



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



# WEBINAIRE NIS 2

PRÉSENTATION DE LA DIRECTIVE ET DE SA  
TRANSPOSITION NATIONALE

# LES OBJECTIFS DU WEBINAIRE

- Présenter l'ANSSI
- Présenter la directive NIS 2, sa genèse, ses objectifs, ses obligations
- Partager les étapes de la transposition nationale et son calendrier général
- Répondre aux premières questions



# 1. PRÉSENTATION DE L'ANSSI

# L'ANSSI

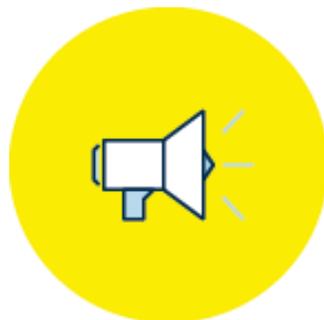
- Agence nationale de la sécurité des systèmes d'information, créée en 2009
- Autorité nationale en matière de cybersécurité et de cyberdéfense
- Service de la Première ministre rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN)
- Mission strictement défensive
- Régulation des OIV (Opérateurs d'importance vitale), des OSE (Opérateurs de services essentiels) et des administrations



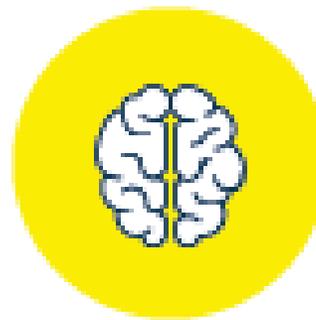
# LES 4 GRANDES MISSIONS DE L'ANSSI



CONNAÎTRE



PARTAGER



ACCOMPAGNER



DÉFENDRE



## 2. GENÈSE ET OBJECTIFS DE LA DIRECTIVE NIS 2



# L'ARRIVÉE DE NIS 1



# NIS 1

## PREMIÈRE DIRECTIVE EUROPÉENNE DE CYBERSÉCURITÉ

- « NIS » pour *Network and Information system Security*
  - En français, directive « SRI » pour Sécurité des réseaux et des systèmes d'information.
- Elle permet un renforcement des capacités de coopération à l'échelle européenne :
  - Obligation pour les Etats membres de définir une stratégie nationale ;
  - Obligation pour les Etats membres de désigner une autorité nationale compétente ;
  - Mise en place du Groupe de coopération (GC) ;
  - Création du *CSIRT Network*.
- Elle cible les grands acteurs économiques du marché intérieur de l'UE au regard des impacts économiques et sociétaux des services fournis.



# LA TRANSPOSITION DE NIS 1

- Délai de transposition de **24 mois** accordé aux Etats membres :
  - Publication de la directive européenne en 2016 ;
  - Transposée en droit français en 2018.
- Environ **300 entités** désignées « Opérateurs de Services Essentiels » (OSE) à date
  - Sur désignation unitaire par arrêté de la Première ministre en concertation avec les ministères de tutelle.
- Le **délai de transposition** accordé aux Etats membres de l'UE est différent des **délais de mise en conformité** aux exigences françaises accordés aux OSE.



# L'ANSSI EN TANT QUE RÉGULATEUR NIS 1

- Désignée **autorité nationale compétente** au regard des obligations émanant de la directive européenne
- **Représente la France** lors des échanges européens
  - Groupe de coopération NIS
  - Réseau des CSIRT via le CERT-FR
  - Cheffe de file des négociations de la directive NIS 2
- Régule les OSE :
  - Désigne les OSE
  - Définit les **exigences de sécurité**
  - Réceptionne les **déclarations d'incidents majeurs** par les OSE
  - **Contrôle** les OSE vis-à-vis de la bonne implémentation des exigences

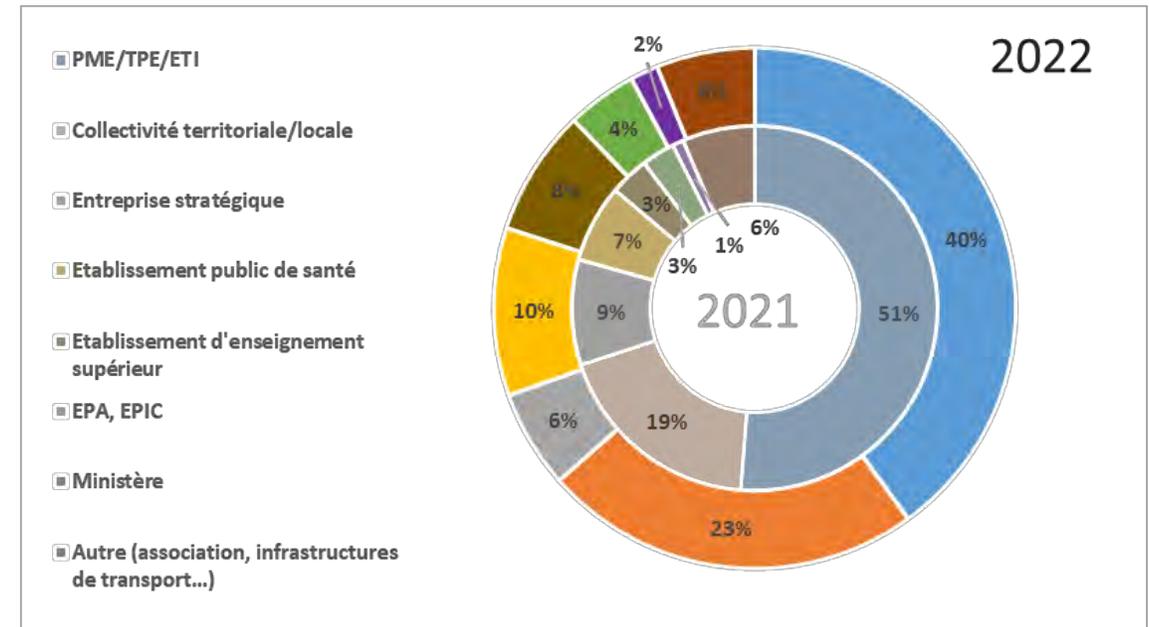


# DE NIS 1 À NIS 2



# UNE ÉVOLUTION NÉCESSAIRE À L'ÉCHELLE EUROPÉENNE

- Une hétérogénéité importante entre les Etats membres de l'UE
- Une évolution de la menace et des impacts sur la société :
  - De nouvelles cibles (PME, ETI, collectivités territoriales)
  - Les conséquences dramatiques des rançongiciels
  - La chaîne d'approvisionnement



Source : ANSSI - panorama de la menace 2022



# NIS 2 : DE LA CYBERSÉCURITÉ DES OPÉRATEURS CRITIQUES VERS LA CYBERSÉCURITÉ DE MASSE

- Fin 2020, décision de la Commission européenne d'étendre le périmètre et les ambitions de la directive :
  - Des milliers d'entités se retrouveront concernées par la directive NIS 2 à l'échelle nationale
- Nécessité de préciser le **périmètre**, les **exigences de sécurité** et les **mécanismes de régulation** :
  - NIS 2 est plus prescriptive que NIS 1
- **Nécessité d'une évolution soutenue par la France** :
  - **Prise de conscience massive**
  - Intégration des premiers éléments de base de la cybersécurité
  - Proportionnalité des exigences face aux enjeux des entités et des secteurs concernés, à leur capacité



# 3. PRÉSENTATION DU CONTENU DE LA DIRECTIVE

# NIS 2

## ÉLÉMENTS GÉNÉRAUX

### Thèmes abordés dans cette section

- Le périmètre des entités régulées sous NIS 2
- Les obligations issues de NIS 2
- La régulation des entités concernées par NIS 2

### Quelques précisions :

- Cette présentation ne se veut pas exhaustive
- Certains détails restent à définir dans le cadre de la transposition nationale (*cf. partie suivante*)
  - La directive contient des éléments très prescriptifs
  - La directive offre des options sur certains sujets
  - La directive laisse une marge d'interprétation nationale pour les Etats membres



# LE PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## L'EXTENSION DU PÉRIMÈTRE

Quelques remarques générales sur l'extension du périmètre

- Changement de sémantique au niveau national
  - « Opérateurs » devient « entités »
- Couverture a minima de 18 secteurs d'activités
- Secteurs répartis sur deux annexes (1 et 2)
- Inclusion de l'administration publique
- Inclusion d'une grande partie des acteurs de la chaîne d'approvisionnement, notamment au sein de l'annexe 2

# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## LES SECTEURS DE L'ANNEXE 1 DE LA DIRECTIVE

SECTEUR	SOUS-SECTEUR
01. ÉNERGIE	Électricité
	Réseaux de chaleur et de froid
	Pétrole
	Gaz
	Hydrogène
02. TRANSPORTS	Transports aériens
	Transports ferroviaires
	Transports par eau
	Transports routiers
03. SECTEUR BANCAIRE	
04. INFRASTRUCTURES DES MARCHÉS FINANCIERS	
05. SANTÉ	
06. EAU POTABLE	
07. EAUX USÉES	
08. INFRASTRUCTURE NUMÉRIQUE	
09. GESTION DES SERVICES TIC	
10. ADMINISTRATION PUBLIQUE	Administration centrale
11. ESPACE	

# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## LES SECTEURS DE L'ANNEXE 2 DE LA DIRECTIVE

SECTEUR	SOUS-SECTEUR
01. SERVICES POSTAUX ET D'EXPÉDITION	
02. GESTION DES DÉCHETS	
03. FABRICATION, PRODUCTION ET DISTRIBUTION DE PRODUITS CHIMIQUES	
04. PRODUCTION, TRANSFORMATION ET DISTRIBUTION DES DENRÉES ALIMENTAIRES	
05. FABRICATION	Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro
	Fabrication de produits informatiques, électroniques et optiques
	Fabrication d'équipements électriques
	Fabrication de machines et équipements
	Construction de véhicules automobiles, remorques et semi-remorques
	Fabrication d'autres matériels de transport
06. FOURNISSEURS NUMÉRIQUES	
07. RECHERCHE	



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

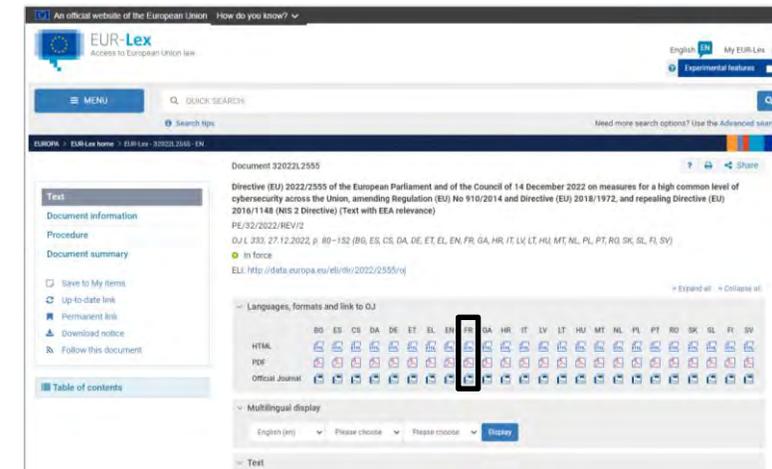
## LES CRITÈRES DE SÉLECTION DES ENTITÉS : LE TYPE D'ENTITÉ

Pour chaque secteur/sous-secteur, des « types d'entité » ont été identifiés pour détourner le périmètre :

- Cela correspond à des activités métier
- Ils sont définis sur la base :
  - De définitions précises issues de réglementations déjà existantes
  - De la classification européenne des activités NACE (*NAF en France*)
  - De définitions ad hoc

La liste est présente aux pages 64-67 de la directive européenne 2022/2555 :

- <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555>
- Recherche internet :
  - Rechercher « LEX 2022/2555 » sur moteur de recherche
  - Sélectionner le fichier en version FR





# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## EXEMPLE DE TYPE D'ENTITÉ

### ANNEXE I

#### SECTEURS HAUTEMENT CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil <sup>(1)</sup> , qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		— Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		— Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		— Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil <sup>(2)</sup>
		— Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944
		— Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	— Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil <sup>(3)</sup>
	c) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		— Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil <sup>(4)</sup>
	d) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8), de la directive 2009/73/CE du Parlement européen et du Conseil <sup>(5)</sup>
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la directive 2009/73/CE
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE
— Exploitants d'installations de raffinage et de traitement de gaz naturel		
e) Hydrogène	— Exploitants de systèmes de production, de stockage et de transport d'hydrogène	



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## LES CRITÈRES DE SÉLECTION DES ENTITÉS : LA TAILLE DE L'ENTITÉ

De manière générale, les entités de taille moyenne, intermédiaire ou grande, réalisant des activités identifiées dans les annexes 1 et/ou 2 seront concernées par NIS 2.

Les critères et seuils correspondant aux entités de taille moyenne, intermédiaire ou grande sont :

- Nombre d'employés supérieur ou égal à 50

*OU*

- Chiffre d'affaires ou bilan annuel supérieur ou égal à 10 millions d'euros



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## QUELQUES EXCEPTIONS ET CAS PARTICULIERS

- La France aura la possibilité **d'intégrer unitairement**, et à la marge, des entités ne respectant pas les critères de base sur la base d'une analyse de risque nationale.
- La France aura également la possibilité **d'exclure unitairement** des entités au regard de la clause de défense et de sécurité nationale prévue par la directive.
- Pour les entités des types suivants, la directive s'applique quelle que soit leur taille :
  - Fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ;
  - Prestataires de services de confiance ;
  - Fournisseur de registre des noms de domaine de premier niveau et fournisseurs de services de système de noms de domaine



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

## EN SYNTHÈSE

- Règle par défaut de délimitation du périmètre
- Mécanismes d'ajustement à la marge du périmètre
- Clarification nécessaire sur le détail de certains types d'entité, prévue via la transposition en droit national *(cf. suite de la présentation)*



# LES ENTITÉS ESSENTIELLES ET LES ENTITÉS IMPORTANTES



# LES ENTITÉS ESSENTIELLES ET IMPORTANTES

## L'INTÉGRATION DE LA PROPORTIONNALITÉ

NIS 2 intègre deux typologies d'entités différentes :

- Les entités essentielles (EE)
- Les entités importantes (EI)

NIS 2 intègre la proportionnalité entre EE et EI dans :

- Les mesures de sécurité
  - Possibilité d'avoir des niveaux d'exigences différents entre les EE et les EI, notamment pour prendre en considération les moyens et enjeux d'une grande entreprise versus d'une PME.
- La régulation
  - Pour les EE : régulation dite « ex-ante » (contrôle à discrétion de l'ANSSI)
  - Pour les EI : régulation dite « ex-post » (contrôle en cas de connaissance d'une non-conformité)
- Les sanctions
  - Seront d'une ampleur comparable à celui du RGPD
  - De manière simplifiée, sanctions pouvant aller jusqu'à 2% du CA mondial pour les EE et 1,4% pour les EI



# LES ENTITÉS ESSENTIELLES

## RÈGLE DE BASE

Parmi les entités de taille moyenne, intermédiaire et grande, réalisant des activités relatives aux types d'entité de l'annexe 1 :

- Les **EE** correspondent à l'ensemble des entités de taille intermédiaire et grande
- Cela correspond aux critères et seuils suivants :
  - Nombre d'employés supérieur ou égal à 250 ;  
*OU*
  - Chiffre d'affaires supérieur ou égal à 50 millions d'euros ;  
*OU*
  - Bilan annuel supérieur ou égal à 43 millions d'euros.

Annexe	Secteur
1	01. Énergie
1	02. Transports
1	03. Secteur bancaire
1	04. Infrastructures des marchés financiers
1	05. Santé
1	06. Eau potable
1	07. Eaux usées
1	08. Infrastructure numérique
1	09. Gestion des services TIC
1	10. Administration publique
1	11. Espace



# LES ENTITÉS ESSENTIELLES

## RÈGLES SECONDAIRES

Sont également considérées **entités essentielles** :

- les prestataires de services de confiance qualifiés et les registres de noms de domaine de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille ;
- les fournisseurs de réseaux publics de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent des entreprises de taille moyenne ;
- toute entité soumise à la directive Résilience des Entités Critiques (REC) ;
- toute entité désignée Opérateur de Service Essentiel au titre de NIS 1 ;
- certaines entités désignées unitairement par la France au regard de certains critères spécifiques.
  - Mécanisme d'ajustement à la marge
  - Cela concerne également l'annexe 2 de la directive



# LES ENTITÉS IMPORTANTES

## RÈGLE DE BASE

- Toute autre entité du périmètre (*annexe 1 et 2 et taille moyenne et plus*) qui n'est pas **essentielle** au regard des critères et cas précédemment exposés sera par défaut **importante**.
- Autrement dit, hors exception d'ajustement à la marge, seront **importantes** :
  - Toutes les entités de taille **moyenne** réalisant des activités correspondant aux types d'entité de l'annexe 1 ;
  - Toutes les entités de taille **moyenne et plus** réalisant des activités correspondant aux types d'entité de l'annexe 2.

Annexe	Secteur
1	01. Énergie
1	02. Transports
1	03. Secteur bancaire
1	04. Infrastructures des marchés financiers
1	05. Santé
1	06. Eau potable
1	07. Eaux usées
1	08. Infrastructure numérique
1	09. Gestion des services TIC
1	10. Administration publique
1	11. Espace

Annexe	Secteur
2	01. Services postaux et d'expédition
2	02. Gestion des déchets
2	03. Fabrication, production et distribution de produits chimiques
2	04. Production, transformation et distribution des denrées alimentaires
2	05. Fabrication
2	06. Fournisseurs numériques
2	07. Recherche

# LES ENTITÉS ESSENTIELLES ET IMPORTANTES

## SCHÉMATISATION SIMPLIFIÉE DE LA RÈGLE DE BASE

TAILLE ENTITE	NOMBRE D'EMPLOYÉS	CHIFFRE D'AFFAIRES (MILLIONS D'EUROS)	BILAN ANNUEL (MILLIONS D'EUROS)	ANNEXE 1	ANNEXE 2
INTERMÉDIAIRE ET GRANDE	$x \geq 250$	$y \geq 50$	$z \geq 43$	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
MOYENNE	$50 \geq x \geq 250$	$10 \geq y > 50$	$10 \geq z > 43$	ENTITES IMPORTANTES	ENTITES IMPORTANTES
MICRO ET PETITE	$x < 50$	$y < 10$	$z < 10$	<i>Non concernées</i>	<i>Non concernées</i>



# PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS

## LA JURIDICTION À L'ÉCHELLE EUROPÉENNE

- Par défaut, les entités relevant du champ d'application de la directive sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont **établies**.
- Exceptions :
  - Les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public relèvent de la compétence de l'État membre dans lequel ils fournissent leurs services.
  - Les **acteurs du numérique** relèvent de la compétence de l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité.

Les acteurs du numériques correspondent aux types d'entités suivants :

Annexe 1 :

- Les fournisseurs de services DNS
- Les registres des noms de domaine de premier niveau
- Les entités fournissant des services d'enregistrement de noms de domaine
- Les fournisseurs de services d'informatique en nuage
- Les fournisseurs de services de centres de données
- Les fournisseurs de réseaux de diffusion de contenu
- Les fournisseurs de services gérés
- Les fournisseurs de services de sécurité gérés

Annexe 2 :

- Les fournisseurs de places de marché en ligne
- Les fournisseurs de moteurs de recherche en ligne
- Les fournisseurs de plateformes de services de réseaux sociaux



# OBLIGATIONS POUR LES ENTITÉS



# LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

## NOTIFICATION, CONTACT ET DÉCLARATION DES INCIDENTS MAJEURS

### Notification à l'ANSSI

- La France envisage de mettre en place un mécanisme permettant aux entités de se notifier auprès de l'ANSSI

### Communication des informations de contact et mise à jour

- Type d'information à communiquer a minima :
  - Nom de l'entité
  - Adresse et coordonnées actualisées
  - Secteur(s) d'activité
  - Liste des Etats membres de l'UE dans lesquels sont fournis les services

### Déclaration à l'ANSSI des incidents majeurs

- La déclaration d'incident s'effectuera en plusieurs étapes :
  - Notification
  - Rapport d'avancement
  - Rapport final



# LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

## MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2

Mesures à prendre par les entités pour gérer les risques liés à l'utilisation du numérique

### Périmètre d'application des mesures de sécurité

- *« Les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services. »*

### Aparté au regard de NIS 1

- Suppression de la notion de service essentiel
- Extension du périmètre des systèmes d'information à sécuriser qui n'est plus restreint aux « systèmes d'information essentiels »



# LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

## MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2

1. les politiques relatives à l'analyse des risques et à la sécurité des SI ;
2. la gestion des incidents ;
3. la continuité des activités (sauvegardes, PRA gestion des crises) ;
4. la sécurité de la chaîne d'approvisionnement (fournisseurs/prestataires) ;
5. la sécurité de l'acquisition, du développement et de la maintenance des SI ;
6. des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
7. les pratiques de base (cyberhygiène et formation à la cybersécurité) ;
8. des politiques et des procédures relatives à l'utilisation de la cryptographie ;
9. la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
10. 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.

# LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

## MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2 – CAS PARTICULIER

Les acteurs du numérique ne seront pas soumis aux exigences relatives aux mesures de sécurité transposées à l'échelle nationale.

Ils seront soumis à un acte d'exécution publié par la Commission européenne au plus tard le 17 octobre 2024 qui précisera les mesures à appliquer.

Les acteurs du numérique correspondent aux types d'entités suivants :

Annexe 1 :

- Les fournisseurs de services DNS
- Les registres des noms de domaine de premier niveau
- Les entités fournissant des services d'enregistrement de noms de domaine
- Les fournisseurs de services d'informatique en nuage
- Les fournisseurs de services de centres de données
- Les fournisseurs de réseaux de diffusion de contenu
- Les fournisseurs de services gérés
- Les fournisseurs de services de sécurité gérés

Annexe 2 :

- Les fournisseurs de places de marché en ligne
- Les fournisseurs de moteurs de recherche en ligne
- Les fournisseurs de plateformes de services de réseaux sociaux



# LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

## LES DÉLAIS À RESPECTER

Certains délais de mise en conformité sont fixés par la directive et d'autres sont laissés à l'appréciation des États membres.

Les délais non fixés par la directive feront partie des sujets instruits lors des consultations avec l'écosystème des futures entités régulées (*cf. suite de la présentation*)

Quelques exemples :

- Sont fixés par la directive :
  - Délai de mise à jour des informations de contact en cas d'évolution de ces dernières (15j) ;
  - Notification initiale d'un incident sous 24H.
- Seront fixés dans le cadre de la transposition nationale :
  - Délai de notification à l'ANSSI ;
  - Délai d'implémentation des mesures de sécurité.



# OBLIGATIONS POUR L'ANSSI



# OBLIGATIONS POUR L'ANSSI

## LE RENFORCEMENT DU RÔLE DE RÉGULATEUR

Supervision du périmètre et remontée d'informations à la Commission Européenne

- Rapports sur l'étendue du périmètre et le détail par secteur
- Rapports statistiques sur les incidents remontés à l'ANSSI

Précision des actions de régulation de l'ANSSI. Quelques exemples :

- Inspection sur place, à distance
- Scans automatisés
- Injonction (*ex : mise en place d'un correctif d'une vulnérabilité critique*)
- Demander la suspension temporaire ou non d'une certification
- Demander la suspension temporaire d'exercer les responsabilités dirigeantes de l'entité pour la personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal



# 4. TRANSPOSITION NATIONALE ET AMBITIONS



# LES AMBITIONS DE L'ANSSI AU REGARD DE LA TRANSPOSITION NATIONALE DE NIS 2

# LES GRANDS PRINCIPES DIRECTEURS DE LA TRANSPOSITION NATIONALE POUR L'ANSSI

- Des délais de transposition nationale fixés par l'UE
- Créer un dispositif qui ait un **réel impact** sur la sécurisation des entités
- **Participation** aux travaux d'harmonisation européenne
- S'assurer de la **prise en compte** de la **diversité** des situations des entités
- Informer les futurs écosystèmes régulés tout au long de la transposition
- **Coconstruire** avec les secteurs concernés



# LA TRANSFORMATION DE L'ANSSI AU REGARD DE NIS 2

Conserver en tant que régulateur une mission d'accompagnement, tout en intégrant la capacité de sanction et en renforçant l'activité de contrôle

Transformer les actions de l'ANSSI pour passer à l'échelle :

- Adapter l'accompagnement aux nouvelles entités régulées ;
- Développer des services numériques ;
- Développer des relais locaux et industriels.



# LES GRANDES ETAPES DE LA TRANSPOSITION NATIONALE DE NIS 2



# LA TRANSPOSITION EN DROIT NATIONAL

## Objectif :

- Transcription des obligations et options européennes en exigences nationales en droit français au travers de textes législatif et réglementaires.
- Échéance européenne : **17/10/2024**
- Articulation et simplification du cadre réglementaire :
  - REC / LPM 2013 / DORA

## Quelques informations :

- Les travaux ont déjà été lancés depuis longtemps en interne pour s'assurer du respect des délais
- Processus législatif : consultations obligatoires, Conseil d'Etat, Parlement, adoption
- Les phases de consultation sont prévues sur S2 2023 et portent sur l'élaboration des textes réglementaires (décrets, arrêtés)



# LES CONSULTATIONS À VENIR

- Réparties en trois séquences pour trois thématiques :
  - Périmètre des entités régulées
  - Interactions entre entités régulées et régulateur
  - Mesures de sécurité
- Objectif de travailler avec des représentations des différents secteurs concernés pour s'assurer de couvrir le maximum d'entités possibles
  - L'ANSSI travaillera avec les fédérations professionnelles pour les acteurs du privé
  - Les entités qui souhaitent s'investir sont invitées à se rapprocher de leur fédérations professionnelles/sectorielles.



# LES CONSULTATIONS À VENIR

## PÉRIMÈTRE DES ENTITÉS

Objectifs de la consultation :

- Clarifier le périmètre lorsque cela est nécessaire, notamment au regard des définitions de la directive
- S'assurer que les définitions sont comprises et partagées entre l'administration de l'Etat et les secteurs d'activités
- Clarifier les cas particuliers (notamment les entreprises à structure complexe)
- Apporter les éléments de réponse aux questions :
  - « Suis-je concerné ? »
  - « Suis-je EE ou EI ? »



# LES CONSULTATIONS À VENIR

## INTERACTIONS AVEC LE RÉGULATEUR

Objectifs de la consultation :

- Clarifier les **modalités d'échange** d'information entre les entités régulées et l'ANSSI :
  - Mécanisme de notification
  - Mécanisme de transmission et mise à jour des **contacts**
  - **Déclaration des incidents**
  - **Descentes d'information** de l'ANSSI vers les entités (régulation, accompagnement)
- Apporter les éléments de réponse aux questions :
  - « Que dois-je communiquer et comment ? »
  - « Que puis-je recevoir de l'ANSSI et sous quel format ? Dois-je y répondre ? »



# LES CONSULTATIONS À VENIR

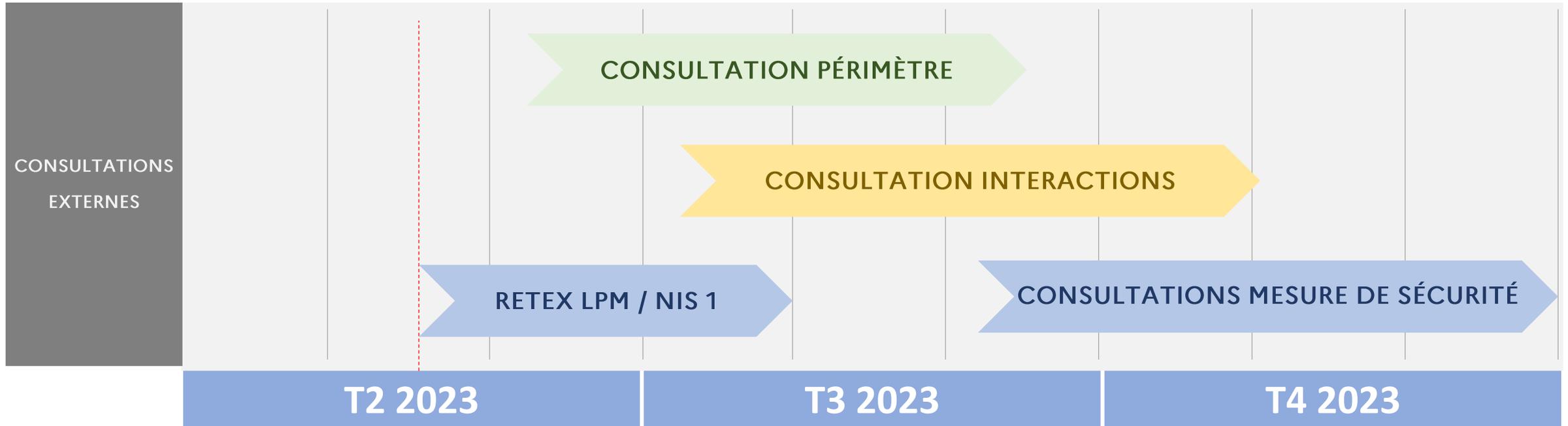
## MESURES DE SÉCURITÉ

Objectifs de la consultation :

- Coconstruire la déclinaison des mesures de sécurité NIS 2 pour les **EE** et les **EI**
- Echanger sur les modalités d'atteinte des objectifs de sécurité associés
  - Méthode
  - Temporalité / délai d'implémentation
  - Mécanisme de présomption de conformité
- Apporter les éléments de réponse aux questions :
  - « Que dois-je mettre en œuvre ? »
  - « Comment m'y prendre ? »
- En parallèle, une réflexion sur le modèle actuel NIS 1 vient d'être lancée avec des experts du secteur de la cybersécurité

# LES CONSULTATIONS À VENIR

## CALENDRIER PRÉVISIONNEL





# QUESTIONS / RÉPONSES



# MERCI POUR VOTRE ATTENTION