France

Réussir sa conformité NIS2 : Lien avec la norme ISO/IEC 27001 et bonnes pratiques en Cybersécurité

PECB REGIONAL WEBINARS

Bechir SEBAI

CEO et Fondateur d'ACG Cybersecurity

Introduction

- 34 nouveaux cyberadversaires identifiés en 2023;
- Augmentation de 75 % des intrusions sur le cloud;
- Bond de 76 % du nombre de victimes de vol de données mentionnées sur le Dark Web;
- 2 minutes, 7 secondes : temps de propagation le plus rapide enregistré pour une activité cybercriminelle;
- 75 % des attaques n'utilisaient pas de logiciel malveillant;
- +300% d'attaques sur les infrastructures critiques entre 2020 et 2023;

Introduction

Besoins et nécessités

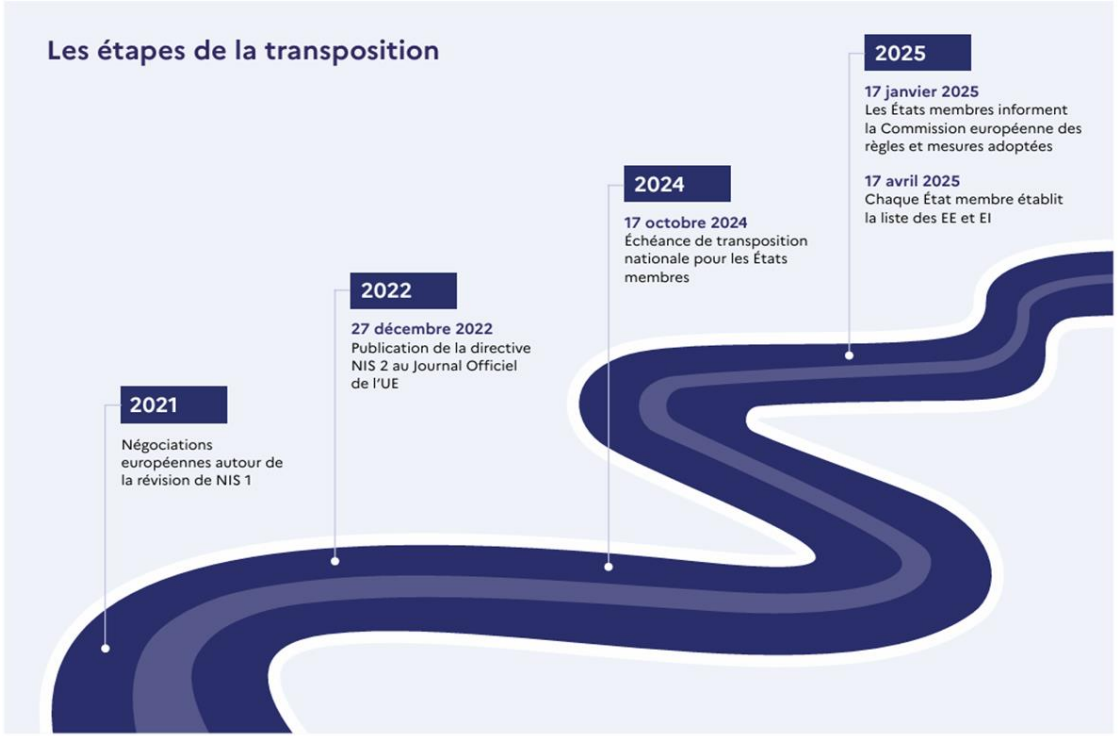
- Uniformiser les cadres réglementaires et combler les lacunes de NIS1 (2016)
- Renforcer la résilience des infrastructures critiques dans l'Union européenne.
- améliorer la gouvernance et la gestion des risques cyber.
- Éviter les disparités entre pays membres en matière de gestion des risques cyber
- Protéger l'économie numérique de l'UE contre des interruptions majeures.

Agenda


I
Dispositions du NIS2
II
Conformité à la directive NIS2
III
Complémentarité entre NIS2 et ISO/IEC 27001
IV
Préparation à la Directive NIS2

Axes de base du NIS2

NIS2 - Dates & Structure -



Axes de base du NIS2

NIS2 - Dates & Structure -

- 144 Considerations
- 46 Articles
- 3 Annexes

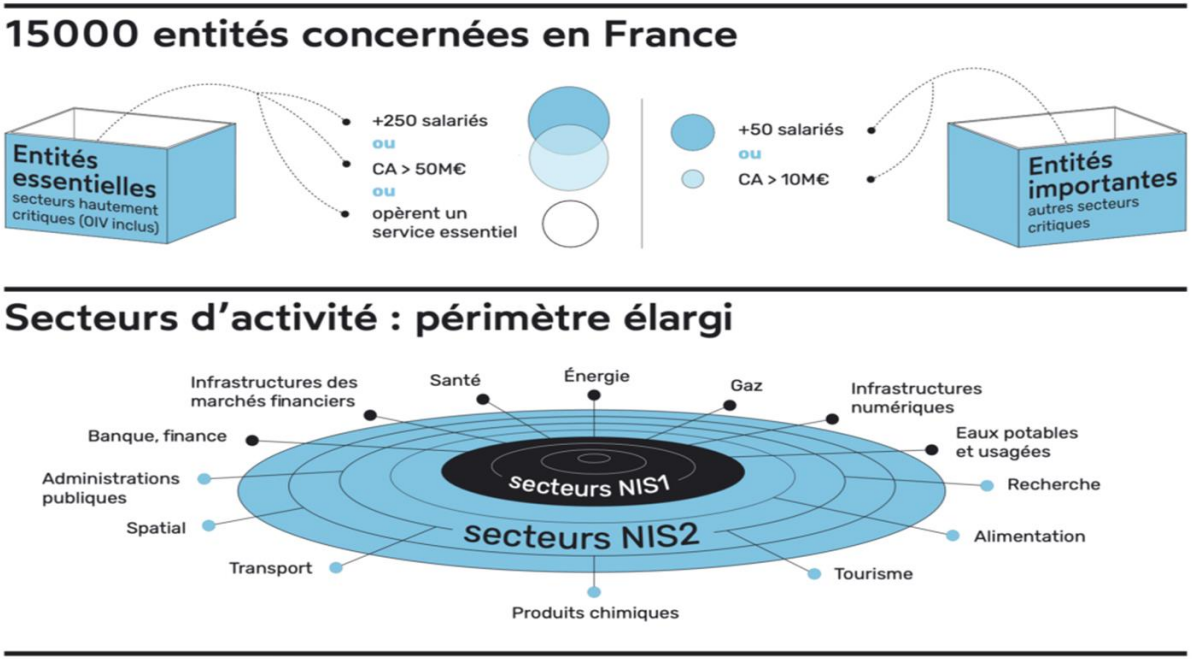
Axes de base du NIS2

Objectifs Clés de la Directive NIS2

Axes de base du NIS2

Champs d'Action - Hautement Critique

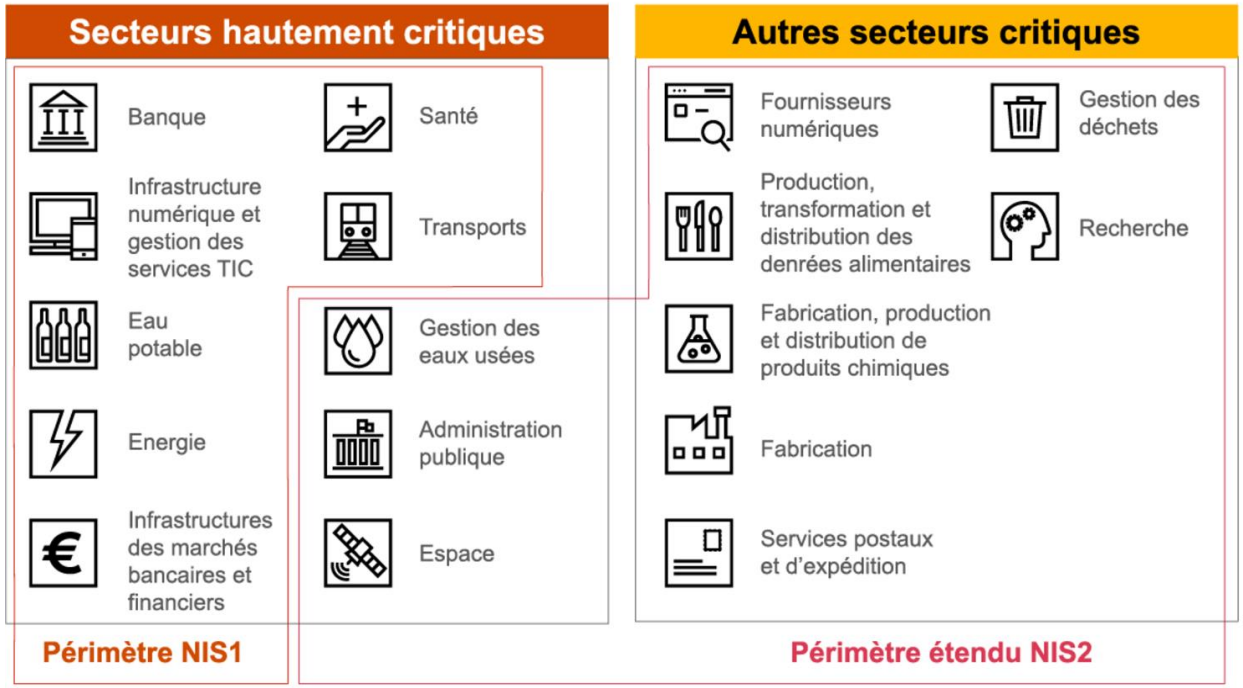
Qui est Concerné par NIS2 ?



Axes de base du NIS2

Champs d'Action - Hautement Critique

Qui est Concerné par NIS2 ?



Axes de base du NIS2

Champs d'Action - Hautement Critique -

Qui est Concerné par NIS2 ?

- L'énergie
- Les transports
- Le secteur bancaire
- Les infrastructures des marchés financiers
- La santé
- La fourniture et la distribution d'eau potable
- La gestion des eaux usées
- Les infrastructures numériques
- La gestion des services numériques TIC
- L'administration publique
- L'espace

Axes de base du NIS2

Champs d'Action - Critique

Qui est Concerné par NIS2 ?

- Les services postaux et d'expédition
- La gestion des déchets
- La fabrication, la production et la distribution de produits chimiques
- La production, la transformation et la distribution de denrées alimentaires
- La fabrication
- Les fournisseurs numériques
- La recherche

Axes de base du NIS2

Champs d'Action - EI & EE -

Axes de base du NIS2

Champs d'Action - EI & EE -

Taille d'entreprise	Nombre d'employés	Chiffre d'affaires (millions d'euros)	Bilan annuel (millions d'euros)	Annexe 1	Annexe 2
Intermédiaire et grande	x ≥ 250	y ≥ 50	z ≥ 43	Entités Essentielles *	Entités Importantes
Moyenne	50 ≥ x ≤ 250	10 ≥ y ≤ 50	10 ≥ z ≤ 43	Entités Importantes	Entités Importantes
Micro et petite	x < 50	y < 10	z < 10	*Non concernées par NIS 2*	

Dispositions du NIS2

Obligations imposées par la directive NIS2

Gestion des risques	Gouvernance	Devoir d'information
• Gestion des incidents • PCA, PRA, PCI, PRI • Sécurité de la chaine d'approvisionnement • Evaluation des mesures de gestion de risques • Formation	• Responsabilisation des directions • Mise en place d'une politique de formation liée aux enjeux de la cybersécurité	• Obligation de prévenir les autorités compétentes (CSIRT) dans les 24h avec : • Formalisation de la gravite • Type de menace • Mesures d'atténuation appliquées

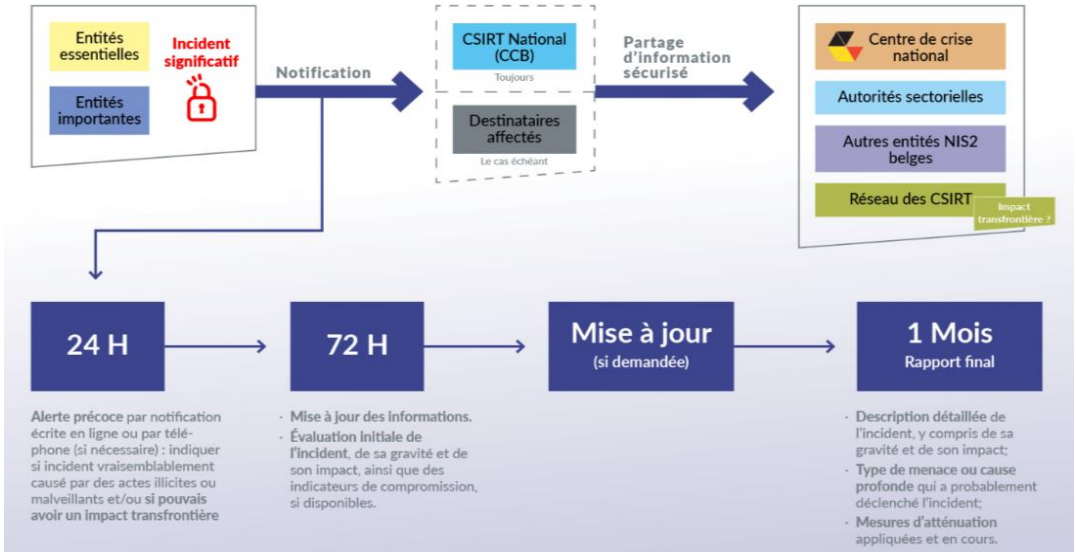
- Adhésion de la direction : La cybersécurité doit être soutenue par les équipes dirigeantes;
- Formation des dirigeants : Les dirigeants doivent acquérir une connaissance de base des cybermenaces;
- Engagement des salariés : La participation de l'ensemble des collaborateurs est primordiale

10 mesures de cybersécurité

- Analyse de risques et politique de sécurité
- Gestion des incidents
- Continuité des activités
- Sécurité de la chaîne d'approvisionnement
- Sécurité des réseaux et SI (de l'achat à la maintenance)
- Evaluation de la gestion des risques et des politiques
- Cyber hygiène et formation) à la cybersécurité
- Politique et procédures relatives à la cryptographie
- Sécurité des RH, contrôle d'accès et gestion des actifs
- Utilisation de solutions d'authentification adaptées

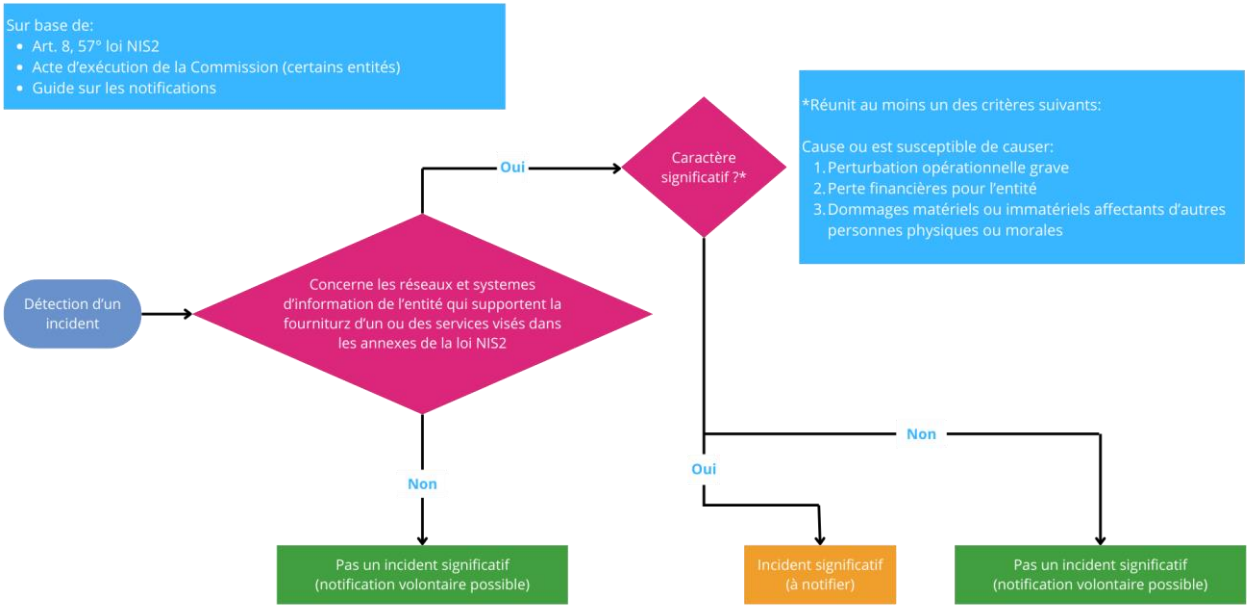
Dispositions du NIS2

Obligation de notification - Article 23 -

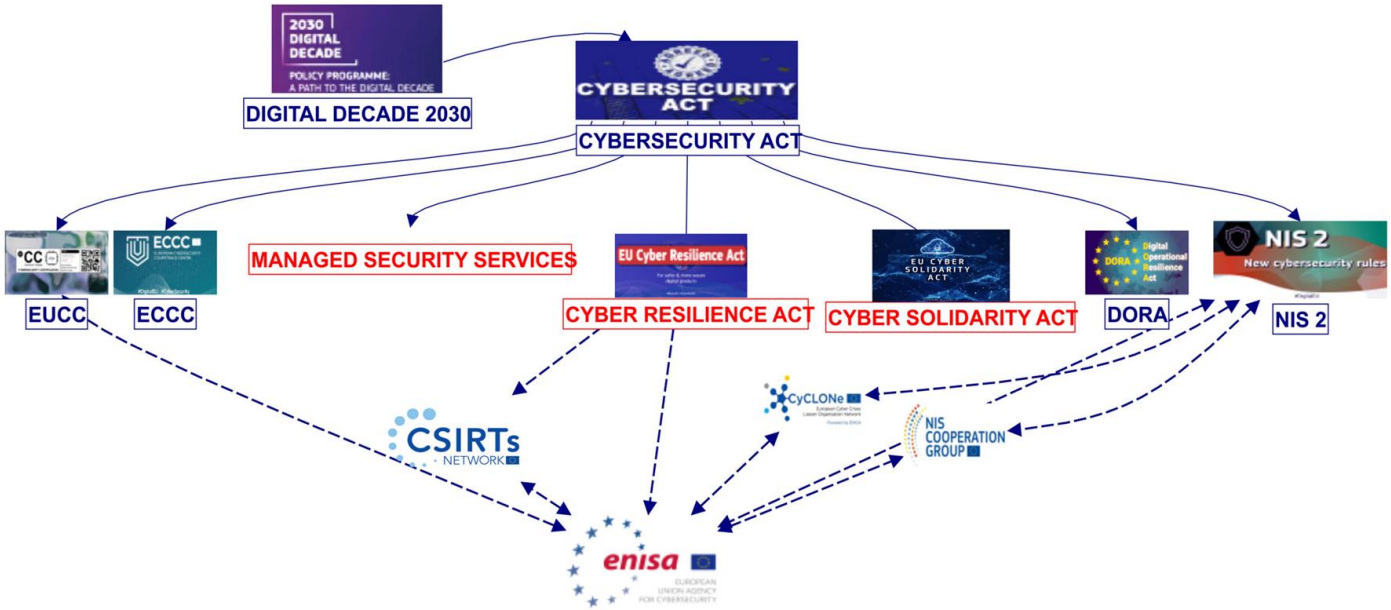


Dispositions du NIS2

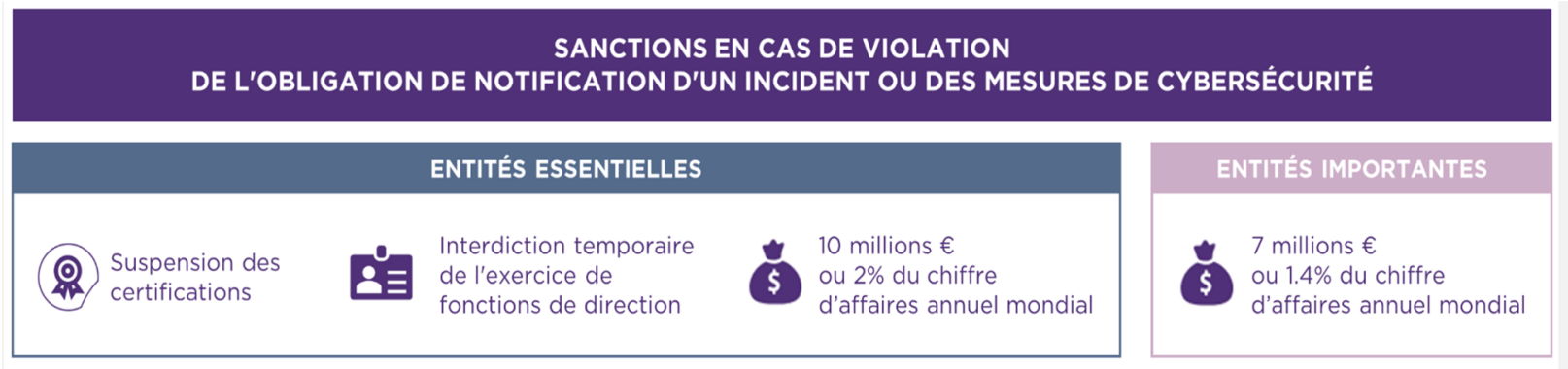
Obligation de notification – Processus -



Dispositions du NIS2
Coordination européenne



Amendes administratives lourdes et chiffrées



Amendes administratives lourdes et chiffrées

- Des amendes jusqu'à "au moins" 10M€ ou 2% du CA annuel mondial;
- Pour les Entités Importantes (EI) : au moins 7 millions d'euros ou à au moins 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise;
- Pour les Entités Essentielles (EE): au moins 10 millions d'euros ou à au moins 2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise.

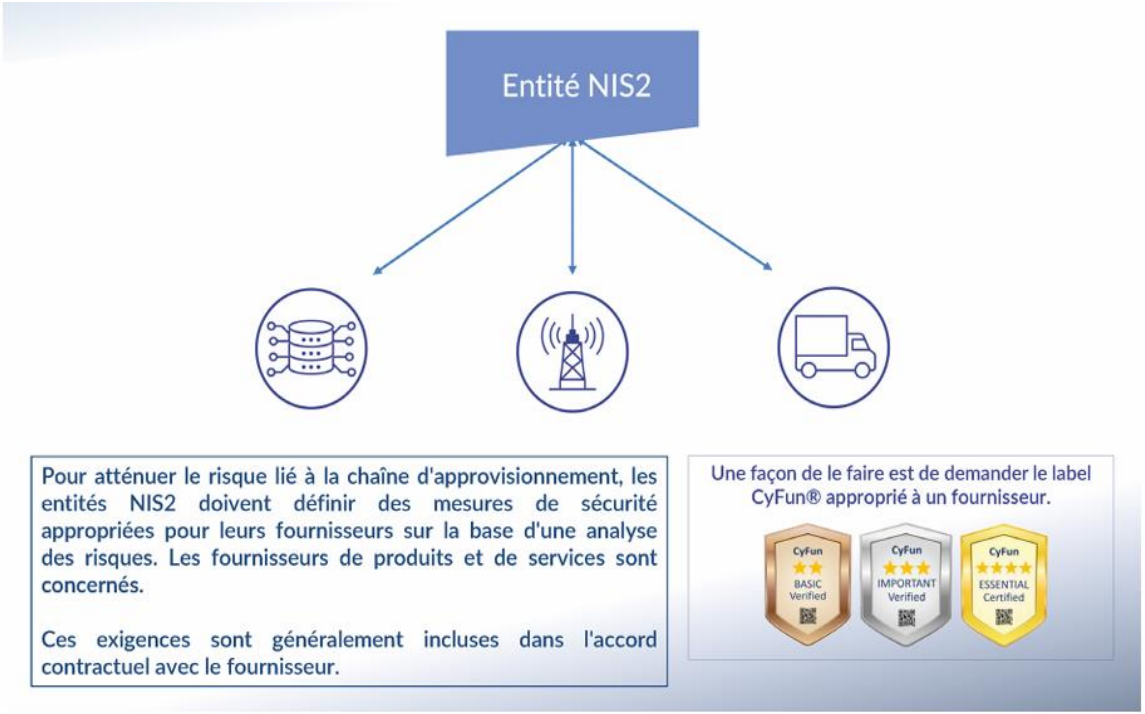
Sanctions prévues pour le top management

- **Suspension des certifications et autorisations** concernant les services ou activités fournis par l'organisation ;

- **Interdiction temporaire d'exercer des fonctions de direction** au sein de l'entité pour toute personne exerçant des responsabilités de direction à un niveau de directeur général ou de représentant légal.

Dispositions du NIS2

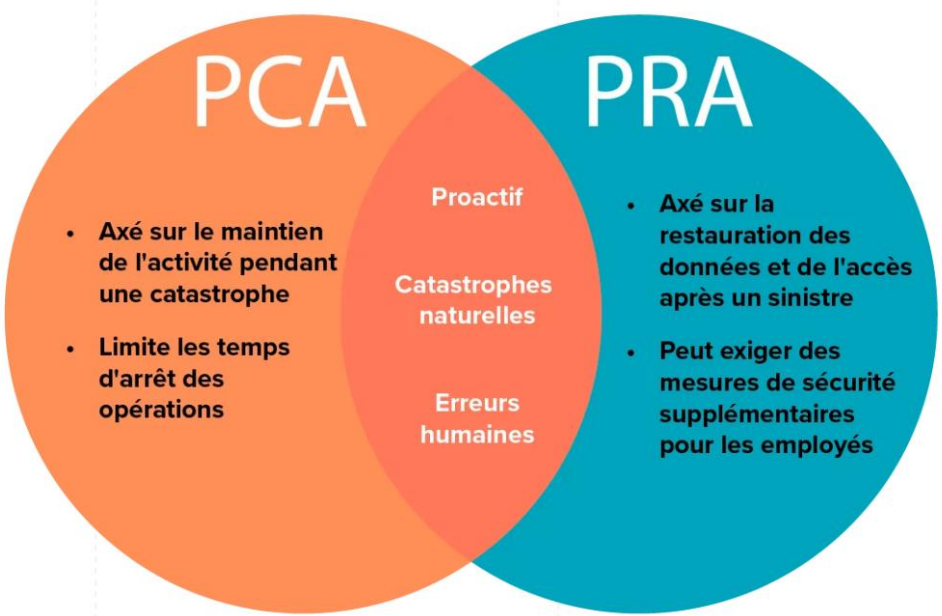
Chaîne d'Approvisionnement et NIS2



Plan de continuité de l'Activité

Vs

Plan de Reprise de l'Activité

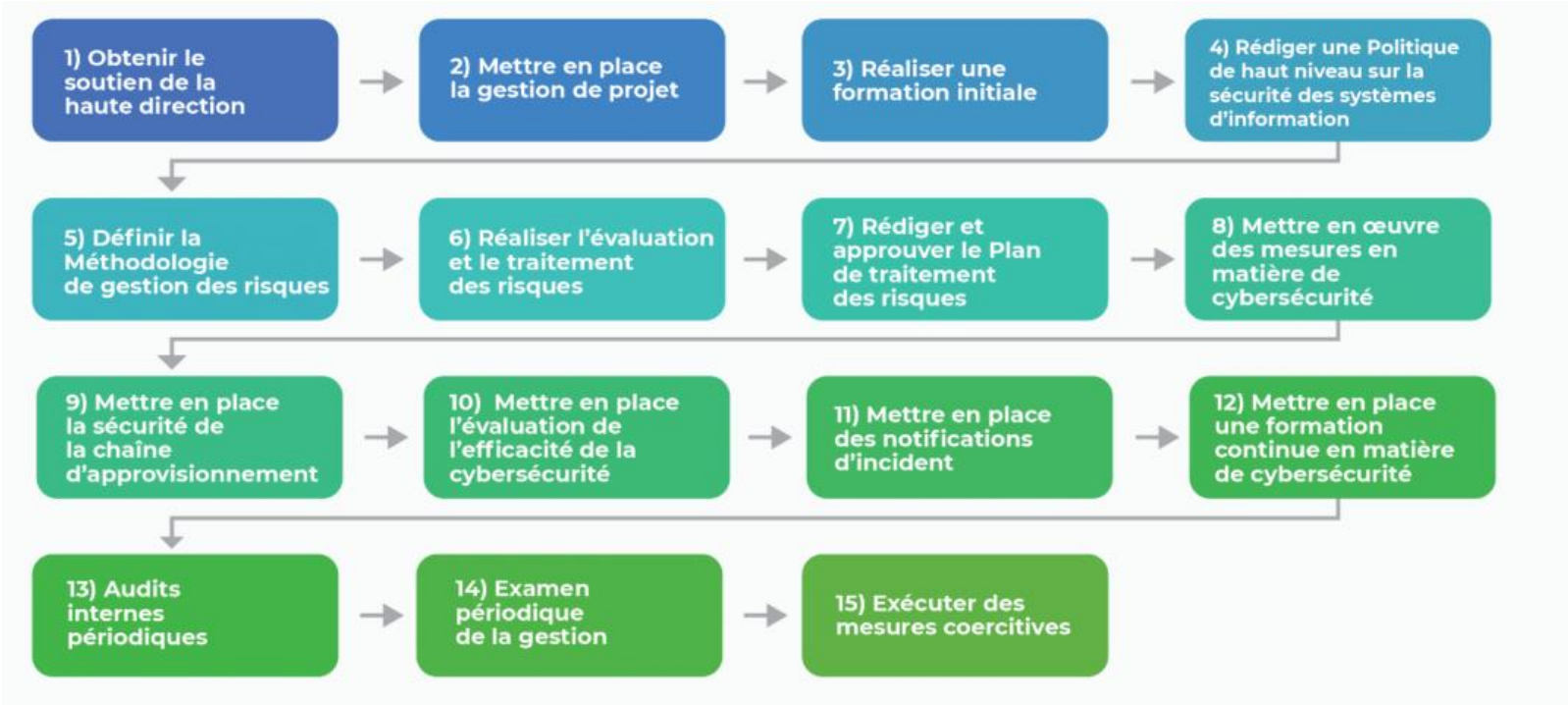


Agenda


I
Dispositions du NIS2
II
Conformité à la directive NIS2
III
Complémentarité entre NIS2 et ISO/IEC 27001
IV
Préparation à la Directive NIS2

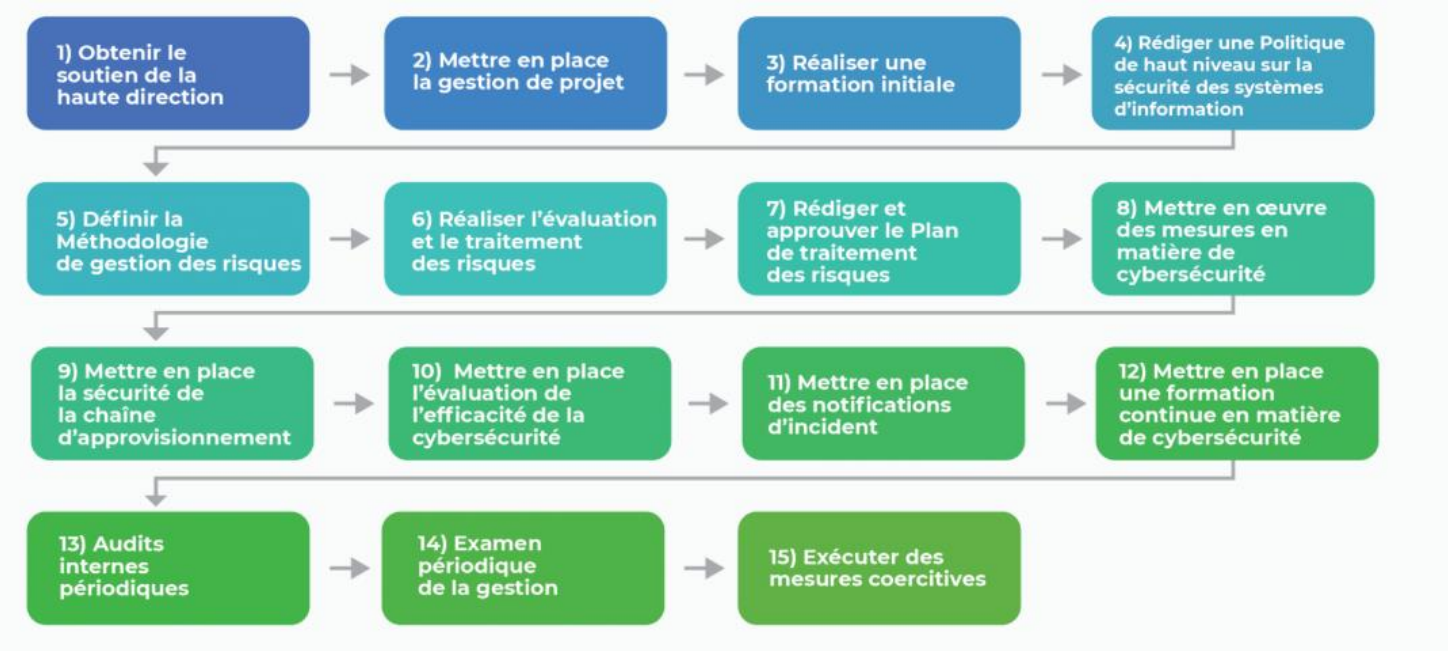
Conformité à la directive NIS2

15 étapes de mise en œuvre: 1-2



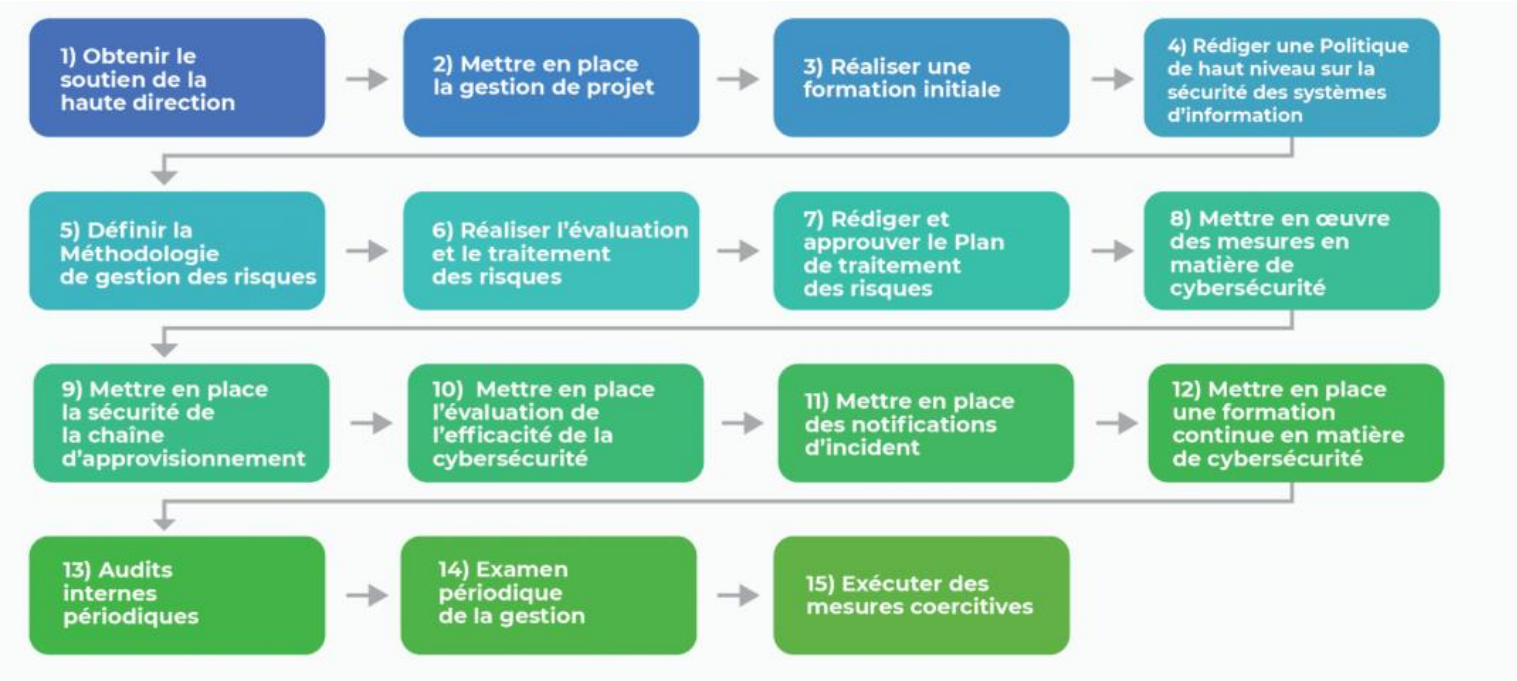
Conformité à la directive NIS2

15 étapes de mise en œuvre: 3-4



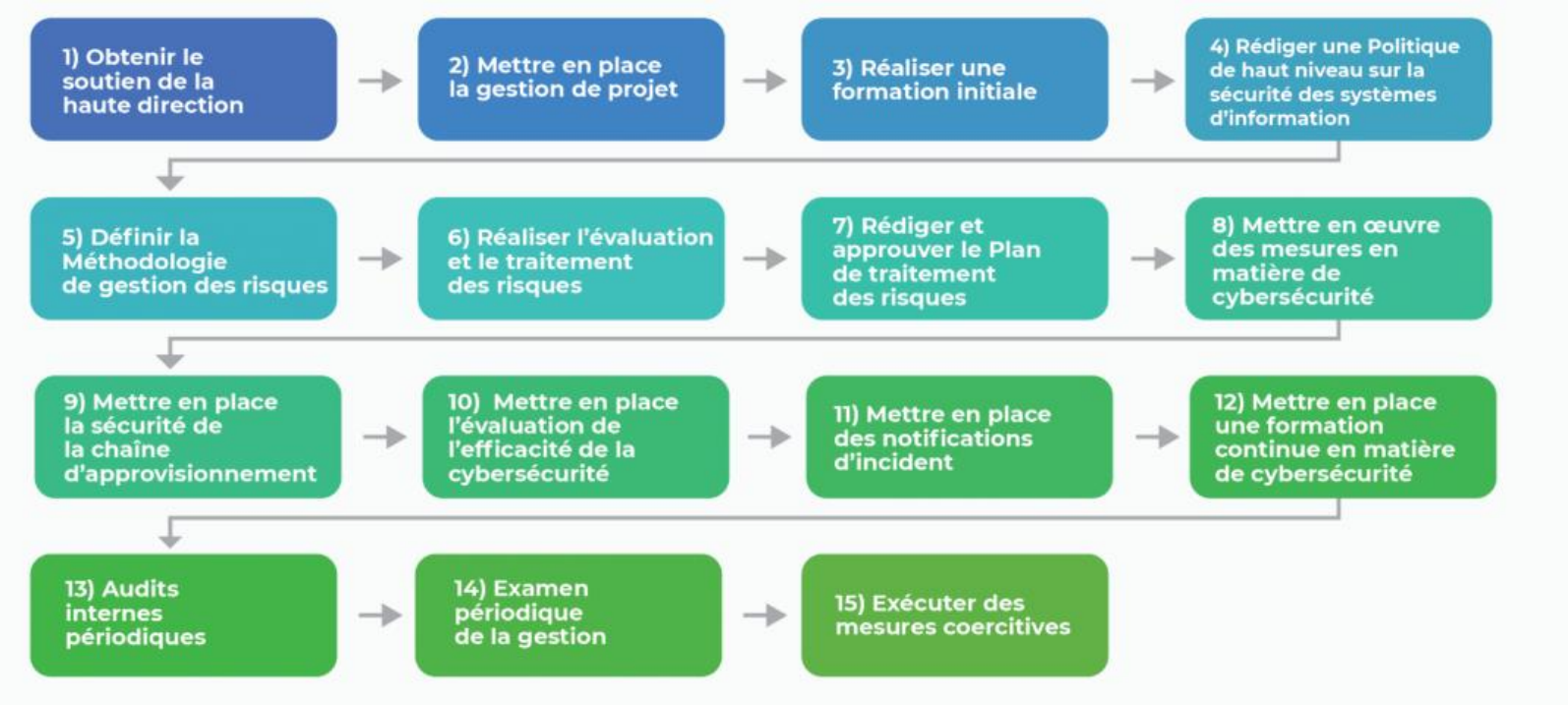
Conformité à la directive NIS2

15 étapes de mise en œuvre: 5-6-7 et 8

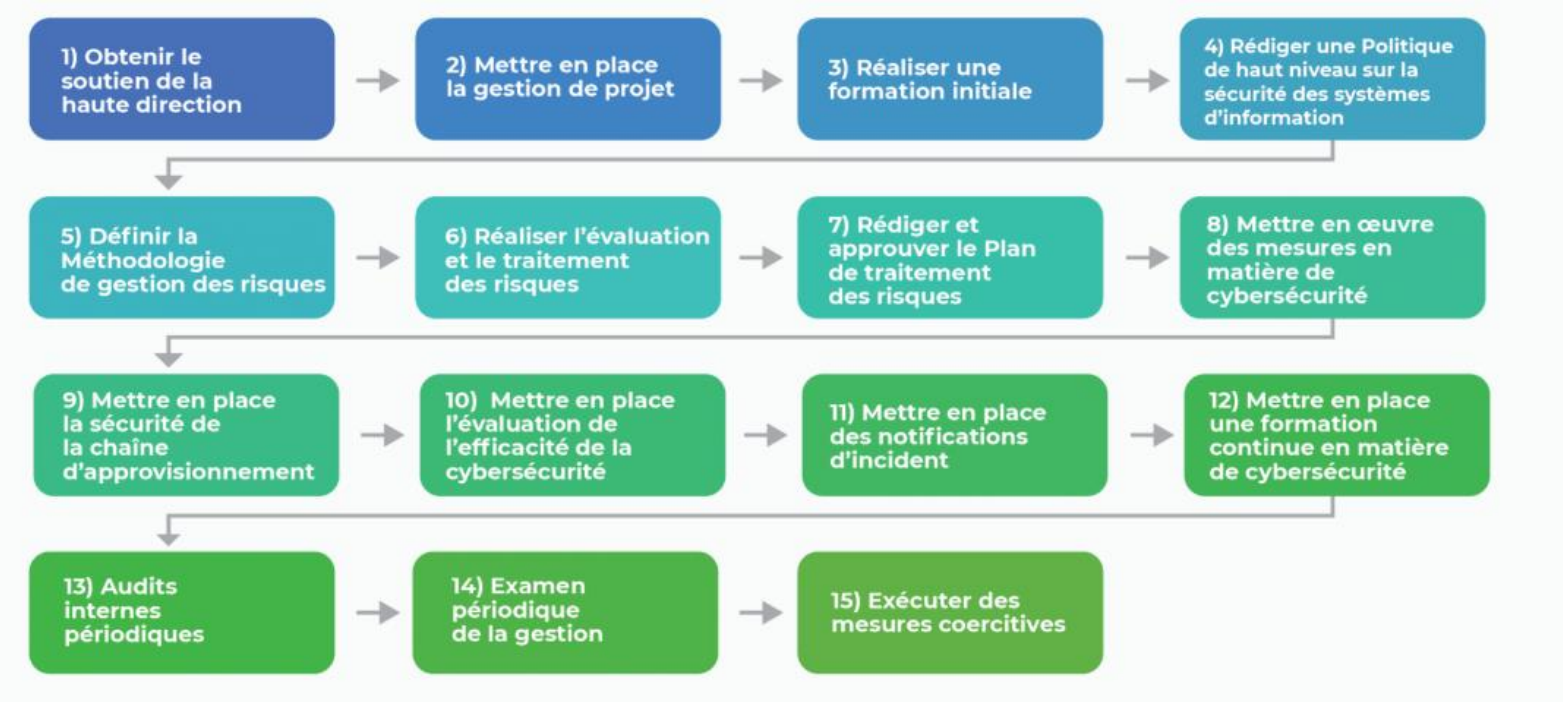


Conformité à la directive NIS2

15 étapes de mise en œuvre

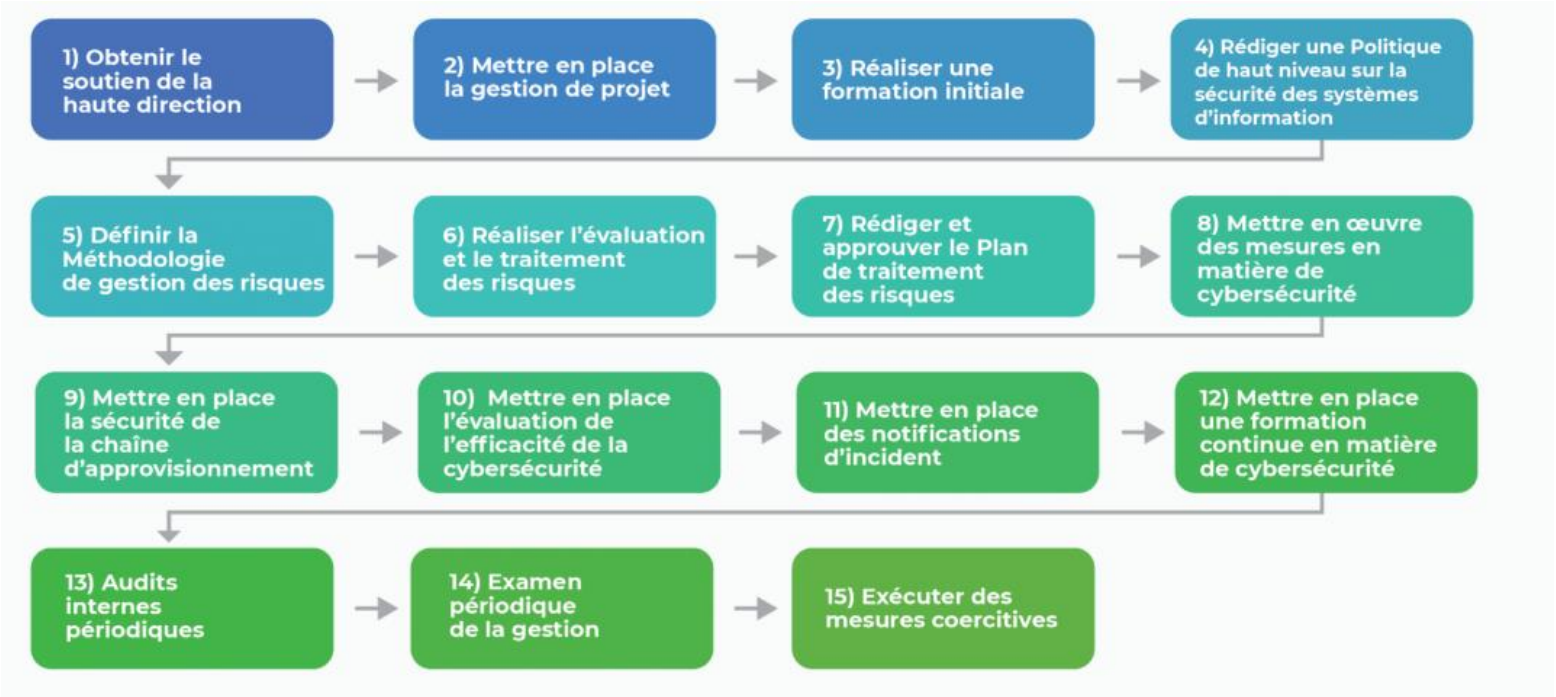


Conformité à la directive NIS2
15 étapes de mise en œuvre



Conformité à la directive NIS2

15 étapes de mise en œuvre 1-2



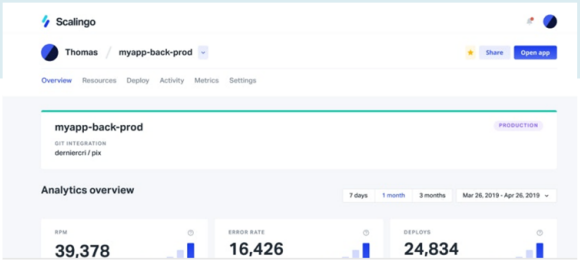
Conformité à la directive NIS2
ANSSI - MonEspaceNIS2 -

MonEspaceNIS2

Organisation responsable	AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI)
Autorité d'homologation	Emmanuel Naegelen | Directeur adjoint de l'ANSSI
Date d'homologation	21/03/2024
Durée et échéance de l'homologation	6 mois | 21/09/2024

Décision d'homologation de sécurité
Référentiel général de sécurité

https://scalingo.com/

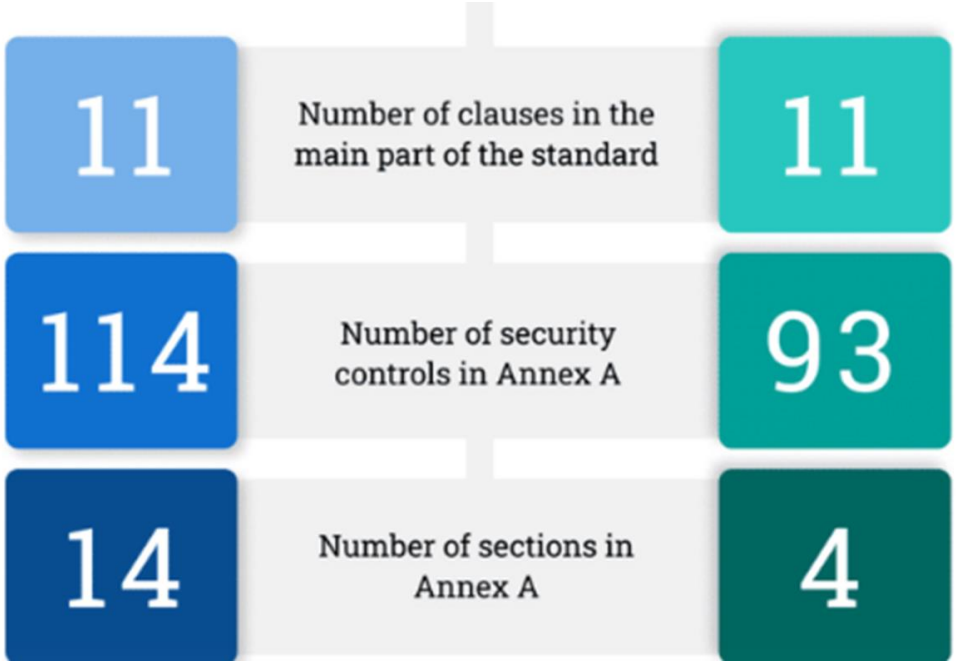


Agenda


I
Dispositions du NIS2
II
Conformité à la directive NIS2
III
Complémentarité entre NIS2 et ISO/IEC 27001
IV
Préparation à la Directive NIS2

Complémentarité entre NIS2 et ISO/IEC 27001

La norme ISI/IEC 27001 -11 nouveaux contrôles



Complémentarité entre NIS2 et ISO/IEC 27001
La norme ISI/IEC 27001 - 2013 vs 2022 -

- L'ENISA a développé un outil qui met en correspondance les clauses et contrôles de l'ISO 27001 avec les anciennes exigences de la NIS (la prédécesseuse de la NIS 2).
- Dans son rapport intitulé « Mapping of OES Security Requirements to Specific Sectors » publié en 2017, l'ENISA a déclaré que « l'ISO 27001 est apparue, selon l'enquête, comme la norme la plus couramment suivie » par les opérateurs de services essentiels (OSE),
- Dans son rapport intitulé « NIS Investments » publié en 2021, l'ENISA a indiqué que, parmi les entreprises devant se conformer à l'ancienne directive NIS, « une majorité d'organisations (51,1 %) certifient leurs systèmes et processus, par exemple sur la base de la certification ISO 27001.

Article 20 et 21

Directive NIS2	ISO/IEC 27001
Article 20: Gouvernance	A.5.1-A.5.31-A.5.34-A.5.35-A.5.36-A.6.3
Article 21 : Mesures de gestion des risques de cybersécurité : (A) Politiques sur l'analyse des risques et la sécurité des systèmes d'information	5.2 -6.1.2-6.1.3-8.2-8.3 et A.5.1,
Article 21 : Mesures de gestion des risques de cybersécurité : (B) Gestion des incidents	A.5.24 -A.5.25 -A.5.26 :-A.5.27 -A.5.28 -A.8.16

Article 21 : Mesures de gestion des risques de cybersécurité (Suite)

Directive NIS2	ISO/IEC 27001
(C) Continuité des activités, telles que la gestion des sauvegardes, la reprise après sinistre et la gestion de crise	A.5.29 -A.5.30 -A.8.13-A.8.14-A.8.15 -A.8.16.
(D) Sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs	A.5.19 -A.5.20 -A.5.21 -A.5.22 -A.5.23.
(E) Sécurité dans l'acquisition, le développement et la maintenance des systèmes d'information et de réseau, y compris la gestion et la divulgation des vulnérabilités	

Article 21 : Mesures de gestion des risques de cybersécurité (Suite)

Directive NIS2	ISO/IEC 27001
(F) Politiques et procédures pour évaluer l'efficacité des mesures de gestion des risques de cybersécurité	9.1 -9.2 -9.3 -A.5.35 et A.5.36.
(G) Pratiques de base en hygiène cybernétique et formation à la cybersécurité.	7.3 -7.4 -A.5.15 -A.5.16 -A.5.18-A.5.24 -A.6.3-A.6.5 -A.6.8 -A.8.2 -A.8.3 :-A.8.5 -A.8.7 -A.8.9 -A.8.13 -A.8.15 -A.8.19.

Article 21 : Mesures de gestion des risques de cybersécurité (Suite)

Directive NIS2	ISO/IEC 27001
(H) Politiques et procédures concernant l'utilisation de la cryptographie et, le cas échéant, le chiffrement	A.8.24
(I) Sécurité des ressources humaines, politiques de contrôle d'accès et gestion des actifs	A.5.9 -A.5.10 -A.5.11 -A.5.15 -A.5.16 -A.5.17 -A.5.18 :-A.6.1 -A.6.4 :-A.6.5 -A.6.6.
(J) Utilisation de solutions d'authentification multi-facteurs ou d'authentification continue, de communications vocales, vidéo et texte sécurisées, ainsi que de systèmes de communication d'urgence sécurisés au sein de l'entité, lorsque cela est approprié	A.5.14 -A.5.16 et A.5.17.

Article 23 et 24

Directive NIS2	ISO/IEC 27001
Article 23 : Obligations de notification	A.5.14 et A.6.8
Article 24 : Utilisation des schémas de certification de cybersécurité européens	A.5.20

ISO/IEC 27001:2022 et l'adoption d'un SMSI permettra de couvrir une grosse partie des exigences de conformité introduites par NIS2

Résultats Attendus de l'Alignement

- **Avantages organisationnels :**
  - Réduction des coûts liés à la mise en conformité.
  - Processus unifiés pour gérer les audits et les incidents.

- **Résultats opérationnels :**
  - Temps de réponse aux incidents réduit.
  - Meilleure résilience face aux menaces.

Agenda


I
Dispositions du NIS2
II
Conformité à la directive NIS2
III
Complémentarité entre NIS2 et ISO/IEC 27001
IV
Préparation à la Directive NIS2

Préparation à la Directive NIS2

Plan en 10 étapes

- ❑Évaluation de l'applicabilité
- ❑Compréhension des obligations
- ❑Adoption d'un SMSI basé sur l'ISO 27001
- ❑Analyse des risques
- ❑Mise en œuvre des mesures de sécurité

Préparation à la Directive NIS2

Plan en 10 étapes

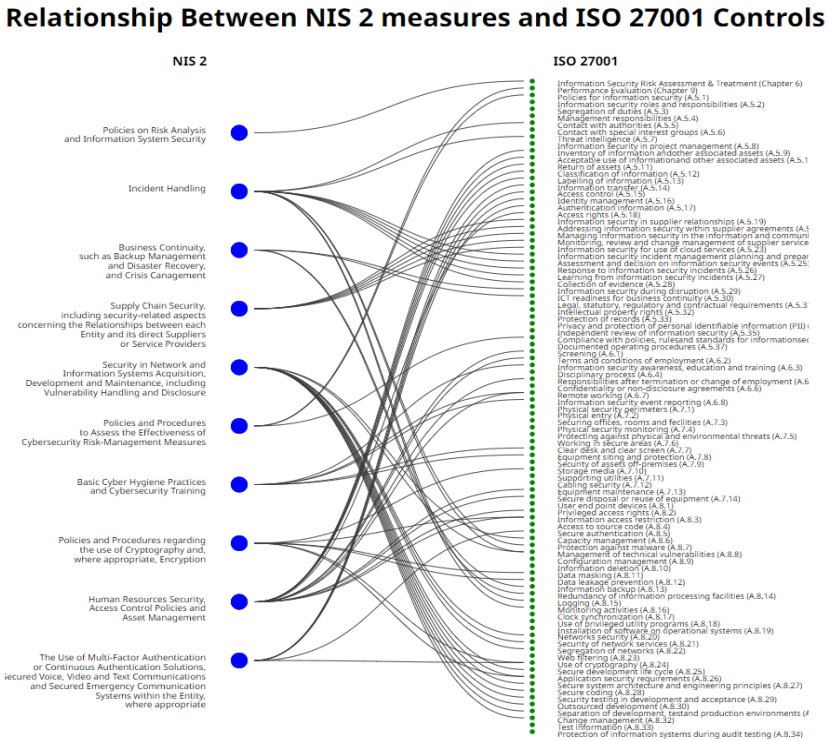
- ❑Formation et sensibilisation
- ❑Notification des incidents
- ❑Révision et amélioration continue
- ❑Préparation aux audits
- ❑Partage d'informations et coopération

Préparation à la Directive NIS2
Approche Multi référentiels

NIS 2
&
ISO/IEC 27001

Préparation à la Directive NIS2

Approche Multi référentiels



Bonnes pratiques

Notification, gestion et reporting des incidents

Outils de détection et d'analyse automatisés des incidents

Modèles de rapport d'incident pré-formatés

Canaux de communication directs

Exercices de simulation d'incidents

chaîne d'approvisionnement sécurisée.

Bonnes pratiques

Gestion des risques de la chaîne d'approvisionnement

Bonnes pratiques

Mise en place d'un PRA et d'un PCA

Bonnes pratiques

Formation et sensibilisation des collaborateurs

Formations régulières

Campagnes de phishing

Contrats de travail et obligations

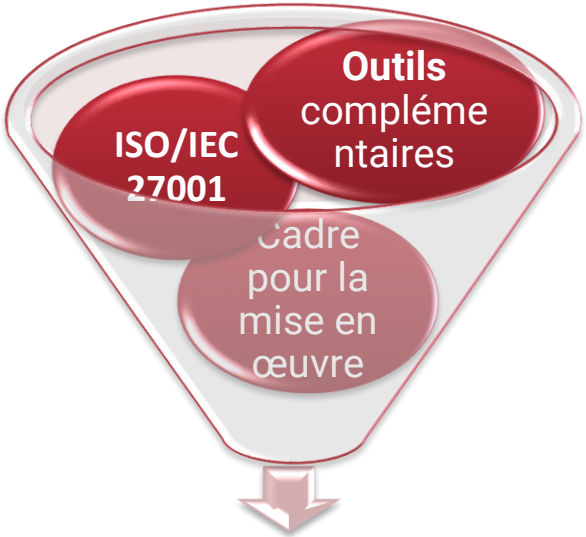
Outils de sécurité

Bonnes pratiques

Tests et audits

- Audit complet
- scans automatisés
- Priorisation
- Scenario de PN
- Checklist audit
- Audits réguliers et des droits d'accès.

CONCLUSION



La directive NIS2 et la norme ISO 27001 sont donc inextricablement liées.

Q&A Session

Contact

acgcybersecurity.fr

acgcyberacademy.fr

Merci pour votre attention !

For any questions or comments you can contact us below:

- support@pecb.com