SEPTEMBRE 2026

Rapport sur les incidents majeurs DORA déclarés à l'AMF en 2025

AUTORITÉ DES MARCHÉS FINANCIERS

AUTORITÉ DES MARCHÉS FINANCIERS

INTRODUCTION

Le règlement (EU) 2022/2554 dit « DORA » (*Digital Operational Resilience Act*) sur la résilience opérationnelle numérique dans le secteur financier a été publié au Journal Officiel de l'Union Européenne le 27 décembre 2022. Faisant partie de la série de mesures relatives à la finance numérique en Europe (« *Digital finance package* ») publiée par la Commission le 24 septembre 2020, **ce règlement est entré en pleine application le 17 janvier 2025**.

Le renforcement de la résilience opérationnelle des entités financières a pour objectif de limiter les risques systémiques financiers avec la mise en place d'une supervision des risques cyber au niveau des autorités compétentes nationales et européennes.

Visant à harmoniser à l'échelle de l'Union européenne les dispositions relatives à la cybersécurité dans le secteur financier, **le périmètre du règlement DORA inclut la majorité des entités financières** selon un principe de proportionnalité. Par ailleurs, le règlement DORA définit des principes clés de gestion du risque lié au recours à des prestataires tiers **fournissant des services liés aux technologies de l'information et de la communication (TIC)**.

Il comprend des dispositions[1] imposant aux entités financières :

- d'appliquer un cadre de **gestion du risque lié aux TIC dont le risque d'origine cyber** fait partie ;
- de **notifier les incidents** majeurs liés aux TIC aux autorités compétentes ;
- d'effectuer des **tests de résilience opérationnelle** numérique ;
- de gérer le risque lié au **recours à des prestataires tiers de services TIC**, incluant notamment de nouvelles exigences au niveau contractuel ;
- de **partager des informations opérationnelles** relatives aux menaces d'origine cyber et vulnérabilités entre **acteurs du secteur financier**.

Il impose également **un cadre de supervision pour les prestataires tiers de services TIC considérés comme « critiques »** (incluant par exemple des fournisseurs de services informatiques en nuage), susceptibles d'avoir un impact systémique sur la stabilité, la continuité ou la qualité de la fourniture de services financiers.

Comme évoqué précédemment, le règlement DORA établit un cadre relatif aux déclarations des incidents majeurs liés aux TIC. Par ailleurs, l'article 19 précise que les entités financières peuvent notifier, à titre volontaire, les cybermenaces importantes à l'autorité compétente concernée lorsqu'elles estiment que la menace est pertinente pour le système financier, les utilisateurs de services ou les clients.

S'agissant des obligations de déclaration des incidents majeurs liés aux TIC, les entités rencontrant un incident cyber doivent transmettre les éléments suivants à leur autorité compétente :

- **une notification initiale** : l'entité financière réalise une notification initiale dans les 4 heures qui suivent la classification de l'incident comme majeur et au plus tard 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 ;
- **un 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 ;

[1] Plus de détails figurent dans le dossier thématique publié par l'AMF : https://www.amf-france.org/fr/actualites-publications/actualites/dora-lamf-publie-un-dossier-thematique-dedie-la-mise-en-oeuvre-du-reglement

- **un 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.

L'AMF est l'autorité compétente pour la réception de ces notifications d'incident pour les sociétés de gestion de portefeuille (SGP)[2], les prestataires de services en financement participatif (PSFP), les entreprises de marché et les prestataires de services sur crypto actifs (PSCA).

1. L'ETAT DES LIEUX DES INCIDENTS MAJEURS EN 2025

1.1. LES CHIFFRES CLES

Au cours de l'année 2025, les SGP ont notifié 47 déclarations initiales d'incident majeur aux services de l'AMF. Après échanges avec les acteurs, **31 incidents ont été confirmés majeurs** et déclinés de la manière suivante :

- **27 incidents (87%) sont issus des prestataires des SGP, que ce soit l'indisponibilité de leurs services ou une cyberattaque dont ils ont fait l'objet.** Lors d'une compromission d'un prestataire, plusieurs SGP sont concernées par ruissellement, ce qui en fait une cible privilégiée des attaquants ;
- **22 incidents (71%) issus de cyberattaques** dont 15 (48%) ayant conduit à une exfiltration de données internes et 7 (23%) ayant conduit à une usurpation des outils de la SGP ;
- **Ainsi, 9 incidents (29%) sont opérationnels**, 5 (16%) parmi eux ont pour origine une indisponibilité de services informatiques et 4 (13%) sont liés à une défaillance des systèmes de la SGP.

La majorité des incidents majeurs subis par les SGP est donc causée par des **cyberattaques de formes diverses** (rançongiciel[3], ingénierie sociale[4], etc.) **généralement subies par leurs prestataires**.

Ces incidents impactent toute la chaîne de valeur des SGP dont chaque fonction est susceptible d'être interrompue. Les fonctions critiques ou importantes[5] impactées par ces incidents sont majoritairement :

- **le suivi des portefeuilles/PMS (22%)** perturbant la valorisation, le calcul des performances et le *reporting* client ;
- **le passage d'ordre/OMS (22%)** entravant la transmission et l'exécution sur les marchés ;
- **l'accès aux données internes (22%)** exposant des informations sensibles telles que des données clients ou financières ;
- **les procédures de KYC (13%)** ralentissant l'entrée en relation et le suivi des clients, tout en augmentant les risques de non-conformité.

Les critères retenus de classification en incident majeur[6] sont principalement :

- **la durée et l'interruption de services (28%)** impliquant notamment des indisponibilités totales ou partielles pour les clients ou les contreparties financières ;
- **les services critiques affectés (25%)** pouvant impacter la capacité de la SGP à satisfaire ses exigences règlementaires ;

[2] A l'exception des 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, et qui n'ont pas opté pour l'application intégrale de cette directive.

[3] Programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon – CyberDico de l'ANSSI.

[4] Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes – CyberDico de l'ANSSI.

[5] Au sens de l'article 3 du règlement DORA.

[6] Au sens de l'article 9 du règlement délégué 2024/1772.

- **la perte de données (14%) rendant temporairement ou durablement inaccessibles ou inutilisables les données de la SGP**.

Par ailleurs, le secteur entier de la gestion d'actifs est fortement exposé au risque cyber, classé 6ème risque le plus critique à court terme par le Forum économique mondial[7]. En ce sens, les incidents majeurs notifiés concernent des SGP de tout type de gestion et de toute taille :

- à la fois **gestion traditionnelle** (45%), **sous mandat** (45%), **non cotée** (7%) ou **immobilière** (3%) ;
- pour des encours **de 40 millions à 250 milliards** d'euros et des effectifs de **5 ETP à 1 200 ETP** ;
- par ailleurs, ces SGP font aussi **bien partie d'un groupe bancaire** (52%) que **non** (48%).

Les **prestataires de services sur crypto-actifs** (PSCA) et **entreprises de marché** ont notifié **2 incidents majeurs au titre de DORA au cours de l'année 2025**. Ce faible nombre d'incidents s'explique notamment par le faible nombre de PSCA agréés en 2025. Avec la fin de période transitoire PACTE – MiCA, et l'extinction du statut PSAN au 1er juillet 2026, le nombre d'acteurs agréés PSCA est désormais bien supérieur à celui de 2025, et le nombre d'incidents devrait de facto être plus important au cours de l'année 2026, en particulier au regard des menaces pesant sur l'écosystème des crypto-actifs. Aucun incident majeur n'a été déclaré au titre de DORA par **les prestataires de services en financement participatif** (PSFP) en 2025.

1.2. ETUDE DE CAS

1.2.1. Exfiltration de données d'un prestataire supportant une fonction critique

Un prestataire d'outils d'agrégation et suivi de portefeuille a fait l'objet d'une cyberattaque conduisant à l'isolement de son système d'information et l'indisponibilité de tous ses services. Le prestataire informe alors ses partenaires qu'il s'agit d'une attaque de type rançongiciel. Pour les acteurs de la gestion d'actifs, l'incident peut affecter des fonctions clés : diligences liées à l'entrée en relation (KYC/LCB-FT/obligations MiFID d'effectuer des tests d'adéquation pour la gestion discrétionnaire) et le service client (communication aux clients d'une vue agrégée de leurs portefeuilles, CRM, requêtage pour analyse du portefeuille de la clientèle).

- Par ruissellement, les données extraites du prestataire peuvent contenir des informations sur ses SGP clientes, les porteurs de parts de leurs fonds et leur activité interne. **Les prestataires supportant une fonction critique génèrent ainsi de nombreux risques de résilience que les SGP doivent mesurer et maîtriser.**

1.2.2. Usurpation d'identité d'un gérant financier

Un gérant financier utilise son ordinateur personnel non sécurisé pour accéder à son espace de travail. Des e-mails frauduleux ont été envoyés à partir de sa boîte mail compromise par *phishing*, usurpant ainsi son identité. Les attaquants ont produit de fausses instructions de paiement à partir des documents disponibles dans ses mails passés. Ces instructions ont été adressées directement au dépositaire, ce qui a conduit à l'exécution de virements non autorisés. L'incident a été identifié par la SGP après plusieurs transactions. Les comptes concernés ont été bloqués à titre de mesure d'atténuation. Pour autant, une partie des fonds volés ont déjà été transférés dans différents pays.

- Le manque de maîtrise sur la connexion à ses systèmes internes et de contrôle sur les transactions effectuées peut conduire une SGP à perdre la trace de ses flux financiers. **Du fait des volumes traités par les SGP, des principes de résilience doivent guider l'ensemble de la chaîne de gestion.**

[7] *The Global Risks Report 2026*, World Economic Forum

2. PRINCIPAUX ENSEIGNEMENTS RELATIFS AUX INCIDENTS MAJEURS DECLARES EN 2025

2.1. UNE ANNEE D'IMPLEMENTATION MARQUEE PAR DES PROBLEMATIQUES DE QUALITE DES DONNEES

Pour rappel, le processus permettant aux entités supervisées de remplir leur obligation déclarative des incidents majeurs de TIC a été mis en place dès le premier jour d'entrée en application du règlement DORA.[8]

S'agissant des SGP, une première phase de rodage soulevait les problématiques suivantes :

- transmission hors délais des déclarations d'incidents ;
- transmission de déclarations d'incidents incomplètes ;
- transmission de déclarations comportant des informations incohérentes avec la nature de l'incident ;
- besoin fort d'accompagnement des SGP dans la classification des incidents. En effet, seuls les incidents majeurs font l'objet d'une déclaration obligatoire conformément à l'article 19 du règlement DORA.

Cette phase de rodage inhérente à une année d'implémentation a duré environ 6 mois durant lesquels l'AMF a renforcé ses actions d'accompagnement. Une amélioration de la qualité des déclarations a été observée durant le second semestre 2025. Bien que des progrès aient été constatés, il demeure encore une marge de progression. En effet, le questionnaire d'auto-évaluation soumis par les SGP, en novembre 2025, souligne que près d'un quart des SGP (23%) n'ont toujours pas mis en place un dispositif de déclaration des incidents majeurs conforme au règlement DORA.

2.2. L'EXPOSITION DU SECTEUR DE LA GESTION D'ACTIFS AU RISQUE LIE AUX TIC

Les déclarations d'incidents majeurs ont mis en lumière que (i) la gestion d'actifs constitue un secteur fortement exposé au risque lié aux TIC et que (ii) le risque lié aux TIC n'est pas inhérent à une typologie de SGP.

2.2.1. La gestion d'actifs : un secteur fortement exposé au risque lié aux TIC

Tout d'abord, l'ensemble de la chaîne de valeur des SGP est soutenue par les technologies de l'information et de la communication. En effet, les incidents ont impacté des fonctions critiques dont la gestion financière (comprenant le passage d'ordres), la valorisation des instruments financiers et la conformité (entrée en relation, KYC, LCB-FT). Ainsi, l'absence de dispositif de résilience opérationnelle numérique expose les SGP à des impacts financiers, réglementaires et réputationnels.

Par ailleurs, les SGP opèrent dans un environnement hautement interconnecté. En effet, la gestion de fonds implique des flux informatiques avec de nombreux acteurs tels que le valorisateur, le dépositaire, le centralisateur, le teneur de compte, les fournisseurs de données, les distributeurs, etc. Ainsi, la multiplicité des flux avec les tiers augmente les sources de risque lié aux TIC. En complément de l'interconnexion, l'adoption des nouvelles technologies (digitalisation du parcours de souscription, intelligence artificielle, etc.) dans une logique d'efficience opérationnelle constitue également une source de risque à encadrer.

En outre, la majorité des SGP françaises sont des structures entrepreneuriales de petite et moyenne taille avec une organisation (i) centrée sur le cœur d'activité, à savoir la gestion des fonds et (ii) s'appuyant sur l'externalisation des fonctions supports dont l'informatique. La majorité des SGP ne dispose pas en interne de moyens humains spécialisés dans la sécurité des systèmes d'informations. Ainsi, l'accompagnement par des prestataires qualifiés est nécessaire afin de renforcer la résilience numérique des SGP.[9]

Les SGP françaises constituent une population présentant un intérêt économique pour les cyberattaquants dans la mesure où les encours sous gestion sont élevés et croissent. Le *phishing* évoqué dans le cas 2.2.2 met en lumière ce constat. Par ailleurs, les SGP détiennent un nombre important de données sur les investisseurs susceptibles

[8] Précisé sur le site internet de l'AMF : https://www.amf-france.org/fr/formulaires-et-declarations/dora

[9] En ce sens, l'ANSSI met en place des référentiels d'exigences pour les services liés aux systèmes d'information, dont PACS (accompagnement et conseil), PASSI (audit de sécurité), PDIS (détection des incidents) et PRIS (réponse aux incidents)

d'intéresser des cyberattaquants. Ainsi, des attaques de type *ransomware* subies directement ou indirectement au travers de prestataires (cas 2.2.1) ont été déclarées.

2.2.2. Absence de profil type de SGP exposée au risque lié aux TIC

Comme indiqué, *supra* et au travers de l'analyse des notifications d'incidents majeurs transmises, toutes les SGP françaises sont exposées au risque de TIC indépendamment de leur taille, du type de gestion ou de leur structure actionnariale (SGP entrepreneuriales, SGP appartenant à un groupe bancaire/assurantiel, etc.). Ainsi, toutes les SGP doivent intégrer un cadre de gestion du risque lié aux TIC. Suivant leur activité, la surface d'exposition numérique des SGP est variable et le cadre de gestion doit être adapté. Par exemple, une SGP spécialisée dans la gestion de crypto-actifs aura un degré d'interconnexion et de digitalisation élevé, nécessitant une gestion spécifique de ces risques. L'analyse des dépendances de tiers et la cartographie des actifs informationnels et de TIC requises par le règlement DORA permettent d'établir un cadre de gestion propre à l'activité de la SGP.

2.3. L'IMPORTANTE GESTION DES RISQUES LIÉS AUX PRESTATAIRES TIERS DE SERVICES TIC

L'analyse statistique des incidents majeurs révèle l'importance du risque lié aux prestataires tiers de services TIC. Comme présenté, *supra*, 87% des incidents majeurs déclarés par les SGP sont issus d'une défaillance d'un prestataire qu'elle soit accidentelle (19%) ou la conséquence d'une cyberattaque (68%).

Cette statistique confirme que la dépendance vis-à-vis des prestataires de services TIC est de nature à générer un risque sur la sécurité des systèmes d'information des entités financières dont les SGP. C'est d'ailleurs pour cette raison que les prestataires tiers critiques font l'objet d'une supervision au niveau européen. L'objectif de cette supervision européenne étant de limiter un risque systémique lié à la concentration de la dépendance vis-à-vis de ces acteurs. A une échelle moindre, le cas 2.2.1 confirme que la défaillance d'un prestataire peut impacter de nombreuses entités financières. L'occurrence de cas similaires pourrait augmenter dans la mesure où la cybercriminalité s'industrialise[10]. Afin de réaliser des « économies d'échelle », les cyberattaquants peuvent privilégier une attaque sur un prestataire afin d'élargir leur surface d'attaque en touchant indirectement plusieurs entités.

Par conséquent, la définition d'une stratégie de résilience opérationnelle numérique doit impérativement inclure la gestion du risque lié aux prestataires tiers de services TIC. Le règlement DORA dédie une thématique entière à ce risque avec l'instauration de règles de gouvernance, de mise en place de processus de sélection et d'évaluation des prestataires potentiels de services TIC, d'évaluation des risques avant la conclusion de tout accord contractuel, d'intégration de clauses minimales, de stratégies de sortie avec des prestataires de services TIC soutenant des fonctions critiques ou importantes, etc.

Toutefois, l'implémentation des obligations relatives à la gestion du risque lié aux prestataires tiers de services TIC a présenté des difficultés pour les SGP. Ces difficultés se résument en quatre points.

- Certains prestataires refusent d'être identifiés comme prestataire tiers de services TIC de manière à ne pas avoir à se conformer au règlement DORA ;
- Pour certains prestataires tiers de services TIC, les SGP ont rencontré de grandes difficultés dans l'intégration des clauses DORA au sein des contrats. Il est important de rappeler que la majorité des SGP françaises sont des structures entrepreneuriales de petite et moyenne taille :
  - Ainsi, le rapport de force avec certains prestataires peu substituables n'est pas en leur faveur. Ces prestataires proposent généralement des contrats standardisés qui ne répondent pas totalement au règlement DORA ;
  - Des coûts supplémentaires ont été demandés par les prestataires afin de répondre à des obligations réglementaires (ex : droit à l'audit, réalisation de tests d'intrusion, coopération avec les autorités).

[10] *Rapport annuel sur la cybercriminalité 2025* du Ministère de l'Intérieur.

- Certains prestataires ne connaissent pas les exigences du règlement DORA et remettent en cause le besoin de remédiation contractuelle. Certaines exigences du règlement sont perçues comme trop intrusives pour des prestataires.
- Le temps d'échange entre les différents services juridiques est très long d'autant plus qu'il faut inclure la chaîne de sous-traitants. Certains petits fournisseurs ne sont pas prêts et pas outillés, et ont du mal à répondre dans les délais raisonnables.

Par conséquent, la gestion du risque lié aux prestataires tiers de services TIC devrait constituer une thématique clé dans les actions de supervision. En 2026, l'AMF a inscrit l'anticipation des nouveaux risques et la résilience opérationnelle des professionnels régulés parmi ses axes d'action prioritaires. Il est également attendu que cette thématique fasse l'objet d'une vigilance particulière au sein des entités financières, y compris dans le cadre des dispositifs de contrôle interne.

Il est enfin rappelé qu'aux termes du règlement DORA les prestataires tiers de services TIC jugés critiques pour les entités financières dans leur ensemble sont placés sous la supervision des autorités européennes de supervision.