AUTORITÉ DES MARCHÉS FINANCIERS

Le règlement sur la résilience opérationnelle numérique dans le secteur financier (DORA)

26 février 2025

Le règlement européen sur la résilience opérationnelle numérique du secteur financier (DORA) établit un cadre commun pour la gestion des risques liés aux technologies de l'information et de la communication (TIC). Il définit des règles en matière de cyber-sécurité et de gestion des risques informatiques qui s'appliquent à un grand nombre d'entités financières.

Qu'est-ce que le règlement DORA ?

Issu d'une série de mesures relatives à la finance numérique en Europe (Digital finance package), le règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier (Digital Operational Resilience Act, « DORA ») établit des règles en matière de cyber-sécurité et de gestion des risques informatiques, dont le risque d'origine cyber, pour un grand nombre d'entités financières.

Le règlement comprend notamment des dispositions imposant aux entités financières :

- la mise en œuvre d'un cadre de gestion du risque lié aux TIC dont le risque cyber fait partie ;
- la notification des incidents majeurs liés aux TIC aux autorités compétentes ;
- la réalisation de tests de résilience opérationnelle numérique ;

- la gestion du risque lié au recours à des prestataires tiers de services TIC, incluant notamment de nouvelles exigences au niveau contractuel ainsi que la tenue d'un registre d'information des accords contractuels conclus avec ces prestataires ;

- le partage volontaire des informations opérationnelles relatives aux menaces d'origine cyber et vulnérabilités entre acteurs du secteur financier.

Le règlement impose également un cadre de supervision au niveau européen pour les prestataires tiers de services TIC considérés comme « critiques », c'est-à-dire susceptibles d'avoir un impact systémique sur la stabilité, la continuité ou la qualité de la fourniture de services financiers dans l'Union Européenne.

Qui est concerné par le règlement DORA ?

Le règlement DORA impose un cadre de résilience numérique dont le périmètre inclut la majorité des institutions financières. Les entités assujetties sont listées à l'article 2(1) du règlement, incluant -notamment les sociétés de gestion de portefeuille, les infrastructures de marché, les entreprises d'investissement (telles que définies par l'article 4(1)(1) de la Directive MIF 2) ou les prestataires de services sur crypto-actifs.

Par ailleurs, un nouveau cadre de supervision européen s'applique aux prestataires tiers de services TIC considérés comme critiques, qui seront désignés par les trois autorités européennes de supervision (ESMA, EBA et EIOPA) en 2025 selon des critères exposés dans le règlement et dans un acte délégué de la Commission européenne sur la base du registre d'informations reporté par les entités financières.

Il est à noter que le règlement introduit un principe de proportionnalité au regard duquel certaines entités financières de petite taille, ainsi que les entités désignées sous le terme de « microentreprises », (définies à l'article 3 (60) de DORA) pourront bénéficier de régimes simplifiés ou allégés. Ainsi, en application de ce principe, DORA prévoit un cadre simplifié de gestion des risques liés aux TIC pour les microentreprises et les entités financières de plus petite taille fournissant certains services.

Certaines entités sont exclues du périmètre d'application à l'article 2(3) du règlement, incluant notamment :

- les gestionnaires de fonds d'investissement alternatifs qui gèrent, directement ou indirectement, par l'intermédiaire d'une société avec laquelle ils sont liés dans le cadre d'une communauté de gestion ou de contrôle, ou par une importante participation

directe ou indirecte, des portefeuilles de FIA dont les actifs gérés ne dépassent pas le plafond AIFMD ;

- les personnes physiques ou morales exemptées en vertu des articles 2 et 3 de la Directive MIF 2.

Calendrier d'application du règlement DORA

Le règlement DORA sera applicable à partir du 17 janvier 2025.

Quelles sont les principales mesures du règlement DORA ?

Gestion du risque lié aux TIC

Le règlement prévoit un cadre harmonisé de gestion du risque lié aux TIC que les entités financières doivent intégrer pour parer au risque lié aux TIC de manière rapide, efficiente et exhaustive, et garantir un niveau élevé de résilience opérationnelle numérique.

Ces mesures à mettre en place par les entités concernées comprennent notamment :

- la mise en place d'un cadre de gouvernance et de contrôle interne, ainsi qu'une stratégie de résilience opérationnelle numérique. Ce cadre de gestion des risques doit par exemple comprendre des systèmes, protocoles et outils de TIC qui doivent être tenus à jour ;
- l'identification de toutes les sources de risques liés aux TIC et l'évaluation de ces risques selon une classification devant être revue à minima une fois par an ; l'élaboration d'une politique de sécurité de l'information qui définit des règles visant
- à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données selon une approche fondée sur les risques ;
- l'instauration d'une politique complète de continuité des activités de TIC, ainsi que des procédures de sauvegarde, de restauration et de rétablissement. Cette politique comprend par exemple des tests à effectuer au moins une fois par an ;
- la mise en place des mécanismes d'examens à la suite d'incidents liés aux TIC, pour déterminer les améliorations à apporter et voir si les procédures établies ont été suivies et efficaces, avec des programmes de formations à destination du personnel ;
- l'instauration de plans de communication interne et externe en cas de crise.

Notification des incidents majeurs aux autorités compétentes

Les entités financières sont tenues de classifier les incidents liés aux TIC ainsi que les cyber-menaces sur la base de plusieurs critères, comprenant par exemple la criticité des services concernés ou le nombre et l'importance des clients impactés ou potentiellement impactés par ces évènements.

Sur la base de cette classification, les entités financières doivent déclarer les incidents considérés comme majeurs à leur autorité sectorielle compétente. Cette déclaration aux autorités consiste en une notification initiale, un rapport intermédiaire et un rapport final.

Les entités financières sont tenues d'informer rapidement leurs clients des incidents majeurs liés aux TIC lorsque cela a une incidence sur les intérêts financiers de ces clients. Dans le cas d'une cyber-menace, les entités financières communiquent à leurs clients, susceptibles d'être affectés, les potentielles mesures de protection que ceux-ci pourraient adopter pour réduire ces risques.

Première étape : La classification des incidents

Les entités financières doivent procéder à la classification de leurs incidents TIC selon les critères fixés par DORA. Les critères permettant de classifier les incidents TIC sont indiqués dans un règlement délégué URL = [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401772] dédié. Un incident est considéré majeur si les conditions suivantes sont remplies :

1 • l'incident
   - **a** • touche ou a touché des services TIC ou des réseaux et des systèmes d'information qui soutiennent des fonctions critiques ou importantes de l'entité financière ;
   - **b** • touche ou a touché des services financiers fournis par l'entité financière qui nécessitent un agrément ou un enregistrement ou qui sont surveillés par les autorités compétentes ou ;
   - **c** • constitue ou a constitué un accès réussi, malveillant et non autorisé aux réseaux et aux systèmes d'information de l'entité financière.

2 • Et lorsque l'une des conditions suivantes (a ou b) est remplie :
   - **a** • les réseaux et les systèmes d'information sont l'objet d'un accès réussi, malveillant et non autorisé et susceptible d'entraîner des pertes de données ;
   - **b** • au moins 2 seuils d'importance significative ci-dessous sont atteints, parmi les suivants :

- **le seuil « clients, contreparties financières et transactions »**, qui est atteint lorsque l'une des conditions suivantes est remplie :
  - le nombre des clients touchés dépasse 10 % de l'ensemble des clients qui utilisent le service touché,
  - le nombre des clients touchés qui utilisent le service touché dépasse 100 000,
  - le nombre des contreparties financières touchées dépasse 30 % de l'ensemble des contreparties financières qui exercent des activités liées à la fourniture du service touché,
  - le nombre des transactions touchées dépasse 10 % du nombre moyen journalier des transactions effectuées par l'entité financière liées au service touché,
  - la valeur moyenne des transactions touchées dépasse 10 % de la valeur moyenne journalière des transactions effectuées par l'entité financière liées au service touché,
  - des clients ou des contreparties financières considérés comme importants ont été touchés ;
- **le seuil « atteinte à la réputation »**, qui est atteint lorsque l'une des conditions suivantes est remplie :
  - l'incident a été relayé par les médias,
  - l'incident a donné lieu à des plaintes répétées de la part de différents clients ou contreparties financières concernant des services en contact direct avec la clientèle ou des relations commerciales critiques,
  - l'entité financière ne pourra pas satisfaire à certaines exigences réglementaires, ou il est probable qu'elle ne le pourra pas, en raison de l'incident,
  - l'entité financière perdra, ou il est probable qu'elle perdra, des clients ou des contreparties financières en raison de l'incident, au grand détriment de son activité ;
- **le seuil « durée et interruptions de service »**, qui est atteint lorsque l'une des conditions suivantes est remplie :
  - la durée de l'incident dépasse 24 heures,
  - l'interruption de service dépasse 2 heures pour les services TIC qui soutiennent des fonctions critiques ou importantes ;

- **le seuil « répartition géographique »**, qui est atteint lorsque l'incident a une incidence dans deux Etats membres de l'Union européenne ou plus,

- **le seuil « pertes de données »**, qui est atteint lorsque l'une des conditions suivantes est remplie :
  - l'incidence sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données, nuit ou nuira à la mise en œuvre des objectifs opérationnels de l'entité financière ou à sa capacité de satisfaire aux exigences réglementaires,

  - les réseaux et les systèmes d'information sont l'objet d'un accès réussi, malveillant et non autorisé non couvert par le point précédent et susceptible d'entraîner des pertes de données ;

- **le seuil « conséquences économiques »**, qui est atteint lorsque les coûts et les pertes supportés par l'entité financière en raison de l'incident ont dépassé, ou sont susceptibles de dépasser, 100 000 EUR.

Enfin, des dispositions prévoient également que des incidents récurrents qui, pris isolément, ne seraient pas considérés comme un incident majeur, puissent être qualifiés d'incidents majeurs lorsqu'ils remplissent certaines conditions.

Seconde étape : La notification d'incident majeur

Lorsqu'un incident est classé comme majeur par une entité financière, celle-ci doit notifier l'incident à l'autorité compétente dans les conditions suivantes :

1. notification initiale : l'entité financière réalise une notification initiale dans les 4 heures qui suivent la classification de l'incident comme majeur et pas plus tard que 24 heures après sa détection. Elle précise notamment la ou les entités concernées par l'incident, ainsi qu'une description de l'incident, les conditions de sa découverte et les critères qui ont conduit à la classification comme incident majeur ;
2. rapport intermédiaire : dans les 72 heures après la notification initiale, l'entité financière envoie un rapport intermédiaire. Ce rapport précise notamment le détail des impacts (financiers, en termes d'indisponibilité du service, réputationnels, etc.), les services impactés, les mesures temporaires de résolution de l'incident ;
3. rapport final : sous un mois, l'entité financière communique un rapport final détaillant notamment l'analyse des causes à l'origine de l'incident et le plan d'action pour remédier à ces causes.

Le format de la notification initiale et des rapports intermédiaires et finaux est précisé dans une norme technique d'exécution dédiée (ITS).

Les entités financières devant notifier leurs incidents à l'AMF devront utiliser un modèle de notification et transmettre les informations via la messagerie sécurisée de l'AMF (Sesterce). Ce modèle sera mis à disposition sur la page Formulaire et déclaration URL = [https://www.amf-france.org/fr/formulaires-et-declarations-1] du site de l'AMF.

Les cyber-menaces importantes, qui sont des risques potentiels pour les entités financières et non des incidents avérés en tant que tels, doivent être enregistrées par les entités financières. Les critères permettant de déterminer l'importance d'une cyber-menace sont précisés dans le règlement délégué URL = [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401772] dédié à l'article 10. Les entités financières sont invitées à notifier ces cyber-menaces importantes à leur autorité compétente, sur une base volontaire.

L'AMF recommande fortement aux entités financières de notifier ces cyber-menaces.

Le modèle de notification de ces cyber-menaces est précisé dans une norme technique d'exécution (ITS) dédiée et sera également mis à disposition des déclarants dans l'espace Formulaire et déclaration. URL = [https://www.amf-france.org/fr/formulaires-et-declarations-1]

Les tests de résilience opérationnelle numérique

Afin de gérer correctement leurs risques liés aux TIC, les entités financières sont tenues de mettre en place un programme de tests de résilience opérationnelle numérique et de réexaminer ce programme. Ces tests doivent être effectués par des parties indépendantes, internes ou externes, et comprendre notamment :

- des analyses de vulnérabilité ;
- des évaluations de la sécurité des réseaux ;
- des examens de la sécurité physique ;
- des tests visant à simuler une crise de bout en bout ;
- des tests cyber de pénétration fondés sur la menace.

Elles réalisent également des tests sur les systèmes et applications de TIC soutenant des fonctions critiques au moins une fois par an.

A la suite de ces tests, ces entités financières veillent à définir des stratégies permettant de résoudre les faiblesses mises en évidence pendant cette phase de test.

Certaines entités financières importantes notamment sur la base de leur caractère systémique ou de leur profil de risque lié au TIC, devront également mettre en place des tests plus avancés au moyen de tests de pénétration « fondés sur la menace » au moins tous les trois ans. Les critères de désignation des entités soumises à ces tests avancés sont plus amplement précisés dans une norme technique de réglementation (RTS) dédiée.

Ce test avancé doit couvrir a minima plusieurs fonctions critiques ou importantes de l'entité financière. A l'issue de ces tests, les entités financières assujetties fournissent à l'autorité compétente une synthèse des conclusions des tests ainsi que les mesures correctives envisagées.

La gestion des risques liés aux prestataires tiers de services TIC et le registre d'information

Le règlement DORA définit des principes clés de gestion du risque lié au recours à des prestataires tiers de services TIC. Les entités financières doivent identifier et intégrer les risques liés au recours à ces prestataires dans leur cadre de gestion des risques, et demeurent pleinement responsables du respect des obligations du règlement DORA lorsqu'elles ont recours à ces tiers.

Le règlement DORA prévoit un certain nombre d'obligations pour les entités financières découlant de leurs relations avec des prestataires tiers de services TIC, comprenant notamment :

- la définition et l'application d'un cadre de gestion du risque lié aux prestataires tiers, comprenant notamment la signature de contrats comprenant certaines clauses minimales précisées à l'article 30 du règlement DORA ;
- la tenue d'un registre d'information actualisé (RoI) des accords contractuels conclus avec ces prestataires, qui doit être communiqué à l'autorité compétente au moins une fois par an ;
- la notification à l'autorité compétente, au moins une fois par an, des nouveaux accords contractuels relatifs à l'utilisation de services TIC. Les projets d'accords portant sur des services TIC soutenant des fonctions critiques doivent également être communiqués ;
- la réalisation d'audits avant de conclure un accord, et ne conclure des accords qu'avec des prestataires tiers de services TIC respectant des normes adéquates en matière de sécurité

de l'information ;

- le fait d'être attentif à ce qu'un contrat puisse être résilié dans certaines circonstances, notamment lorsque le prestataire tiers présente certaines carences en matière de gestion des risques liés aux TIC ;
- la mise en place de stratégies de sortie pour les services TIC soutenant des fonctions critiques ou importantes, en cas de défaillance du prestataire.

Le registre d'information en pratique

Le registre d'information, contenant la liste des prestataires tiers de services TIC et de leurs sous-traitants, devra être communiqué par l'entité financière à son autorité compétente au moins une fois par an, à date fixe.

Les modèles types pour le registre d'information sont précisés dans cette norme technique d'exécution dédiée URL = [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202402956] (ITS).

Les registres devront être soumis à l'AMF via l'interface ROSA selon le format et la structure requises par les autorités européennes de supervision, disponible ici URL = [https://www.eba.europa.eu/risk-and-data-analysis/reporting-frameworks/reporting-framework-35].

Le calendrier de soumission des registres à l'AMF (incluant une période de tests d'envoi des registres) et une procédure détaillée de soumission via ROSA seront mis à disposition au début 2025.

Le règlement DORA met également en place un nouveau système de supervision au niveau européen des prestataires tiers dits « critiques » de services TIC. Ces prestataires feront l'objet d'une supervision particulière sous la coordination d'une des ESA, afin de vérifier qu'ils ont mis en place des règles suffisantes afin de gérer le risque lié au TIC.

Concernant le recours à des prestataires critiques établis dans des pays tiers, le règlement DORA précise que les entités financières ne peuvent utiliser des services TIC de prestataires tiers désignés comme critiques établis dans des pays tiers qu'à la condition qu'ils aient établi

une filiale dans l'Union européenne. Si la filiale européenne n'existe pas, le prestataire tiers critique a un an pour établir sa filiale dans l'Union une fois désigné.

Les textes d'application

Le règlement DORA prévoit l'adoption d'un certain nombre de textes d'application (normes techniques de réglementation (RTS) et d'exécution (ITS)) élaborés par les trois autorités européennes de supervision (EBA, EIOPA, ESMA).

Ces normes techniques permettent d'harmoniser les exigences de sécurité informatique et la gestion du risque lié aux TIC à l'échelle de l'Union Européenne. Elles apportent également des précisions aux entités financières quant à leur mise en conformité avec les obligations de DORA.

Les textes d'application pertinents pour les entités financières sont détaillés dans le tableau suivant, comprenant les différents liens vers les textes d'application publiés au Journal Officiel de l'Union européenne (à la date du 26 février 2025) :

Gestion du risque lié aux TIC (Chapitre II de DORA)	— RTS sur la mise en place d'un cadre de gestion des risques TIC et d'un cadre de gestion simplifié des risques TIC ; — Orientations sur les coûts et les pertes agrégés résultant d'incidents majeurs.
Gestion, classification et notification des incidents liés aux TIC (Chapitre III de DORA)	— RTS sur les critères de classification des incidents liés aux TIC ; — RTS et ITS sur le contenu, les délais et les modèles de rapports d'incidents ou de cyber-menaces.
Tests de résilience opérationnelle numérique (Chapitre IV de DORA)	— RTS sur les tests de pénétration fondés sur la menace.
Gestion des risques liés aux prestataires tiers de services TIC (Chapitre V de DORA)	— ITS sur les modèles de registre d'information ; — RTS visant à préciser la politique relative aux services TIC fournis par des prestataires tiers ; — RTS sur la sous-traitance de fonctions critiques ou importantes.

Les versions finales de ces différents textes sont répertoriées sur la page dédiée URL = [https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en?

etrans=fr&prefLang=fr] du site de la Commission européenne.

En savoir plus

- Règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (dit « DORA »)
- Directive (UE) 2022/2556 du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier
- Lien vers le site de la Commission européenne recensant les différents textes de niveau 2 et 3
- Lien vers le site de l'ESMA recensant les différents travaux sur les textes de niveau 2 et 3

Mentions légales :
Responsable de la publication : Le Directeur de la Direction de la communication de l'AMF. Contact : Direction de la communication, Autorité des marchés financiers - 17, place de la Bourse - 75082 Paris Cedex 02