RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LA DIRECTIVE NIS 2

PRÉSENTATION DE LA DIRECTIVE ET DE SA TRANSPOSITION NATIONALE

LES OBJECTIFS DE LA PRESENTATION

1. Présenter **la directive NIS 2, sa genèse, ses objectifs, ses obligations**

2. Partager **les étapes de la transposition nationale, son calendrier général et ce qui peut être mis en œuvre** dès maintenant

3. Répondre à **vos questions**

Avant-propos

- Cette présentation s'adresse à **plusieurs milliers d'entités essentielles et importantes** qui exercent leurs **services et leurs activités en France**, ainsi qu'aux **acteurs de l'écosystème cyber, publics et privés**, tous impliqués dans la réponse coordonnée et collective attendue face à la cybermenace.

- Elle a pour but d'offrir un **éclairage sur la mise en œuvre de la directive NIS 2**, **les étapes clés et les outils mis à disposition par l'Agence**. Les travaux de transposition de la directive NIS 2 étant actuellement en cours, elle **rend accessible les concepts de la directive NIS 2** mais **ne peut aborder les mesures règlementaires** et les aspects techniques à ce stade.

- **En attendant la finalisation des textes officiels**, l'ANSSI souhaite donc mettre à disposition des futures entités assujetties cette présentation afin de **sensibiliser et de clarifier les éléments à venir**.

- Enfin, l'ANSSI, en tant que chef de fil, contribue au **processus d'élaboration des textes en concertation avec les ministères, le Parlement**, ainsi qu'**avec les organisations professionnelles et associations d'élus**.

1. GENÈSE ET OBJECTIFS DE LA DIRECTIVE NIS 2

L’ARRIVÉE DE NIS 1

LA DIRECTIVE 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'Union européenne au regard des impacts économiques et sociétaux des services fournis.

- Adoptée en 2016 par le Parlement et le Conseil de l'UE puis transposée en droit français en 2018.

L'ANSSI EN TANT QUE RÉGULATEUR NIS 1

DESIGNEE AUTORITE NATIONALE COMPETENTE AU TITRE DE LA DIRECTIVE

- 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

- Environ **300 entités** désignées « Opérateurs de Services Essentiels » (OSE) à date
  - Sur désignation unitaire par arrêté du Premier ministre en concertation avec les ministères de tutelle.

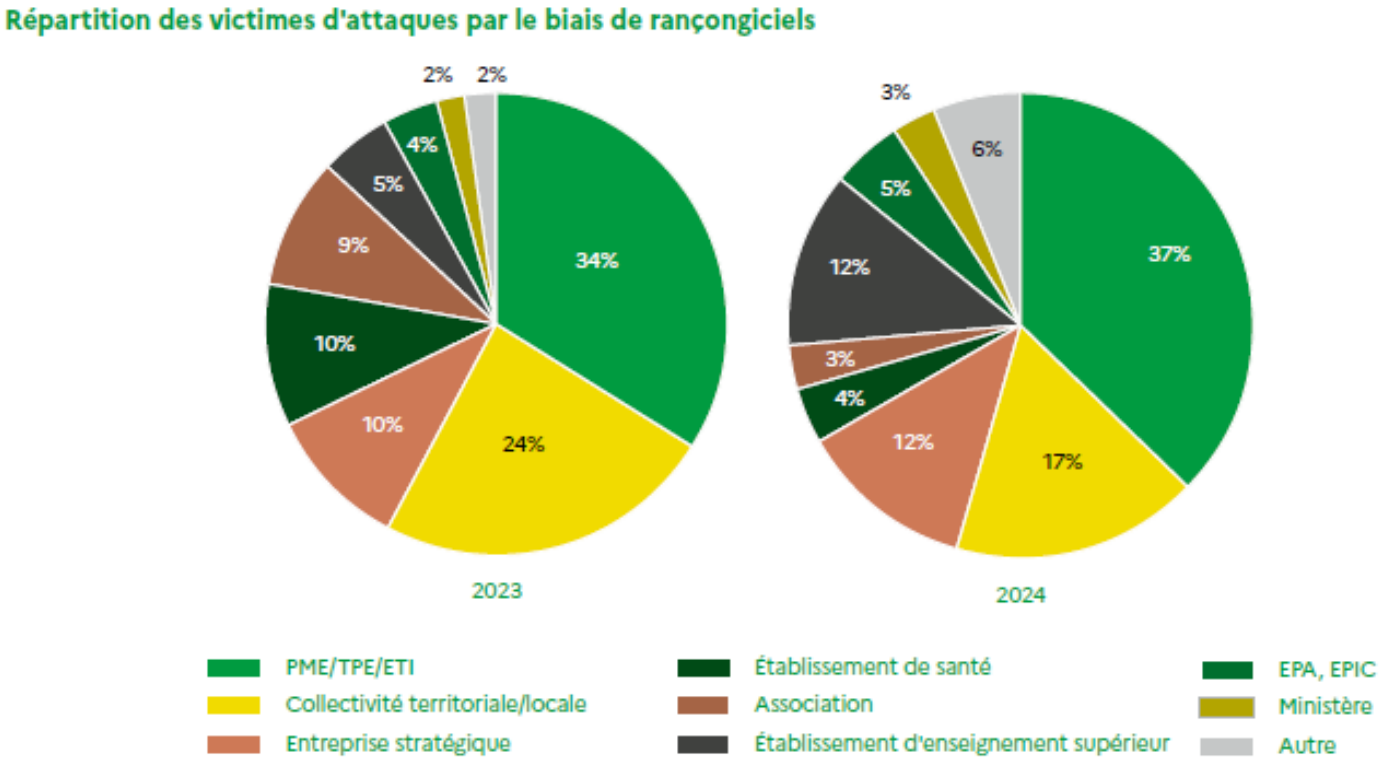
DE NIS 1 À NIS 2

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 (TPE /PME/ ETI, collectivités territoriales)** ;
  - Les conséquences dramatiques des **rançongiciels ;**
  - La **chaîne d'approvisionnement.**



UNE MENACE SYSTEMIQUE, TOUCHANT TOUT TYPE D'ACTEURS

- **Un même constat au sein de l'UE : une menace cybercriminelle toujours très élevée**
  - Une menace devenue systémique, touchant désormais tout type d'acteur, de la petite à la grande entreprise, en passant par les administrations de l'Etat et les collectivités territoriales.

- **Des attaques massives, qui ne ciblent personne mais qui touchent tout le monde : elles peuvent déstabiliser tout un secteur économique ou toute une zone géographique…**

- **Les conséquences sont parfois catastrophiques, allant parfois jusqu'à la fermeture d'entreprises.**

- **Une plus grande exposition aux menaces** due à :
  - une transformation numérique rapide
  - une dépendance aux nouvelles technologies
  - une interconnexion croissante de la société avec des échanges transfrontières importants

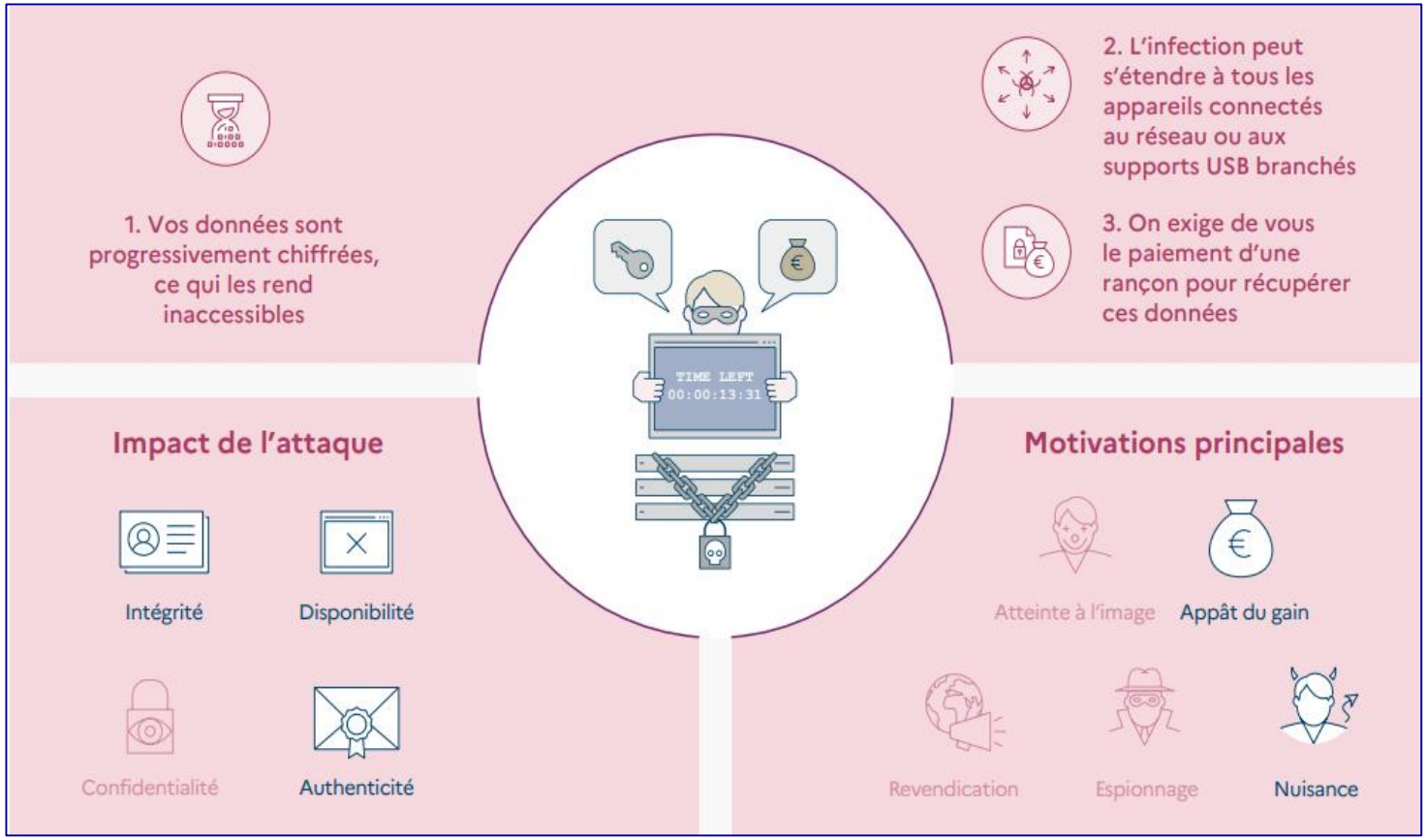
QU'EST-CE QU'UN RANÇONGICIEL ?

Une maison dont on aurait changé les clefs et les serrures, et ce, à l'insu de son propriétaire…

Lors d'une attaque par rançongiciel, l'attaquant met **l'ordinateur ou le système d'information hors d'état** de fonctionner de manière réversible.

La plupart des rançongiciels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système, rendant leur consultation ou **leur utilisation impossibles**.

L'attaquant adresse alors un message non chiffré à la victime où **il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.**



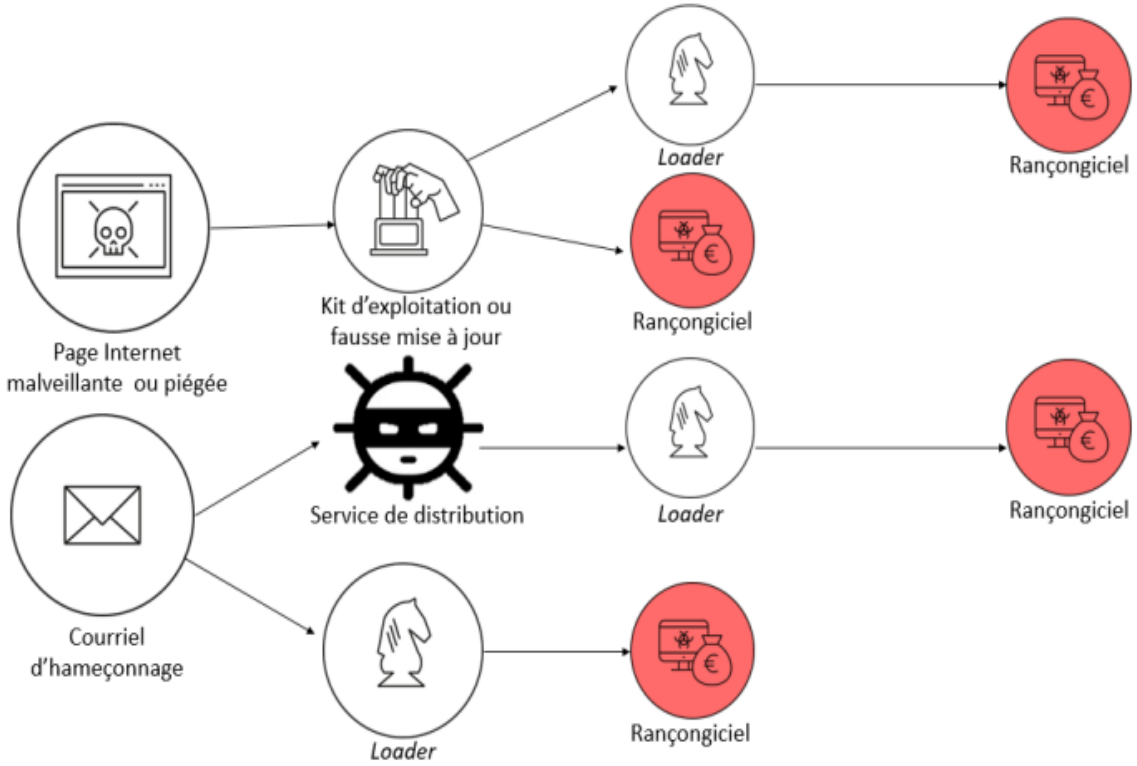
QUE SE PASSE-T-IL UNE FOIS INFECTÉ ?

LE CHIFFREMENT ET LA DEMANDE DE RANÇON

- Une fois déployé, le rançongiciel arrête de nombreux processus dont les logiciels de sécurité.

- Il chiffre les données et demande une rançon à la victime. **Des menaces peuvent se poursuivre** :
  - Exfiltration des données et publication sur Internet des données extorquées
  - Attaques DDoS
  - Révélation aux médias, aux clients, etc.

- Montant variable de la rançon : des cas montrent qu'il peut osciller entre **200 000 et 10 millions de dollars**.



QUELS SONT LES DÉGÂTS D'UNE ATTAQUE PAR RANÇONGICIEL ?

UNE MENACE AUX CONSEQUENCES SOUVENT DRAMATIQUES

- Des coûts très élevés pour les victimes :
  - Estimés à plusieurs dizaines de millions d'euros minimum.
  - Des **pertes financières au-delà de la rançon** :
    - **Coût des investigations** pour restaurer le système d'information
    - **Coût de la remédiation** du système d'information
    - Perte d'exploitation à durée variable (ex : arrêt de la production pour une usine)

  - **Risque sur la vie des citoyens** (par exemple : pour les établissements de soins)
  - **Atteinte à l'image** et perte de confiance à l'égard de l'organisation victime
  - **Perte de données** : R&D, comptabilité, facturation, projets, données de clients…

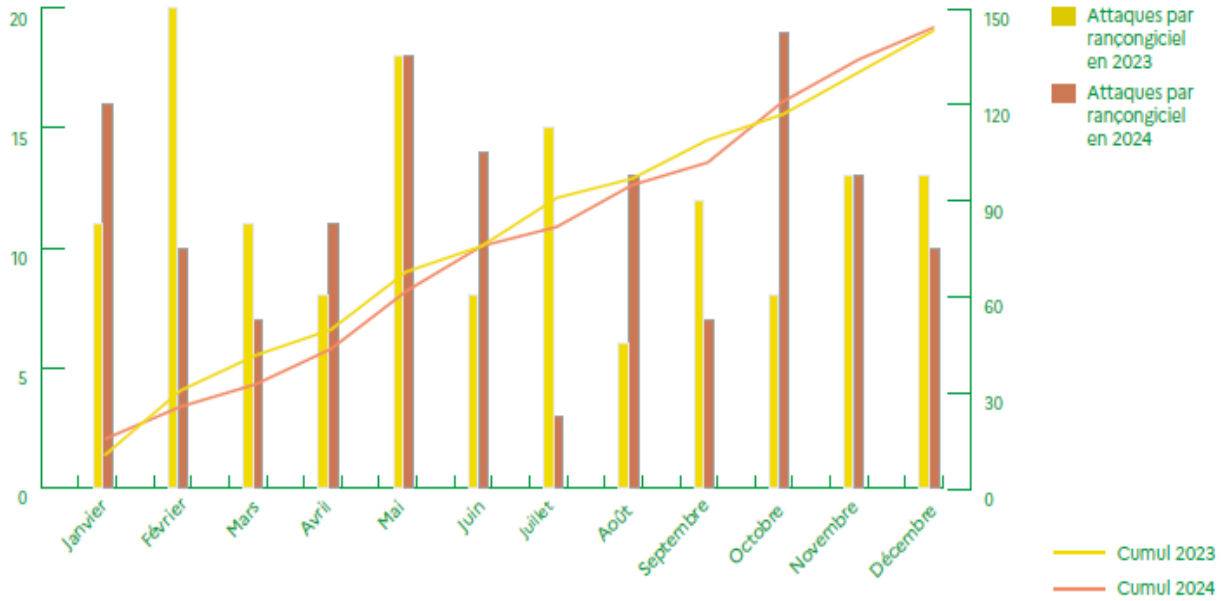
COMMENT LA CYBERCRIMINALITÉ S'ORGANISE ?

UNE MENACE PAR RANCONGICIEL CROISSANTE

- « **Ransomware-as-a-service** » :
  - Désormais, des rançongiciels disponibles sur les marchés cybercriminels
  - Sophistication des moyens et écosystème criminel fournissant un support sur toute la chaîne d'infection.

- Des **revenus estimés en millions de dollars** pour les attaquants, disposant de moyens de pression forts :
  - Recherche de la rupture d'activité
  - Exfiltration de données, etc.

- Une **rentabilité des attaques bien supérieure au coût de mise en œuvre**, d'où une prolifération des attaques et des attaquants.



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

UNE OPPORTUNITE POUR FAIRE FACE COLLECTIVEMENT A LA MENACE SYSTEMIQUE

- **Fin 2020 : décision de la Commission européenne d'étendre le périmètre et les ambitions de la directive** afin de soutenir largement les acteurs économiques et politiques de l'UE dans la maîtrise de leur cybersécurité.
  - Des milliers d'entités concernées par la directive NIS 2 à l'échelle nationale

- **2022 : adoption de la directive NIS 2 et transposition en droit français en cours** pour préciser le périmètre, les exigences de sécurité et les mécanismes de régulation.

- **Les mesures de la directive NIS 2 garantiront, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté aux risques existants.**
  - Elles restent dans la lignée de l'actuelle réglementation NIS 1 tout en la précisant.
  - Elles sont également dans la continuité des principes de cyber hygiène demandés par l'ANSSI depuis sa création afin que le maximum d'entités puissent se protéger face à la cybermenace.

2. PRÉSENTATION DU CONTENU DE LA DIRECTIVE

LE PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2 : COMMENT SAVOIR SI MON ENTITÉ EST CONCERNÉE ?

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

A QUI S'ADRESSE NIS 2 ?

- La directive NIS 2, en France concerne plusieurs milliers d'entités fournissant leurs services ou exerçant leurs activités, sur **18 secteurs d'activité**.

- Ces milliers d'entités, publiques ou privées, peuvent être regroupées en **plusieurs catégories. Les principales catégories concernées sont :**
  - Les grandes entreprises
  - Les entreprises de taille intermédiaire
  - Les moyennes entreprises
  - Les administrations centrales et leurs EPA sous tutelle
  - Les collectivités territoriales

- **Les très petites et petites entreprises ne sont pas concernées par NIS 2** (sauf certains cas très spécifiques détaillés ci-après).

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

EXEMPLE DE TYPE D'ENTITÉ AU SEIN DU SECTEUR « ENERGIE »

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 [1], 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 [2] — 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 [3]
	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 [4]
	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 [5]
		— 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, **seront concernées par NIS 2 les entités de taille moyenne, intermédiaire ou grande**, réalisant des activités au sein de l'Union européenne et identifiées dans les annexes 1 et/ou 2 (sauf certaines exceptions, cf. diapositive suivante).

- De manière simplifiée, les critères et seuils correspondant aux entités régulées par NIS 2 sont :
  - Nombre d'**employés supérieur ou égal à 50**

  OU

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

Pour en savoir plus :

La directive NIS 2 reprend les seuils fixés à l'article 2 de l'annexe de la recommandation 2003/361/CE définissant des catégories d'entreprises, accessible ici : **Recommandation de la Commission Européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises**

La Commission européenne a également rédigé un guide expliquant la recommandation à l'usage des PME, au lien suivant : **Guide de l'utilisateur pour la définition des PME - Publications Office of the EU (europa.eu)**

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 généraux **selon des critères de criticité (cf. article 2.2, points b) à e) de la directive).** Ces désignations unitaires ne pourront intervenir **qu'une fois le processus de transposition de la directive NIS 2 finalisé**.

- 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 certains types d'entités** visés à l'annexe 1 ou 2, la directive s'applique **quelle que soit leur taille** :
  - Les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public
  - Les prestataires de services de confiance
  - Les registres de noms de domaine de premier niveau
  - Les fournisseurs de services de systèmes de noms de domaine.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

QUELQUES EXCEPTIONS ET CAS PARTICULIERS : LES FSEND

- Les **entités fournissant des services d'enregistrement de noms de domaine (FSEND)** sont également régulées par la directive NIS 2. Cependant, elles **n'entrent pas dans la catégorie des entités essentielles ou importantes.**

- Conformément à la directive NIS 2, elles disposent néanmoins de plusieurs obligations spécifiques, à savoir :
  - **L'enregistrement de l'entité auprès de l'autorité nationale compétente**
  - La **collecte des données d'enregistrement de noms de domaine et le maintien de leur exactitude** et de leur complétude **au sein d'une base de données spécialisée**, en conformité avec le RGPD.

- **Dans le cas où un FSEND serait également EE ou EI, il devra également mettre en œuvre les obligations incombant aux EE ou EI respectivement** :
  - Dans le cas où il exercerait une ou plusieurs activités des annexes 1 et 2 et atteindrait les seuils correspondants (par ex., s'il est qualifié aussi comme « fournisseur de services DNS ») ;
  - Ou s'il est désigné comme EE ou EI par l'Etat membre.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

QUELQUES EXCEPTIONS ET CAS PARTICULIERS : L'ARTICULATION AVEC NIS 1 ET REC

Différentes mécaniques sont également prévues dans la directive afin d'assurer une continuité avec les réglementations existantes et faciliter l'articulation avec d'autres réglementations :

- **La continuité avec la directive NIS 1 :**
  - Toute entité désignée « opérateur de service essentiel » au titre de NIS 1 deviendra « entité essentielle » au titre de NIS 2

- **L'articulation avec la directive Résilience des Entités Critiques (REC) :**
  - Toute entité désignée comme « opérateur critique au titre de la directive REC sera automatiquement « entité essentielle » au titre de NIS 2

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

QUELQUES EXCEPTIONS ET CAS PARTICULIERS : L'ADMINISTRATION PUBLIQUE

- Le **périmètre précis de l'administration publique et des collectivités territoriales** régulées par NIS 2 sera défini **à l'issue du processus législatif et réglementaire** prévue par la transposition :
  - Collectivités territoriales : l'article 2.5 de la directive NIS 2 laisse la possibilité aux Etats membres de les inclure dans le périmètre de la directive.
  - L'ANSSI a saisi cette opportunité en proposant l'intégration dans le projet de loi des plus grandes collectivités territoriales qui exercent les activités les plus sensibles et au regard de l'impact sur la population. En effet, en 2023, les collectivités territoriales ont représenté 24% des victimes d'attaques par rançongiciel constatés par l'ANSSI.
  - Leur statut définitif dépendra de l'issue du débat parlementaire, notamment leur catégorisation entre « entités essentielles» et « entités importantes ».

- Par ailleurs, la directive NIS 2 **ne s'applique pas aux entités de l'administration publique** qui exercent leurs **activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi,** y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

QUELQUES EXCEPTIONS ET CAS PARTICULIERS : LES « ACTEURS DU NUMERIQUE »

- La directive NIS 2 prévoit des mécaniques particulières pour certains acteurs, appelés **« acteurs du numérique »** par souci de simplification. **En raison de la nature transfrontalière de leurs services** et afin d'harmoniser leur supervision par les Etats membres, ces entités **font l'objet d'un traitement spécifique concernant** :
  - La mécanique de rattachement à un Etat membre en ce qui concerne la juridiction et les mécaniques de supervision.
  - Les obligations relatives à la notification d'incident et aux mesures de gestion des risques cyber du règlement d'exécution 2024/2690 de la Commission européenne (cf. lien suivant : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202402690

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

Annexe 1, secteurs 8 et 9 :

- 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, secteur 6 :

- 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

A noter : le règlement d'exécution s'applique également aux prestataires de service de confiance mais ceux-ci ne sont pas soumis aux obligations de l'article 26 de la directive NIS 2 concernant la juridiction et l'établissement.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

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**.

- La **notion « d'établissement » correspond à l'exercice effectif d'une activité**, au moyen d'une installation permanente, indépendamment de la forme juridique adoptée (siège statutaire, succursale, etc.).
  - ➢ La notion d'entité « établie » sur le territoire d'un Etat membre est donc **indépendante de la localisation des SI** qui peuvent être hébergés dans un autre Etat membre, voire hors de l'Union européenne.
- A noter : si une EE ou EI **relève de la compétence d'un ou plusieurs Etats membres, elle se conforme aux lois en vigueur dans cet(ces) Etat(s)** et met en œuvre les obligations subséquentes.

PÉRIMÈTRE DES ENTITÉS RÉGULÉES PAR NIS 2

LA JURIDICTION À L'ÉCHELLE EUROPÉENNE : EXCEPTIONS (cf. article 26 de la directive)

- **Exceptions concernant la notion « d'établissement » :**
  - 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 » (hors prestataires de services de confiance)** 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.

- **Pour déterminer l'Etat de juridiction d'un « acteur du numérique », se poser les questions suivantes, dans l'ordre suivant** :
  - Où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité ?
  - Si un tel Etat membre ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union européenne, où les opérations de cybersécurité sont-elles effectuées ?
  - Si un tel Etat membre ne peut être déterminé, dans quel pays de l'UE l'entité possède-t-elle l'établissement comptant le plus de salariés ?
  - Si *in fine*, un acteur du numérique n'est pas établi dans l'Union européenne, alors il doit désigner un représentant dans un Etat membre de l'Union européenne, dans l'un des Etats membres dans lesquels les services sont fournis.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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.
- **Les régimes de supervision :**
  - Pour les **EE** : régulation proactive, dite « ex-ante » (contrôle à discrétion de l'autorité nationale compétente) ou réactive, dite « ex-post » (contrôle en cas de connaissance ou de suspicion forte d'une non-conformité)
  - Pour les **EI** : régulation réactive ou dite « ex-post » exclusivement
- **Les sanctions**
  - Seront d'une ampleur comparable à celles 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 ***ET*** 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

Rappel : sont également considérées **entités essentielles**

- toute entité soumise à la directive Résilience des Entités Critiques (REC) ;
- toute entité désignée Opérateur de Service Essentiel au titre de NIS 1.

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 ≥ 250	OU	(y ≥ 50	ET	z ≥ 43)	ENTITES ESSENTIELLES	ENTITES IMPORTANTES
MOYENNE	250 > x ≥ 50	OU	(50 > y ≥ 10	ET	43 > z ≥ 10)	ENTITES IMPORTANTES	ENTITES IMPORTANTES
MICRO ET PETITE	x < 50	ET	(y < 10	OU	z < 10)	*Non concernées*	*Non concernées*

LES ENTITÉS ESSENTIELLES ET IMPORTANTES

EN SYNTHESE :

- Les **petites et micro-entreprises ne sont pas concernées**, à l'exception des :
  - Fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public
  - Prestataires de services de confiance
  - Registres de noms de domaine de premier niveau
  - Fournisseurs de services de systèmes de noms de domaine
  - Désignations unitaires prévues par la directive

- En règle générale, sauf cas particuliers, les **moyennes entreprises seront « entités importantes »**.
  - Les ETI et grandes entreprises de l'annexe 1 seront « entités essentielles ».
  - Les ETI et grandes entreprises de l'annexe 2 seront « entités importantes ».

- Les exceptions concernent :
  - les entités soumises à REC et à NIS 1
  - les entités désignées unitairement

i

Ressources utiles : Consulter aussi la FAQ sur MonEspaceNIS2
Quels sont les seuils financiers et d'effectifs à prendre en compte pour déterminer si mon entité est régulée ? | FAQ MonEspaceNIS2 Bêta

LES ENTITÉS ESSENTIELLES ET IMPORTANTES

EN SYNTHESE :

- **Les acteurs du numérique :**
  - **Peuvent être EE ou EI en fonction de leurs types d'entités ;**
  - Disposent de règles spécifiques pour définir l'Etat membre de l'Union européenne compétent pour les superviser (hormis pour les prestataires de services de confiance) ;
  - Devront mettre en œuvre des **mesures de gestion des risques cyber spécifiques** avec certaines différences par rapport au cas général, **notamment concernant les obligations relatives à la notification « d'incidents importants ».**

- Les **FSEND :**
  - Ne sont ni EE ni EI.
  - Ne seront soumis qu'à l'obligation d'enregistrement et l'entretien de la base de données des noms de domaines.
  - Seront également soumis à la mécanique spécifique de l'article 26 de la directive concernant l'établissement et la juridiction.

- **Règle par défaut** de délimitation du périmètre. La directive est globalement très prescriptive.

- **Néanmoins, mécanismes d'ajustement à la marge** du périmètre et **clarification nécessaire** sur le détail de certains types d'entité, prévue via la transposition en droit national.

OBLIGATIONS POUR LES ENTITÉS

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

NOTIFICATION & CONTACT : COMMENT S'ENREGISTRER ?

1) Enregistrement auprès de l'autorité nationale compétente

- Obligation de **fournir certaines informations de contact à l'autorité nationale** désignée et de les mettre à jour en cas de modification.

- Pour y répondre de manière simple, **l'enregistrement s'effectuera via un portail numérique** mis à disposition par l'ANSSI. Il permettra, dans la mesure du possible, de rapatrier des données préalablement communiquées à l'Administration française.

Données nécessaires à minima pour l'enregistrement :

- Dénomination ou raison sociale de l'entité
- Numéro SIREN le cas échéant
- Taille de l'entité (effectifs, chiffre d'affaires et bilan)
- Adresse et coordonnées actualisées
- Secteur(s) d'activité
- Liste des Etats membres de l'UE dans lesquels sont fournis les services
- Noms, coordonnées et qualité de la personne procédant à l'enregistrement
- Coordonnées et qualité d'un point de contact « sécurité numérique » désigné auprès de l'ANSSI pour les sujets relatifs à la sécurité numérique
- Plages d'IP exposées sur internet

Autres données spécifiques à fournir pour les « acteurs du numérique » (hors prestataires de services de confiance) :

- Coordonnées des autres établissements légaux dans l'UE
- Coordonnées, si l'entité n'est pas établie dans l'UE, de son représentant désigné dans l'UE.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

NOTIFICATION & CONTACT : POURQUOI S'ENREGISTRER ?

- Au-delà du respect des obligations réglementaires, **s'enregistrer auprès de l'ANSSI permettra de bénéficier d'un certain nombre de services**, aidant l'entité au quotidien dans la gestion du risque cyber et le renforcement de sa protection contre la menace systémique.

- Exemple de services :
  - Recevoir des **alertes**, alertant par exemple sur la vulnérabilité d'un produit ;
  - Des **lettres d'information** sur des sujets cyber spécifiques ;
  - Des **actualités sur les services et les propositions de l'ANSSI** pour accompagner les entités dans leur conformité ;
  - Etc.

- A noter : l'enregistrement devra être réalisé par une personne ayant officiellement le mandat pour représenter son entité auprès de l'ANSSI.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

DÉCLARATION DES INCIDENTS IMPORTANTS : COMMENT DECLARER SES INCIDENTS ?

2) Déclaration à l'ANSSI des incidents importants

- La directive demande aux EE et EI de **déclarer tout incident ayant un « impact important »** sur la fourniture de leurs services et activités.
  - Un décret en Conseil d'Etat fixera les modalités d'application de la déclaration de ces incidents, notamment les critères d'appréciation de leur caractère important inspirés probablement de ceux du règlement d'exécution 2024/2690.

- La déclaration d'incident s'effectuera en **plusieurs étapes** :
  - Notification sous 24H
  - Rapport intermédiaire, avec d'éventuelles informations complémentaires si disponibles
  - Rapport final

Définition d'un incident important dans la directive :	**Il est qualifié d'« important » lorsque :**
Un incident est défini par la directive à l'article 6.6 comme « un 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 ».	« a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ; b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables. » *NB : les acteurs du numérique devront se baser sur le règlement d'exécution 2024/2690 pour déterminer les incidents importants à notifier à l'ANSSI.*

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

DÉCLARATION DES INCIDENTS MAJEURS : POURQUOI DECLARER SES INCIDENTS ?

- **Au-delà du respect pur et simple de ses obligations réglementaires, notifier ses incidents a des retombées positives à tous les niveaux :**
  - Au niveau national et européen, cela permet à l'autorité nationale d'avoir une meilleure visibilité sur l'état de la menace, de détecter d'éventuelles attaques de grande ampleur et de réagir le plus vite possible.
  - En parallèle de son rôle d'autorité de supervision NIS 2, l'ANSSI est depuis toujours engagée dans l'accompagnement et l'assistance, notamment des victimes. Ainsi, être tenu au courant nous permettra de vous aiguiller si besoin vers des solutions de remédiation.
- **L'objectif de la réglementation est de réduire le nombre d'incidents et de savoir y réagir !**
- **Avoir un incident n'est pas nécessairement gage d'une mauvaise implémentation des mesures de cybersécurité.**

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2

Périmètre d'application des mesures de sécurité :

- **Cf. article 21 de la directive** : *« 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 »
- Mais **continuité entre NIS 1 et NIS 2** : d'ici à l'entrée en vigueur de NIS 2, les exigences NIS 1 demeurent applicables et les futures exigences NIS 2 s'inscriront dans le prolongement des efforts de NIS 1.
- Tous les travaux d'ores et déjà entrepris par les opérateurs seront valorisés dans NIS 2.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2

Des mesures de gouvernance définies dans l'article 20 de la directive … :

- **Les organes de direction des entités régulées approuvent les mesures de gestion des risques cyber** prises par ces entités, **afin de se conformer à l'article 21 de la directive et de superviser sa mise en œuvre**.
- En outre, les membres de ces organes de direction doivent également **suivre une formation**.
- Ils sont aussi **encouragés à offrir régulièrement une formation similaire aux membres de leur personnel** afin que ceux-ci acquièrent des connaissances et des compétences suffisantes :
  - pour déterminer les risques ;
  - et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2 :

…et des mesures de gestion des risques cyber, listées à l'article 21 de cette même directive :

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 (ex : gestion des sauvegardes, reprise d'activité, 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 (cyber-hygiène 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 : LE REFERENTIEL NATIONAL

Ce que prévoit la directive :

- **Gouvernance par les organes de décision**
  - Que les organes de direction des entités régulées approuvent les mesures cyber et leur supervision
  - Cf. article 20 de la directive
- **Mesures de gestion des risques afin d'assurer la continuité des activités quotidiennes et des services fournis par l'entité**
  - 10 thématiques
  - Cf. article 21 de la directive

Ce que prévoit l'ANSSI :

- **Les objectifs à atteindre**
  - Traduction technique, opérationnelle et organisationnelle des mesures des articles 20 et 21 de la directive en objectifs de sécurité. Ils seront obligatoires.
- **Les mesures de sécurité pour atteindre ces objectifs**
  - Elles constituent des « moyens acceptables de mise en œuvre » dont le respect permet d'atteindre les objectifs.
  - Elles sont non obligatoires, l'entité reste libre de mettre en œuvre les moyens qu'elle souhaite tant qu'ils permettent l'atteinte des objectifs susmentionnés.
- **Une proportionnalité respectée entre EE & EI : définir un niveau pertinent au regard de la menace systémique mais atteignable**
  - En projet : 2 référentiels apparentés, l'un pour les EE, l'autre pour les EI
    - Certains objectifs applicables qu'aux EE
    - Pour certains objectifs communs aux EE & EI, un niveau d'exigence à atteindre moindre pour les EI

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

EN SYNTHESE :

- EXPERIENCE ANSSI : LPM, NIS 1
- CONTINUITE NIS1/NIS2
- LA MENACE (notamment rançongiciels)
- MESURES NIS2 UE

ANALYSE DE RISQUES

NIVEAU DE CYBERSÉCURITÉ adapté à la menace & atteignable

PROPOR--TIONNALITÉ

- RÉFÉRENTIEL EE
- RÉFÉRENTIEL EI

A noter : un référentiel en cours de rédaction en coordination avec les associations professionnelles et d'élus, notamment pour prendre en compte la réalité des petites structures.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2 : LE CAS DES ACTEURS DU NUMERIQUE

- En tant qu'EE ou EI, **ils disposent des mêmes obligations que dans le cas général** (enregistrement de l'entité, notification des incidents importants, mise en œuvre des mesures de cybersécurité).

- Néanmoins, ils seront **soumis aux exigences relatives aux mesures de sécurité du règlement d'exécution (UE) 2024/2690** publié par la Commission européenne et **non celles transposées à l'échelle nationale.**

- Ces **exigences sont détaillées dans l'annexe de ce règlement** et sont définies pour chacune des 13 thématiques, qui reprennent celles des mesures de cybersécurité listées à l'article 21.2 de la directive NIS 2 :
  1) Politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;
  2) Gestion des incidents ;
  3) Continuité des activités ; Etc.

- Respect du **principe de proportionnalité** : les entités doivent assurer un niveau de cybersécurité adapté selon leur exposition aux risques, leur taille et la probabilité de survenance d'incidents et de leur gravité.

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2 : LE CAS DU SECTEUR FINANCIER

- Les entités relevant des secteurs d'activité « **secteur bancaire** » et « **infrastructures des marchés financiers** » de l'annexe 1 de la directive NIS 2 et les entités du secteur financier désignées OSE au titre de la réglementation NIS 1 (assurances…) **sont également régulées par le règlement (UE) DORA 2022/2554 pour la Résilience Opérationnelle Numérique**, applicable en l'état dans tous les Etats membres de l'Union européenne depuis le 17 janvier 2025.

- **Réglementation DORA comme *lex specialis* de la directive NIS 2**, ce qui signifie qu'elle prime sur la réglementation NIS 2 pour une partie des obligations de cette dernière.

- Pour ces entités, **les obligations du règlement DORA** en matière de gestion des risques, de notification d'incidents et de supervision **se substitueront donc aux obligations du même type de la directive NIS 2**.

- **En revanche, les autres obligations de la directive NIS 2 demeureront** (ex : celles relatives à l'enregistrement des EE et EI auprès de l'autorité nationale compétente).

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

EN SYNTHESE :

OBLIGATIONS NIS 2	ENTITES NIS 2						
		ENTITES IMPORTANTES			ENTITES ESSENTIELLES		
	FSEND*	Cas général**	Acteurs du numérique ***	Prestataires de service de confiance	Cas général**	Acteurs du numérique ***	Prestataires de service de confiance
ENREGISTREMENT							
Communication des informations de contact	✓	✓	✓	✓	✓	✓	✓
Informations complémentaires sur les établissements le cas échéant	✓	-	✓	-	-	✓	-
Informations complémentaires sur le représentant le cas échéant	✓	-	✓	-	-	✓	-
NOTIFICATION D'INCIDENT							
Définition d'un incident au niveau national	-	✓	-	-	✓	-	-
Définition d'un incident spécifique par le règlement d'exécution	-	-	✓	✓	-	✓	✓
REGLES DE CYBERSECURITE							
Référentiel national EI	-	✓	-	-	-	-	-
Référentiel national EE	-	-	-	-	✓	-	-
Règles de cybersécurité spécifiées par le règlement d'exécution	-	-	✓	✓	-	✓	✓
SUPERVISION ET CONTRÔLE							
Ex-post	-	✓	✓	✓	✓	✓	✓
Ex-ante	-	-	-	-	✓	✓	✓
SANCTIONS (sous réserve du vote du projet de loi)							
≤ 1,4% du CA mondial ou ≤ 7 millions €	-	✓	✓	✓	-	-	-
≤ 2% du CA mondial ou ≤ 10 millions €	-	-	-	-	✓	✓	✓

(*) : FSEND : Fournisseurs de Services d'Enregistrement de Noms de Domaine

(**) : Le cas de figure des entités soumises au règlement DORA sera explicité après adoption des textes de transposition de la directive NIS2.

(***) : Les secteurs d'entités concernés par le règlement d'exécution au titre des annexes I et II de la directive NIS 2, cf. liste de l'encart du slide 27.

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 font partie des sujets instruits lors des **consultations avec l'écosystème** des futures entités régulées.

Quelques exemples :

- Sont fixés par la directive :
  - **Délai de mise à jour** des informations de contact en cas d'évolution de ces dernières (15 jours) ;
  - **Notification initiale d'un incident** sous 24H.

- Seront fixés dans le cadre de la transposition nationale, par décret :
  - **Délai d'enregistrement** auprès de l'autorité nationale compétente et de mise en œuvre de l'obligation de déclaration des incidents : l'ANSSI propose un délai de 6 mois après promulgation des textes législatifs et réglementaires
  - **Délai de mise en conformité avec les objectifs de sécurité** : l'ANSSI propose un délai de 3 ans, après promulgation des textes législatifs et réglementaires, avant d'exiger une conformité complète

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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 simplifiés :
  - Inspection sur place et 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 des preuves de la mise en œuvre des politiques de cybersécurité, tels que les résultats d'audits de sécurité

- **Une supervision qui respectera le principe :**
  - de proportionnalité entre EE et EI (cf. supra) ;
  - et d'impartialité : refonte des processus en cours à l'ANSSI pour séparer missions d'appui aux victimes et les missions de contrôle et d'instructions en amont de sanctions.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

- 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 écosystèmes concernés (secteurs d'activité et collectivités territoriales)

LA TRANSFORMATION DE L'ANSSI AU REGARD DE NIS 2

UNE MISSION INCONTOURNABLE : RÉPONDRE AUX BESOINS D'ACCOMPAGNEMENT

- Tout en intégrant la capacité de sanction et en renforçant l'activité de contrôle, conserver en tant que régulateur **une mission d'accompagnement.**

- Adapter l'accompagnement aux nouvelles entités régulées, **par une communication proactive et en partenariat avec les associations et les fédérations consultées par l'ANSSI.**

- Développer des **services numériques** comme par exemple MonEspaceNIS2, MesServicesCyber, MonAideCyber ou MonServiceSécurisé.

- Développer des relais locaux et industriels : **mobiliser et & coordonner tout un écosystème**
  - Les ministères, dans leur rôle de coordination sectorielle
  - Les organisations professionnelles
  - Des acteurs comme le groupement d'intérêt public Cybermalveillance, accompagnant de nombreuses petites structures
  - Des relais locaux comme les Chambres de Commerce & d'Industrie
  - Les CSIRT territoriaux, etc.

3. TRANSPOSITION NATIONALE

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.
- Articulation et simplification du cadre réglementaire : REC / LPM 2013 / DORA

Quelques informations :

- **Le projet de loi « Résilience des infrastructures critiques et renforcement de la cybersécurité » a été présenté en Conseil des Ministres** puis **déposé au Parlement** le 15 octobre 2024**.**
- Suite à **l'adoption du projet de loi par le Sénat le 13 mars** 2025, les **débats parlementaires se poursuivront, notamment à l'Assemblée Nationale,** pour aboutir à la version finale de la loi qui sera votée et promulguée. **Le calendrier des travaux parlementaires est à la main du Parlement**.
- En parallèle de cette procédure **existe un processus de consultations**, démarré en 2023 et qui se poursuivra par les **consultations réglementaires prévues dans les prochains mois.**

i Pour en savoir plus, consulter le projet de loi et les documents associés :
https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

4. ANTICIPER LA MISE EN ŒUVRE DE NIS 2

COMMENT SE PREPARER DES MAINTENANT ?

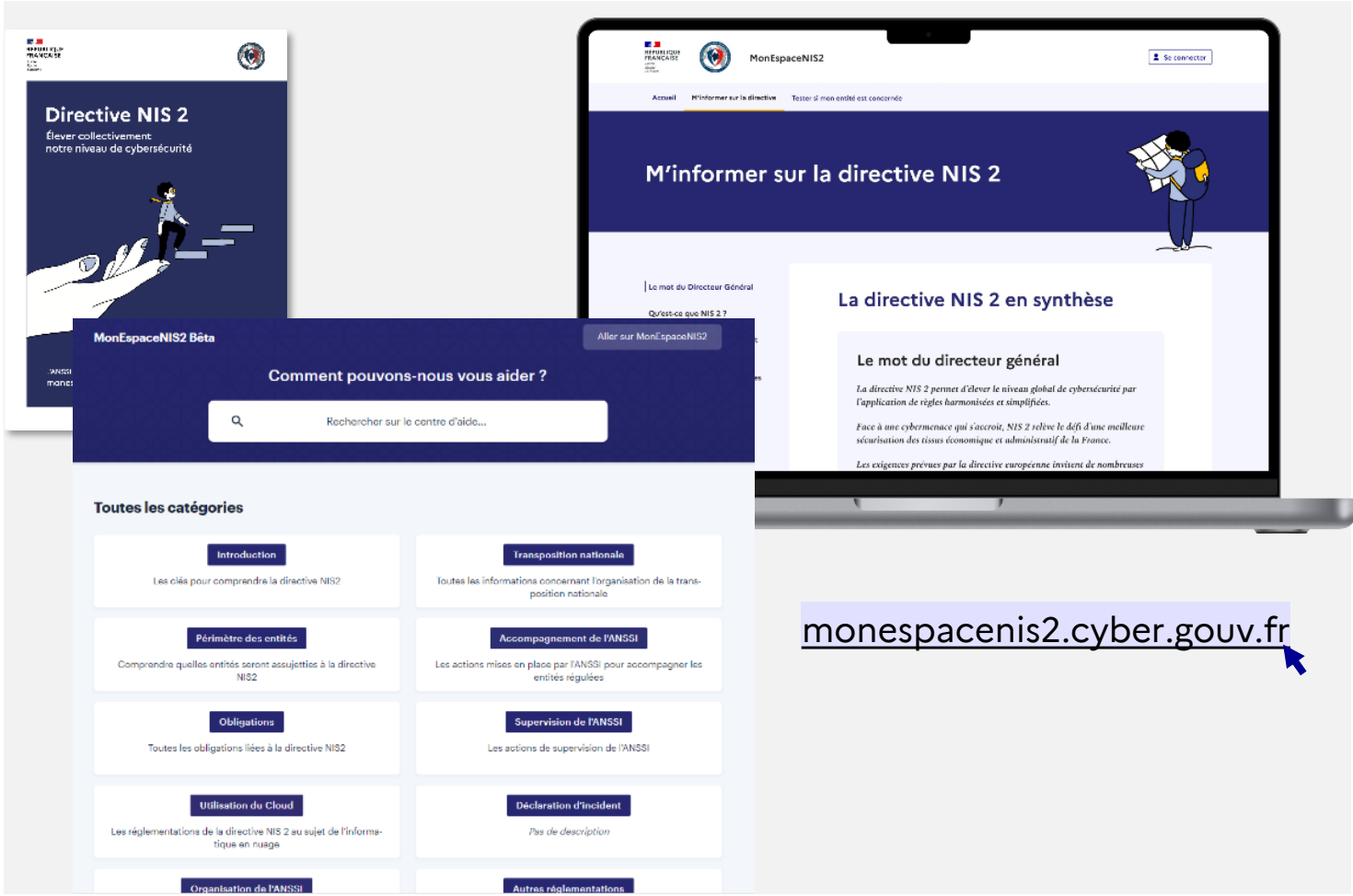
S'INFORMER : « MONESPACENIS2 »

- **Une page d'information générale sur la directive,** qui traite notamment des secteurs concernés, des obligations, etc.

- **Une FAQ, alimentée et enrichie régulièrement**, par les questions qui sont posées.

- **Inscription à la newsletter :** en laissant un email de contact, afin d'être informé de l'avancement de la transposition, des évolutions du site des évènements en lien avec NIS 2…

Les contenus sont mis à jour au fur et à mesure de l'avancement de la transposition en droit national.



monespacenis2.cyber.gouv.fr

COMMENT SE PREPARER DES MAINTENANT ?

DETERMINER SI MON ENTITE EST CONCERNEE PAR NIS 2

- **Utiliser le simulateur « Suis-je concerné ? » sur MonEspaceNIS2 :**
  - Un parcours **simple et rapide** pour **savoir si votre entité est régulée**
  - Et avoir une première indication sur son **statut « essentiel » ou « important »**

- **Y associer des compétences juridiques pour fiabiliser les résultats du test :**
  - Attention au risque de **confusion entre le secteur d'activités réalisées par l'entité et le secteur d'activité des clients qu'elle fournit** ou dont elle est sous-traitante ! Une telle confusion fausse les résultats du test.
  - Les entités utilisant le simulateur sont invitées à **renseigner les différentes rubriques avec soin**.
    - Exemple : *un fournisseur de turbine d'éolienne pouvant se considérer comme étant du secteur « Énergie », sera en réalité associé au secteur « Fabrication » (correspondant à l'industrie manufacturière) selon le prisme établi par la directive NIS 2.*
    - Exemple : p*our les entités du secteur de l'industrie manufacturière, consulter avec attention le secteur « Fabrication » de ce simulateur, qui regroupe plus de 500 activités distinctes.*

COMMENT SE PREPARER DES MAINTENANT ?

SE PREPARER AUX PREMIERES OBLIGATIONS

- **Identifier un responsable en charge de NIS 2**
  - Identifier une **personne qui prendra en charge le projet de mise en œuvre des obligations de la directive** et du maintien dans le temps du niveau de sécurité numérique de l'entité.

- **Se pré-enregistrer**
  - L'ANSSI mettra à disposition prochainement une **première version du service d'enregistrement** pour permettre aux entités d'anticiper l'obligation d'enregistrement.
  - Le service prévoira un parcours guidé pour répondre aux attentes de la directive et inclura des saisies automatiques dans la mesure du possible. Le lien vers le service de pré-enregistrement sera accessible depuis le site MonEspaceNIS2.

- **S'organiser pour être en mesure de notifier ses incidents importants**
  - Elle sera une obligation **dès la promulgation des textes législatifs et réglementaires**. La directive impose notamment qu'elle soit effectuée sans retard injustifié ou dans les 24 heures après avoir eu connaissance de l'incident important.
  - Il n'est pas nécessaire d'attendre l'entrée en vigueur des obligations pour déclarer à l'ANSSI ses incidents. Les entités sont invitées à le faire **dès à présent sur ClubSSI** afin de bénéficier d'un accompagnement à la remédiation le cas échéant.

COMMENT SE PREPARER DES MAINTENANT ?

MAÎTRISER LE PERIMETRE NIS 2 DE MON ENTITE

- **La directive NIS 2 impose de maîtriser ses risques cyber sur l'ensemble de ses systèmes d'information (SI)** y compris les SI qui sont tout ou partie externalisés.
- **Il est conseillé aux entités d'élaborer la liste de leurs SI (ou de la mettre à jour).**
- **Cette liste, intitulée « cartographie des systèmes d'information » constitue un élément de base pour les travaux de mise en œuvre à venir. Elle permet de :**
  - délimiter le périmètre des travaux de mise en œuvre des exigences de sécurité
  - identifier les systèmes les plus critiques pour l'entité
  - identifier les systèmes les plus vulnérables (en fonction de leur exposition à Internet par exemple)

i

Ressources utiles :
Question n°1 du **guide des TPE/PME**

Pour aller plus loin :
Le guide de l'ANSSI pour réaliser la cartographie des SI : **https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation**

COMMENT SE PREPARER DES MAINTENANT ?

DEMARRER LES PREMIERES ACTIONS DE SECURISATION

En attendant de connaître l'ensemble des obligations NIS 2, l'ANSSI recommande de se référer aux bonnes pratiques de sécurité numérique :

- **Pour les entités qualifiées d'« entités importantes** », en particulier les entités ayant un plus faible niveau de maturité cyber : **le Guide des TPE/PME** est une base solide de mesures concrètes par laquelle débuter.
  - **L'outil « MonAideCyber »** est recommandé pour amorcer une première étape de sécurisation cyber.

- **Pour les entités qualifiées d'« entités essentielles** » : le **Guide d'hygiène d'informatique** contient une liste de mesures et de grandes thématiques, permettant de réfléchir à une organisation en lien avec ces dernières.
  - Plus largement**, le référentiel de mesures de sécurité NIS 1** reste une source d'information significative.

L'ANSSI invite à la prudence quant aux informations circulant sur les mesures à mettre en œuvre ne provenant pas de l'ANSSI : la rédaction du référentiel NIS 2 est en cours et dépend du vote de la loi « Résilience ».

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

QUESTIONS / RÉPONSES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MERCI POUR VOTRE ATTENTION