AYI NEDJIMI Consultants

NIS 2 et DORA : double conformité du secteur financier

Catégorie : Conformité Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Mettez en conformité votre organisation financière avec NIS 2 et DORA simultanément. Analyse croisée, mutualisation et exigences TLPT décryptées.

Résumé exécutif

Les organisations du secteur financier européen font face à un double défi de conformité réglementaire sans précédent avec l'application simultanée de la directive NIS 2 et du règlement DORA qui imposent des exigences complémentaires mais distinctes en matière de cybersécurité et de résilience opérationnelle numérique. Ce guide analyse en profondeur les chevauchements et les spécificités de chaque texte, propose une méthodologie structurée de mise en conformité mutualisée évitant la duplication des efforts, détaille les obligations opérationnelles concrètes à respecter en termes de gestion des risques, de notification des incidents, de tests de résilience et de supervision des prestataires TIC, et fournit une feuille de route pragmatique permettant aux banques, assureurs, sociétés de gestion et infrastructures de marché d'atteindre la conformité simultanée dans les délais impartis par les régulateurs.

Le paysage réglementaire de la cybersécurité financière en Europe a connu une transformation radicale avec l'entrée en application de deux textes majeurs qui redéfinissent les obligations des acteurs du secteur en matière de protection de leurs systèmes d'information et de résilience face aux perturbations numériques. La **directive NIS 2**, applicable depuis octobre 2024, élargit considérablement le périmètre des entités soumises à des obligations de cybersécurité en incluant désormais la quasi-totalité des acteurs financiers dans les catégories d'entités essentielles ou importantes. Le *règlement DORA* (Digital Operational Resilience Act), applicable depuis janvier 2025, impose des exigences spécifiques et détaillées de résilience opérationnelle numérique à l'ensemble du secteur financier européen incluant les établissements de crédit, les entreprises d'investissement, les compagnies d'assurance, les fonds de pension, les plateformes de négociation, les contreparties centrales et les prestataires de services de crypto-actifs. Pour les organisations financières, la question n'est plus de savoir si elles doivent se conformer mais comment orchestrer efficacement cette double mise en conformité en mutualisant les efforts, en évitant les redondances coûteuses et en construisant un dispositif de cybersécurité et de résilience cohérent répondant simultanément aux deux ensembles d'exigences dans un calendrier contraint et sous la supervision attentive des autorités compétentes nationales et européennes.

Quelles différences entre NIS 2 et DORA pour le secteur financier ?

NIS 2 et DORA partagent l'objectif commun de renforcer la cybersécurité et la résilience des organisations européennes, mais ils diffèrent significativement dans leur approche, leur périmètre et leur niveau de prescription. NIS 2 est une **directive** d'application générale transposée en droit national par chaque État membre, couvrant 18 secteurs d'activité et imposant des obligations de moyens en matière de gestion des risques cyber, de notification des incidents et de supervision de la supply chain. DORA est un **règlement** directement applicable sans transposition nationale, spécifique au secteur financier et nettement plus prescriptif dans ses exigences opérationnelles.

Le principe de lex specialis établi par l'article 4 de NIS 2 clarifie l'articulation entre les deux textes : lorsque les dispositions de DORA sont au moins équivalentes à celles de NIS 2, les exigences de DORA prévalent pour les entités financières. En pratique, DORA couvre la majorité des obligations de NIS 2 pour le secteur financier mais avec un niveau de détail et de prescription supérieur. Certaines obligations de NIS 2 restent cependant applicables en complément, notamment les dispositions relatives à la gouvernance et à la responsabilité des dirigeants. Cette articulation juridique nécessite une analyse fine pour identifier les exigences cumulatives et éviter les angles morts de conformité, en s'appuyant sur les travaux de conformité NIS 2.

Votre organisation financière a-t-elle réalisé une analyse d'écart croisée NIS 2 et DORA, ou traitez-vous les deux conformités en silos séparés avec le risque de duplications et de lacunes ?

Comment mutualiser la mise en conformité NIS 2 et DORA ?

La mutualisation de la mise en conformité NIS 2 et DORA repose sur l'identification d'un **socle commun d'exigences** couvert par les deux textes et sur l'ajout progressif des exigences spécifiques de chaque réglementation. Le socle commun couvre la gestion des risques ICT (article 6 de DORA / article 21 de NIS 2), la gestion et la notification des incidents (articles 17-19 de DORA / articles 23-24 de NIS 2), la supervision des prestataires tiers de services TIC (articles 28-30 de DORA / article 21.2.d de NIS 2) et les mesures de gouvernance incluant la responsabilité de l'organe de direction (article 5 de DORA / article 20 de NIS 2).

Les exigences spécifiques de DORA non couvertes par NIS 2 incluent les **tests de résilience opérationnelle numérique** avancés (articles 24-27), incluant les tests de pénétration fondés sur la menace (TLPT) pour les entités significatives, le **cadre de gestion des risques liés aux tiers** prestataires TIC avec un registre d'information détaillé et des clauses contractuelles obligatoires standardisées, et le **cadre de surveillance directe** des prestataires TIC critiques par les autorités européennes de surveillance. La méthodologie de mise en conformité mutualisée s'articule avec la conformité RGPD pour les volets protection des données.

Mon avis : Les organisations financières qui traitent NIS 2 et DORA comme deux projets séparés commettent une erreur stratégique coûteuse. J'ai vu des banques monter deux équipes projet indépendantes pour NIS 2 et DORA, chacune rédigeant ses propres politiques et procédures

avec des approches différentes. La facture est double et le résultat incohérent. La seule approche raisonnable est un programme de conformité unique couvrant les deux textes avec un référentiel commun et des extensions spécifiques.

Domaine d'exigence	NIS 2 (article)	DORA (article)	Articulation
Gestion des risques ICT	Art. 21	Art. 6-16	DORA prévaut (plus détaillé)
Notification incidents	Art. 23-24	Art. 17-19	DORA prévaut (délais spécifiques)
Tests de résilience	Non spécifié	Art. 24-27	DORA uniquement
Gestion tiers TIC	Art. 21.2.d	Art. 28-30	DORA prévaut (registre obligatoire)
Gouvernance direction	Art. 20	Art. 5	Cumulatif (NIS 2 ajoute formations)
Supervision directe	Art. 31-33	Art. 31-44	DORA pour prestataires TIC critiques
Sanctions	Art. 34-36	Art. 50-52	Les deux applicables selon domaine

L'incident Kaseya de juillet 2021, bien que touchant principalement des MSP et leurs clients, a eu des répercussions sur plusieurs institutions financières européennes utilisant les services de prestataires TIC compromis via la chaîne d'attaque. Cet événement a directement influencé la rédaction des exigences de DORA relatives à la supervision des prestataires TIC critiques et au registre d'information obligatoire, démontrant que la résilience du secteur financier dépend étroitement de la sécurité de l'ensemble de sa chaîne d'approvisionnement numérique, comme le confirme l'approche développée dans notre analyse de la gestion des vulnérabilités.

Quelles obligations de tests de résilience impose DORA ?

DORA impose un programme de tests de résilience opérationnelle numérique structuré en deux niveaux. Le premier niveau, applicable à toutes les entités financières, exige la réalisation de **tests de base** incluant des évaluations de vulnérabilités, des analyses de sources ouvertes, des évaluations de sécurité réseau, des analyses d'écarts, des revues de sécurité physique, des questionnaires et des tests de performance. Ces tests doivent couvrir les systèmes et applications TIC critiques au moins annuellement.

Le deuxième niveau, applicable aux entités financières significatives identifiées par les autorités compétentes, exige la réalisation de *tests de pénétration fondés sur la menace* (TLPT - Threat-Led Penetration Testing) au moins tous les trois ans. Ces tests, conduits selon le cadre TIBER-EU harmonisé au niveau européen, simulent des attaques réalistes basées sur les menaces actuelles identifiées par des équipes de threat intelligence indépendantes. Ils doivent couvrir les fonctions critiques ou importantes de l'entité et impliquer les prestataires TIC soutenant ces fonctions, en coordination avec le SOC et les équipes de réponse aux incidents.

Comment gérer le registre d'information des prestataires TIC ?

L'article 28.3 de DORA impose aux entités financières de maintenir un **registre d'information** détaillé de tous les accords contractuels relatifs à l'utilisation de services TIC fournis par des prestataires tiers. Ce registre doit être mis à jour en permanence et transmis aux autorités compétentes sur demande. Il constitue un outil de supervision permettant aux régulateurs d'identifier les concentrations de risques et les dépendances critiques du secteur financier envers des prestataires communs.

Le contenu du registre est précisé par les normes techniques réglementaires (RTS) développées par les autorités européennes de surveillance. Il doit inclure pour chaque accord contractuel l'identification du prestataire, la description des services fournis, la classification de la criticité du service, la localisation des données et des traitements, les sous-traitants impliqués et les accords de niveau de service en matière de sécurité et de disponibilité. La construction et le maintien de ce registre représentent un effort significatif qui nécessite une collaboration étroite entre la direction des achats, la DSI, le RSSI et la direction juridique. Les recommandations de l'ANSSI sur l'externalisation et de l'ENISA sur la supply chain fournissent des méthodologies complémentaires.

Faut-il créer une fonction dédiée à la résilience opérationnelle ?

DORA exige que les entités financières mettent en place un **cadre de gestion des risques liés aux TIC** complet et documenté, distinct mais complémentaire du cadre général de gestion des risques de l'organisation. La question de la création d'une fonction organisationnelle dédiée à la résilience opérationnelle numérique se pose légitimement pour les entités de taille significative. Cette fonction peut prendre la forme d'un département dédié, d'une cellule rattachée au RSSI ou d'un comité transverse pilotant la convergence des initiatives existantes en matière de cybersécurité, de continuité d'activité et de gestion des risques opérationnels.

L'approche la plus efficace consiste à éviter la création d'une structure organisationnelle nouvelle en silo, mais plutôt à renforcer la coordination entre les fonctions existantes (RSSI, direction des risques opérationnels, responsable continuité d'activité, DPO) via un comité de résilience opérationnelle numérique se réunissant mensuellement sous la supervision de l'organe de direction. Ce comité assure la cohérence de l'ensemble du dispositif et pilote le programme de tests de résilience, le registre des prestataires TIC et le reporting réglementaire vers les autorités de supervision compétentes.

Comment piloter le programme de conformité NIS 2 et DORA ?

Le pilotage du programme de conformité mutualisé NIS 2 et DORA nécessite une gouvernance projet structurée avec un sponsor au niveau de la direction générale, un chef de programme dédié disposant d'une vision transverse sur l'ensemble des chantiers, et des référents métier et technique dans chaque direction impactée. Le programme se structure typiquement en six à

huit chantiers thématiques couvrant la gouvernance et l'organisation, la gestion des risques ICT, la gestion des incidents, les tests de résilience, la gestion des prestataires TIC, la continuité d'activité, la formation et sensibilisation, et le reporting réglementaire.

Chaque chantier dispose d'un responsable identifié, d'un plan d'action détaillé avec des jalons trimestriels et d'indicateurs de progression mesurables. Le comité de pilotage du programme se réunit mensuellement pour suivre l'avancement, arbitrer les difficultés rencontrées et valider les livrables clés. Un comité stratégique trimestriel associant la direction générale et les régulateurs métier (directeur des risques, directeur de la conformité) valide les orientations majeures et les arbitrages budgétaires significatifs. La trajectoire de conformité doit être présentée régulièrement aux autorités de supervision dans le cadre du dialogue prudentiel, démontrant la maîtrise du calendrier et l'engagement de l'organisation dans la démarche de mise en conformité.

Sources et références : CNIL · ANSSI

Quels impacts organisationnels pour le secteur financier ?

La mise en conformité simultanée NIS 2 et DORA génère des impacts organisationnels profonds qui dépassent largement le périmètre de la direction des systèmes d'information et de la sécurité. La direction des risques opérationnels doit intégrer les risques ICT dans son dispositif de cartographie et de suivi avec une granularité nouvelle. La direction des achats doit adapter ses processus de sélection et de contractualisation des fournisseurs pour intégrer les exigences du registre d'information DORA et les clauses contractuelles standardisées imposées par le règlement.

La direction juridique doit mettre à jour l'ensemble des contrats avec les prestataires TIC pour y insérer les clauses obligatoires prévues par l'article 30 de DORA, incluant les droits d'audit, les obligations de notification des incidents, les plans de sortie et les clauses de sous-traitance. La direction des ressources humaines doit planifier les recrutements nécessaires en compétences cybersécurité et résilience, dans un marché de l'emploi tendu où ces profils sont très recherchés. L'organe de direction lui-même doit adapter son fonctionnement pour intégrer la supervision de la résilience opérationnelle numérique dans son agenda régulier, conformément aux obligations de gouvernance imposées par les deux textes réglementaires.

À retenir : Pour les entités financières, DORA constitue le texte de référence principal qui couvre et dépasse la majorité des exigences de NIS 2 en matière de cybersécurité et de résilience. La mise en conformité doit être conduite via un programme unique mutualisé évitant les duplications. Les exigences spécifiques de DORA en matière de tests TLPT, de registre des prestataires TIC et de supervision directe des prestataires critiques nécessitent des investissements et des compétences spécifiques à anticiper dans la planification budgétaire.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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