EduGroupe

Accompagner pour réussir

Webinaire Cybersécurité :

Comprendre et se conformer

aux Directives NIS2 et DORA

- Accueil et présentation des intervenants
- Stratégie de cybersécurité pour la décennie numérique
- Directive NIS2 : Principaux Axes et Exigences
- Directive DORA : Renforcer la Résilience Opérationnelle Digitale
- Formation et sensibilisation des équipes internes
- Questions / Réponses

EduGroupe

Accompagner pour réussir

Nos intervenants

Expertise Cybersécurité

- **Formations**
- **Conseil**
- **Audit**
- **Accompagnement des entreprises et des DSI**

Autour des sujets :

- ***Normes famille ISO 27000***
- ***Intelligence économique***
- ***Analyse des risques***
- ***Audit de certification***
- ***Gestion des crises***
- ***Conformité réglementaire***

Jamal SAAD
Expert Cybersécurité

Monter en compétences grâce aux formations informatiques

- **Formations**
- **Conseil**
- **Accompagnement des entreprises et des DSI**

Autour des sujets :

- ***Management de la Sécurité, Gestion des risques, Techniques Cybersécurité, Sécurité Offensive et Défensive...***
- ***Big data, Intelligence Artificielle ….***
- ***ITSM, Méthodologie de projet, Management***
- ***Green IT et Responsabilité Sociétale***

Nicolas BIENVENUE
Direction Commerciale & Associé
Mob. +33(0)6 69 58 34 80
Nicolas.bienvenue@edugroupe.com

EduGroupe

Accompagner pour réussir

Stratégie de Cybersécurité pour la décennie numérique

1. Description de la stratégie
2. Instruments règlementaires

Description de la Stratégie de Cybersécurité pour la décennie numérique :

Cette stratégie vise à mettre en place une Europe robuste et respectueuse de l'environnement face à la dépendance croissante a des outils numériques dans des secteurs vitaux.

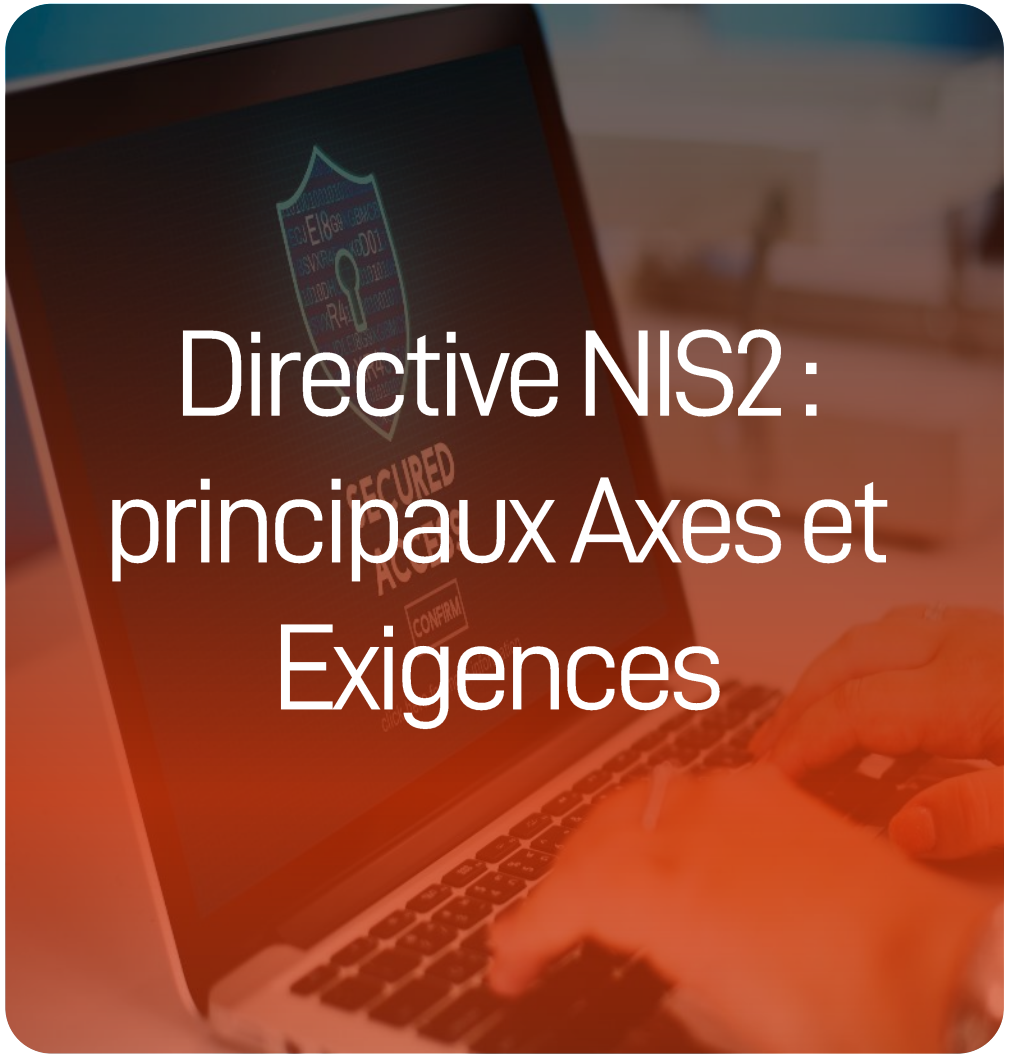
Elle va décrire la stratégie de l'union européenne pour protéger ses citoyens ses entreprises et ses institutions contre le cybermenace et son engagement à promouvoir la collaboration international dans la sécurisation d'un internet mondial et sans restriction

Cet objectif sera atteint en recourant à des instruments réglementaires sous trois domaines d'action :

- Améliorer la résilience l'indépendance technologique et le leadership;
- Promouvoir les progrès d'un cyberspace mondial et inclusif
- Renforcer les capacités opérationnelles

EduGroupe

Accompagner pour réussir



Directive NIS2 : principaux Axes et Exigences

1. Publication de la Directive NIS2
2. Principaux changements entre NIS et NIS2
3. Champs d'application : identification des secteurs et entreprises concernées
4. Description des principales exigences de la directive NIS 2

Publication de la Directive NIS2

- La directive NIS 2 est publiée dans le cadre d'une série de directives et de règlements.
- La publication complète Journal officiel de l'UE contient :

1

Règlement de l'UE (2022/2554) - DORA pour le secteur financier

2

Directive européenne (2022/2555) - Directive NIS 2

3

Directive européenne (2022/2556) 6 modifie d'autres directives pour les rendre conformes à DORA.

4

Directive de (2022/2557) - traite de la résilience des entités critiques.

- 16 décembre 2020 acceptation de la commission européenne de mettre à jour NIS 1 vers NIS2.
- Entrée en vigueur le 16 janvier 2023.
- Les états membres doivent adopter et rendre publique les mesures de transposition pour adhérer à la directive NIS2 avant le 17 octobre 2024.

EduGroupe

Accompagner pour réussir

Principaux changements

DE LA CYBERSÉCURITÉ DES OPÉRATEURS CRITIQUES VERS LA CYBERSÉCURITÉ DE MASSE

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

Principaux changements

Entre les directives NIS 1 et NIS 2

La directive NIS 2 introduit plusieurs changements importants par rapport à la directive NIS 1 :

Approche Proactive	Retours d'informations et enseignements tirés
Notification des menaces et des incidents (Article 23 CSIRT et ANSSI)	
Processus d'établissement de rapport à plusieurs niveaux	
Alerte précoce	Renseignements sur les menaces et partage d'informations
Notification d'incident	
Rapport intermédiaire	
Rapport final	
Rapport d'avancement	

Publication et Objectifs de NIS2

Les principaux objectifs de la Directive NIS 2 sont les suivants :

1

Créer des systèmes cyber-résilients

2

Minimiser les incohérences en matière de résilience entre les différents secteurs du marché intérieur.

3

Amélioration de la connaissance de la situation commune et de la capacité collective à gérer efficacement les menaces et les défis cybernétiques.

EduGroupe

Accompagner pour réussir

Structure de la directive NIS 2

La directive NIS 2 est divisée, comme les autres directives et règlements de l'UE, en 2 grandes parties :

- les **considérants** : **144**
- les **articles** : **46** complétés
  - en ANNEXE 1, les secteurs hautement critiques
  - en ANNEXE 2 , les secteurs critiques

Les **considérants** fournissent un contexte, une orientation et des conseils afin de faciliter la compréhension des exigences

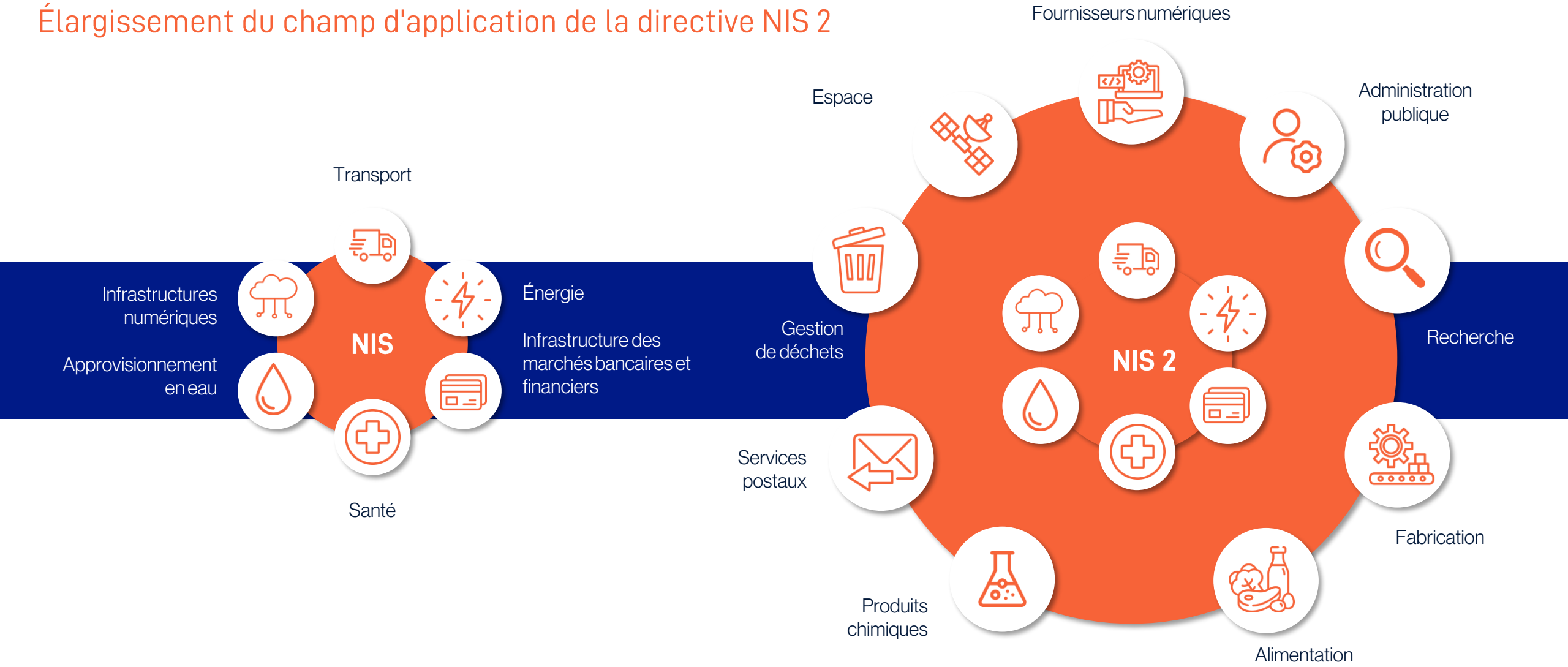
Les **articles** précisent les exigences auxquelles les entités entrant dans le champ d'application de la directive doivent se conformer.

EduGroupe

Accompagner pour réussir

CHAMPS D'APPLICATIONS DES DIRECTIVES NIS 1 ET NIS 2

Élargissement du champ d'application de la directive NIS 2



Périmètre des entités régulées par NIS 2

Les secteurs de l'annexe 1 de la directive

Secteur	Sous-secteur
1. ENGERGIE	Electricité Réseaux de chaleur et de froid Pétrole Gaz Hydrogène
2. TRANSPORT	Transports aériens Transports ferroviaires Transports par eau Transports routiers
3. SECTEUR BANCAIRE	
4. INFRASTRUCTURE DES MARCHES FINANCIERS	
5. SANTE	
6. EAU POTABLE	
7. EAUX USEES	
8. INFRASTRUCTURE NUMERIQUES	
9. GESTION DES SERVICES TIC	
10. ADMINISTRATION PUBLIQUE	Administration centrale
11. ESPACE	

Périmètres des entités régulées par NIS2

Les secteurs de l'annexe 2 de la directive

Secteur	Sous-secteur
1. SERVCES POSTAUX ET D'EXPEDITION	
2. GESTION DES DECHETS	
3. FABRICATION, PRODUCTION ET DISTRIBUTION DE PRODUITS CHIMIQUES	
4. PRODUCTION, TRANSFORMATION ET DISTRIBUTION DES DENREES ALIMENTAIRES	
5. 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
6. FOURNISSEURS NUMERIQUES	
7. RECHERCHE	

Les entités essentielles

Règles 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
  - Chiffre d'affaires supérieur ou égal à 50 millions d'euros
  - Bilan annuel supérieur ou égal à 43 millions d'euros

Annexe	Secteur
1	1. Energie
1	2. Transports
1	3. Secteur bancaire
1	4. Infrastructures des marchés financiers
1	5. Santé
1	6. Eau potable
1	7. Eaux usées
1	8. Infrastructures numériques
1	9. Gestion des services TIC
1	10. Administrations publiques
1	11. Espace

Les entités essentielles

Règles secondaires

Sont également considérées entités essentielles :

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

Les entités importantes

Règles 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**.

Annexe	Secteur
1	1. Energie
1	2. Transports
1	3. Secteur bancaire
1	4. Infrastructures des marchés financiers
1	5. Santé
1	6. Eau potable
1	7. Eaux usées
1	8. Infrastructures numériques
1	9. Gestion des services TIC
1	10. Administrations publiques
1	11. Espace

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
2	1. Services postaux et d'expédition
2	2. Gestion des déchets
2	3. Fabrication, production et distribution de produits chimiques
2	4. Production, transformation et distribution des denrées alimentaires
2	5. Fabrication
2	6. Fournisseurs Numériques
2	7. Recherche

EduGroupe

Accompagner pour réussir

Les obligations pour les entités régulées

Notification, contact et déclaration des incidents majeurs

Notification à l'ANSSI

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

Communication des informations de contact et mise à jour

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

Déclaration à l'ANSSI des incidents majeurs

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

EduGroupe

Accompagner pour réussir

Descriptions des obligations pour les entités régulées

Mesures de sécurité prévues par NIS 2

01 Les politiques relatives à l'analyse des risques et à la sécurité des SI

02 La gestion des incidents

03 La continuité des activités (sauvegardes, PRA gestion des crises)

04 La sécurité de la chaîne d'approvisionnement (fournisseurs/prestataires)

05 La sécurité de l'acquisition, du développement et de la maintenance des SI

Les obligations pour les entités régulées

Mesures de sécurité prévues par NIS 2

06 Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité

07 Les pratiques de base (cyberhygiène et formation à la cybersécurité)

08 Des politiques et des procédures relatives à l'utilisation de la cryptographie

09 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

EduGroupe

Accompagner pour réussir

Directive DORA : renforcer la résilience opérationnelle digitales

1. Publication de la Directive DORA
2. Champs d’application : identification des secteurs et entreprises concernées
3. Description des principales exigences de la directive DORA

EduGroupe

Accompagner pour réussir

Digital Operationally Resilience Act

La Réglementation sur la Résilience Opérationnelle Numérique (DORA)

La Réglementation sur la Résilience Opérationnelle Numérique (DORA) est une nouvelle réglementation qui vise à renforcer la sécurité des technologies de l'information et de la communication (TIC) des entités financières dans l'Union européenne (UE). Elle a été publiée au Journal officiel de l'UE le 27 décembre 2022 et entrera en vigueur le 16 janvier 2023 DORA sera applicable à partir du **17 janvier 2025**.

(ACPR) l’Autorité de contrôle prudentiel et de résolution est en charge de l'agrément et de la surveillance des établissements bancaires.

Les autorités nationales compétentes et l'Autorité bancaire européenne (ABE) superviseront et veilleront au respect du règlement DORA, ce qui peut inclure des inspections sur place, la publication d'orientations et l'imposition de sanctions en cas de non-respect.

(ACPR en France Adossée à la Banque de France)

PRINCIPAUX OBJECTIFS

OBJECTIF 1

L'objectif principal de DORA est de prévenir et de réduire les menaces cybernétiques et de garantir que les entités financières peuvent résister, répondre et se remettre de toutes sortes de perturbations et de menaces liées aux TIC.

OBJECTIF 1

Elle vise à atteindre un niveau élevé de résilience opérationnelle numérique dans tous les États membres de l'UE.

CHAMPS D'APPLICATIONS : IDENTIFICATION DES SECTEURS ET ENTREPRISES CONCERNÉES

Qui est concerné par DORA ? (Liste non-exhaustive)

- Établissements de crédit
- Institutions de paiement
- Prestataires de services d'information sur les comptes
- Institutions de monnaie électronique
- Entreprises d'investissement
- Prestataires de services de crypto-actifs
- Dépositaires centraux de titres
- Entreprises d'assurance et de réassurance
- Intermédiaires d'assurance et de réassurance
- Institutions de retraite professionnelle
- Référentiels de titrisation
- Contreparties centrales
- Plateformes de négociation
- Référentiels centraux
- Gestionnaires de fonds d'investissement alternatifs
- Sociétés de gestion
- Prestataires de services de rapportage de données
- Dépositaires centraux de titres
- Agences de notation de credit
- Administrateurs de référentiels critiques
- Prestataires de services de financement participative
- Prestataires de services TIC tiers

Structure de DORA

DORA est divisée en deux grandes parties (les considérants et les articles), comme les autres directives et règlements de l'UE. Elle se compose de 106 considérants et de 64 articles.

Les considérants fournissent un contexte, une orientation et des conseils afin de faciliter la compréhension des exigences.

Les articles précisent les exigences auxquelles les entités entrant dans le champ d'application de DORA doivent se conformer.

DESCRIPTION DES PRINCIPALES EXIGENCES DE LA DIRECTIVE DORA

Les nouvelles règles prévues par le Règlement DORA recouvrent 6 catégories :

Une gouvernance renforcée, qui implique notamment une pleine responsabilité de l'organe de direction dans la gestion des risques liés aux TIC (article 5).

Une gestion des risques liés aux TIC : mise en place d'un cadre de gestion des risques (cartographie des risques, mécanismes de détection rapide, procédures de réponse et de rétablissement, ...), réexamen annuel du cadre de gestion des risques, réalisation d'audits internes réguliers

La gestion, la classification (sur la base des critères définis par le règlement) et la notification des incidents : processus de gestion des incidents (indicateurs d'alerte précoce, remontée d'information, communication de crise, etc.), notification des incidents majeurs (notification initiale, rapport intermédiaire, rapport final) dans les délais à fixer par les autorités européennes de surveillance.

DESCRIPTION DES PRINCIPALES EXIGENCES DE LA DIRECTIVE DORA

Les nouvelles règles prévues par le Règlement DORA recouvrent 6 catégories :

La conduite de tests de la résilience opérationnelle numérique : mise en place d'un programme de tests (analyses de vulnérabilité, analyses de sources ouvertes, tests fondés sur des scénarios, tests de performance, tests de bout en bout, tests de pénétration, etc.), suivi et réexamen du programme.

L'encadrement des prestataires de services de TIC : évaluation et gestion des risques en amont de la contractualisation selon les critères définis par le règlement (article 28, 1) ; clauses obligatoires (description des niveaux de services) suivi permanent de la performance et de la qualité du service.

Le partage d'informations en matière de cybersécurité entre les entités concernées, afin d'échanger des renseignements liés aux cybermenaces, tels que les indicateurs, tactiques, techniques et procédures, alertes de cybersécurité et outils de configuration (article 45).

EduGroupe

Accompagner pour réussir

Formation et sensibilisation des équipes

1. Pourquoi se former et avec qui ?
2. Les formations EduGroupe
3. Les financements

Pourquoi nous choisir ?

+ de 35 ans d'expérience

+ 16 000

stagiaires formés en 2023

+ 97 %

d'entre eux ont évalué la formation suivie avec une note supérieure à 9/10

+ 400

Consultants formateurs

+ 800

Formations proposées dans notre catalogue

- Les valeurs Humaines
- Approche partenariale
- Conseil
- Ingénierie pédagogique
- Experts reconnus
- Gain de temps
- Présence nationale

Nos agréments éditeurs

Microsoft Partner
PeopleCert All talents, certified.
aws
SAP
CITRIX
cisco
vmware
PECB
Trailblazer WORKFORCE PARTNER
AUTODESK

Tests & certifications

Organisme de formation agréé
PeopleCert, PECB, TOSA, SCRUM.ORG

Focus sur l'essentiel

Déroulement de la formation

En présentiel OU À distance OU En Hybride

Formations certifiantes

PECB

4 nouvelles formations

- Sensibilisation à la directive NIS2
  1 jour (7 heures)
- Sensibilisation au règlement DORA
  1 jour (7 heures)
- NIS2 Directive Lead Implémenter (examen inclus)
  - Certification incluse
  - 5 jours (35 heures)
- **DORA Lead Manager (examen inclus)**
  - Certifications incluses
  - 5 jours (35 heures)

EduGroupe

Accompagner pour réussir

Sensibilisation à la directive NIS 2

- Introduction à la Directive NIS2
- Compréhension des Principes Fondamentaux de la Directive NIS2
- Mise en pratique de la Directive NIS2
- Bonnes Pratiques et Conformité à la Directive NIS2
- Clôture de la journée de Sensibilisation

EduGroupe

Accompagner pour réussir

NIS2 Directive Lead Implémenter (examen inclus)

- Jour 1 : Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2
- Jour 2 : Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques
- Jour 3 : Contrôles de cybersécurité, gestion des incidents et gestion de crise
- Jour 4 : Communication, tests, surveillance et amélioration continue de la cybersécurité
- Jour 5 : Examen de certification

EduGroupe

Accompagner pour réussir

SENSIBILISATION AU RÈGLEMENT DORA

- Introduction
- Comprendre DORA : Concepts Clés et Objectifs
  - Examen Détaillé des Exigences de DORA
  - Exigences de gestion des risques ICT
  - Signalement et gestion des incidents
  - Tests de résilience opérationnelle
  - Gestion des risques liés aux tiers
  - Partage d'informations et coordination
- Évaluation et Gestion des Risques
- Formation et Sensibilisation des Équipes Internes
  - Importance de la formation continue et de la sensibilisation
  - Conception d'un programme de formation efficace
  - Offres de formation et ressources d'EduGroupe
- Session de questions/réponses

EduGroupe

Accompagner pour réussir

DORA LEAD MANAGER (EXAMEN INCLUS)

- Jour 1 : Introduction des concepts et exigences de DORA
- Jour 2 : Gestion des risques et incidents liés aux ITC
- Jour 3 : Gestion des risques liés aux prestataires tiers et partages des informations
- Jour 4 : Réévaluation et amélioration continuelle
- Jour 5 Examen de certification

Les financements possibles

- Plan de développement des compétences
- FNE
- Actions collectives ATLAS
- Fonds Personnels

Accompagner pour réussir

EduGroupe

Accompagner pour réussir

QUESTIONS et REPONSES

MERCI

A bientôt

www.edugroupe.com