silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Guide sur le Règlement DORA

Présentation complète

Mars 2025

DORA constitue une avancée réglementaire essentielle pour la **sécurisation du secteur financier face aux cybermenaces**. Sa mise en œuvre impose aux acteurs financiers un **renforcement substantiel de leurs pratiques en matière de gestion des risques TIC et de cybersécurité**. L'anticipation et la mise en conformité proactive seront des facteurs clés pour limiter les risques et assurer une transition fluide vers ce nouveau cadre réglementaire exigeant.

Table des matières

1 | Objectif 2
Nature de DORA 2
Objectif général 2
Résilience opérationnelle numérique 2
Objectifs spécifiques 2
Contexte et justification 2
2 | Champ d'application 3
Large éventail d'entités concernées 3
Exceptions possibles 3
Entités exclues du champ d'application 4
3 | Obligations clés 4
Cadre de gestion des risques liés aux TIC 4
Stratégie de résilience opérationnelle numérique 4
Politique de continuité des activités TIC 5
Procédures de sauvegarde et de restauration 6
Plans de communication en situation de crise 6
Gestion des incidents 6
Veille sur les cybermenaces 7
Tests de résilience opérationnelle numérique 7
Gestion des risques liés aux prestataires tiers 7
Gouvernance et organisation 7
Sécurité des réseaux et des systèmes d'information 8
4 | Sanctions et mise en conformité 8
Mise en conformité 8
5 | Impacts et enjeux de DORA 8
6 | Date d'entrée en vigueur et état d'application 9

1 | Objectif

Nature de DORA

Le **règlement DORA**, également appelé **loi sur la résilience opérationnelle numérique**, représente une initiative législative majeure de l'Union Européenne. Il est centré sur la **cybersécurité des entités financières**, telles que les banques et les entreprises d'assurance. DORA est un texte législatif majeur de l'Union européenne sur la cybersécurité des entités financières. En français, DORA répond au nom de Règlement sur la résilience opérationnelle du numérique.

Objectif général

DORA a pour but de consolider et d'améliorer les exigences relatives au **risque lié aux TIC** (technologies de l'information et de la communication) dans le cadre des exigences relatives au risque opérationnel. Son objectif principal est de renforcer la résilience opérationnelle numérique au sein du secteur financier de l'UE en établissant un cadre juridique commun.

- DORA vise à harmoniser le paysage juridique fragmenté de l'UE concernant les risques liés aux TIC.
- Le règlement DORA crée un cadre réglementaire sur la résilience opérationnelle numérique qui contraint toutes les entreprises à s'assurer de pouvoir résister à tous les types de perturbations et de menaces liées aux TIC, à y répondre et à s'en remettre.

Résilience opérationnelle numérique

DORA vise à garantir la capacité des entités financières à maintenir l'intégrité et la fiabilité de leurs opérations, même en cas de perturbations.

- La **résilience opérationnelle numérique** est définie comme la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations.
- L'objectif de DORA est d'atteindre un niveau élevé de résilience opérationnelle numérique pour toutes les entités financières réglementées.

Objectifs spécifiques

L'objectif est de rendre le secteur financier de l'Union plus résilient afin de garantir sa sûreté technologique et son bon fonctionnement, tout en préservant la confiance des consommateurs et des marchés.

- DORA met l'accent sur la disponibilité et l'intégrité des services financiers, même en cas de perturbations, d'incidents ou d'attaques.
- DORA cherche à limiter au maximum les perturbations et la durée d'indisponibilité des systèmes et des données.

Contexte et justification

Le corpus réglementaire unique, qui englobe l'ensemble de la législation de l'Union européenne relative aux établissements financiers, ne fait que survoler les risques opérationnels liés aux technologies de l'information et de la communication (TIC).

- Le cadre législatif actuel est incomplet ou harmonisé de manière incohérente, ce qui entrave le marché unique des services financiers.
- Le secteur financier de l'Union européenne est régi par un corpus réglementaire unique harmonisé, mais celui-ci traite à peine de la résilience opérationnelle numérique ou de la sécurité des TIC.

2 | Champ d'application

Large éventail d'entités concernées

DORA s'applique à **21 types d'entités financières**. Le règlement DORA couvre largement le secteur financier de l'UE.

- Les **établissements de crédit**.
- Les **sociétés de financement**.
- Les **entreprises d'investissement**.
- Les **établissements de paiement**, y compris les établissements de paiement exemptés en vertu de la directive (UE) 2015/2366.
- Les **prestataires de services sur crypto-actifs** agréés et les émetteurs de jetons se référant à un ou des actifs.
- Les **dépositaires centraux de titres**.
- Les **entreprises d'assurance** et de réassurance.
- Les **gestionnaires de fonds d'investissement alternatifs (AIFM)**.
- Les **prestataires tiers de services TIC**.
- Les **prestataires de services d'information sur les comptes**.
- Les **établissements de monnaie électronique**, y compris les établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE.
- Les **contreparties centrales**.
- Les **plateformes de négociation**.
- Les **référentiels centraux**.
- Les **sociétés de gestion**.
- Les **prestataires de services de communication de données**.
- Les **intermédiaires d'assurance**, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire.
- Les **institutions de retraite professionnelle**.
- Les **agences de notation de crédit**.
- Les **administrateurs d'indices de référence d'importance critique**.
- Les **prestataires de services de financement participatif**.
- Les **référentiels des titrisations**.

Exceptions possibles

Les États membres ont la possibilité d'exclure certaines entités nationales spécifiques du champ d'application de DORA.

Les États membres peuvent choisir d'exclure du scope de DORA certaines entités nationales de crédit ou d'investissement très spécifiques, telles que visées à l'Article 2(5) de la directive

2013/36/UE. En France par exemple, l'État pourrait choisir d'épargner la Caisse des dépôts et consignations.

Entités exclues du champ d'application

- **les gestionnaires de fonds d'investissement alternatifs** visés à l'Article 3(2) de la directive 2011/61/UE.
- **les entreprises d'assurance et de réassurance** en fonction de leur taille, telles que visées à l'Article 4 de la directive 2009/138/CE.
- **les institutions de retraite professionnelle** qui gèrent des régimes de retraite qui, ensemble, ne comptent pas plus de quinze affiliés au total.
- **les personnes physiques ou morales** exemptées en vertu des Articles 2 et 3 de la directive 2014/65/UE.
- **les intermédiaires d'assurance, intermédiaires de réassurance et intermédiaires d'assurance à titre accessoire** qui sont des micro-entreprises ou des PME. La définition est donnée dans l'article 4(60) de DORA : qui emploie moins de dix personnes et dont le CA annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros.
- **les offices des chèques postaux** visés à l'article 2(5.3), de la Directive 2013/36/UE.

3 | Obligations clés

Cadre de gestion des risques liés aux TIC

Les entités financières doivent mettre en place un **cadre de gestion du risque lié aux TIC (technologies de l'information et de la communication) solide, complet et bien documenté**.

Ce cadre doit faire partie intégrante de leur système global de gestion des risques.

Il doit inclure les **stratégies, politiques, procédures, protocoles et outils TIC nécessaires à la protection des actifs informationnels et des actifs TIC**.

Le cadre de gestion du risque lié aux TIC doit être documenté et réexaminé au moins une fois par an.

Le réexamen s'inscrit dans un processus d'amélioration permanente sur la base des enseignements tirés de la mise en œuvre et du suivi.

Le cadre de gestion du risque lié aux TIC doit être solide et documenté, détaillant les mécanismes et les mesures permettant une gestion rapide, efficace et complète du risque lié aux TIC, y compris en ce qui concerne la protection des composantes et infrastructures physiques pertinentes.

Les entités financières doivent mettre en place un processus de suivi formel, comprenant des règles pour la vérification et la correction en temps utile des constatations d'importance critique de l'audit des TIC.

Stratégie de résilience opérationnelle numérique

Les entités financières doivent définir une **stratégie de résilience opérationnelle numérique** qui précise les méthodes mises en place pour parer les risques et atteindre les objectifs de résilience.

Cette stratégie doit être améliorée en continu grâce aux enseignements tirés des examens obligatoires après un incident majeur, des difficultés rencontrées lors de l'activation des plans de continuité des activités, de la veille sur les cybermenaces et des tests de résilience opérationnelle.

Un compte-rendu doit être fait aux organes de direction de l'entité au moins une fois par an.

La stratégie de résilience opérationnelle numérique précise les méthodes pour parer au risque lié aux TIC et atteindre des objectifs spécifiques en matière de TIC.

Les entités financières contrôlent l'efficacité de la mise en œuvre de leur stratégie de résilience opérationnelle numérique.

La stratégie de résilience opérationnelle numérique précise les méthodes mises en place pour parer les risques et atteindre les objectifs de résilience.

Elle doit expliquer comment le cadre soutient la stratégie d'entreprise et les objectifs de l'entité financière.

Elle doit déterminer le niveau de tolérance au risque lié aux TIC.

Elle doit définir des objectifs clairs en matière de sécurité de l'information.

Elle doit décrire l'architecture des TIC de référence et les changements nécessaires pour atteindre des objectifs spécifiques de l'entité financière.

Elle doit présenter les différents mécanismes mis en place pour détecter et prévenir les incidents liés aux TIC, ainsi que pour se protéger contre leurs effets.

Elle doit présenter la situation actuelle en matière de résilience opérationnelle numérique sur la base du nombre d'incidents majeurs liés aux TIC signalés et de l'efficacité des mesures de prévention.

Elle doit mettre en œuvre des tests de résilience opérationnelle numérique.

Elle doit définir une stratégie de communication en cas d'incidents liés aux TIC qui doivent être divulgués.

Politique de continuité des activités TIC

Les entités financières doivent établir une **politique de continuité des activités TIC complète**, qui doit être testée au moins une fois par an.

Les entités doivent tenir un registre des activités en cas de perturbations.

La politique de continuité des activités de TIC doit permettre de garantir la continuité des fonctions critiques ou importantes de l'entité financière et de répondre aux incidents et les résoudre rapidement.

Les entités financières mettent en œuvre la politique de continuité des activités de TIC au moyen de dispositifs, de plans, de procédures et de mécanismes spécifiques, appropriés et documentés.

Dans le cadre de la politique globale de continuité des activités, les entités financières procèdent à une analyse des incidences sur les activités de leurs expositions à de graves perturbations de leurs activités.

Les entités financières mettent en place, maintiennent et testent périodiquement des plans de continuité des activités de TIC appropriés, notamment en ce qui concerne les fonctions

critiques ou importantes externalisées ou sous-traitées dans le cadre d'accords avec des prestataires tiers de services TIC.

Les entités financières doivent tester les plans de continuité des activités de TIC et les plans de réponse et de rétablissement des TIC concernant les systèmes de TIC soutenant toutes les fonctions au moins une fois par an ainsi qu'en cas de modifications substantielles apportées aux systèmes de TIC qui soutiennent des fonctions critiques ou importantes.

Procédures de sauvegarde et de restauration

Les entités financières doivent prévoir des **procédures de sauvegarde, de restauration et de rétablissement des données et des systèmes**, ainsi que les politiques associées.

Les entités financières définissent et documentent des politiques et procédures de sauvegarde qui précisent la portée des données concernées par la sauvegarde et la fréquence minimale de celle-ci, en fonction de la criticité des informations ou du niveau de confidentialité des données.

Plans de communication en situation de crise

Les entités financières doivent préparer des **plans de communication en situation de crise** pour informer les clients, les contreparties et le public en cas d'incidents majeurs liés aux TIC ou de vulnérabilités majeures.

Elles doivent désigner un responsable des communications de crise.

En cas de cybermenace importante, les entités financières informent, le cas échéant, leurs clients susceptibles d'être affectés de toute mesure de protection appropriée que ces derniers pourraient envisager de prendre.

Les entités financières mettent en place des plans de communication en situation de crise qui favorisent une divulgation responsable, au minimum, des incidents majeurs liés aux TIC ou des vulnérabilités majeures aux clients et aux contreparties ainsi qu'au public, le cas échéant.

Les entités financières mettent en œuvre des politiques de communication à l'intention des membres du personnel interne et des parties prenantes externes.

Gestion des incidents

Les entités financières doivent mettre en œuvre un **processus de gestion des incidents** pour enregistrer toutes les cybermenaces importantes et tous les incidents, et classer les incidents selon des critères définis.

Ce processus doit permettre d'enregistrer toutes les cybermenaces importantes et tous les incidents.

Le processus de gestion des incidents doit mettre en place des indicateurs d'alerte précoce et instaurer des procédures destinées à identifier, suivre, consigner, catégoriser et classer les incidents en fonction de leur priorité et de leur gravité, et en fonction de la criticité des services touchés.

Il doit attribuer les rôles et les responsabilités qui doivent être activés pour différents types et scénarios d'incidents et établir des plans pour la communication à l'intention du personnel, des parties prenantes externes et des médias.

Il doit permettre de notifier au minimum les incidents majeurs aux membres de la direction concernés, et de communiquer leurs incidences, la réponse à leur apporter et les contrôles

supplémentaires à mettre en place par la suite et définir des procédures de réponse en cas d'incident, afin d'en atténuer les effets et de garantir que les services redeviennent opérationnels et sécurisés en temps utile.

Les entités financières mettent en place des procédures et des processus adéquats pour assurer une surveillance, un traitement et un suivi cohérents et intégrés des incidents liés aux TIC, pour veiller à ce que les causes originelles soient identifiées et documentées et qu'il y soit remédié pour éviter que de tels incidents ne se produisent.

Veille sur les cybermenaces

Les entités financières doivent opérer une **veille sur les cybermenaces** et se doter de capacités pour recueillir des informations sur les vulnérabilités.

La veille doit être assidue, collective et continue.

Les entités financières disposent de capacités et d'effectifs pour recueillir des informations sur les vulnérabilités et les cybermenaces, et sur les incidents liés aux TIC, en particulier les cyberattaques, et analyser leurs incidences probables sur leur résilience opérationnelle numérique.

Tests de résilience opérationnelle numérique

Les entités financières doivent établir un **programme de tests de la résilience opérationnelle numérique** permettant d'évaluer l'état de préparation à la gestion d'incidents liés aux TIC et d'identifier les faiblesses, les déficiences et les lacunes de la résilience opérationnelle numérique.

Gestion des risques liés aux prestataires tiers

Les entités financières doivent adopter une **stratégie en matière de risques liés aux prestataires tiers de services TIC** et la réexaminer régulièrement.

Cette stratégie doit inclure une politique relative à l'utilisation des services qui soutiennent des fonctions critiques ou importantes.

L'organe de direction doit examiner régulièrement les risques identifiés pour ces mêmes services et accords contractuels.

Les entités financières devraient adopter une approche proportionnée du suivi des risques survenant au niveau des prestataires tiers de services TIC en tenant dûment compte de la nature, de l'ampleur, de la complexité et de l'importance de leurs relations de dépendance liées aux TIC.

Les entités financières devraient être tenues de disposer d'un registre d'informations contenant tous les accords contractuels relatifs à l'utilisation des services TIC fournis par des prestataires tiers de services TIC.

Gouvernance et organisation

Les entités financières doivent disposer d'un **cadre de gouvernance et de contrôle interne** qui garantit une gestion efficace et prudente du risque lié aux TIC.

L'organe de direction de l'entité financière définit, approuve, supervise et est responsable de la mise en œuvre de toutes les dispositions relatives au cadre de gestion du risque lié aux TIC.

Les membres de l'organe de direction de l'entité financière maintiennent activement à jour des connaissances et des compétences suffisantes pour comprendre et évaluer le risque lié aux TIC et son incidence sur les opérations de l'entité financière.

Sécurité des réseaux et des systèmes d'information

Les entités financières doivent élaborer, documenter, mettre en œuvre et tenir à disposition du superviseur les politiques de sécurité des TIC, la sécurité de l'information et les procédures, protocoles et outils y afférents qui garantissent la sécurité des réseaux et comportent des garanties contre les intrusions et les utilisations abusives des données.

4 | Sanctions et mise en conformité

DORA laisse aux États membres et à leurs autorités compétentes le soin de déterminer les sanctions applicables.

Les autorités compétentes peuvent adopter toute mesure, y compris pécuniaire, pour assurer le respect des obligations légales par les entités financières.

Les États membres doivent s'assurer que les autorités compétentes ont le pouvoir d'imposer des sanctions administratives et des mesures correctives en cas de violation du règlement DORA. Ces sanctions doivent être efficaces, proportionnées et dissuasives.

Les autorités compétentes doivent disposer de tous les pouvoirs de surveillance, d'enquête et de sanction nécessaires à l'exécution de leurs tâches en vertu du règlement.

Les autorités compétentes devraient inclure la tâche consistant à vérifier le respect matériel des recommandations formulées par le superviseur principal dans le cadre de leurs fonctions en ce qui concerne la surveillance prudentielle des entités financières.

Mise en conformité

La mise en conformité avec DORA demandera des ressources, du temps et de la rigueur. Il est conseillé de commencer par la rédaction et la mise en œuvre des politiques obligatoires.

DORA fonctionne comme un système de politiques imbriquées, et une approche méthodique est à privilégier.

Le cadre de gestion du risque lié aux TIC doit s'accompagner d'une stratégie de résilience opérationnelle, d'une politique de continuité des activités TIC, de procédures de sauvegarde, de restauration et de rétablissement, d'un registre des activités en cas de perturbations, d'un processus de gestion des incidents, d'un plan de réponse aux incidents et de plans de communication en situation de crise.

Les entités financières sont tenues de mettre en œuvre un cadre formel de gouvernance et de gestion des risques liés aux TIC.

5 | Impacts et enjeux de DORA

Changement de paradigme : DORA représente une transformation significative dans la gestion des risques numériques pour le secteur financier.

Renforcement de la sécurité et de la stabilité financière : Le règlement vise à améliorer la sécurité et la stabilité financière en réponse aux cyberattaques.

Uniformisation des normes de cybersécurité : DORA harmonise les standards de cybersécurité à l'échelle de l'UE, créant un cadre juridique commun.

Contrôle accru des prestataires TIC : Le règlement renforce le contrôle des prestataires de services TIC (technologies de l'information et de la communication) et réduit les risques de concentration.

Nécessité d'investissements technologiques : Les entités financières doivent accroître leurs investissements technologiques pour se conformer aux exigences de DORA.

Maîtrise du risque lié aux TIC : Afin de conserver la maîtrise totale du risque lié aux TIC, les entités financières doivent disposer de capacités globales permettant une gestion solide et efficace du risque lié aux TIC, ainsi que de mécanismes et de politiques spécifiques pour le traitement de tous les incidents liés aux TIC et pour la notification des incidents majeurs liés aux TIC.

Harmonisation des exigences clés : Il est nécessaire de procéder à une harmonisation plus poussée des exigences clés en matière de résilience opérationnelle numérique pour toutes les entités financières.

Gestion des risques liés aux TIC : Les entités financières soumises à DORA sont tenues de mettre en œuvre un cadre formel de gouvernance et de gestion des risques liés aux TIC.

Stratégie de résilience opérationnelle numérique : Les entités financières doivent fournir des informations sur leur stratégie de résilience opérationnelle numérique et sur l'organisation de leur cadre de gestion des risques associés aux TIC.

6 | Date d'entrée en vigueur et état d'application

- **Entrée en vigueur** : DORA est entré en application le 17 janvier 2025.
- **Obligation de conformité** : Les entités financières doivent être conformes à DORA à partir de cette date.
- **Supervision** : L'ACPR (Autorité de contrôle prudentiel et de résolution) et les autorités européennes de surveillance (EBA, ESMA, EIOPA) supervisent l'application du règlement.
- **Première année d'entrée en vigueur** : Le rapport établi au titre de la première année d'entrée en vigueur du cadre réglementaire DORA (2025) décrit les éléments du cadre de gestion des risques liés aux TIC et souligne les sujets encore en développement ou qui restent à approfondir.
- **Adresse de contact** : À partir du 17 janvier 2025, les entités financières devront s'adresser à leur service de contrôle habituel.