NEXIALOG CONSULTING

NEXIASEARCH

DORA : Cadre Européen de Résilience des Systèmes Financiers Numériques

IBNLKHAYAT Otman
KTARI Wassim
ZAGHAL Sami

THINK SMART ACT DIFFERENT

TABLE DES MATIÈRES

Présentation synthétique du réglement DORA

Le réglement DORA (Digital Operational Resilience Act) sur la résilience opérationnelle est un règlement voté en 2022 par le Conseil et le Parlement européen visant à renforcer la résilience opérationnelle des institutions financières face aux risques liés à l'utilisation des technologies de l'information et de la communication (TIC).DORA établit des directives pour maintenir la continuité des opérations financières en cas de cyberattaques ou de pannes technologiques, en mettant en place des mesures spécifiques pour la gestion des risques, la réalisation de tests de résilience, et la notification d'incidents. Ces actions visent à renforcer la solidité du secteur financier européen, en préparant les entités à anticiper et gérer efficacement les risques. Le règlement met également l'accent sur la prévention, en obligeant les institutions financières à se préparer aux menaces numériques futures, par l'adoption d'une approche proactive.

Définition NIS

NIS 1 & 2 :

Alors que DORA se focalise sur l'augmentation de la résilience numérique au sein du secteur financier, la directive NIS (Network and Information Security) de l'Union européenne cherche à améliorer la cybersécurité à l'échelle du marché européen. NIS 2, succédant à NIS 1, élargit considérablement le périmètre d'application pour englober des secteurs additionnels tels que les administrations publiques et les services postaux. Cet élargissement a pour but de renforcer la protection des systèmes d'information dans une gamme plus étendue de domaines en Europe.

NIS 2 vs DORA

	NIS 2	DORA
Objectifs	Renforcer la cybersécurité dans l'UE	Assurer l'intégrité et la disponibilité du secteur financier
Nature législative	Directive européenne	Règlement européen
Transposition nationale	Doit être transposée dans le droit national, entrée en vigueur à partir de janvier 2023	Applicable en l'état dans tous les pays de l'UE à partir du 17 janvier 2025
Entités visées	Entités Essentielles[1] et Entités Importantes[2]	21 types d'entités spécifiques du secteur financier
Impact sur les entités concernées	Les entités concernées par les deux textes doivent se conformer à la fois à NIS2 et à DORA	Les entités du secteur financier concernées par DORA doivent se conformer principalement à DORA, tout en respectant également les obligations de NIS2

[1]: désignent des domaines d'activité dont les services jouent un rôle vital dans le maintien des activités fondamentales au sein de la société ou de l'économie.

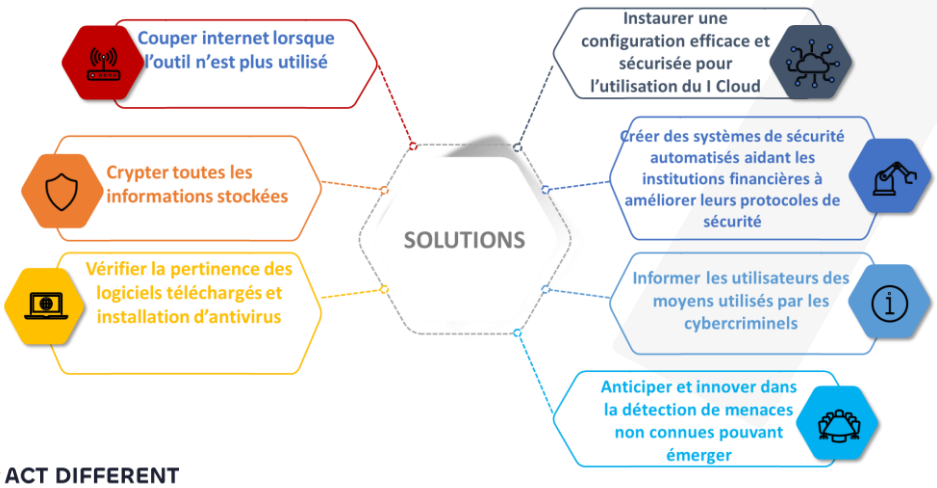
[2] : Réfère à toute entité—administration, entreprise publique ou privée—considérée par le gouvernement comme essentielle pour assurer la stabilité et la continuité du fonctionnement national.

Les menaces de cyber sécurité

La cybersécurité dans le secteur financier est confrontée à des défis liés aux logiciels malveillants, au phishing, au travail à distance, aux données non cryptées, à l'internet des objets, aux virus pour smartphones, aux cyberattaques basées sur le cloud, aux attaques via la chaîne d'approvisionnement en logiciels, aux technologies de l'IA, à l'ingénierie sociale, à la fraude, au vol d'identité, ainsi qu'à l'usurpation d'identité.

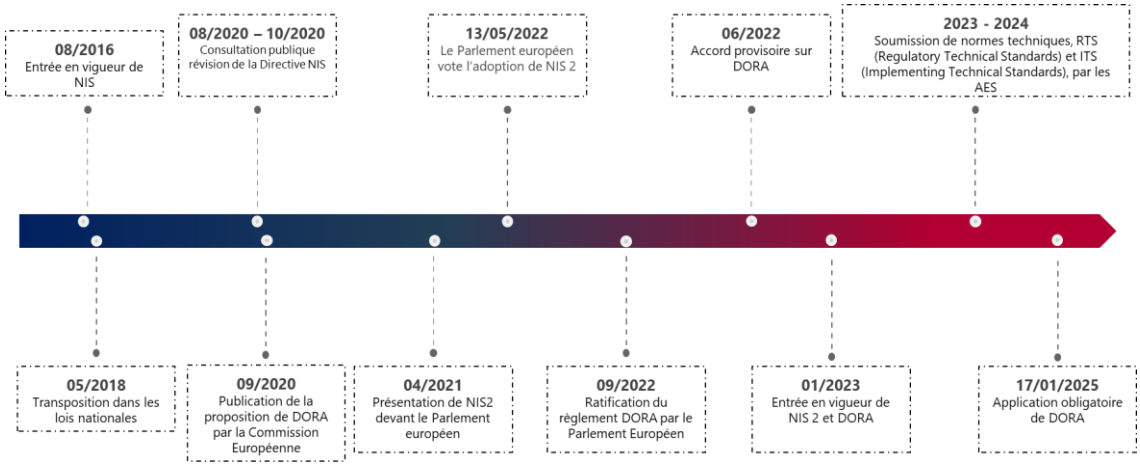
Ainsi, les défis en matière de cybersécurité dans le secteur financier sont nombreux, mais les solutions disponibles sont tout aussi variées. Comme illustré dans le schéma ci-dessous, une approche globale et multicouche est essentielle pour protéger les institutions financières contre ces menaces diverses. Cela peut inclure l'utilisation de pare-feu, de systèmes de prévention des intrusions, de cryptage des données, de programmes de formation en cybersécurité pour les employés, de protocoles de gestion des identités et d'autres mesures de sécurité, etc.

En combinant ces approches, les institutions financières peuvent renforcer leur résilience et réduire les risques liés à la cybercriminalité.



Dates clés à retenir

Mise en application obligatoire du règlement DORA pour le secteur financier. Voici les détails de la timeline :



Cette chronologie illustre les jalons importants de l'évolution réglementaire européenne en matière de cybersécurité et de résilience numérique, couvrant les développements significatifs de deux législations clés : la Directive sur la sécurité des réseaux et des systèmes d'information (NIS) et DORA.

La réglementation DORA prévoit la création de normes techniques réglementaires afin d'assurer une cohérence dans la mise en œuvre des exigences énoncées. Ces Normes Techniques Réglementaires (RTS) détaillent précisément la manière dont les dispositions de DORA doivent être appliquées dans la pratique. Avant leur finalisation, un processus de consultation publique est généralement engagé pour recueillir les avis et les retours d'expérience des parties prenantes.

Une fois adoptées, ces normes techniques garantissent une harmonisation des pratiques et renforcent la résilience du secteur financier européen face aux défis numériques. Les ESAs (Autorités européennes de surveillance) sont responsables du développement de ces normes techniques, qui peuvent couvrir divers aspects tels que la gestion des risques liés aux technologies de l'information et de la communication (TIC), la déclaration des incidents majeurs liés aux TIC, les tests, ainsi que les exigences clés pour une surveillance efficace des risques liés aux tiers en matière de TIC.

Les parties visées par le règlement DORA

Une grande majorité des institutions financières est concernée par la réglementation DORA. Celle-ci affecte ainsi les entités suivantes :

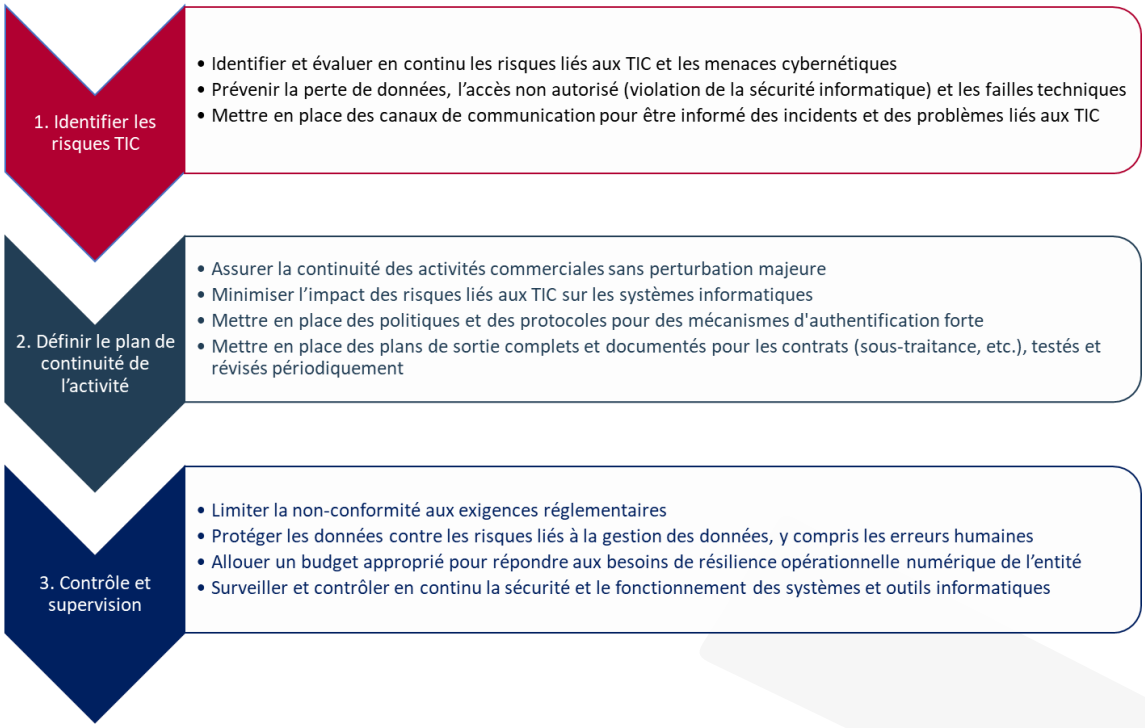
- Les plateformes de négociation
- Les entreprises d'assurance et de réassurance
- Les établissements de paiement
- Les dépositaires centraux
- Les référentiels centraux aux de titres
- Les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire
- Les établissements de monnaie électronique
- Les contreparties centrales
- Les gestionnaires de fonds d'investissement alternatifs et les sociétés de gestion
- Les agences de notation de crédit
- Les entreprises d'investissement
- Les contrôleurs légaux des comptes et les cabinets d'audit
- Les prestataires de services de communication de données
- Les établissements de crédit
- Les prestataires de services sur cryptoactifs
- Les entreprises d'investissement

Les exceptions :

Toutes les entreprises du secteur financier sont concernées par la réglementation DORA, mais les obligations de résilience doivent prendre en considération la taille des entreprises visées. Les structures qui ne sont pas concernées par l'application de DORA sont les suivantes :

- Les gestionnaires de fonds d'investissement alternatifs visés par la directive 2011/61/UE qui gèrent des portefeuilles dont les actifs ne dépassent pas certains seuils, soit 100 millions d'euros avec effet de levier, soit 500 millions d'euros sans effet de levier et sans droit au remboursement pendant cinq ans.
- Les micro-entreprises ayant moins de 10 employés et présentant un chiffre d'affaires annuel inférieur à 2 millions d'euros
- Les institutions de retraite professionnelle qui gère des régimes de retraite ne comptant pas plus de 15 affiliés au total,
- Les entreprises d'assurance et de réassurance visées à l'article 4 de la directive 2009/138/CE,
- Les offices de chèques postaux visés à l'article 2, paragraphe 5, point 3), de la directive 2013/36/UE

Les principaux objectifs du règlement DORA



Les 5 piliers de DORA

DORA repose sur cinq piliers essentiels pour renforcer la résilience opérationnelle numérique dans le secteur financier européen, détaillés ci-dessous.

- **La gestion des risques et la gouvernance des TIC**

DORA établit un cadre et des directives pour la gestion des risques liés à la cybersécurité, aux perturbations technologiques et opérationnelles dans le secteur financier, avec pour objectif d'aider les organisations à développer des programmes de gestion plus efficaces et à renforcer leur résilience opérationnelle. Les entités financières seront tenues de mettre en place un cadre de gestion lié aux technologies de l'information et de la communication (TIC) qui soutient une stratégie de continuité des activités, des plans de récupération et des stratégies de communication. Un canal de communication fiable avec les parties prenantes est essentiel, s'appuyant sur des directives existantes comme celles de l'ABE (Autorité Bancaire Européenne) sur la gestion des TIC et des risques de sécurité.

Les parties prenantes auront la responsabilité de garantir la continuité des activités en participant à diverses tâches, notamment la définition du niveau de tolérance aux risques et aux perturbations des TIC, l'élaboration et l'approbation des stratégies de continuité des activités, des plans de reprise après sinistre, ainsi que la spécification de contrôles de sécurité pour les actifs critiques. Les stratégies de réponse et de rétablissement nécessiteront la mise en place de mesures de secours dans les technologies de l'information et de la communication pour maintenir des opérations commerciales ininterrompues. Cela demandera aux parties prenantes d'investir dans des systèmes incluant des réseaux de sauvegarde et de restauration.

- **La réponse aux incidents et le reporting**

DORA améliore le processus de signalement des incidents liés aux technologies de l'information et de la communication (TIC). Elle exige la production de rapports et des réponses plus rapides aux incidents, réduisant ainsi leurs impacts et permettant la détection d'intrusions dans d'autres réseaux.

Cette réglementation s'attache à instaurer un système de signalement rationalisé au sein de l'Union européenne, supplantant les multiples autorités nationales compétentes (ANC). Ce principe est similaire aux pratiques de reporting des incidents dans la sûreté aérienne, où les données collectées permettent de comprendre les tendances et les failles potentielles, afin d'améliorer la sécurité globale. Dans le secteur financier de l'UE, un centre dédié centralisera les rapports sur les incidents majeurs liés aux technologies de l'information et de la communication. Cette démarche vise à identifier les vulnérabilités courantes et à renforcer la résilience ainsi que la sécurité des systèmes de TIC. Conformément aux nouvelles règles de l'UE, les institutions financières devront soumettre un rapport détaillant les causes d'un incident majeur dans le mois suivant sa survenue, nécessitant ainsi la mise en place d'indicateurs d'alerte précoce. Bien que les détails spécifiques de la loi sur la résilience opérationnelle numérique soient encore en cours de développement et demeurent inconnus, entamer une préparation anticipée dès à présent simplifiera la conformité une fois que la loi sera en vigueur.

- **Les tests de résilience**

Avant de procéder à des « tests de résilience opérationnelle numérique » sur les actifs numériques, qui englobent diverses formes d'actifs financiers ou non financiers présents sous forme numérique, il est essentiel de réaliser un inventaire de ces actifs et de les cartographier en les classant par niveaux de criticité et de risque.

Caractéristiques des tests de résilience opérationnelle numérique

L'ensemble des systèmes et applications TIC soutenant les fonctions centrales doit être soumis à une batterie de tests au moins une fois par an. Les tests peuvent être de différentes natures.

A titre d'illustration, des catégories de tests sont précisées par l'article 25 de la réglementation : des analyses comparatives, des tests de compatibilité, des tests de performance ou encore des tests de pénétration.

- **La gestion des risques liés aux tiers**

DORA vise à harmoniser les aspects essentiels des relations avec les fournisseurs de services, tout en exigeant des responsabilités accrues de la part des entités concernées. La réglementation exige d'elles une évaluation et une documentation plus rigoureuses des risques liés à leurs fournisseurs, en commençant par le risque de concentration, notamment pour ceux considérés comme critiques.

Il est recommandé de mettre en place une surveillance continue de la relation contractuelle. Cette approche proactive contribue à garantir que les risques associés à la sous-traitance ou aux partenariats tiers sont gérés de manière efficace et que les parties impliquées peuvent prendre des mesures appropriées en cas de besoin.

- **Le partage d'information**

DORA renforcera l'échange d'informations sur les menaces cybernétiques au sein de communautés financières de confiance. Des plateformes sécurisées permettront le partage d'alertes et d'analyses, complétées par des bulletins périodiques sur les nouvelles menaces et solutions. Des ateliers et séminaires favoriseront l'échange de meilleures pratiques et la formation sur les tendances actuelles. Des groupes de travail se concentreront sur des aspects spécifiques de la cybersécurité, et des systèmes d'alerte rapide ainsi que des audits partagés amélioreront la réactivité et la résilience opérationnelle. L'objectif est de sensibiliser aux menaces numériques et de discuter des tactiques pour renforcer la sécurité des données.

Les impacts du règlement DORA sur les institutions financières

DORA aura des répercussions significatives sur les institutions financières de l'Union européenne. Ces impacts peuvent être subdivisés en trois catégories.

Impact organisationnel :

La mise en œuvre de la directive DORA exige des investissements substantiels de la part des institutions financières pour développer des processus supplémentaires et répondre à ses exigences. Cette démarche se traduit par une augmentation des coûts de conformité, avec la nécessité de dispenser des formations obligatoires au personnel concerné. De plus, une organisation et une communication renforcées seront essentielles pour informer le personnel de la structure, ainsi que les parties prenantes et les médias.

Impact Technique :

Les pratiques techniques pourraient être adaptées pour se conformer aux nouvelles attentes de DORA, ce qui influencera la gestion des risques et la mise en œuvre de systèmes visant à renforcer la résilience opérationnelle, les rendant ainsi plus efficaces et fiables. La détection des risques (tels que le risque de la perte de données, la criticité des services internes touchés, la propagation d'un incident technique au niveau géographique, etc), la vulnérabilité du système seront des enjeux techniques clés que DORA devra couvrir afin de se préparer au mieux face aux perturbations opérationnelles. Les plans d'action visant à améliorer et sécuriser les systèmes informatiques et les données partagées dans les institutions financières seront régulièrement évalués et ajustés pour rester en conformité avec la réglementation DORA. Cette démarche comprend des audits continus, des tests de sécurité et la mise à jour des protocoles de réponse aux incidents, assurant ainsi une adaptation constante aux exigences techniques et aux menaces émergentes.

Impact Juridique :

La réglementation DORA demande aux entités une surveillance réglementaire accrue afin de renforcer le contrôle et l'évaluation de la résilience opérationnelle. Cette situation nécessite une surveillance juridique accrue pour assurer une conformité constante avec les nouvelles réglementations, ainsi que la mise en place de contrôles normatifs plus détaillés et réguliers. Les exigences imposées aux fournisseurs de services des institutions financières sont également renforcées par la réglementation DORA, nécessitant des accords contractuels détaillés qui documentent clairement les responsabilités et les attentes pour aligner ces relations externes avec les normes de sécurité et de résilience requises.

Les sanctions en cas de non-respect du règlement DORA

Sanctions administratives et mesures collectives :

Les autorités de surveillance (EBA, EIOPA, ESMA) sont dotées des pouvoirs complets de contrôle, d'enquête et de sanction nécessaires à l'exercice de leurs fonctions conformément au règlement. Elles ont notamment le droit de consulter les documents pertinents, de réaliser des inspections sur les lieux, de convoquer des représentants du secteur financier pour des explications, d'interroger des personnes consentantes, et d'imposer des mesures correctives en cas de violations du règlement.

En plus de la possibilité pour les États membres d'appliquer des sanctions pénales conformément à l'article 52, ces derniers sont tenus de mettre en œuvre des sanctions administratives et des mesures correctives, comme stipulé dans l'article 51, en cas de non-respect du règlement. Ces mesures doivent être efficaces, proportionnées et dissuasives pour garantir leur efficacité.

Les États membres autorisent les autorités compétentes à appliquer les sanctions administratives ou mesures correctives suivantes en cas de violation du règlement :

- Ordonner l'arrêt immédiat du comportement non conforme et interdire sa répétition.
- Exiger la cessation temporaire ou permanente de pratiques non conformes.
- Prendre des mesures financières pour garantir la conformité des entités financières.
- Demander les enregistrements de trafic de données, si nécessaire pour enquêter sur des violations.
- Publier des avis publics, incluant l'identité de la personne ou de l'entreprise en violation et la nature de la violation.

Sanctions pénales :

Les États membres ont le choix de ne pas instaurer de dispositions concernant les sanctions administratives ou les mesures correctives pour les infractions qui sont susceptibles de faire l'objet de sanctions pénales en vertu de leur législation nationale.

Lorsque les États membres ont choisi d'instaurer des sanctions pénales en cas de violation du règlement, ils doivent mettre en place des mécanismes permettant aux autorités compétentes de collaborer avec les autorités judiciaires chargées des poursuites pénales.

NEXIALOG CONSULTING

ACTUARIAT | **GESTION DES RISQUES** | **DATA** | **FINANCE DURABLE**

Nexialog Consulting est un cabinet de conseil spécialisé en Stratégie, Actuariat, Gestion des risques et Data qui dessert aujourd'hui les plus grands acteurs de la banque et de l'assurance. Nous aidons nos clients à améliorer de manière significative et durable leurs performances et à atteindre leurs objectifs les plus importants.

Les besoins de nos clients et les réglementations européennes et mondiales étant en perpétuelle évolution, nous recherchons continuellement de nouvelles et meilleures façons de les servir. Pour ce faire, nous recrutons nos consultants dans les meilleures écoles d'ingénieur et de commerce et nous investissons des ressources de notre entreprise chaque année dans la recherche, l'apprentissage et le renforcement des compétences.

Quel que soit le défi à relever, nous nous attachons à fournir des résultats pratiques et durables et à donner à nos clients les moyens de se développer.

CONTACTS

Retrouvez toutes nos publications sur Nexialog R&D

www.nexialog.com

ALI BEHBAHANI

Associé, Fondateur

+33 (0) 1 44 73 86 78

abehbahani@nexialog.com

ARESKI COUSIN

Directeur Scientifique

+33 (0) 7 88 03 51 87

acousin@nexialog.com

CHRISTELLE BONDOUX

Associée, Directrice Commerciale, Recrutement & Marketing

+33 (0) 1 44 73 75 67

cbondoux@nexialog.com

OTMAN IBNLKHAYAT

Manager, Contrôle, Finance, Risques

+33 (0) 6 99 25 13 36

oibnlkhayat@nexialog.com