Lundis de la Cyber - Cyber Résilience - Règlementations

26.02.2024

1. Introduction à la Cyber résilience
2. Règlementation Européenne : Introduction à NIS2 du point de vue opérationnel (exigences cyber)
3. Directive NIS2 : Contrôles, sanctions et responsabilités
4. Suite des réglementations européennes en matière de cyber résilience : REC, CRA, DORA
5. Conclusions

EY
Building a better working world

1

Introduction à la cyber résilience

1. Introduction – A propos de la résilience

Quelques definitions officielles (ENG) :

- Resilience is the ability to continuously deliver the intended outcome despite adverse cyber events *(source : Cyber Resilience – fundamentals for a definition)*

- Organizational resilience is the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper *(Source : BS 65000)*

- Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources *(Source NIST SP 800 v2)*

1. Introduction – Un contexte davantage « anxiogène » pour les organisations

Cyberattaque ou crise active (réactif)

Les cyberattaques ont créé des crises ou des incidents plus larges pour les organisations, ce qui a nécessité une réponse aux incidents à grande échelle.

Surveillance accrue du public (proactif)

Les incidents très médiatisés sur le marché entraînent une pression accrue pour maintenir la réputation et la confiance du public et des usagers/clients en cas d'incident de cybersécurité.

Assurance cybersécurité

La cyber assurance devient de plus en plus difficile à obtenir. Les assureurs ont des exigences plus élevées en matière de preuve d'une capacité d'intervention fonctionnelle.

Exigences relatives aux tiers

Les organisations sont de plus en plus tenues de fournir à leurs tiers la preuve qu'elles ont mis en place des contrôles et des capacités adéquats en matière d'intervention en cas d'incident (p. ex., des procédures de notification et d'intervention).

Événements géopolitiques

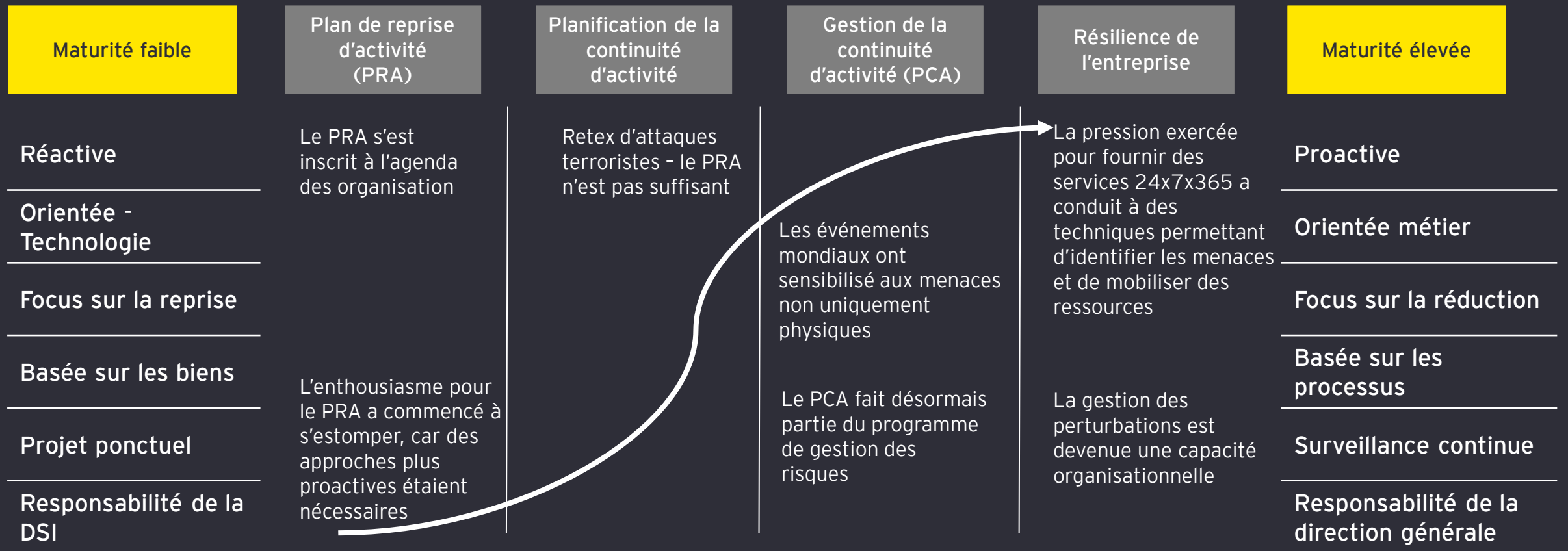
L'augmentation des menaces en raison des événements géopolitiques amplifie le risque que les organisations soient touchées.

Exigences réglementaires

Les exigences réglementaires sont de plus en plus strictes pour que les organisations disposent de capacités de réponse de base qui permettent de détecter efficacement un incident de cybersécurité et d'informer les personnes touchées par une violation de données.

1. Introduction – De la continuité d'activité à la résilience

La continuité des activités et la résilience de l'entreprise sont passées d'une pratique active basée sur la reprise à une pratique proactive et basée sur les risques



La continuité des activités et la résilience de l'entreprise sont un programme complexe et continu à l'échelle de l'organisation qui nécessite un soutien actif et la participation de la direction générale

1. Introduction – Concepts de la résilience

Comment définir la résilience ?

Concevoir et déployer des procédures opérationnelles métiers et des dispositifs qui permettent de fournir un niveau de service acceptable tel que défini par les métiers (et le cas échéant par les exigences réglementaires) dans le cadre d'erreurs, de stress et de défis aux opérations métiers en conditions normales

Les procédures et les biens doivent permettre le retour à la normale des opérations lorsque les facteurs de "stress" ou les perturbations ont été éliminés

Comment mesurer la résilience ?

Mesurer la résilience implique :

- Une capacité à **endurer des stress** brefs ou provisoire ou une capacité à continuer à délivrer des "services au niveaux *cibles* attendus"
- Des **délais limités dans le reporting** réglementaire ou marché en se basant sur des seuils d'acceptance et de perte de revenue
- Une **capacité à favoriser une endurance des opérations** mesurée par la productivité des métiers dans des environnements de pannes étendues (opérations métiers et IT)

1. Introduction – Qu'est-ce qu'être résilient face à la menace cyber ?

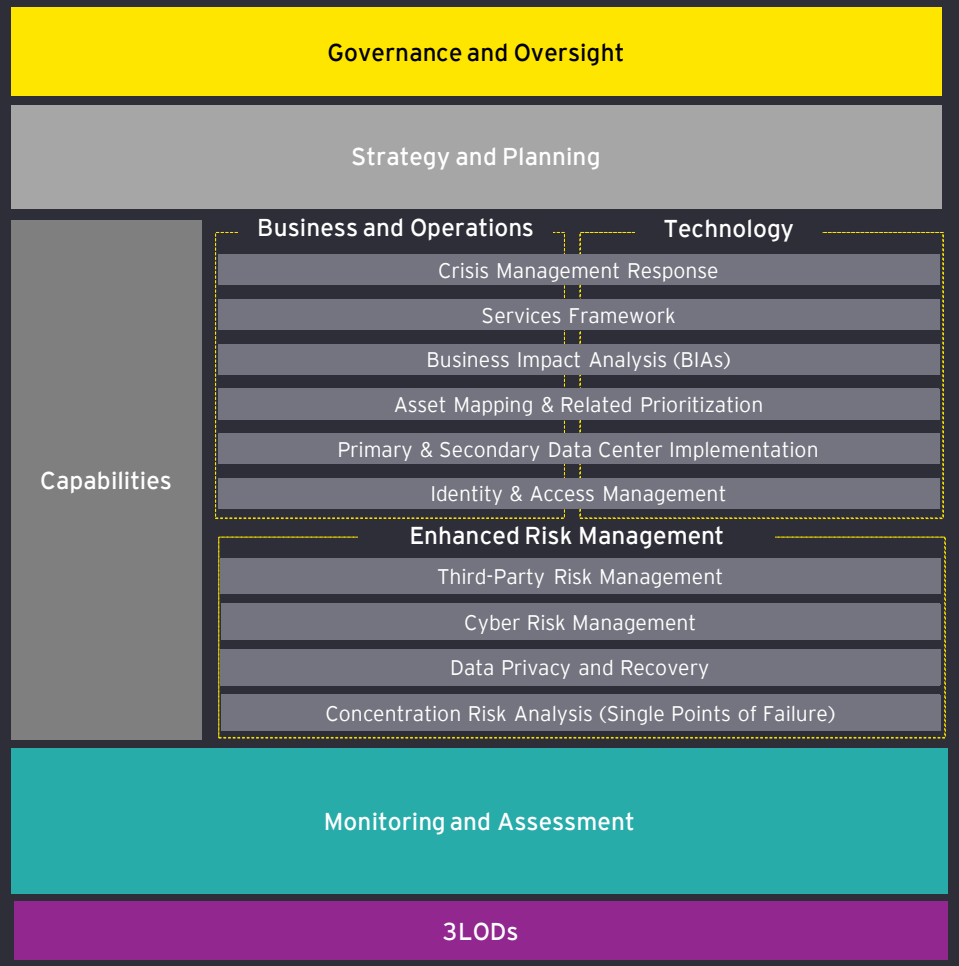
- La capacité d'une organisation à anticiper, résister, se remettre et s'adapter efficacement face à un incident cyber
- Celle-ci comprend à la fois la capacité d'une organisation à anticiper et à gérer le stress subi par ses mécanismes opérationnels et ses services essentiels, et à préserver sa réputation
- Les organisations résilientes sont capables de continuer à fournir des services essentiels, à opérer dans un mode de fonctionnement dégradé et, globalement, à réduire le temps et les coûts associés aux efforts de remédiation.

Anticiper	Maintenir un état de préparation informé face au risque
Résister	Assurer la continuité des opérations de l'organisation dans un climat d'attaque
Récupérer	Rétablir les opérations normales de l'organisation pendant et après l'attaque
Adapter	Modifier les mécanismes de résilience et/ou les capacités de soutien en fonction des leçons apprises et risques anticipés

*National Institute of Standards and Technology. (2021) *Developing Cyber-Resilient Systems* – NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

1. Introduction – Les axes de la cyber résilience

1. Introduction – Un framework complet



- Les administrateurs et le comité exécutif reçoivent-ils des rapports sur les cybermenaces, les risques et les incidents?
- Existe-t-il une appétence pour le cyber-risque avec des politiques et nomes définies ?

- Avez-vous considéré des scénarios pour vos événement BCP et DRP?
- Avez-vous considéré la composante Intégrité des incidents?
- Avez-vous analysé les coûts liés à une faille de sécurité?

- Avez-vous identifié les cyber-risques liés à votre business critique ?
- L'analyse d'impact de vos activités prend-elle en compte des scénarios liés à la cybercriminalité (ex: interruption du système, perte d'intégrité des données)?
- Avez-vous vérifié la vulnérabilité des points d'entrée pour un cyber-attaquant ?
- Savez-vous comment réagir si un cyber-attaquant dispose d'un accès privilégié à vos systèmes critiques?

- Avez-vous évalué le cyber-risque de vos principaux tiers et effectué des tests de pénétration et/ou des tests d'intrusion (red team) ?
- Est-ce qu'un programme de gestion des cyber-risques est en place et intégré ?
- Comment gérez-vous la confidentialité des données en cas de cyberattaque compromettant les systèmes contenant des données client?

- Réalisez-vous régulièrement des simulations/exercices en utilisant différents scénarios et avec différents acteurs?
- Rapportez-vous régulièrement à la direction les cyberincidents, les pertes dues aux cyberattaques et aux vulnérabilités connues?
- Avez-vous intégré la supervision du centre d'opération de sécurité (SOC) à un processus de contrôle plus large?

- La gestion des cyber-risques est-elle intégrée aux trois lignes de défense?

1. Introduction - Les enjeux de la cyber résilience

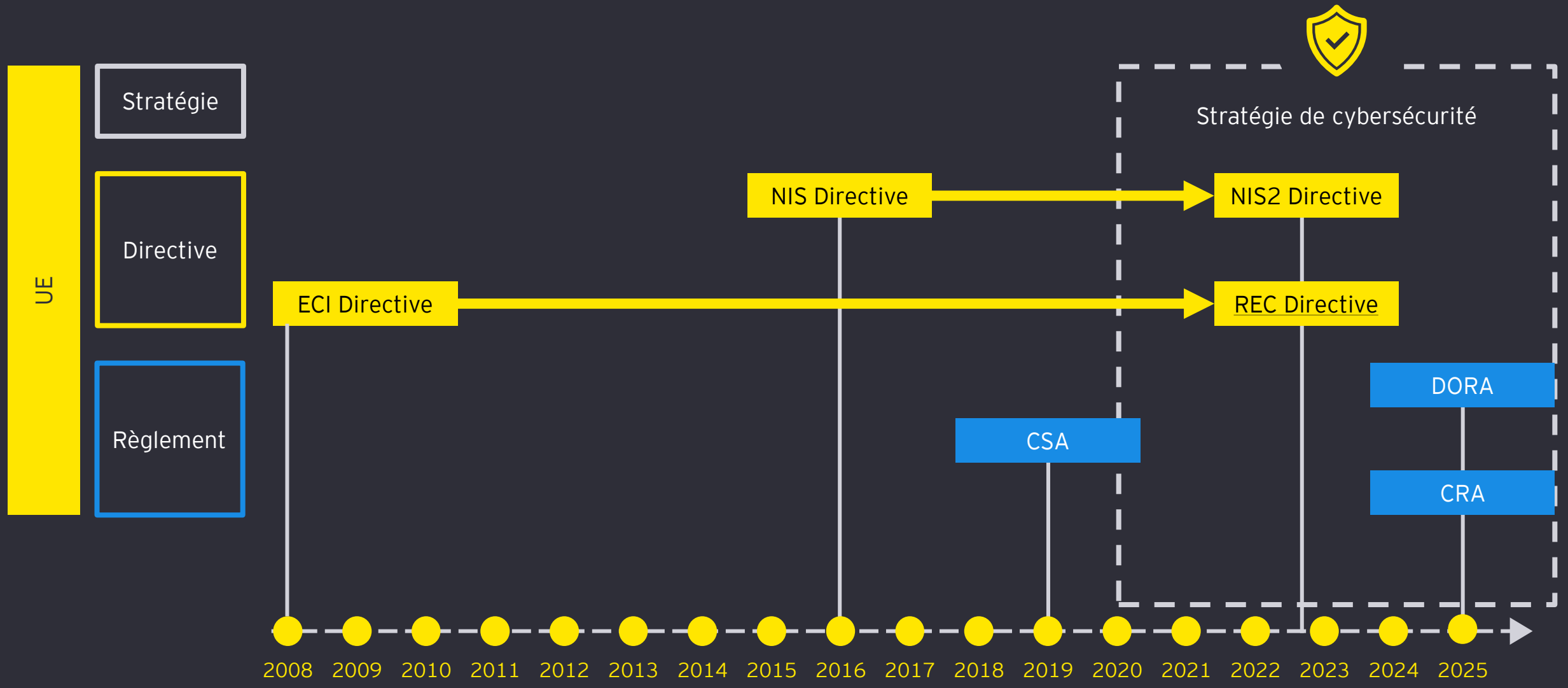
Les principaux défis à relever :

- ►Définir ce qui est **critique,** avec une vision exhaustive de **l'écosystème**
- ►Concevoir des **tests** de bout-en-bout suffisamment représentatifs
- ►Inculquer une **culture** de la cyber résilience et impliquer les métiers

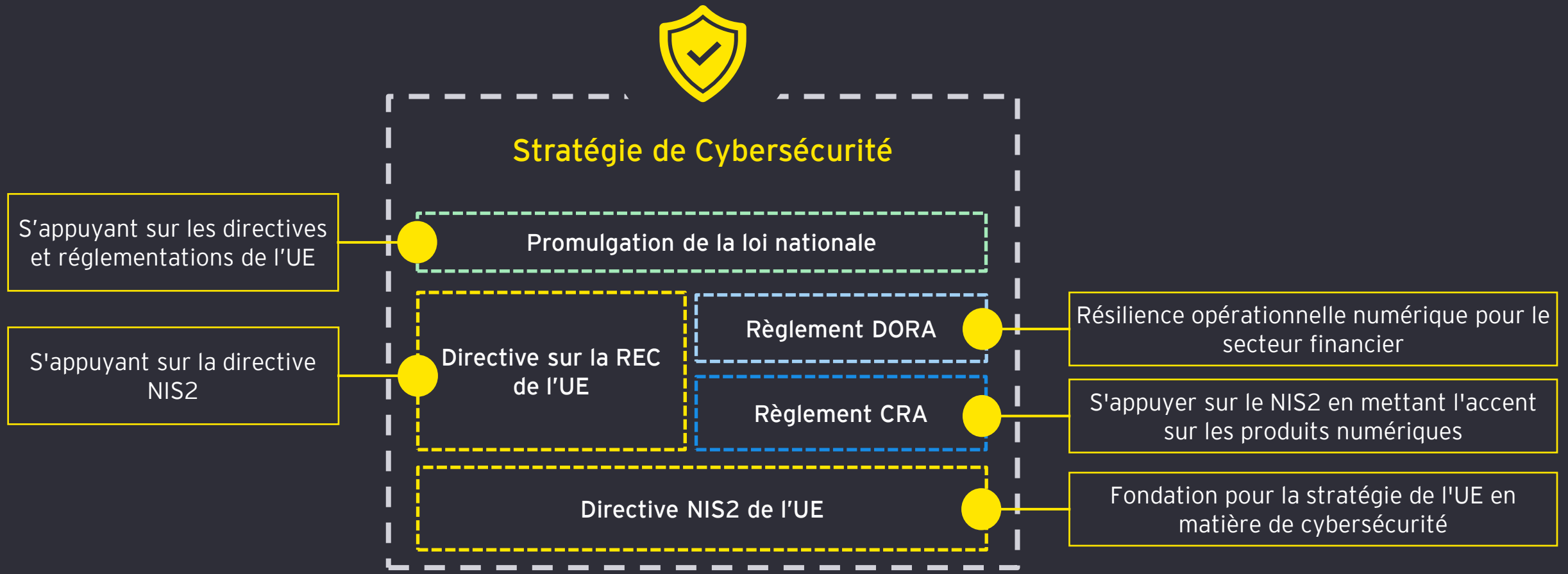
Pour répondre à ces défis, les organisations doivent :

- Gouvernance et prise en compte de l'exposition
- Gestion des tierces parties et des dépendances clés
- Protection des systèmes critiques
- Tests des systèmes et des plans de reprises
- Evaluation des risques
- Détection, réponse, reprise et communication
- Adoption de nouvelles technologies

1. Introduction – Réglementations Européennes



1. Introduction – Réglementations Européennes

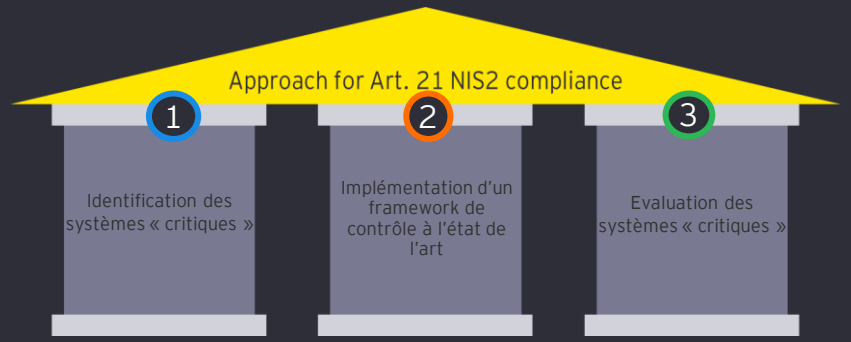


2

Focus sur la directive NIS 2

2. Directive NIS2 (SRI2) - Directive sur la sécurité des réseaux et de l'information

NIS2 redéfinit le cadre des normes minimales dans le domaine de la cybersécurité, élargissant ainsi considérablement le cadre réglementaire au niveau de l'UE en ce qui concerne les exigences en matière de sécurité de l'information pour les entreprises afin de renforcer les capacités de cybersécurité dans l'ensemble de l'Union, d'atténuer les menaces pesant sur les réseaux et les systèmes d'information utilisés pour fournir des services essentiels dans des secteurs clés et d'assurer la continuité de ces services en cas d'incidents



Périmètre

Entreprise moyenne + secteur + activités dans l'UE

- Taille moyenne = 50-250 employés et 10-50 millions d'euros de chiffre d'affaires ou 10-43 millions d'euros de bilan
- 35 secteurs définis (dont 16 suite à NIS 2)

Grandes entreprises + activités dans l'UE

- Ceux qui dépassent les seuils d'une entreprise moyenne

Entreprises spéciales (Secteur + Propriété définie par le NIS2)

- Quelle que soit leur taille

Prérequis*

Mesures de gestion des risques liés à la cybersécurité (article 21)

1 2 Les entités doivent prendre des mesures opérationnelles et organisationnelles pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information qu'elles utilisent pour leurs activités ou pour la fourniture de leurs services, et pour prévenir ou réduire au minimum l'impact des incidents sur les destinataires de leurs services et sur d'autres services.

3 L'entité qui constate qu'elle ne respecte pas les mesures doit prendre toutes les mesures correctives nécessaires, appropriées et proportionnées.

4 **Rapports obligatoires (article 23)**

- Notifier sans délai tout incident significatif
- **Évaluations des risques de sécurité des chaînes d'approvisionnement critiques à l'échelle de l'UE (Art. 22)**

Conséquences légale

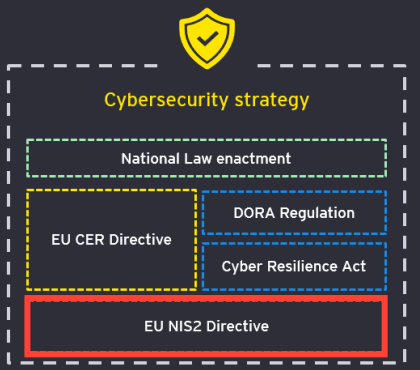
- Responsabilité personnelle des organes de gestion
- Augmentation des amendes
  - Entités ESSENTIELLES : 10 millions d'euros ou 2 % du chiffre d'affaires annuel
  - Entités IMPORTANTES : 8 millions d'euros ou 1,4 % du chiffre d'affaires annuel

Période statutaire

Mise en œuvre jusqu'en octobre 2024

* extrait

2. Directive NIS2 (SRI2) - Définition du périmètre



Directive NIS2

Article 1, paragraphe 1, et article 2 de l'annexe de la recommandation 2003/361/CE

Entreprises moyennes

1. 50-250 employés et 10-50 millions d'euros de chiffre d'affaires ou €10-43 M Bilan
+
2. Dans les secteurs définis à l'annexe I ou II de la directive NIS 2
+
3. Fournir des services ou exercer des activités dans l'UE

Grandes entreprises

1. >250 employés et >50 millions d'euros de chiffre d'affaires annuel ou > Bilan de 43 millions d'euros
+
2. Dans les secteurs définis à l'annexe I ou II de la directive NIS 2
+
3. Fournir des services ou exercer des activités dans l'UE

Les entreprises, quelle que soit leur taille

1. Dans les secteurs définis à l'annexe I ou II de la directive NIS2
+
2. **Exigence spécifique de l'art. 2 du** NIS2
   - Services spécifiques (article 2, paragraphes 2 et 4)
   - Entités critiques au sens de la directive REC (article 2, paragraphe 3)
   - Entités de l'administration publique et établissements d'enseignement (article 2, paragraphe 5)

3

Directive NIS 2 : Contrôles, sanctions et responsabilités

4

Suite des réglementations européennes en matière de cyber résilience : REC, CRA, DORA

4. Réglementations EU : Directive REC (CRE)

Brève description :

- Les entités CRITIQUES, en tant que fournisseurs de services ESSENTIELS, jouent un rôle indispensable dans le maintien de fonctions sociétales vitales ou d'activités économiques sur le marché intérieur dans une économie de l'Union de plus en plus interdépendante.
- Il est essentiel de mettre en place un cadre communautaire visant à :
  1) Renforcer la résilience des entités critiques dans le marché intérieur en établissant des règles harmonisées
  2) Apporter des mesures de soutien et de supervision cohérentes et spécifiques

Champ d'application

Entités Critiques (Art. 6)

Les entités critiques seront identifiées par les États membres d'ici 17 Juillet 2026

- Fournit un ou plusieurs services essentiels
- Opère sur le territoire d'un État membre de l'UE
- L'infrastructure critique pour les services essentiels est située dans un État membre de l'UE
- Un incident aurait des effets perturbateurs significatifs sur la fourniture par l'État d'un service d'assistance technique :
  1) L'entité d'un ou plusieurs services essentiels.
  2) La fourniture d'autres services essentiels dans les secteurs qui dépendent de ce ou ces services essentiels.

Entités critiques d'importance européenne particulière (Art. 17)

Exigences*

Évaluation des risques par les entités critiques (Art. 12)

- Évaluer les risques dans les 9 mois suivant la notification, puis les réviser tous les 4 ans.
- Évaluer tous les risques pertinents de perturbation du service essentiel.

Mesures de résilience (Art. 13)

- Prendre des mesures après évaluation des risques.

Mise en œuvre des vérifications des antécédents (Art. 14)

Rapports obligatoires (Art. 15)

- Notifier sans délai tout incident significatif.

Utilisation des normes européennes et internationales (Art. 16)

Suivi des CE d'importance particulière par le biais de missions consultatives (Art. 17)

*extract

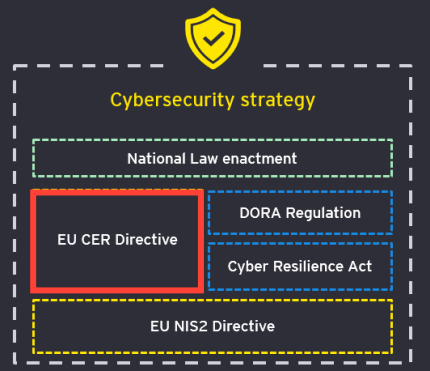
Conséquences juridiques

- Les États membres déterminent le régime des sanctions
- Prendre toutes les mesures nécessaires pour garantir la mise en œuvre des exigences

Période statutaire

- Mise en œuvre obligatoire jusqu'en octobre 2024

4. Réglementations UE : Directive REC (CRE)



Directive REC

Entités critiques (Art. 6)

1. **Fournit au moins un service essentiel**
+
2. Opère sur le territoire d'un État membre de l'UE
+
3. L'infrastructure critique pour les services essentiels est située dans un Etat membre de l'UE
+
4. Un incident aurait des effets perturbateurs significatifs sur la fourniture par:
   1) L'entité d'un ou de plusieurs services essentiels
   2) La fourniture d'autres services essentiels dans les secteurs qui dépendent des services essentiels

Entités critiques d'une importance particulière pour l'EU (Art. 17)

1. **Entité critique** selon l'Art. 6
+
2. **Fournit des services essentiels** identiques à ceux **de six Etats membres** ou plus
+
3. **Après notification** par l'autorité nationale compétente

La mission de l'UE surveille les entités critiques européennes (Art. 18)

- Evaluation des mesures par la mission consultative de l'UE
- Surveillance étroite par l'autorité

4. NIS2 (SRI2) vs. REC (CRE) – Quelle différence entre ces directives ?

	NIS2 Directive	REC Directive
Périmètre	Autodésignation Identification par taille → Approche holistique Entité Essentiel / Entité Importante	Identification à travers les états membres Seulement les services essentiels des entités critiques
Exigences	Mesures de Cyber Sécurité Focus sur la sécurité de l'information et réseaux Reporting obligatoire (Exigences sur chaînes d'appro. par l'UE)*	Focus sur la résilience physique Evaluation des risques
Sanctions	Sanctions concrètes définies Responsabilité personnelle	La définition des sanctions reste du ressort des États membres
Période statuaire	Transposition jusqu'à Oct 2024	

Conclusion

- Les deux directives modifieront le cadre réglementaire (national) au sein de l'UE
- Les entreprises peuvent être soumises aux exigences des deux directives (en fonction de la mise en œuvre nationale)
- Les exigences qui se chevauchent réduisent les efforts à déployer
- Cependant, certaines exigences diffèrent et la portée (par exemple, les systèmes, les processus) peut être différente entre NIS2 et REC.

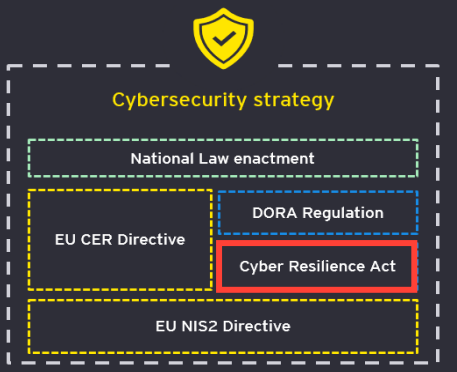
* En attente des résultats de l'évaluation des risques

4. Réglementations UE : CRA – Cyber Resilience Act

Générale: Règlement sur les exigences en matière de cyber pour les produits numériques.

Objectif

- Promouvoir des produits numériques sécurisés en réduisant les vulnérabilités matérielles et logicielles sur le marché et en encourageant les fabricants à prioriser la sécurité tout au long du cycle de vie du produit.
- Permettre aux utilisateurs de prendre en compte la cybersécurité lors du choix et de l'utilisation de produits numériques.



Champ d'application

Produits avec des éléments numériques (Art. 2)

Dont l'utilisation prévue ou raisonnablement prévisible inclut une connexion de données directe ou indirecte, logique ou physique, à un réseau.

La loi divise les produits en trois catégories en fonction de leur niveau de risque :

- Produits numériques (non critique)
- Produits numériques critiques
  - Classe 1
  - Classe 2

La portée de la CRA entraînera des obligations pour les fabricants, les distributeurs et les importateurs.

Exigences*

Intégrer la sécurité de l'information et la cybersécurité dès la conception initiale des produits(Art. 5, 10)

- Exigences de sécurité liées aux propriétés des produits numériques.
- Exigences en matière de gestion des vulnérabilités.

Évaluation des risques en matière de cybersécurité(Art. 10)

Diligence raisonnable lors de la mise sur le marché (Art. 10)
Signaler les vulnérabilités identifiées (Art. 11)

Exigences pour les autres opérateurs que les fabricants (Art. 13-16)

Évaluations de conformité (Art. 24)

La déclaration de conformité de l'UE doit attester de la conformité aux exigences(Art. 20)

Fournir une documentation technique (Art. 23)

*extract

Conséquences légale

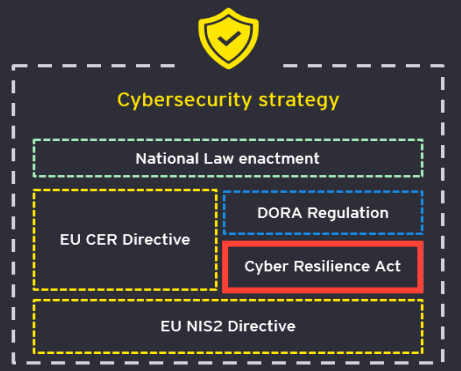
Jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel

Période légale

Le seul projet a été publié en septembre '22 (période de transition de 24 mois, possible entrée en vigueur fin 2025).

Cyber Resilience Act - Fact sheet of the EU Commission

4. Réglementations UE : CRA – Champ d'application



CRA

Article 2 Proposition CRA

Produits numériques

1. Tout produit logiciel ou matériel ainsi que ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels à placer sur le marché séparément

+

2. Le produit n'est pas :
   - Réglementé selon :
     - (EU) 2017/745 (dispositifs médicaux)
     - (EU) 2017/746 (dispositifs médicaux de diagnostic in vitro, abrogeant)
     - (EU) 2019/2144 (les véhicules à moteur et leurs remorques, etc.)
   - Certifié conformément au (UE) 2018/1139 (aviation civile)
   - Développé exclusivement à des fins de sécurité nationale ou militaire, ou à des produits spécifiquement conçus pour traiter des informations classifiées.

Produits critiques

1. Produits numériques

+

2. Présente un risque de cybersécurité selon les critères de l'article 6 (2) de la proposition de CRA (par ex. : conçu pour fonctionner avec des privilèges élevés).

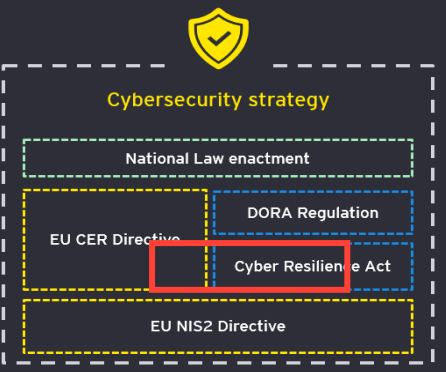
+

3. La fonctionnalité de base est définie à l'Annexe III de la proposition de CRA
   - Produits Classe 1
   - Produits Classe 2

4. Réglementations UE : DORA – Digital Operational Resilience Act

Brève description :

- Générale : Règlement sur les exigences en matière de cybersécurité pour le secteur financier
- Objectif
  - Normaliser les critères pour les entités financières détectant les risques TIC, pour uniformiser à travers l'UE et assurer une concurrence juste.
  - Centraliser la supervision pour gérer les risques des entités financières avec des fournisseurs TIC tiers.



Champ d'application

Entités financières (Art 1-2)

Vise à renforcer la sécurité informatique des entités financières à travers l'Europe :

- Banques (Institutions de crédit, institutions de monnaie électronique)
- Sociétés de gestion (compagnies d'assurance, compagnies de réassurance, dépositaires centraux de titres)
- Sociétés d'investissement (dépositaires centraux de titres, gestionnaires de fonds d'investissement alternatifs)

Le champ d'application de DORA harmonisera les règles relatives à la résilience opérationnelle dans le secteur financier, s'appliquant à 20 types différents d'entités financières et de prestataires de services TIC tiers.

Exigences*

Gouvernance (Art. 5)

Gestion des risques liés aux TIC (Art. 6 to 16)

- Identification
- Protection et prévention
- Détection
- Réponse et récupération
- Apprendre et évoluer
- Communiquer

Rapport sur les incidents liés aux TIC (Art. 17 to 23)

Partage d'informations (Art. 45)

Test de résilience opérationnelle numérique (Art. 24 to 27) – Pentest / RedTeaming / etc...

Risque lié aux tiers fournisseurs de TIC (Art. 28 to 44)

*extract

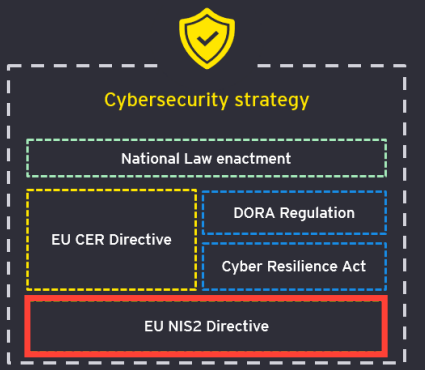
Conséquences légale

- Non spécifié

Période légale

- Fournir des recommandations concrètes et une feuille de route pour une amélioration d'ici janvier 2025.

4. Réglementations UE : DORA – Champ d'application



DORA

Article 1 - 2

Banques

1. **Institutions de crédit**
2. Établissements de monnaie électronique
3. Fournir des services ou réaliser des activités au sein de l'UE

Sociétés de gestion

1. **Compagnies d'assurance**
2. **Compagnies de réassurance**
3. **Dépositaires centraux de valeurs mobilières**

Sociétés d'investissement

1. Dépositaires centraux de titres
2. Gestionnaires de fonds d'investissement alternatifs

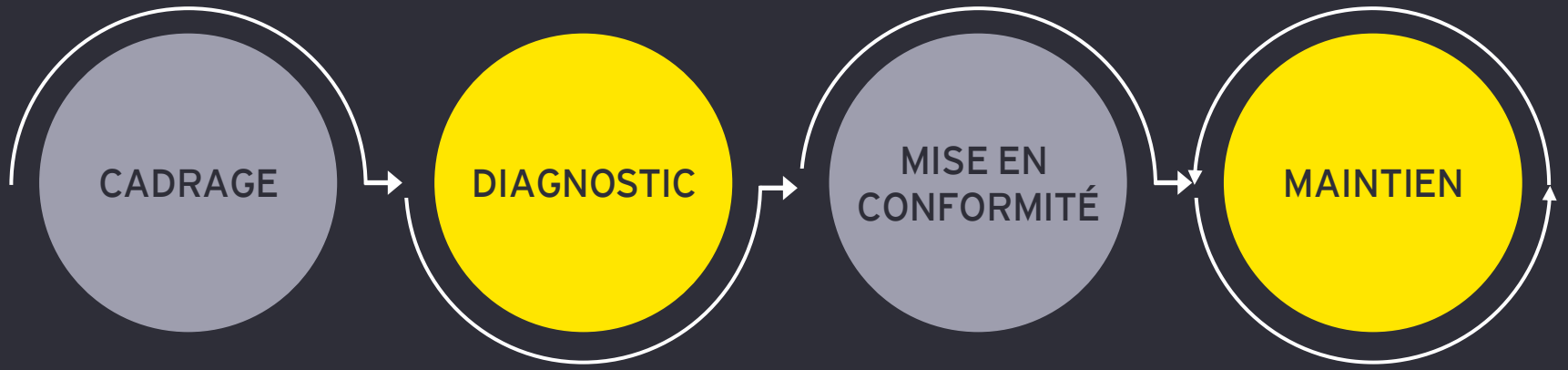
4. Réglementations UE : Différence entre les directives et les règlements de l'UE

	NIS2	REC	CRA	DORA
	La directive NIS2 a la portée la plus large en se concentrant sur l'ensemble de l'organisation en tant que telle, exigeant qu'elle mette en œuvre des mesures de cybersécurité complètes (techniques, opérationnelles et organisationnelles) pour gérer les risques posés à la sécurité des réseaux et systèmes d'information.	La directive CER se concentre sur la sécurité des services essentiels définis afin d'assurer leur résilience face aux menaces, ce qui va au-delà de la portée d'un seul produit. Les exigences CER mettent l'accent sur des mesures générales visant à garantir la résilience (y compris la cybersécurité ainsi que la sécurité physique).	La CRA se concentre sur les fabricants et leurs produits dans son champ d'application et oblige les entreprises à traiter les vulnérabilités en matière d'information et de cybersécurité avec des mesures appropriées tout au long du cycle de vie du produit.	DORA a vocation à renforcer la résilience opérationnelle informatique des acteurs financiers en mettant en place un nouveau cadre de gouvernance et de contrôle interne concernant la gestion des risques informatiques, la déclaration des incidents majeurs, les tests de résilience opérationnelle et la gestion du risque de tiers.
Législation	*Directives de l'UE*		*Règlement de l'UE*	
Période de temps	*Promulguée – Oct 2024.*		*Projet de loi*	*Promulguée - Jan 2025*
Champ d'application	*Entités*	*Services essentiels*	*Produits*	*Secteur Financier*
Objectif	*Systèmes de réseau et d'information sécurisés*	*Services essentiels sécurisés*	*Moins de vulnérabilités au sein des produits numériques*	*Secteur financier résilient face aux menaces numériques*

5 Conclusion

5. Règlementations Européennes - Parcours vers la conformité

DORA
REC
NIS2
CRA



- Compréhension des textes de loi et exigences
- Identification des périmètres concernés

- Réalisation d'un audit de conformité sur les périmètres concernés et au regard des exigences
- Définition d'un plan d'action de mise en conformité

- Définition d'une feuille de route et mise en place du plan d'action de mise en conformité

- Assurer un maintien du niveau de conformité dans le temps

ANSSI NIST ISO 27001 IEC62443