- Documentation réalisée
- Plan d'action pour la conformité complète

Réception Côté entité régulée

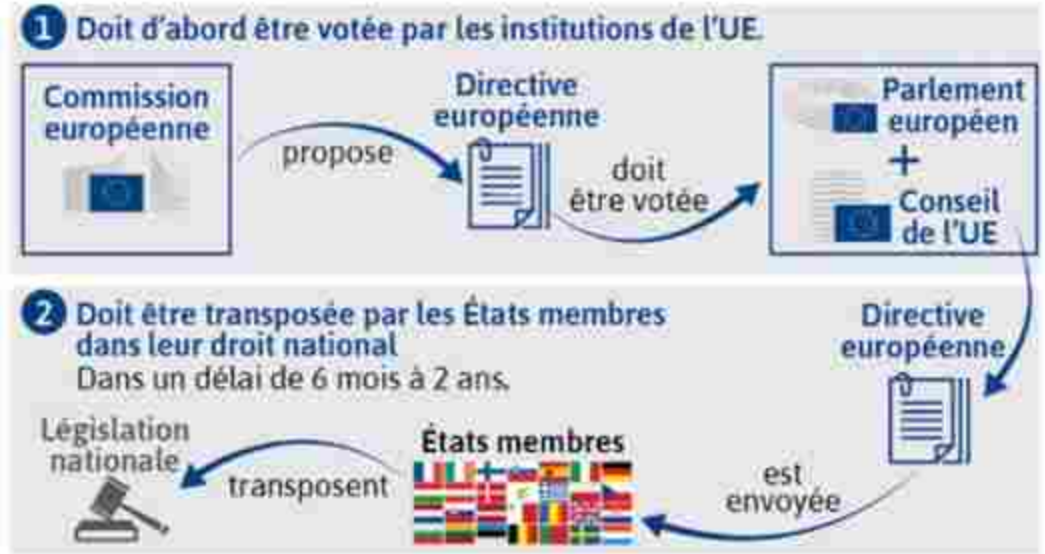
Premiers éléments par voie de presse : "la directive NIS2 va concerner les collectivités territoriales" "NIS1 n'a pas fonctionnée, place à NIS2"

Liste de 20 sujets diffusés par la commission européenne, vision très macro, "sécurisation des endpoints", "supply chain", "Gouvernance"

La directive européenne votée, une 1ère version d'un document de travail de transposition a été rapidement communiquée par l'ANSSI.

La collectivité était amenée à se prononcer et à répondre à un questionnaire en ligne.

Très tôt le CD35 décide de solliciter NIJI pour réaliser une étude de la mise en conformité NIS2 avec un plan d'action pluriannuel de conformité.



2 | Problématiques entités régulées

Applicabilité

Constat : Difficultés pour les organisations de savoir si elles font partie des entités concernées (sauf dans les cas les plus évidents)

Entités concernées par leur secteur d'activité.

Beaucoup de renvoi vers des définitions sectorielles très larges :

Ex : Fabrication de machines et équipements n.c.a. (Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28)

Classes 28.1 (Fabrication de machines d'usage général)

- 28.11 - Fabrication de moteurs et turbines, à l'exception des moteurs d'avions et de véhicules
- 28.12 - Fabrication d'équipements hydrauliques et pneumatiques
- 28.13 - Fabrication d'autres pompes et compresseurs
- 28.14 - Fabrication d'autres articles de robinetterie
- 28.15 - Fabrication d'engrenages et d'organes mécaniques de transmission

Entreprises pas forcément enregistrées avec le bon code NACE

Applicabilité directe, beaucoup d'incertitude sur les organisations publiques

Ex : La CCI est concernée de part son statut juridique de « établissement public administratif ».

- L'article L710-1 du Code de commerce définit les CCI comme étant des établissements publics sous tutelle de l'état (Bercy).
- L'article 8-7a de la proposition de loi REC dispose que « sont des Entités Essentielles les administrations de l'état et leurs établissements publics administratifs » sans critères de seuil.

Or, les CCI n'ont pas de visibilité sur ce sujet et s'attachent aux activités réalisées

Définitions de périmètres à couvrir

Constat : Difficulté de définir un périmètre cohérent et facile à maîtriser

Revirement sur les périmètres soumis aux objectifs : des critères flous

Ancienne version	Version 2.3
L'entité peut, au cas par cas et en le justifiant, exclure des systèmes d'information, parmi ceux [de ses activités], 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.	L'entité précise dans la liste [de ses activités], les systèmes d'information pour lesquelles elle a décidé de ne pas appliquer les objectifs de sécurité définis, l'entité renseigne les justifications de ces choix.

Applicabilité filiale étrangère

Manque de clarification manque de retour d'expérience

2 solutions :

- Chaque filiale applique les mesures cyber de la société mère. La Directive instaure une obligation de coopération entre les autorités de contrôle (Art 37,1 NIS2)
- Chaque filiale applique les mesures de son pays d'établissement.

Problématiques des entités régulées

- Pas d'accompagnement de l'ANSSI : manque de ressources disponibles de la part de l'ANSSI (cellule dédiée (mail ou tel)

- Notion Audit systématique : le Département n'a pas la possibilité d'auditer l'ensemble de ses 150 prestataires. La mutualisation d'audit entre collectivité peut être une solution, mais elle a des limites, parfois pas le même périmètre et agenda.

- L'entité porte la responsabilité de la conformité NIS2 des prestataires : pas de labellisation des outils.

- Interdiction du BYOD : mesure difficile à appliquer car changement total dans les usages - « ne doivent se connecter au SI que des appareils gérés "

3 | RETEX CD35

Démarche

- Pré remplissage de la matrice grâce à la connaissance du contexte
- Mise à jour de la matrice avec les équipes Infrastructures, Applicatifs et la gouvernance
- Formaliser les écarts avec les objectifs de sécurité NIS2
- Identifier les actions nécessaires pour atteindre la conformité
- Restituer le niveau actuel de conformité
- Présenter une feuille de route

Grille d'audit

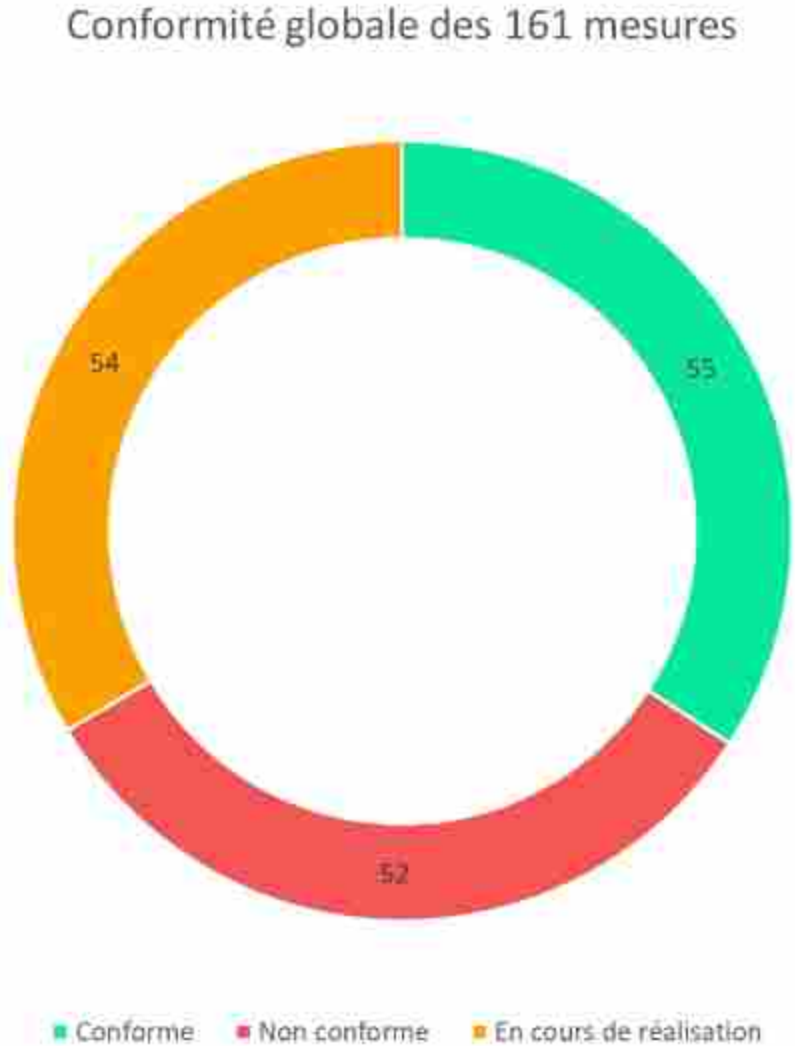
Gouvernance	Protection	Défense	Résilience
•Recensement des SI •Gouvernance de la sécurité •Gestion des risques •Maitrise de l'écosystème •Audit de la sécurité des SIR •Prise en compte de la sécurité numérique des RH	•Maitrise de ses systèmes d'information réglementés •Sécurité physique des locaux •Sécurité de l'architecture des SIR •Sécurité des accès distants aux SIR •Protection des SIR contre les codes malveillants •Sécurité de la configuration des ressources des SIR •Gestion des identités et des accès des utilisateurs des SIR •Administration sécurisée des SIR	•Administration sécurisée des SIR via des ressources dédiées •Supervision de la sécurité des SIR •Gestion des incidents de sécurité	•Continuité et reprise d'activité •Gestion des crises cyber •Vérification du fonctionnement des capacités opérationnelles

Vue globale

Une mesure de sécurité est considérée comme **conforme** si l'action est pleinement réalisée ou si l'action n'est pas applicable au SI du Département.

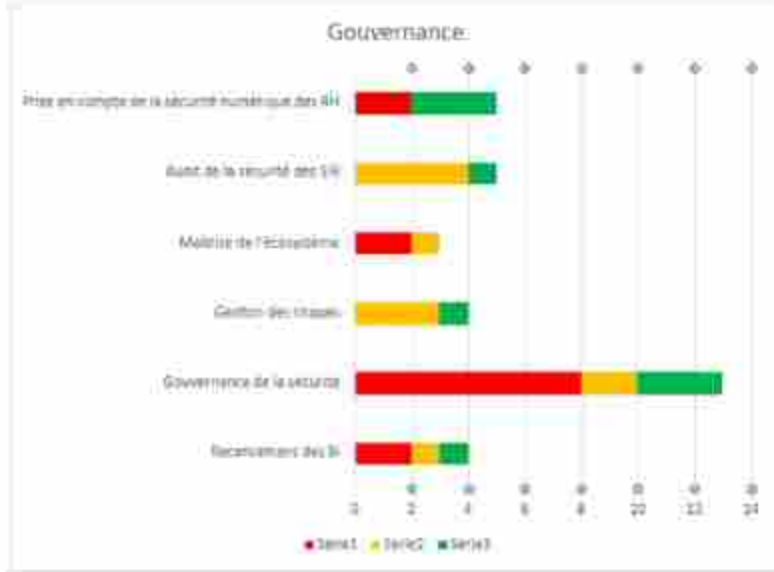
Une mesure est **en cours de réalisation** si les actions mise en œuvre sont suffisantes pour assurer partiellement la conformité à la mesure.

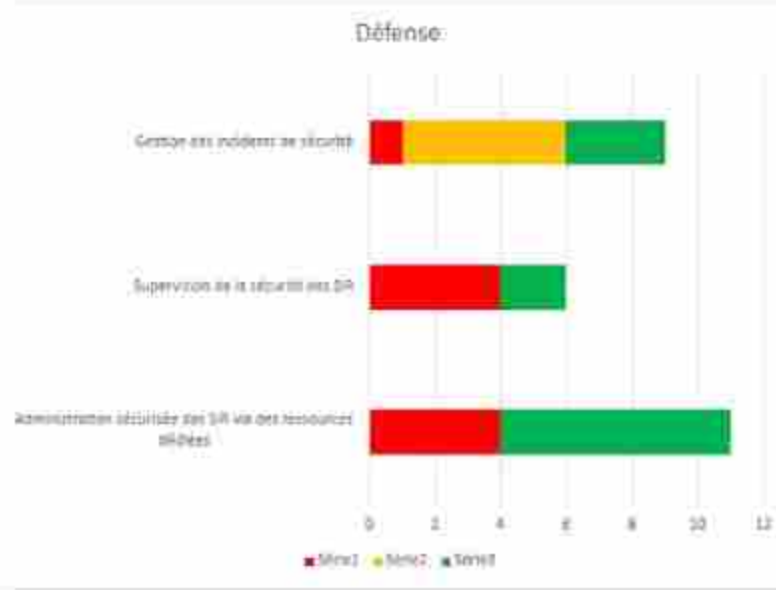
Une mesure de sécurité est **non conforme** lorsque aucune action n'est entreprise ou lorsque les actions ne permettent pas d'assurer une conformité partielle.

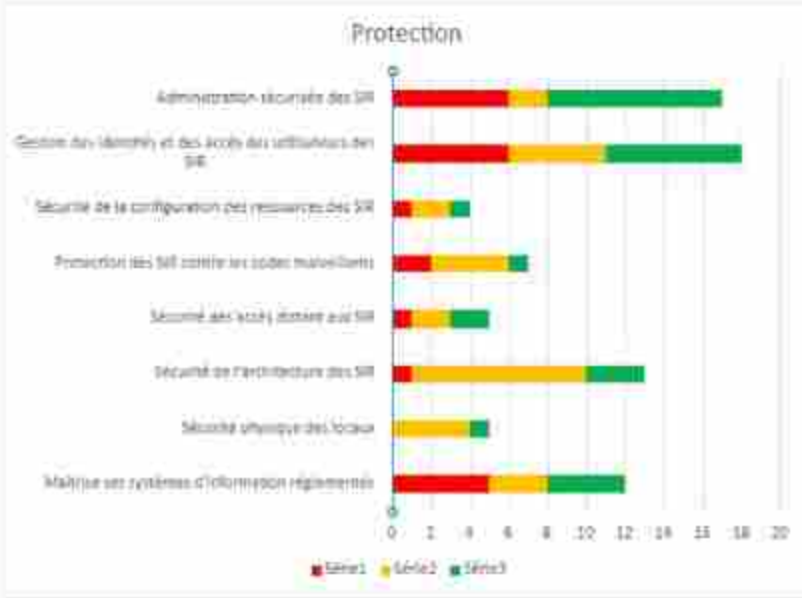


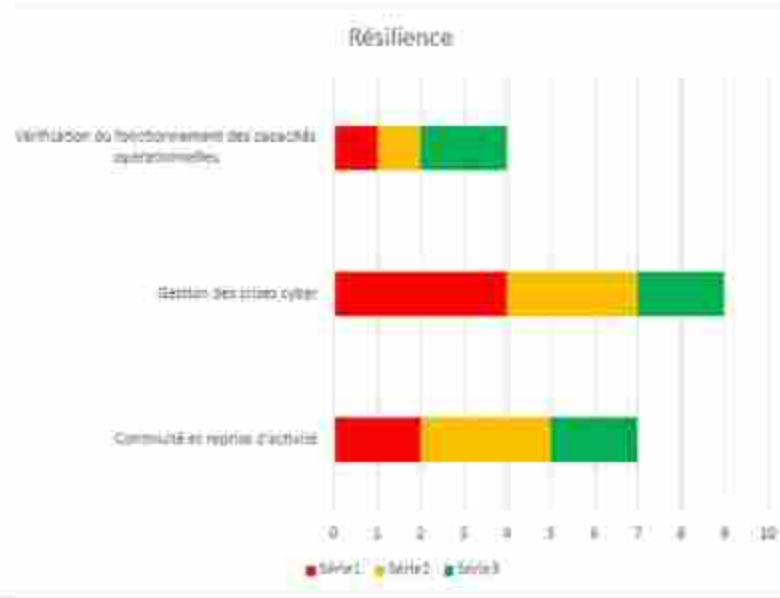
Vue par pilier

- Conforme
- En cours de réalisation
- Non conforme







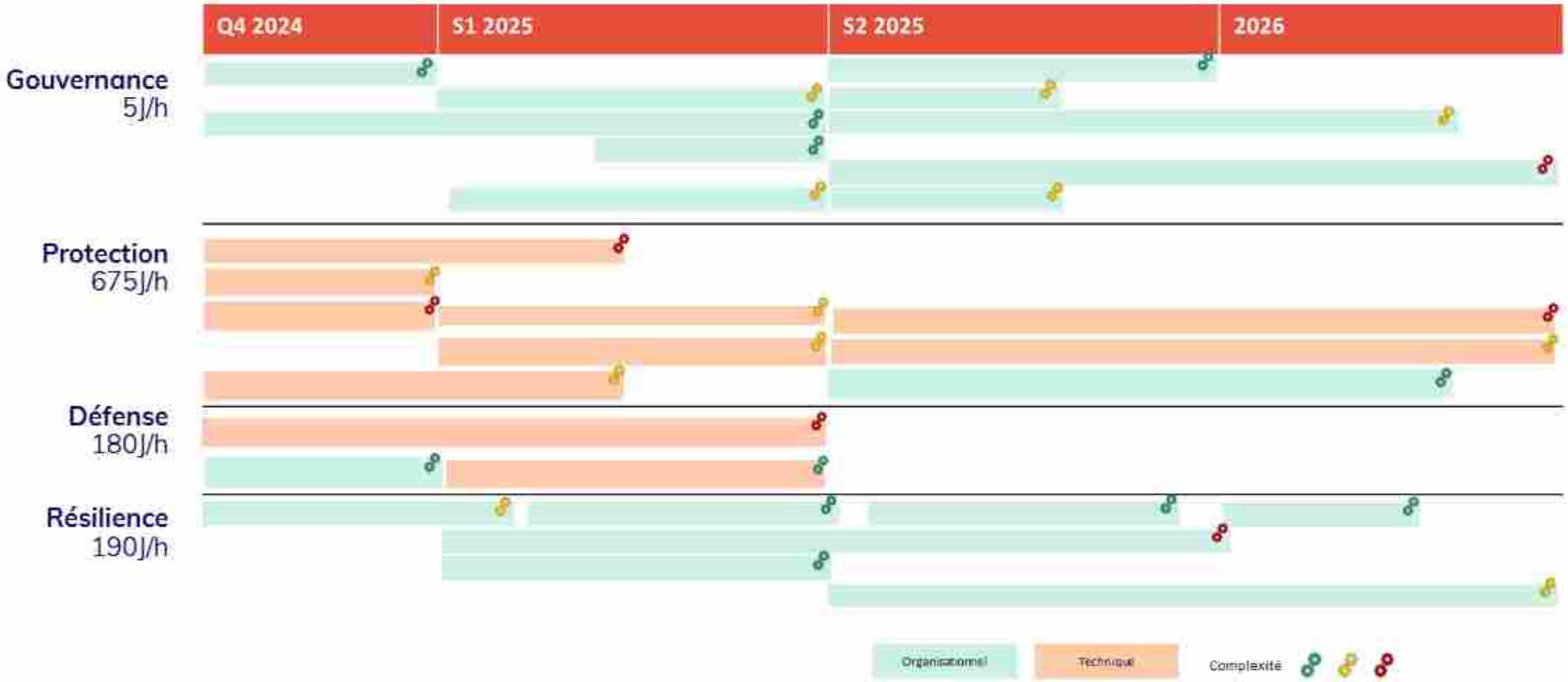


Pilier gouvernance

texte

Plan d’actions global

Macro-planning avec charge de mise en oeuvre (hors licences, études et matériels)



Avez-vous des questions ?

Votre avis compte !

Lien : klaxoon.com

Mot de passe :

RM54VFZ

(un pseudo vous sera demandé)

Vous êtes au ♡ du numérique !

www.adnouest.org

Partagez votre expérience :

@adnouest