# *CYBERSÉCURITÉ*
# Guide pratique DORA

Mise à jour janvier 2026

## Guide professionnel

AFG

## Sommaire




L'AFG remercie les membres du Groupe de travail Cybersécurité
qui ont participé à l'élaboration de ce Guide,
et en particulier son président Wilfried Lauber (Amundi).

Le Groupe de travail Cybersécurité
est rattaché à la Commission Déontologie et Conformité
présidée par Monique Diaz (AXA Investment Managers Paris).

Valentine Bonnet, directrice Gouvernement d'entreprise et Conformité
en charge du Groupe de travail Cybersécurité (AFG), a coordonné ces travaux.

## Introduction

Le règlement DORA (*Digital Operational Resilience Act*), définit un cadre détaillé et complet sur la résilience opérationnelle numérique pour les entités financières, et s'applique donc aux sociétés de gestion (SGP).

Le texte entré **en application le 17 janvier 2025** impose des obligations aux entités financières, mais également à leurs prestataires de services numériques. Ceux-ci doivent revoir régulièrement leurs procédures, contrats, mécanismes et outils assurant la sécurité des systèmes d'information.

## Qu'est-ce que la résilience opérationnelle ?

> **→ La capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles (…) y compris en cas de perturbations. /1**

DORA vise à embarquer le secteur financier vers une réelle maturité dépassant la résilience opérationnelle unitaire de chaque acteur pour atteindre un renforcement du niveau de résilience du secteur dans son ensemble.

De fait au-delà des acteurs financiers désignés comme systémiques pour la Place européenne et des autres acteurs qui participent à sa mise en œuvre, sont englobés les prestataires de service TIC qui devront répondre à un niveau d'exigence et de contrôles importants, pour le bienfait du secteur à terme.

## Qu'est-ce qu'un prestataire TIC ?

> **→ Un prestataire TIC est un prestataire de service informatique, au sens large, qu'il soit fourni en mode cloud ou depuis vos datacenters au travers de vos logiciels utilisés en interne. Cela couvre tous les pans de l'informatique : stockage, traitement, saisie ou fourniture de données.**

Ce guide a pour objectif d'être pratique et actionnable avec pour chaque chapitre cinq sections clés :

**L'existant :** il s'agit de points d'attention pour vérifier que vous répondez effectivement à chacune des exigences posées par DORA, s'agissant de pratiques que vous avez sans doute déjà mises en œuvre.

**Les nouveautés :** les apports de DORA et pour lesquels la marche à gravir semble accessible.

**Les challenges :** des exigences plus complexes à mettre en œuvre impliquant pour les SGP de prévoir des actions.

**Les clés pour le board :** ce sont les points saillants à placer en cible par votre board, que vous pourriez utiliser dans un *"elevator pitch"*.

**Les livrabres clés**

**À noter :** dans ce document, la terminologie "board" désigne votre organe de direction.

*/1 Voir Art 3.1.*

Cinq points principaux sont à considérer :

1. **La stratégie de résilience opérationnelle numérique**
   qui définit le cadre de gestion des risques de la SGP, mais aussi ses ambitions au travers de son appétence au risque.
2. **Le reporting des incidents et des menaces cyber**
   qui implique la mise en place de procédures pour détecter, classifier, gérer et notifier les incidents.
3. **Les tests de résilience opérationnelle numérique**
   une fois par an *a minima* pour les systèmes gérant des fonctions critiques ou importantes. Ces tests, qui incluent les prestataires de service TIC doivent être envisagés sous deux axes :
   - résilience des systèmes face aux attaques
   - résilience des systèmes suite à une attaque.
4. **La gestion des risques liées aux prestataires de services numériques TIC**
   imposant de distinguer parmi les prestataires ceux couvrant des fonctions critiques ou importantes, de cartographier les tiers pour éviter les concentrations et d'inclure des clauses minimales dans les contrats.
5. **Le partage d'information en matière de cybersécurité**
   Dans le but d'une résilience opérationnelle numérique globale du secteur financier, les SGP sont encouragées à partager des informations liées à la cybersécurité.

## À qui s'adresse DORA ?

À toutes les SGP notamment ! Néanmoins, un *Asset Manager* vu comme une microentreprise verra certaines de ses exigences fortement réduites [2].

## Comment s'applique DORA ?

**→ Le principe de proportionnalité fait l'objet d'un article à part entière de DORA : l'article 4 précise ainsi que les mesures applicables aux entités sont « proportionnées à leur taille et à leur profil de risque global, ainsi qu'à leur nature, à l'ampleur et à la complexité des services, activités et opérations ».**

## Quelle articulation avec la directive NIS 2 ?

Si les deux textes se rapprochent en termes de maturité à atteindre, en renforçant notamment les mesures de protection à mettre en œuvre et de notification en cas d'incidents, DORA constitue une *lex specialis* [3] pour les entités financières. La règle spéciale l'emportant en droit sur la règle générale, les SGP doivent donc se concentrer sur la mise en place de DORA.

[2] *Microentreprises : les SGP employant moins de 10 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros seront dispensées de certaines obligations de DORA.*

[3] *Considérant 16.*

# I. Gouvernance et organisation

## En bref

Votre board apparait désormais comme pleinement responsable de l'implémentation des différentes obligations et de la plénitude des livrables demandés.

DORA lui donne un rôle majeur sur un périmètre déjà couvert sous de nombreux aspects par de bonnes pratiques opérationnelles ou organisationnelles.

Il doit ainsi définir, valider et superviser le déploiement du cadre de gestion des risques informatiques.

Ce cadre englobe les différentes politiques, stratégies, procédures et outils informatiques encadrant la cyber-résilience de la SGP, que nous définirons plus précisément dans différents chapitres de ce document.

L'article 5 de DORA définit des différentes obligations notamment :

- la validation explicite des politiques de sécurité,
- l'allocation des budgets de gestion des risques IT,
- la supervision du plan de contrôle IT,
- la mise en place des comités et des canaux de reporting interne.

Il est essentiel que votre board soit régulièrement sensibilisé aux risques liés à la cybersécurité et leurs impacts sur les activités de la SGP.

**Le board doit mettre, *a minima* annuellement à l'ordre du jour de ses réunions, l'intervention du RSSI et prévoir, tout au long de l'année, des éléments complémentaires de reporting et de suivi.**

## L'existant

Les SGP doivent avoir des politiques de sécurité ainsi que des ressources humaines et financières allouées à la gestion du risque IT. Ces ressources doivent pouvoir être clairement identifiées voir même isolées du budget IT.

À titre de comparaison, dans la finance les dépenses moyennes cybersécurité s'élèvent à 6,4 % du budget IT [4].

Il convient de vérifier le contenu de vos procédures actuelles en matière de politiques de sécurité afin de compléter le cas échéant. Il est essentiel d'informer le board sur les risques que connait la société et les mesures mises en œuvre pour minimiser ces risques.

**Nous vous conseillons d'instaurer une revue, au moins annuelle, par le board, de ces risques.**

[4] *Wavestone - Cybersecurity benchmark 2025.*

## Les nouveautés

- Les SGP doivent instituer : un *« rôle de suivi des accords conclus avec les prestataires tiers de services TIC »* ou *« désigner un membre de la direction générale chargé de superviser l'exposition aux risques connexes et la documentation »*.
- **Le board des SGP assume la *« responsabilité ultime »* [5] de la gestion des risques informatiques** et doit définir les rôles et responsabilités liés à la cyber résilience. Votre board doit notamment :
  - **Approuver et examiner périodiquement les plans internes d'audit informatique,** ainsi que les modifications significatives qui y sont apportées [6].
  - **Examiner et approuver la politique de résilience opérationnelle numérique [7] et de continuité des activités informatiques [8].**
  - **Mettre en place des canaux de notification lui permettant d'être informé des accords conclus avec des prestataires de services TIC, des changements significatifs prévus concernant ces prestataires, et des risques qui en découlent [9].**

**L'AFG vous recommande des validations régulières par le board de l'ensemble des points précités incluant la liste des prestataires critiques ou importants.**

- ***« Suivre régulièrement »* [10] une formation spécifique** pour mieux comprendre et évaluer les risques informatiques et leurs incidences sur les opérations de la SGP.

**L'AFG recommande de réaliser ces formations au minimum annuellement.**

## Les challenges

L'appropriation du risque cyber et de la résilience IT par le board recouvre plusieurs challenges comme celui lié à la récurrence de l'exercice annuel, *a minima*, et au reporting régulier à réaliser. De fait, il convient de parvenir à un bon équilibre avec un contenu approprié au conseil en concertation avec celui-ci afin d'alimenter ses attentes.

**En termes de contenu lors d'interventions à une réunion du board, l'AFG vous recommande :**

- d'être très concret en vous basant sur des exemples réels en lien avec l'activité et la sensibilité de votre board
- de garder un fil conducteur dans les passages successifs au board afin que le sujet soit vu dans la continuité et non sporadiquement.

[5] *Art 5.2 (a).*
[6] *Art 5.2 (f).*
[7] *Art 5.2 (d).*
[8] *Art 5.2 (e).*
[9] *Art 5.2 (h).*
[10] *Art 5.4.*

**En termes de reporting, le board attend de vous d'être sollicité pour des actions, des décisions. Attention à ne pas tomber dans un *"all green"* reporting qui ne permet de souligner les points sur lesquels le board devrait mettre l'accent.**

## Clé pour le board

Face à un risque d'attaques à large envergure, le board doit veiller à mettre en place une organisation efficiente en charge des risques IT. Comme le redoute Vincent Strubel, directeur de l'ANSSI : *« Il faut se préparer au grand soir, quand des pans entiers de notre société seront attaqués simultanément »* [11].

La sensibilisation du board, notamment par la présentation des mesures présentes dans ce guide, est essentielle pour poser les premiers jalons en vue d'une mise en place progressive de votre conformité à la réglementation DORA.

## Livrables clés

Étant donné l'exigence de voir formaliser par les SGP la gouvernance de la résilience opérationnelle, nous vous recommandons de garder une preuve :

- des remontées et des réunions d'informations avec le board intégrant à l'ordre du jour, de façon bien visible, la stratégie de cyber résilience de l'entreprise ;
- de l'approbation par le board des différentes politiques définies dans le cadre de la gestion des risques (cf. chapitre 2) ;
- des formations effectuées par le board.

[11] *Discours inaugural de Vincent Strubel aux Assises de la sécurité des systèmes d'information de Monaco, 11 octobre 2023.*

# II. Cadre de gestion des risques

## En bref

Le cadre de gestion des risques lié aux TIC tel que prévu par DORA se doit d'être « **solide, complet et bien documenté** ».

Ce cadre, qui repose sur une stratégie globale de résilience opérationnelle numérique, englobe notamment les différentes politiques, stratégies et mesures que vous mettez en œuvre pour assurer la sécurité de vos systèmes d'information.

Il implique de la part de la SGP une approche proactive face à l'évolution des vulnérabilités.

Des changements importants dans les activités de la société de gestion doivent ainsi conduire à actualiser le cadre défini.

**Nombre de points existent depuis longtemps dans différents référentiels et guides de bonne pratiques, comme ceux publiés par l'AFG. Toutefois à ce stade ils sont appliqués à des degrés divers, DORA innove en les intégrant dans une optique de conformité réglementaire.**

## L'existant

- Les SGP doivent garantir **une séparation adéquate des fonctions** de gestion informatique, des fonctions de contrôle et des fonctions d'audit interne */12*.
- Votre SGP doit avoir une **stratégie de résilience numérique** */13*, définissant les modalités de mise en œuvre du **cadre de gestion des risques informatiques** */14*.
- À ce premier volet s'ajoutent des procédures visant à mettre en place différents livrables (stratégies, politiques, protocoles) ainsi que la formalisation des outils informatiques utilisés pour sécuriser les infrastructures informatiques et minimiser les risques.

## Les nouveautés

**À noter :** le cadre de gestion des risques devra être réexaminé **au moins une fois par an**, ainsi qu'en cas de survenance d'incidents majeurs liés à l'informatique */15*. Aux SGP de privilégier un rapport « sous format numérique ».

DORA intègre un panorama des exigences à formaliser. Votre cadre de gestion des risques informatiques doit notamment déterminer */16* :

- votre **niveau de tolérance au risque informatique**, autrement dit l'appétit aux risques, qui, en fonction de la taille et de la complexité de votre SGP permettra de déterminer une stratégie pour maintenir le risque en deçà de l'appétit ;
- votre **procédure d'évaluation des risques liés aux TIC** (probabilité des vulnérabilités et menaces) ;
- l'**examen annuel des risques résiduels** qui ont été acceptés

*/12 Art 6.4.*
*/13 Art 6.9.*
*/14 Art 6.1*
*/15 Art 6.5.*
*/16 Art 6.8.*

- une politique en matière de chiffrement, de gestion des **actifs matériels/ logiciels**
- des **objectifs clairs en matière de cybersécurité**, les politiques de sécurité devant faire l'objet d'une approbation formelle par votre board ;
- les mécanismes mis en place pour **prévenir les incidents** et **se protéger contre leurs effets**;
- une **stratégie globale multi fournisseur** ;
- le **pilotage des incidents majeurs liés à l'informatique** : volume, objectif, plan d'amélioration et efficacité des mesures de prévention ;
- les modalités de mise en œuvre :
  - des **tests de résilience opérationnelle numérique** (anciens tests de continuité d'activité) : capacité de réaction face à l'incident cyber
  - des tests de pénétration : capacité de résistance face à l'incident cyber
- une **stratégie de communication en cas d'incidents**.

## DORA rappelle que votre gestion des risques doit s'articuler autour de 5 axes :

### 1. L'identification des risques

Identifier, classer, documenter et revoir au moins une fois par an toutes les fonctions métiers liées à l'informatique, **les actifs d'information** *[17]* **et les actifs TIC** *[18]* : DORA impose implique de réaliser un schéma global des interconnexions, différent des schémas classiques par équipe ou par thématique.

### 2. La protection et prévention

Le cadre de gestion des risques doit être proportionné à la taille et au profil de risque de la SGP, et contenir *[19]* :

- une politique de sécurité de l'information visant la résilience de la SGP ;
- des politiques, procédures et contrôles sur la gestion des réseaux et des infrastructures, les accès, l'authentification forte, la gestion des changements informatiques, la gestion des correctifs et des mises à jour ;
- des formations et campagnes de sensibilisation à destination du board et des salariés.

### 3. La détection

Les SGP doivent mettre en place des mécanismes régulièrement testés *[20]* permettant de détecter rapidement les activités anormales *[21]*.

### 4. La réponse

La SGP doit prévoir une « fonction de gestion de crise » afin de gérer les communications internes ou externes *[22]* selon un plan de communication de crise *[23]* déterminé et documenté « qui favorise une communication responsable ».

Des tests doivent être effectués au moins une fois par an *[24]* sen incluant des scénarios de cyber attaques. DORA insiste particulièrement sur les tests concernant des fonctions critiques ou importantes externalisées ou sous-traitées *[25]*.

*[17] Art 3.6 : ensemble d'informations, matérielles ou immatérielles, qui justifie une protection.*
*[18] Art 3.7 : un actif logiciel ou matériel dans les réseaux et les systèmes d'information utilisés par l'entité financière.*
*[19] Art 9.4*
*[20] Art 10.1 et Art 25*
*[21] Art 17.*
*[22] Art 11.7.*
*[23] Art 11.1.*
*[24] Art 11.7.*
*[25] Art 14.*

Les SGP doivent tenir un registre des activités [26] facilement accessible, incluant notamment une politique de continuité des activités informatiques [27] faisant partie de la politique de continuité des activités opérationnelles.

### 5. Le rétablissement

Les entités doivent également mettre en place un plan de rétablissement après sinistre informatique devant faire l'objet d'un audit indépendant également testé au moins une fois par an.

## Les challenges

**L'AFG vous recommande de prioriser le chantier d'identification lié à la cartographie du SI.**

Ce qui n'était jusqu'ici qu'une bonne pratique (analysée par l'AFG via des questionnaires réalisés entre 2018 et 2022 qui montraient peu d'évolution dans la cartographie des SI) devient une obligation.

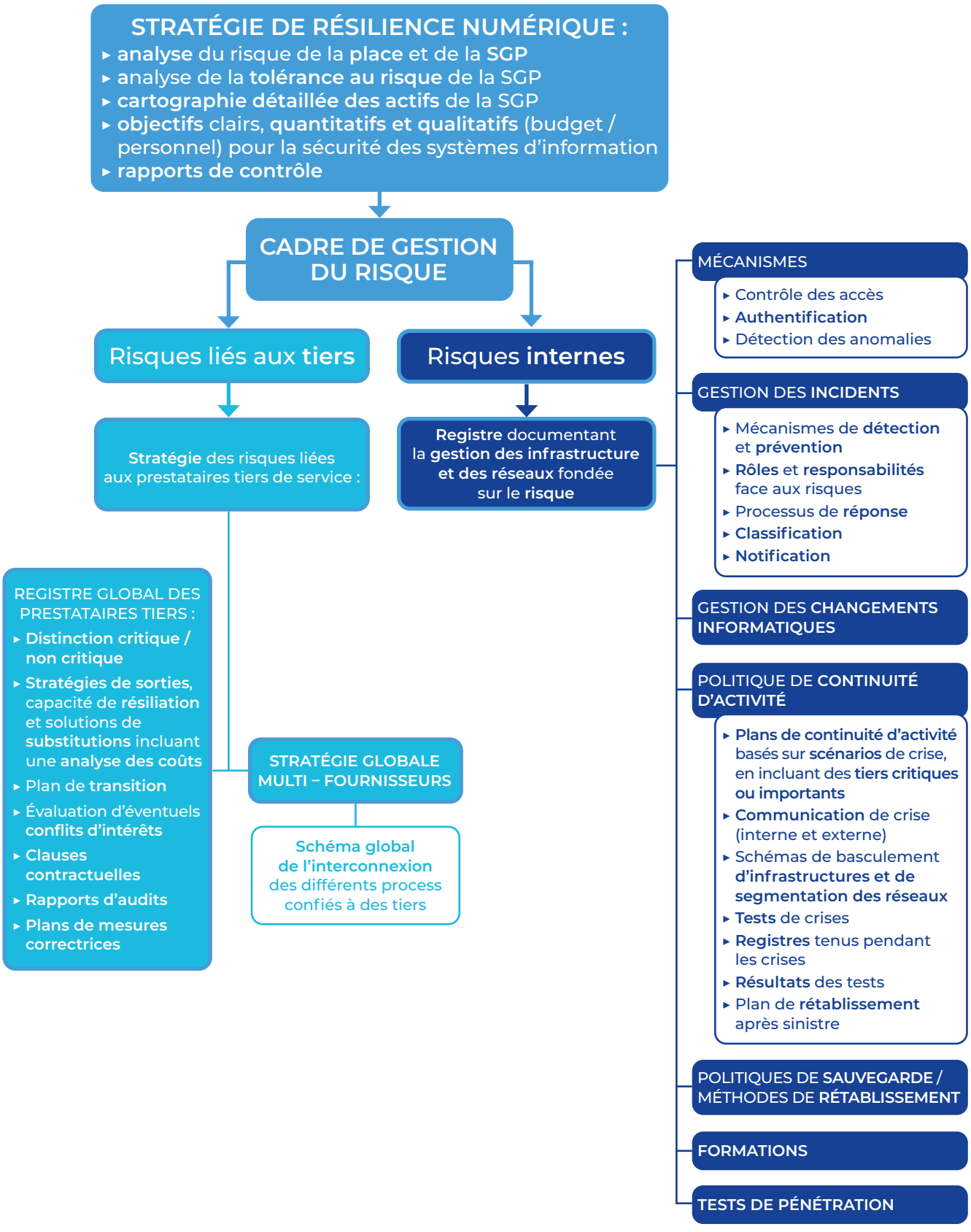
Son existence et sa complétude devraient sans doute faire l'objet de contrôles par les autorités.

La finalité à rechercher est celle d'une vision globale des services métiers liant composant d'infrastructure, applications, logiciels, données et prestataires de services TIC.


[26] Art 11.6
[27] Art 11.4.

## Livrables clés

Cartographie des livrables attendus dans DORA :



# III. Catégorisation et déclaration des incidents

## En bref

DORA renforce les exigences quant à la gestion des incidents dans la perspective de se prémunir des risques systémiques au niveau européen qui implique la mise en place par les SGP d'une politique de gestion des incidents liés aux TIC.

**Pour atteindre cet objectif, il est attendu des SGP qu'elles veillent à la formalisation du processus de gestion des incidents incluant leur catégorisation et leur monitoring.**

**Des outils comprenant des critères précis pourront faciliter cette mise en œuvre.**

**Ces procédures permettront une meilleure effectivité des notifications au board, aux clients et aux autorités compétentes.**

L'avancée dans la mise en place de DORA dans chaque SGP dépendra notamment :

- de la maturité de la société vis-à-vis de son dispositif de gestion des incidents ;
- de la mise en place de plan de réaction (communication, scénario de risque) ;
- du degré de détail souhaité ;
- de sa capacité à monitorer les alertes et à piloter les plans d'action ;
- de la mise en place d'une veille sur les menaces cyber (optionnel).

## L'existant

La gestion des incidents, process qui existe déjà au sein des SGP, implique de :

- vérifier que votre organisation pour la gestion des incidents est opérationnelle ;
- déployer un référencement des process critiques et des sous-traitants clés : des plans de réaction, *a minima* basiques, doivent être mis en place ;
- mettre en œuvre un process de gestion des incidents informatiques pour détecter, gérer, et notifier les incidents [28]. Les incidents doivent être suivis, consignés, catégorisés, priorisés et classés en fonction de leur priorité et de la gravité et de la criticité des services touchés [29].

## Les nouveautés

DORA introduit des critères pour **classifier les incidents liés aux TIC** ;

- la durée de l'incident ;
- l'évolution et la répartition géographique des zones touchées par l'incident ;
- la sécurité des données notamment sensibles ;
- la criticité des services touchés ;
- la stabilité financière ou la continuité du système financier.

[28] *Art 17.1*
[29] *Art 17.3*

La SGP va devoir évaluer si l'incident :

- touche des services TIC ou des réseaux qui soutiennent des fonctions critiques ou importantes ;
- touche des services financiers fournis par la SGP qui nécessitent un agrément ou un enregistrement ou qui sont surveillés par les autorités ;
- constitue un « accès réussi, malveillant et non autorisé aux réseaux et aux systèmes d'information de la SGP.

**Est majeur, un incident lié aux TIC qui a une incidence négative élevée sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'entité financière** (article 3 -10 DORA).

- Les incidents majeurs **doivent être notifiés** :
  - aux autorités selon 3 phases :
    - 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
    - un rapport intermédiaire dans les 72h de la notification initiale
    - un rapport final lorsque l'analyse des causes profondes est réalisée [30].
  - au board [31], en incluant les examens post incidents et mesures à mettre en œuvre
  - aux utilisateurs de services et clients si l'incident est susceptible d'avoir des répercussions sur leurs intérêts financiers [32];

## Les challenges

DORA impose une réelle transparence et un haut niveau de détails sur les incidents majeurs envers vos clients, votre board et votre autorité.

Les SGP doivent indiquer à leur autorité si l'incident a été notifié à d'autres autorités nationales compétentes ou organismes pertinents, et fournir des informations sur la coopération éventuelle avec ces entités.

À la suite de la notification initiale des rapports réguliers doivent être transmis pendant et durant la durée de l'incident. Le niveau des informations à fournir inclut :

- la description de son impact ;
- les causes présumées ;
- les mesures correctives prises ou envisagées pour atténuer les effets de l'incident et prévenir sa récurrence à l'avenir ;
- les données pertinentes sur les systèmes et services affectés ;
- le statut de l'incident notamment l'estimation du délai nécessaire pour le résoudre complètement.

Les SGP doivent prévoir comment organiser leur plan de communication et de réaction en cas d'incident.

[30] *Art 19.4.*
[31] *Art 18.1*
[32] *Art 19.3.*

Vos procédures doivent prévoir de quelle façon mettre en œuvre la classification ainsi que la collecte et la centralisation des informations relatives aux incidents majeurs.

Pour compléter le schéma, des RTS apportent des précisions quant aux informations à fournir s'agissant des :

- niveaux de détail, délais, seuil de déclaration et format de reporting ;
- exigences sur le dispositif de gestion des incidents ;
- exigences sur la gestion des alertes.

Attention, des incidents récurrents liés par une cause originelle apparente similaire qui, pris isolément, ne constituent pas des incidents majeurs doivent faire l'objet d'attention, car susceptibles de révéler des faiblesses importantes dans vos procédures de gestion des risques.

**À noter :** il est également possible, de notifier les menaces à titre volontaire au travers de veille technologique et cyber (comme le font les grands groupes à travers les CERT).

## Clé pour le board

Il convient de mettre en place des indicateurs clés (KPI) permettant un pilotage des incidents avec notamment la qualification de leur sévérité.

Soyez concrets ! Votre board pourra agir sur base de la remontée des incidents majeurs dont il aura connaissance.

Votre board, en se trouvant pleinement impliqué dans la gestion d'incidents, va accroître sa visibilité.

Il est essentiel que votre board connaisse l'existence de plans de réactions pour traiter des situations critiques et de leur efficacité (test) et puisse, si besoin est, réagir en temps voulu et engager des plans d'action.

## Livrables clés

- Un processus de gestion des incidents informatiques qui doit inclure *[33]* :
  - un registre des incidents ;
  - les rôles et responsabilités à activer pour les différents types et scénarios d'incidents ;
  - des procédures de réponse (réaction) pour limiter les effets et la durée des incidents ;
  - des plans de communication pour les salariés, les parties prenantes externes et les médias ;
  - un rapport estimatif des coûts et pertes annuels agrégés des incidents majeurs liés aux TIC (à communiquer sur demande à l'AMF, art. 11-10 DORA).

*[33] Art 17.3.*

# IV. Tests de résilience

## En bref

Dans la perspective « d'évaluer l'état de préparation en vue du traitement d'incidents liés aux TIC » mentionné par DORA, il s'agit de ne pas se limiter à une approche unitaire centré sur le prestataire, l'application ou l'équipe, mais une vision service délivrée par la SGP.
Les tests de résilience opérationnelle sont de deux ordres :

- des test permettant d'évaluer la capacité de résistance des services (incluant les prestataires) à des attaques ;
- des test permettant d'évaluer la continuité d'activité suite à une défaillance ou dégradation du service (quelle qu'en soit l'origine).

## L'existant

À ce stade les SGP évaluent périodiquement leur sécurité en effectuant des tests *(pentests)*, des audits de sécurité ou des tests de continuité d'activité.

## Les nouveautés

DORA prévoit que les **tests de résilience opérationnelle et de sécurité numérique** [34] s'intègrent selon une approche par les risques.

Ceux-ci sont liés de manière proportionnée à la taille de la SGP et à son profil de risque global, ainsi qu'à la nature, à l'ampleur et à la complexité de ses services, activités et opérations.

Ces tests doivent couvrir les fonctions critiques et s'appuyer sur les outils et méthodes à disposition actuellement [35] tels que scans de vulnérabilités, *pentests*, analyses d'écarts, audits, tests de bout en bout…

Le programme de tests comprend une série d'évaluations, de tests, de méthodologies, de pratiques et d'outils à appliquer.

Ces tests sont réalisables **en interne ou externe** à condition d'être réalisés par des parties indépendantes. En cas de tests réalisés en interne, il convient d'éviter les conflits d'intérêts pendant les phases de conception et d'exécution du test [36].

À la suite des *pentests*, réaliser des rapports et plans d'actions liés à des vulnérabilités critiques.

Les systèmes et applications informatiques critiques ou importants devront subir des tests au moins une fois par an.

**À noter :** il est possible de bénéficier des résultats d'un test de sécurité sur un tiers externe en mutualisant l'audit avec d'autres entités.

L'AFG vous conseille de partager avec vos pairs afin d'optimiser vos programmes de tests (périmètre et fréquence).

[34] *L'article 24.1 exclut d'ailleurs les micro-entreprises du programme de tests de résilience imposé*
[35] *Article 25.1 pour la liste exhaustive.*
[36] *Art 24.4.*

## Les challenges

**Tester au moins une fois par an, tous les systèmes et applications de TIC qui soutiennent des fonctions critiques ou importantes** en incluant les prestataires soutenant ces fonctions.

S'agissant des ***pentests***, il n'est pas nécessaire pour les SGP de recourir à des *pentesters* certifiés. Néanmoins, il est souhaitable de s'appuyer sur des testeurs justifiant d'une expertise ou certifiés (par exemple PASSI ou autre certification européenne) ou encore adhérent à des codes de conduite et qui possèdent une assurance [37].

Si vous avez recours à des *pentesters*, pensez aux clauses relatives à la protection des données personnelles.

Des tests de pénétration fondés sur la menace (**TLPT** : *threat led pentest*).couvrant plusieurs ou la totalité des fonctions critiques ou importantes sont à effectuer par les entités financières désignées comme systémiques. [38]

L'analyse de la menace va alimenter la cartographie des risques, le programme de cyber résilience et le training du board.

Les tests doivent être effectués sur les environnements de production avec toutes les précautions que cela induit.

Dans le cadre de la réglementation, la SGP doit prendre les mesures et garanties nécessaires pour assurer la participation des prestataires tiers de services TIC aux tests, tout en conservant sa responsabilité de veiller au respect du règlement.

## Clé pour le board

Le règlement DORA implique d'évaluer de façon périodique sa résilience aux risques liés à la technologie, de s'améliorer et de le démontrer. Les scénarios doivent permettre à la SGP de viser ses axes essentiels et d'adapter en conséquence ses plans d'action.

Le board doit être au courant des rapports et plans d'actions liées aux vulnérabilités critiques détectées lors d'audits.

Nous vous recommandons de **contextualiser le niveau de vulnérabilité détaillé par les *pentesteurs* pour rendre les mesures actionnables par le board** : décrire le scénario permettant l'attaque et les mesures concrètes à mettre en œuvre dans un langage permettant au board de comprendre le risque et l'intérêt des mesures.

## Livrables clés

- Rapports d'audits.
- Analyse des résultats des tests.
- Plan de mesures correctives.

[37] *Art 27.*
[38] *RTS 2025/1190, article 2.*

# V. Management des tiers

## En bref

Les SGP doivent intégrer les prestataires TIC à leur dispositif de gestion des risques.

Les SGP vont leur appliquer autant que possible les mesures qu'elles s'imposent à elles mêmes.

La consolidation des informations collectées au niveau européen devrait permettre de renforcer la stabilité de la Place financière européenne.

### L'existant

La SGP reste **responsable** du respect des services TIC fournis par des prestataires et doit définir une **stratégie de gestion des risques** liés aux prestataires de services TIC, incluant **réexamen régulier** annuel et prise en compte de la **stratégie multi-fournisseurs** *[39]*.

### Les nouveautés

**DORA rend impératives :**

**a.** La mise en place d'une **gouvernance** permettant une supervision et un pilotage approprié des relations avec les prestataires.

**b.** **La formalisation d'exigences en matière de sécurité et de continuité.** Ces exigences devront être contractualisées au travers de conventions de services incluant des niveaux de services attendus. Les niveaux y seront définis avec des indicateurs permettant d'en mesurer la bonne réalisation (indicateurs de performance de la prestation mais aussi de sécurité, tel que le nombre d'incidents sécurité *a minima*).

La stratégie de maitrise des risques doit spécifiquement considérer, et donc identifier, les prestations supportant la fourniture de services soutenant les **fonctions critiques ou importantes**, c'est-à-dire susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers *[40]*.

DORA impose également des obligations accrues s'agissant des procédures à mettre en place :

**a.** **Tenue d'un registre d'information des engagements contractuels,** devant notamment contenir *[41]* :

- une analyse de la criticité du tiers, le registre devant être divisé entre les tiers critiques ou importants et les non critiques ou importants ;
- une analyse du risque et de la conformité des modalités de conclusion du contrat vis-à-vis de DORA ;
- si le tiers est établi dans un pays étranger, le respect par ce tiers des différentes législations (RGPD sur lequel DORA insiste notamment, législation en matière d'insolvabilité) *[42]* ;

*[39] Art 6.9.*
*[40] Art 3.22.*
*[41] Art 28.4 et 28.5*
*[42] Art 29.2.*

- pour les tiers soutenant des fonctions critiques ou importantes, des stratégies de sorties [43] incluant des solutions de substitution et des plans de transition documentés.

**b. Communication une fois par an du registre aux autorités compétentes** et information préalable des projets contractuels de service TIC supportant des fonctions critiques ou importantes.

**c. Un contrat écrit unique définissant les droits et obligations du prestataire tiers de services TIC et de la SGP** [44] incluant des clauses renforcées pour les services TIC soutenant des fonctions critiques ou importantes [45].

**À noter :** Il est important de veiller à ne conclure d'accords contractuels qu'avec des tiers de services TIC qui respectent des normes adéquates en matière de sécurité de l'information

## Les challenges

Avant la contractualisation d'une nouvelle prestation, la SGP doit veiller à :

**a. Réaliser une analyse préliminaire afin d'évaluer le risque de concentration** des services TIC externalisés auprès des prestataires. En effet, la défaillance d'un prestataire concentrant un nombre significatif de services TIC pour une SGP, pourrait impacter la continuité d'activité de cette SGP.

**b. Étudier les potentiels risques de conflits d'intérêts.**

**c. Prendre en considération les cas de sous-traitance en cascade** : Lorsque que vos accords prévoient la possibilité pour l'un de vos prestataires de sous-traiter un service TIC, ce facteur est à intégrer dans votre analyse de risque par référence aux utilisations prévues par ce sous-traitant.

Pensez à encadrer vos exigences et celles que requiert la réglementation européenne dans des clauses adaptées ;

**d. Se conformer aux exigences supplémentaires prévues pour les prestataires supportant des fonctions critiques ou importantes.** A noter qu'en ce cas DORA impose des règles supplémentaires en cas de recours à des prestataires TIC soutenant des fonctions critiques ou importantes, parmi lesquelles celle de mettre en œuvre des stratégies de sortie afin de garantir la continuité d'activité. Par ailleurs, avant de sous-traiter des services TIC concernant des fonctions critiques ou importantes, référerez-vous au Règlement délégué de la Commission Européenne 2025/532 du 24/03/2025 entièrement dédié aux exigences requises. Sont ainsi mentionnées :

- les diligences précontractuelles applicables en cas de recours à des sous-traitants qui soutiennent des fonctions critiques ou importantes, afin d'évaluer le risque associé, (article 3)
- les clauses contractuelles à inclure en cas de recours à des sous-traitants qui soutiennent des fonctions critiques ou importantes (article 4),

[43] *Art 28.8.*
[44] *Art 30.1.*
[45] *Art 30.3.*

## Clé pour le board

**La SGP reste responsable du respect des services TIC fournis par des prestataires** ce qui oblige à une analyse de risque renforcée.

Il est important que le board soit avisé que le contenu des nouveaux contrats intègre bien les exigences prévues par DORA et veille à la mise en œuvre des travaux sur l'existant en vue de sa mise en conformité.

Les ESAs ont publié la liste prestataires TIC critiques ou importants placés sous leur surveillance soumis à des exigences accrues de sécurité, ce qui va impacter positivement leur niveau de maturité.

La connaissance et la validation annuelle par votre board des process et sous-traitants critiques de votre SGP sont nécessaires.

## Livrables clés

- Registre d'information intégrant tous les accords contractuels.
- Politique relative à l'utilisation des services informatiques qui soutiennent des fonctions critiques ou importantes fournis par des tiers [46].
  - Plan stratégique de sortie.
  - Schéma global de l'interconnexion
- avec des tiers qui soutiennent des fonctions critiques ou importantes [47].

[46] Art 28.2 .
[47] Art 8 .

# VI. Le partage en guise de conclusion

## Le règlement DORA

DORA prône le partage d'informations entre entités financières et entre pairs.

Ce partage a pour objectif de faire bénéficier à l'ensemble des acteurs d'éléments leur permettant de pouvoir renforcer leur niveau de cyber résilience.

Il est positif de voir que la sécurité s'organise de façon collective face à une menace, qui, elle aussi, s'est structurée.

Ensemble nous serons plus forts.

En s'appuyant sur des prestataires de services TIC sur lesquels nous serons de plus en plus exigeants, nous serons encore plus résilients face à ces nouvelles menaces.

L'ambition de cyber résilience de la place financière répond à un contexte où la transformation digitale s'est opérée très rapidement ces dernières années. Elle met au cœur de nos préoccupation les enjeux de cybersécurité et de résilience.

C'est aussi l'opportunité pour les SGP de mettre en place des synergies en interne autour de la cybersécurité et de la continuité d'activité.

## L'AFG et le groupe de travail cybersécurité

**« Ensemble, s'investir pour demain »**, les valeurs de l'AFG s'imposent particulièrement face au règlement DORA.

Le groupe de travail cybersécurité s'attelle depuis des années à partager les bonnes pratiques de cybersécurité au travers de publications régulières de documents pratiques mettant en avant la proportionnalité.

Dans la gestion d'actifs tout particulièrement, les effets d'échelle d'une société à l'autre sont très importants et un même modèle ne peut s'appliquer à tous. La diversité est source de richesse dans le cadre de nos travaux.

Les différents questionnaires cybersécurité réalisés par l'AFG font apparaître une réelle amélioration du niveau de maturité cybersécurité du secteur de la gestion d'actifs et de la prise en compte du risque cyber.

Le règlement DORA appuie cette dynamique.

Nous espérons que ce guide vous permettra de mettre un plan pragmatique et proportionné à votre SGP. Au travers de ce guide, le Groupe de travail Cybersécurité a souhaité vous livrer l'analyse d'experts du secteur de la gestion d'actifs afin que vous puissiez estimer votre niveau de maturité vis-à-vis du règlement DORA, d'engager les actions nécessaires à votre future conformité et d'avoir en cible les points clés sur lesquels mettre l'accent.

*L'AFG remercie René Amirkhanian (DNCA Investments), Walif El Hitti (Comgest), Clément Civeit (Moneta), Bruno Ducamp (Syquant), Mohamed Ghayati (Tikehau), Frederic Gleizer (BNPP AM), Stéphane Graux (Ostrum Asset Management), Alexandre Joachim (LBP AM), Wilfried Lauber (Amundi), Stanislas Perney (BDL Gestion), Tristan Quiles (Amundi) et Olivier Tomatis (Groupama AM), Mamadou Wane (OFI Invest) qui ont activement participé à l'écriture de ce guide.*

*Valentine Bonnet a coordonné ces travaux.*

**L'Association Française de la Gestion financière (AFG) représente et promeut l'utilité de la gestion d'actifs pour les investisseurs et l'avenir de notre pays.**

Elle regroupe plus de 400 membres, dont environ 330 sociétés de gestion, qui gèrent 90 % des encours sous gestion en France. Le montant de ces encours s'élève à 5 400 milliards d'euros, montant le plus élevé des Etats membres de l'Union européenne.

L'AFG soutient le développement de la gestion d'actifs française au bénéfice des épargnants, des investisseurs et des entreprises. L'AFG s'investit pour une réglementation stable, efficace et compétitive, avec un engagement fort : permettre aux épargnants de financer leurs projets de vie tout en mobilisant l'épargne privée vers les entreprises qui se transforment.

**AFG**
17 Square Edouard VII,
75009 Paris

Avenue des Arts 56,
1000 Bruxelles

**www.afg.asso.fr**

AFG