AYI NEDJIMI Consultants

NIS2, DORA et RGPD : Cartographie des Exigences Croisées

Catégorie : Conformité Lecture : 12 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Cartographie complète des exigences croisées NIS2, DORA et RGPD : matrice de correspondance, synergies réglementaires, stratégie GRC unifiée, rôles.

2.1 NIS2 : la sécurité des réseaux et systèmes d'information

La **directive NIS2** (Directive (UE) 2022/2555), entrée en vigueur le 16 janvier 2023 et devant être transposée en droit national avant le 17 octobre 2024, élargit considérablement le champ d'application de la directive NIS originale. En France, la transposition est désormais effective depuis début 2025, avec l'ANSSI comme autorité compétente. Cartographie complète des exigences croisées NIS2, DORA et RGPD : matrice de correspondance, synergies réglementaires, stratégie GRC unifiée, rôles. Le cadre réglementaire européen impose des exigences croissantes aux organisations. Ce guide sur nis2 dora rgpd exigences croisees fournit les clés de compréhension et de mise en conformité. Nous abordons notamment : 7. checklist opérationnelle de conformité triple, questions frequentes et 8. conclusion : transformer la contrainte en avantage compétitif. Les professionnels y trouveront des recommandations actionnables, des commandes prêtes à l'emploi et des stratégies de mise en œuvre adaptées aux environnements d'entreprise.

NIS2 distingue deux catégories d'entités :

- **Entités essentielles** : énergie, transports, santé, eau potable, infrastructures numériques, espace, administration publique, secteur bancaire. Régime de supervision proactif, contrôles ex ante.
- **Entités importantes** : services postaux, gestion des déchets, fabrication, production alimentaire, fournisseurs numériques (SaaS, marketplaces, moteurs de recherche). Supervision réactive, contrôles ex post.

Les obligations principales : **analyse de risques** formalisée, **mesures de sécurité** proportionnées, **notification des incidents** significatifs à l'autorité compétente (alerte précoce sous 24h, notification complète sous 72h, rapport final sous 1 mois), **gouvernance** avec responsabilité de la direction, **sécurité de la chaîne d'approvisionnement**, et **formation** des dirigeants. Pour une analyse approfondie de la phase opérationnelle, consultez notre article sur NIS2 phase opérationnelle 2026.

2.2 DORA : la résilience opérationnelle numérique du secteur financier

Le **règlement DORA** (Règlement (UE) 2022/2554), applicable depuis le 17 janvier 2025, est un règlement (pas une directive) -- il s'applique directement sans transposition nationale. Il cible spécifiquement le secteur financier : banques, assurances, sociétés de gestion, prestataires de services de paiement, établissements de monnaie électronique, et de manière inédite, les **prestataires tiers critiques de services TIC** (cloud providers, data centers, éditeurs de logiciels).

DORA repose sur cinq piliers :

1. **Gestion des risques liés aux TIC** : cadre de gestion des risques incluant identification, protection, détection, réponse et récupération.
2. **Gestion des incidents TIC** : classification, notification (alerte initiale sous 4h pour incidents majeurs, rapport intermédiaire sous 72h, rapport final sous 1 mois), registre des incidents.
3. **Tests de résilience opérationnelle numérique** : tests de pénétration avancés (TLPT - Threat-Led Penetration Testing) obligatoires tous les 3 ans pour les entités significatives.
4. **Gestion des risques liés aux prestataires tiers de services TIC** : registre des contrats, clauses contractuelles obligatoires, stratégie de sortie, droits d'audit et d'accès.
5. **Partage d'informations** : échange volontaire de renseignements sur les cybermenaces entre entités financières.

Comment démontrez-vous l'accountability exigée par le RGPD en cas de contrôle ?

Pour un bilan complet de conformité, voir notre article DORA 2026 : bilan de conformité.

2.3 RGPD : la protection des données personnelles

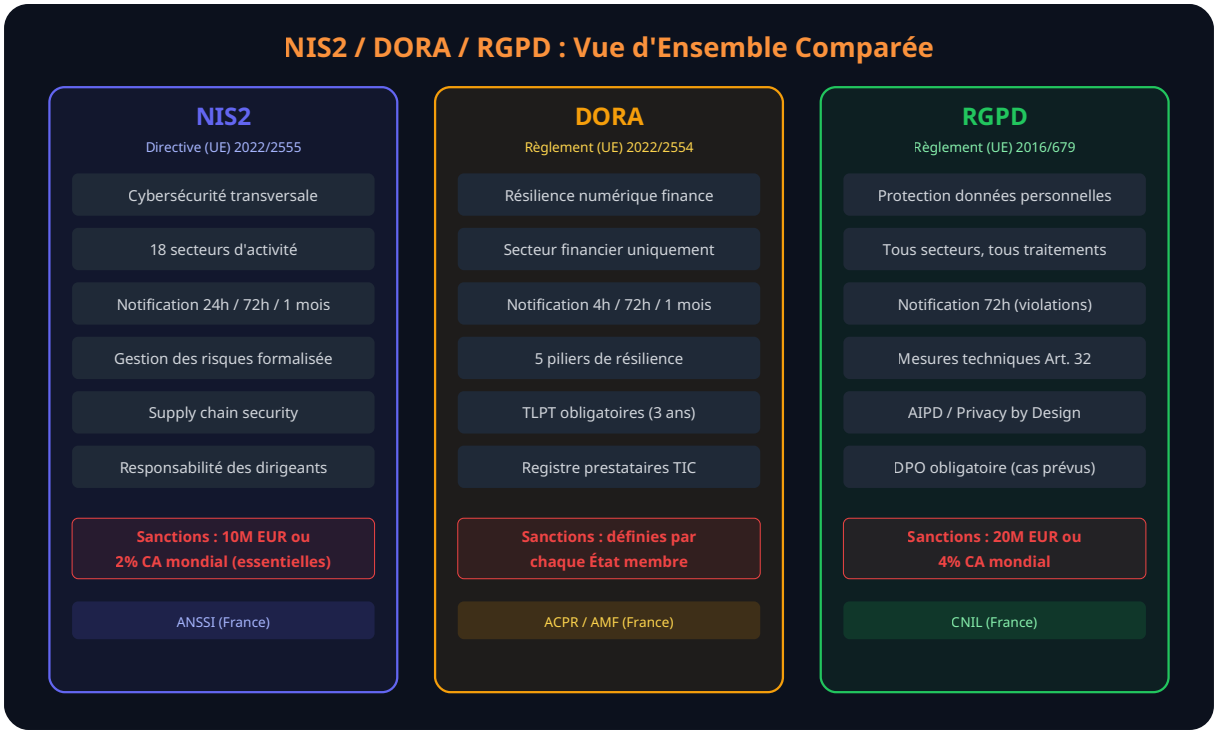
Le **RGPD** (Règlement (UE) 2016/679), applicable depuis le 25 mai 2018, reste la pierre angulaire de la protection des données en Europe. Son article 32 impose des **mesures techniques et organisationnelles appropriées** pour assurer un niveau de sécurité adapté au risque, incluant le chiffrement, la pseudonymisation, la confidentialité, l'intégrité, la disponibilité des systèmes, et la capacité de rétablir les données après un incident.

Du point de vue cybersécurité, le RGPD impose :

- **Notification de violation** (Art. 33-34) : notification à l'autorité de contrôle (CNIL en France) dans les **72 heures** suivant la prise de connaissance d'une violation de données personnelles. Notification aux personnes concernées si risque élevé.
- **Analyse d'impact (AIPD/DPIA)** (Art. 35) : pour les traitements à risque élevé. Inclut une évaluation de la nécessité, de la proportionnalité et des mesures de sécurité.
- **Privacy by Design & by Default** (Art. 25) : intégration de la protection des données dès la conception des systèmes.
- **Registre des traitements** (Art. 30) : inventaire exhaustif des traitements de données personnelles.

- **Désignation d'un DPO** (Art. 37-39) : obligatoire pour les organismes publics, les traitements à grande échelle et le suivi systématique de personnes.

En 2026, la CNIL renforce ses contrôles sur la sécurité technique, comme détaillé dans notre article RGPD 2026 : sécurité et exigences CNIL.



Notre avis d'expert

L'audit de conformité n'est utile que s'il débouche sur des actions correctives concrètes et mesurables. Nos missions d'accompagnement privilégient l'approche par les risques plutôt que la conformité checkbox, ce qui garantit une amélioration réelle de la posture de sécurité.

Les trois textes imposent une **responsabilité au niveau de la direction** (board-level accountability), mais avec des degrés d'exigence variables :

- **NIS2** (Art. 20) : les organes de direction doivent **approuver les mesures de gestion des risques**, **superviser leur mise en oeuvre** et **suivre une formation** en cybersécurité. Ils sont **personnellement responsables** en cas de manquement. C'est le texte le plus explicite sur la responsabilité personnelle des dirigeants.
- **DORA** (Art. 5) : l'organe de direction est responsable du cadre de gestion des risques TIC. Il doit définir les rôles, approuver la stratégie de résilience et allouer les ressources. Obligation de formation spécifique sur les risques TIC.
- **RGPD** : le responsable de traitement (l'organisation) est responsable de la conformité. La responsabilité personnelle des dirigeants n'est pas explicitement prévue dans le texte, mais la CNIL peut sanctionner les personnes physiques selon le droit national. Le DPO rend compte "au niveau le plus élevé de la direction" (Art. 38).

3.4 Audits, contrôles et tests

Chaque texte prévoit des mécanismes d'audit et de contrôle, avec des niveaux de formalisme croissants :

Aspect	NIS2	DORA	RGPD
Audits de sécurité	Audits réguliers des mesures de sécurité (fréquence non spécifiée)	Programme de tests annuel obligatoire + TLPT tous les 3 ans	Évaluation régulière de l'efficacité des mesures (Art. 32.1.d)
Tests de pénétration	Implicite dans les mesures de sécurité	TLPT obligatoire, basé sur TIBER-EU, réalisé par des testeurs qualifiés	Non explicitement requis, mais recommandé par la CNIL
Contrôles de l'autorité	Inspections, audits de sécurité, scans ad hoc par l'ANSSI	Inspections par l'ACPR, audits sur pièces et sur place	Contrôles CNIL (sur place, en ligne, sur pièces, sur audition)
Certification	Possibilité de recourir à des certifications (ISO 27001, etc.)	Standards techniques de régulation (RTS/ITS)	Codes de conduite et certifications (Art. 40-43)

DORA TLPT : l'exigence la plus contraignante
Les tests TLPT (Threat-Led Penetration Testing) de DORA sont les plus exigeants des trois textes. Ils doivent simuler des scénarios d'attaque réalistes, couvrir les fonctions critiques et être réalisés par des testeurs indépendants qualifiés. En se préparant au TLPT DORA, une organisation couvre automatiquement les exigences d'audit NIS2 et les recommandations de tests RGPD. C'est pourquoi nous recommandons d'utiliser le TLPT comme **test de référence commun**.

3.5 Sanctions : l'addition peut être salée

Un manquement à un seul incident peut entraîner des sanctions au titre des **trois textes simultanément**. Les sanctions ne se substituent pas -- elles se cumulent :

- **NIS2** : jusqu'à 10 millions d'euros ou 2 % du CA mondial pour les entités essentielles ; 7 millions ou 1,4 % pour les entités importantes. Plus : **responsabilité personnelle des dirigeants** et possibilité de suspension temporaire de l'exercice de fonctions de direction.
- **DORA** : sanctions définies par chaque État membre, incluant amendes, injonctions et publication des décisions. Les prestataires TIC critiques sont soumis à des astreintes journalières (jusqu'à 1 % du CA mondial quotidien).
- **RGPD** : jusqu'à 20 millions d'euros ou 4 % du CA mondial (le montant le plus élevé). En 2025, la CNIL a prononcé des sanctions cumulées dépassant 500 millions d'euros.

Pour une banque soumise aux trois textes, un incident majeur avec fuite de données personnelles pourrait théoriquement entraîner : 2 % CA (NIS2) + sanctions ACPR (DORA) + 4 % CA (RGPD) = potentiellement **6 % du CA mondial en amendes cumulées**, sans compter les dommages réputationnels et les coûts de remédiation.

Cas concret
L'entrée en vigueur de NIS2 en octobre 2024 a élargi le périmètre des organisations soumises à des obligations de cybersécurité en Europe. Les secteurs essentiels et importants doivent désormais notifier les incidents significatifs dans les 24 heures et maintenir des mesures de gestion des risques proportionnées.

Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

L'utilisation d'ISO 27001:2022 comme framework de base offre un avantage considérable : sa Déclaration d'Applicabilité (DdA) peut être étendue pour intégrer les exigences spécifiques de NIS2, DORA et RGPD non couvertes par la norme. De plus, la certification ISO 27001 est explicitement reconnue par NIS2 (considérant 79) comme preuve de conformité aux mesures de sécurité, et par DORA comme référentiel technique. Un SMI basé sur ISO 27001 réduit l'effort d'audit en permettant une **certification unique** qui satisfait 70 à 80 % des exigences des trois textes.

Le DPO (Délégué à la Protection des Données) intervient sur les volets RGPD mais aussi sur les aspects « données personnelles » de NIS2 et DORA :

- **Registre des traitements :** Maintenir le registre RGPD Art. 30 et l'enrichir avec les traitements liés aux mesures NIS2/DORA (logs de sécurité, surveillance réseau).
- **AIPD :** Réaliser les analyses d'impact relatives à la protection des données pour les nouveaux traitements, y compris ceux imposés par NIS2/DORA.
- **Notifications CNIL :** Piloter les notifications de violation de données personnelles (72h RGPD) en coordination avec le RSSI.
- **Droits des personnes :** Gérer les demandes d'exercice de droits (accès, effacement, portabilité) qui peuvent être impactées par les obligations de conservation NIS2/DORA.

5.4 La direction générale : responsabilité personnelle

NIS2 et DORA imposent une **responsabilité personnelle des dirigeants** en matière de cybersécurité. Concrètement, la direction doit :

- **Approuver** les politiques de sécurité et de résilience (NIS2 Art. 20, DORA Art. 5)
- **Suivre une formation** en cybersécurité (NIS2 Art. 20.2) -- obligation personnelle, non délégable
- **Superviser** la mise en oeuvre des mesures de gestion des risques (NIS2 Art. 20.1)
- **Rendre compte** aux régulateurs en cas d'incident majeur
- **Assumer les sanctions** en cas de manquement, y compris la suspension temporaire de leurs fonctions (NIS2 Art. 32.5)

Risque personnel pour les dirigeants
NIS2 introduit une innovation majeure : la possibilité pour les autorités compétentes de **suspendre temporairement l'exercice de fonctions de direction** en cas de manquement grave et répété aux obligations de cybersécurité (Art. 32.5.b). Cette disposition, sans équivalent dans DORA ou le RGPD, vise à responsabiliser personnellement les dirigeants. En pratique, cela signifie que le CEO ou le DSI d'une entité essentielle peut être temporairement écarté de ses fonctions par décision administrative.

Phase 3 : Implémentation (Mois 7-12)

- Déployer les mesures techniques manquantes (chiffrement, MFA, segmentation, monitoring)
- Mettre en place le programme de tests de sécurité (pentests annuels, préparation TLPT)

- Auditer et contractualiser les prestataires TIC critiques (DORA Art. 28-30)
- Déployer un plan de continuité et de reprise couvrant les trois textes
- Lancer les campagnes de sensibilisation du personnel

Phase 4 : Maturité et amélioration continue (Mois 12+)

- Réaliser un audit blanc croisé NIS2/DORA/RGPD
- Préparer les dossiers de conformité pour les régulateurs (ANSSI, ACPR, CNIL)
- Automatiser le reporting et les contrôles récurrents
- Envisager la certification ISO 27001 comme socle fédérateur
- Déployer un cycle d'amélioration continue (revue de direction semestrielle)

6.3 Budget et ROI de la conformité unifiée

Le coût de mise en conformité varie considérablement selon la taille de l'organisation et son niveau de maturité initial. Voici des ordres de grandeur pour une ETI (500-5 000 collaborateurs) :

Poste	Approche silo (x3)	Approche unifiée	Économie
Consulting / accompagnement	450-750 K€	200-350 K€	-50 %
Outillage GRC	150-300 K€	80-150 K€	-47 %
Mesures techniques	300-600 K€	250-500 K€	-17 %
Formation / sensibilisation	90-150 K€	40-70 K€	-55 %
Audits / certifications	120-200 K€	60-100 K€	-50 %
Total estimé	1,1 - 2,0 M€	630 K - 1,2 M€	-40 à -43 %

Le ROI de la conformité unifiée se calcule non seulement par les économies directes (40-43 % sur le budget de mise en conformité), mais aussi par les coûts évités : sanctions potentielles (jusqu'à 6 % du CA cumulé), coûts de remédiation post-incident (en moyenne 4,5 M€ pour un incident majeur selon IBM 2025), et préservation de la réputation.

7. Checklist opérationnelle de conformité triple

Cette checklist synthétise les actions prioritaires pour atteindre la conformité croisée NIS2/DORA/RGPD. Chaque item indique les textes couverts.

Gouvernance et organisation

- ☐ Désigner un RSSI et un DPO (ou vérifier leur nomination) [NIS2 + DORA + RGPD]
- ☐ Constituer un comité de pilotage conformité triple avec participation de la DG [NIS2 + DORA + RGPD]
- ☐ Formaliser la matrice RACI des rôles et responsabilités [NIS2 + DORA + RGPD]
- ☐ Former les membres de la direction à la cybersécurité [NIS2 Art. 20.2]
- ☐ Rédiger / mettre à jour la politique de sécurité SI unifiée [NIS2 + DORA + RGPD]

Gestion des risques

- ☐ Réaliser une analyse de risques unifiée (EBIOS RM ou ISO 27005) [NIS2 + DORA + RGPD]
- ☐ Intégrer les risques « données personnelles » dans l'analyse de risques cyber [RGPD Art. 32]
- ☐ Réaliser les AIPD pour les traitements à risque élevé [RGPD Art. 35]
- ☐ Cartographier les fonctions critiques et importantes (DORA) [DORA Art. 8]
- ☐ Maintenir un registre des risques consolidé avec plan de traitement [NIS2 + DORA + RGPD]

Gestion des incidents

- ☐ Formaliser un processus de gestion des incidents unifié [NIS2 + DORA + RGPD]
- ☐ Créer des fiches de qualification multi-régime (NIS2/DORA/RGPD) [NIS2 + DORA + RGPD]
- ☐ Préparer les templates de notification (ANSSI, ACPR, CNIL) [NIS2 + DORA + RGPD]
- ☐ Tester le processus par un exercice de crise cyber [NIS2 + DORA]
- ☐ Configurer un registre des incidents et violations [NIS2 + DORA + RGPD]

Mesures techniques et continuité

- ☐ Déployer le chiffrement des données au repos et en transit [NIS2 + DORA + RGPD]
- ☐ Installer l'authentification multi-facteurs (MFA) [NIS2 + DORA]
- ☐ Déployer un SIEM/SOC pour la détection des incidents [NIS2 + DORA]
- ☐ Formaliser et tester le PCA/PRA [NIS2 + DORA + RGPD]
- ☐ Planifier le programme de tests annuel (pentests + préparation TLPT) [DORA Art. 24-27]

Gestion des tiers et supply chain

- ☐ Inventorier tous les prestataires TIC et sous-traitants [NIS2 + DORA + RGPD]
- ☐ Réaliser une évaluation des risques fournisseurs [NIS2 + DORA]
- ☐ Mettre à jour les contrats avec les clauses NIS2/DORA/RGPD [NIS2 + DORA + RGPD]
- ☐ Définir une stratégie de sortie pour les prestataires critiques [DORA Art. 28.8]

Pour approfondir ce sujet, consultez notre outil open-source pci-dss-audit-tool qui facilite l'audit de conformité PCI DSS.

Questions frequentes

Comment appliquer NIS2, DORA et RGPD dans un environnement de production ?

La mise en œuvre de NIS2, DORA et RGPD en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi NIS2, DORA et RGPD est-il essentiel pour la securite des systemes d'information ?

NIS2, DORA et RGPD constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quel est le délai réaliste pour se mettre en conformité avec NIS2, DORA et RGPD : Cartographie des Exigences Croisées ?

Comptez entre 6 et 18 mois selon la maturité de votre SI. Les entreprises qui partent de zéro doivent prévoir 12 mois minimum avec un accompagnement externe dédié.

Sources et références : CNIL · ANSSI

Articles connexes

- Audit de Sécurité du SI : Méthodologie Complète et

> Points clés à retenir
>
> - 7. Checklist opérationnelle de conformité triple
> - Questions frequentes
> - 8. Conclusion : transformer la contrainte en avantage compétitif

8. Conclusion : transformer la contrainte en avantage compétitif

Le triptyque NIS2/DORA/RGPD représente un défi de conformité majeur, mais aussi une **opportunité stratégique**. Les organisations qui adoptent une approche unifiée obtiennent trois bénéfices majeurs :

- **Économie substantielle :** 40 à 43 % d'économie sur le budget de mise en conformité par rapport à une approche en silo.
- **Cohérence renforcée :** Un système de management intégré élimine les contradictions, les redondances et les angles morts entre les textes.
- **Avantage concurrentiel :** La capacité à démontrer une conformité triple aux clients, partenaires et régulateurs devient un différenciateur commercial, en particulier dans les secteurs régulés (finance, santé, énergie).

Les clés du succès résident dans :

- **L'engagement de la direction :** Sans sponsor exécutif, aucun programme de conformité ne peut aboutir. NIS2 renforce cet impératif en engageant la responsabilité personnelle des dirigeants.
- **Le choix d'un socle fédérateur :** ISO 27001:2022 offre le meilleur rapport couverture/effort pour fédérer les trois textes.

- **La priorisation pragmatique :** Commencer par les exigences communes (gestion des risques, incidents, gouvernance) avant de traiter les spécificités de chaque texte.
- **L'outillage GRC adapté :** Un outil de gouvernance, risques et conformité capable de gérer plusieurs référentiels simultanément est indispensable.

Dernière réflexion : La conformité réglementaire n'est pas une fin en soi. C'est un **levier de maturité** qui, bien exécuté, améliore réellement la posture de sécurité de l'organisation. Les textes NIS2, DORA et RGPD, malgré leur complexité, poussent les organisations vers des pratiques que tout professionnel de la cybersécurité recommanderait indépendamment de toute obligation légale : gestion des risques, surveillance continue, tests réguliers, et gouvernance responsable.

Références et ressources externes

- EUR-Lex -- Directive NIS2 (2022/2555) -- Texte officiel de la directive NIS2
- EUR-Lex -- Règlement DORA (2022/2554) -- Texte officiel du règlement DORA
- EUR-Lex -- RGPD (2016/679) -- Texte officiel du RGPD
- ENISA -- NIS2 Implementation -- Ressources ENISA pour l'implémentation NIS2
- EBA -- Operational Resilience (DORA) -- Standards techniques DORA de l'Autorité bancaire européenne
- CNIL -- Le RGPD -- Guide RGPD de la CNIL
- ANSSI -- EBIOS Risk Manager -- Méthode d'analyse de risques de l'ANSSI

Ayi NEDJIMI

Expert en Cybersécurité & Intelligence Artificielle

Consultant senior avec plus de 15 ans d'expérience en sécurité offensive, audit d'infrastructure et développement de solutions IA. Certifié OSCP, CISSP, ISO 27001 Lead Auditor et ISO 42001 Lead Implementer. Intervient sur des missions de pentest Active Directory, sécurité Cloud et conformité réglementaire pour des grands comptes et ETI.

LinkedIn Profil complet Tous ses articles

Besoin d'un accompagnement expert ?

Nos consultants vous accompagnent dans votre mise en conformité NIS2, DORA et RGPD. Devis personnalisé sous 24h.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr