GUIDE PROFESSIONNEL DÉCEMBRE 2023

Cybersécurité – Guide pratique DORA

AFG

SOMMAIRE

Introduction 1

1. Gouvernance et organisation 3

2. Cadre de gestion des risques 5

3. Catégorisation des incidents 9

4. Test de résilience 12

5. Management des tiers 14

6. Le partage en guise de conclusion 17

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 (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 qui entrera **en application le 17 janvier 2025** impose des obligations aux entités financières, mais également à leurs prestataires de services numériques. Ceux-ci devront 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 qui seront désignés comme systémiques pour la Place européenne et des autres acteurs qui participeront 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. Chaque chapitre sera divisé en quatre 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"*.

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 cyber sécurité.

▪ À qui s'adresse DORA ?

À toutes les SGP notamment !
Néanmoins, un *Asset Manager* vu comme une microentreprise verra 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 ».

À l'heure où ce guide est écrit, il semble qu'aucune SGP, quelle que soit sa taille, ne soit vue comme un acteur systémique.

▪ 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.

▪ Toutes les informations sont-elles disponibles à ce stade ?

L'entrée en application de DORA est fixée au 17 janvier 2025. A ce stade, 10 normes techniques (RTS/ITS) venant compléter DORA manquent, celles-ci n'ayant pas encore été publiées par les autorités européennes de surveillance financière (ESMA, EBA et EIOPA). Ce guide sera complété au fur et à mesure de leur publication.

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.

1. 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, d'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 identifiés voir même isolées du budget IT.

À titre de comparaison, dans la finance les dépenses moyennes cyber sécurité s'élèvent à 5,4 % 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.

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 »*[6] 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[7].
  - **Examiner et approuver la politique de résilience opérationnelle numérique[8] et de continuité des activités informatiques[9].**

4) Wavestone - Cybersecurity benchmark 2023. 5) Art 5.3. 6) Art 5.2 (a). 7) Art 5.2 (f). 8) Art 5.2 (d). 9) Art 5.2 (e).

- 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**[10]**.**

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 »***[11] **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.**

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 »*[12].

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 (pouvant figurer à l'ordre du jour).

10) Art 5.2 (h). 11) Art 5.4. 12) Discours inaugural de Vincent Strubel aux Assises de la sécurité des systèmes d'information de Monaco, 11 octobre 2023.

2. Cadre de gestion des risques

En bref

Le cadre de gestion des risques prévu par DORA impose une documentation détaillée précisée ci-après.

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.

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 u**ne séparation adéquate des fonctions** de gestion informatique, des fonctions de contrôle et des fonctions d'audit interne[13].
- Votre SGP doit avoir une **stratégie de résilience numérique**[14], définissant les modalités de mise en œuvre du **cadre de gestion des risques informatiques**[15].
- 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.

À noter : ce 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[16].

13) Art 6.4. 14) Art 6.9. 15) Art 6.1. 16) Art 6.5.

Les nouveautés

DORA intègre de manière exhaustive les exigences à formaliser. Votre cadre de gestion des risques informatiques doit notamment déterminer[17] :

- 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 ;
- des **objectifs claires en matière de cyber-sécurité**, à partager avec 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**.

17) Art 6.8.

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**[18] **et les actifs TIC**[19] : derrière cette terminologie se cache vos données, ainsi que les logiciels et ressources informatiques les supportant. DORA impose de réaliser un schéma des interconnexions, différent des schémas classiques réalisés actuellement par équipe ou par thématique. Le schéma doit être global et permettre une convergence des équipes, par exemple entre équipes IT, équipes achats et le DPO pour la gestion des tiers.

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[20] :

- 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[21] permettant de détecter rapidement les activités anormales[22].

4. LA RÉPONSE

La SGP doit prévoir une « fonction de gestion de crise » afin de gérer les communications internes ou externes[23] selon un plan de communication de crise[24] déterminé et documenté « qui favorise une communication responsable ».

Des tests doivent être effectués au moins une fois par an[25] sen incluant des scénarios de cyber attaques. DORA insiste particulièrement sur les test concernant des fonctions critiques ou importantes externalisées ou sous-traitées[26].

Les SGP doivent tenir un registre des activités[27] facilement accessible, incluant notamment une politique de continuité des activités informatiques[28] 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.

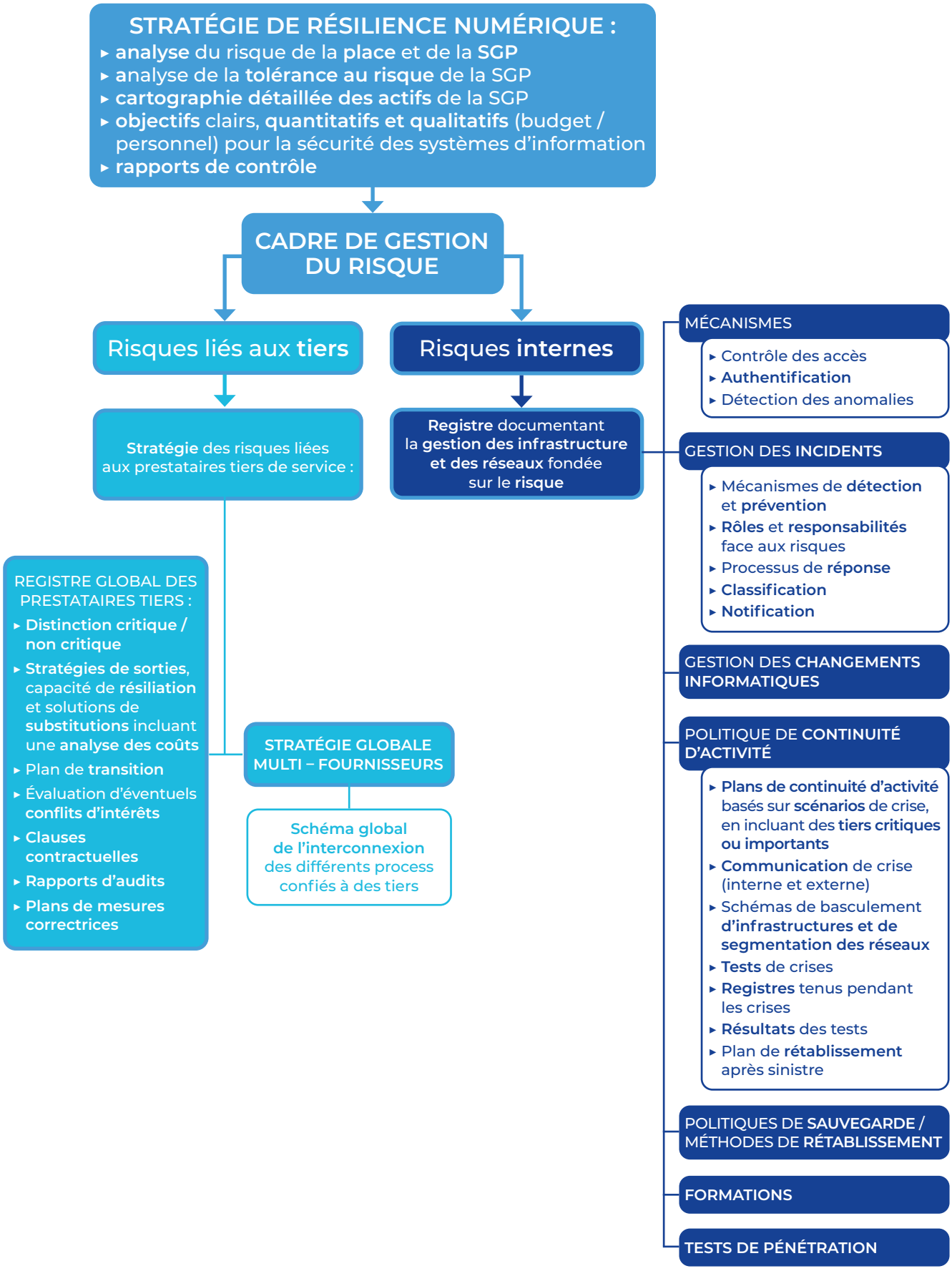
Son existence et sa complétude devraient sans doute faire l'objet de contrôles par les autorités.

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.

18) Art 3.6 : ensemble d'informations, matérielles ou immatérielles, qui justifie une protection. 19) Art 3.7 : un actif logiciel ou matériel dans les réseaux et les systèmes d'information utilisés par l'entité financière. 20) Art 9.4. 21) Art 10.1 et Art 25. 22) Art 17. 23) Art 11.7. 24) Art 11.1. 25) Art 11.7. 26) Art 14. 27) Art 11.6. 28) Art 11.4.

Livrables clés

Cartographie des livrables attendus dans DORA :



3. Catégorisation des incidents

En bref

DORA renforce les exigences quant à la gestion des incidents à travers :

- la mise en place d'un format unifié et consolidé au niveau européen. Cette consolidation doit permettre une vision globale des incidents et détecter les risques systémiques au niveau européen ;
- des notifications au board, aux clients de la SGP et aux autorités compétentes sans délai ;
- la catégorisation des incidents sur base d'une classification propre à DORA sera clé et devra être mise en place dans le cadre d'une procédure intégrant le cas échéant les sous-traitants critiques et importants.

Pour atteindre cet objectif, un renforcement de la qualification des incidents et du monitoring sera nécessaire. L'utilisation d'outils, comprenant des critères précis pourra faciliter le traitement de cette mesure.

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[29].
  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[30].

Les nouveautés

DORA introduit des critères pour déterminer quels incidents sont à qualifier de critiques.

Ces critères seront davantage précisés dans les RTS à publier par les ESAs.
Des normes techniques sont également à venir concernant l'harmonisation des contenus et des modèles des rapports de notification.

- **Les critères de classification** de l'incident incluent[31] :
  - l'impact sur la continuité opérationnelle des services financiers ;
  - 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.

29) Art 17.1. 30) Art 17.3. 31) Art 17.1 (l'article 18 définit les critères de classification des incidents, qui seront précisés par des normes techniques de règlementation).

- **Les incidents majeurs** doivent être notifiés :
  - au board[32], 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[33] ;
  - **aux autorités selon 3 phases :**
    - **une notification initiale immédiate**
    - **un rapport intermédiaire au plus tard après une semaine**
    - **un rapport final lorsque l'analyse des causes profondes est réalisée[34].**

Les challenges

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

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, effectuée **dès que possible**, des rapports réguliers doivent être transmis pendant 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.

Il convient de commencer à concevoir votre organisation pour à la gestion des incidents.

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 apporteront des précisions quant aux informations à fournir s'agissant des :

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

Ces précisions devraient permettre une homogénéisation des critères et reporting avec d'autres exigences existantes (CNIL, BCE, etc.).

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

32) Art 18.1. 33) Art 19.3. 34) Art 19.4.

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.

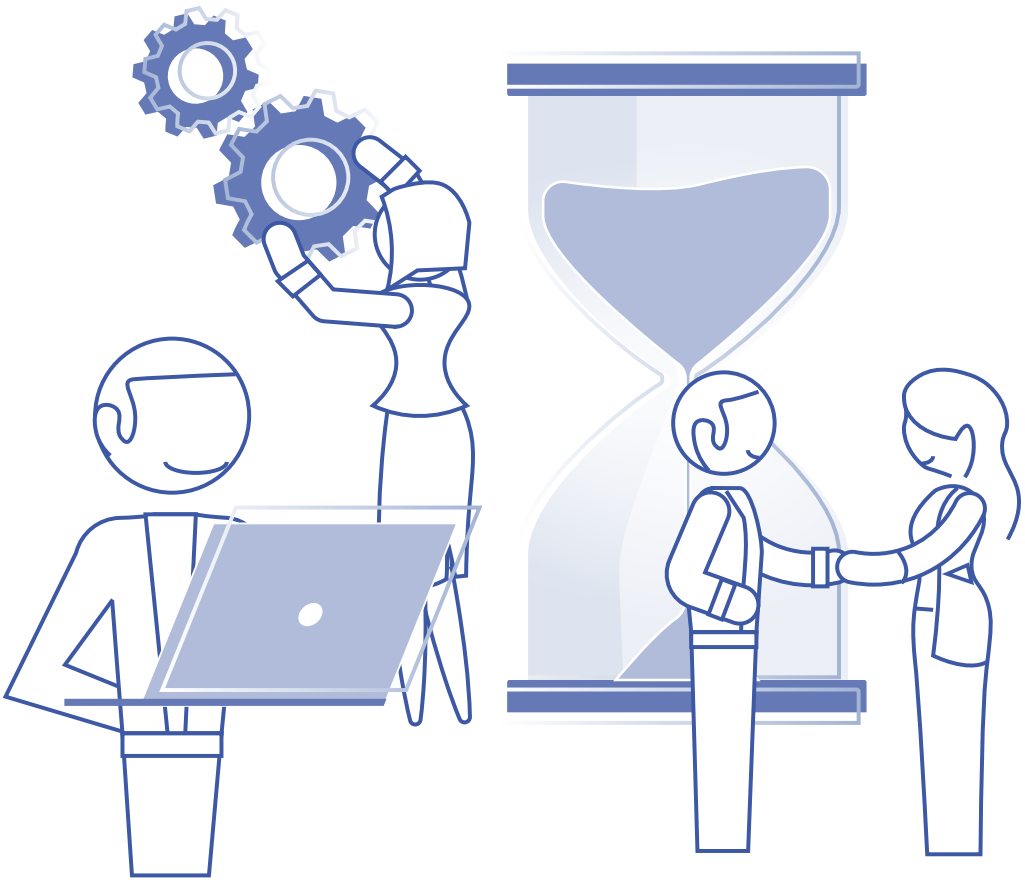
Votre board, en se trouvant pleinement impliqué dans la gestion d'incidents, va accroître sa visibilité.

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.

La connaissance et validation par votre board des process et sous-traitants critiques de votre SGP sont également importantes.

Livrables clés

- Un processus de gestion des incidents informatiques qui doit inclure[35] :
  - 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.



35) *Art 17.3.*

4. Test 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'agira 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[36] 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[37] 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[38].

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.

36) L'article 24.1 exclut d'ailleurs les micro-entreprises du programme de tests de résilience imposé.37) Article 25.1 pour la liste exhaustive.
38) Art 24.4.

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

Les challenges

Tester au moins une fois par an, tous les systèmes et applications de TIC qui soutiennent des fonctions critiques ou importantes à des tests appropriés, ce qui inclut des 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[39].

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

Les SGP doivent effectuer au moins tous les trois ans des tests avancés au moyen d'un test de pénétration fondé sur la menace *(TLPT : threat led pentest)*. Les TLPT doivent couvrir plusieurs ou la totalité des fonctions critiques ou importantes.

L'AFG vous recommande de vous appuyer sur cette analyse de la menace pour alimenter votre cartographie des risques, programme de cyber résilience et training de votre board.

Ces 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 au test, 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.

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.

39) *Art 27.*

5. Management des tiers

En bref

Les SGP doivent bien 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 elle 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 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**[40].

Les nouveautés

DORA rend impératives :

a. La mise en place d'une gouvernance permettant une supervision et un pilotage appropriée de la relation avec l'ensemble des prestataires.

b. La définition et 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[41].

40) Art 6.9. 41) Art 3.22.

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

a. Tenue d'un **registre d'information des engagements contractuels** au niveau de l'entité mais aussi consolidé par organisation, ce registre doit notamment contenir[42] :
   - 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 de 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 (le RGPD sur lequel DORA insiste notamment, la législation en matière d'insolvabilité et relative à la récupération des données)[43] ;
   - pour les tiers soutenant des fonctions critiques ou importantes, des stratégies de sorties[44] 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 aux autorités compétentes** des projets contractuels de **service TIC supportant des fonctions critiques ou importantes**.

c. Un contrat unique définissant les droits et obligations du prestataire tiers de services TIC et de la SGP[45] incluant des clauses renforcées pour les services TIC soutenant des fonctions critiques ou importantes[46].

À noter : des normes techniques à venir apporteront des modèles types pour le registre d'information, la stratégie multi-fournisseurs, la politique de gestion des accords contractuels ainsi que les éléments qu'une SGP doit déterminer et évaluer lorsqu'elle sous-traite des fonctions critiques.

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. **Prendre en considération les cas de sous-traitance en cascade :** si les accords prévoient la possibilité qu'un prestataire sous-traite un service TIC alors l'entité intègre ce facteur dans son analyse de risque et référence l'utilisation de ce sous-traitant. Le nombre de degrés de sous-traitance à superviser sera clarifié, pensez à encadrer a minima vos exigences dans des clauses adaptés.

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

Il est important que les SGP de veiller à ne conclure **d'accords contractuels** qu'avec des p**restataires** tiers de services TIC **qui respectent des normes adéquates** en matière de sécurité de l'information.

Pour les prestataires fournissant des services critiques et important, les entités financières doivent prendre en considération, **avant la conclusion des accords**, l'utilisation par les prestataires tiers de services TIC des normes les plus actualisées.

DORA précise par ailleurs les conditions pouvant déclencher la résiliation de la prestation.

42) Art 28.4 et 28.5. 43) Art 29.2. 44) Art 28.8. 45) Art 30.1. 46) Art 30.3.

Pour les prestataires supportant des services critiques ou importants : il est nécessaire de prévoir les stratégies de sortie afin de garantir la continuité d'activité des fonctions critiques ou importantes supportées par lesdites prestations TIC. Un grand nombre de contrats historiques n'intègrent pas cette exigence, pensez à y remédier.

Clé pour le board

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

Il est important que le board soit avisé que l'ensemble des nouveaux contrats intègre bien ces nouvelles exigences et organise un plan de revue de l'existant en vue d'une mise en conformité à horizon 2025.

Les ESAs désigneront les prestataires TIC critiques ou importants qu'elles placeront sous leur surveillance en leur imposant des exigences accrues de sécurité, ce qui va impacter positivement le niveau de maturité de ces prestataires.

Livrables clés

- Registre des tiers.
- Politique relative à l'utilisation des services informatiques qui soutiennent des fonctions critiques ou importantes fournis par des tiers[47] et registre d'information incluant tous les accords contractuels.
- Plan stratégique de sortie.
- Schéma global de l'interconnexion avec des tiers qui soutiennent des fonctions critiques ou importantes.[48]

47) Art 28.2 . 48) Art 8 .

6. 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 cyber sécurité 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), Clément Civeit (Moneta), Bruno Ducamp (Syquant), Walif El Hitti (Comgest), Mohamed Ghayati (Tikehau), Frederic Gleizer (BNPP AM), Stéphane Graux (Ostrum Asset Management), Alexandre Joachim (LBP AM), 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.

L'AFG fédère les professionnels de la gestion d'actifs depuis 60 ans,

au service des acteurs de l'épargne et de l'économie.

- Elle se mobilise pour la gestion d'actifs et **sa croissance**.
- Elle définit des **positions communes**, qu'elle porte et défend auprès des pouvoirs publics.
- Elle contribue à l'émergence de **solutions bénéfiques à tous les acteurs** de son écosystème.
- Elle s'engage, dans l'intérêt de tous, **à favoriser le rayonnement** de l'industrie, en France, en Europe et au-delà.
- Elle s'investit pour **l'avenir**.

AFG
Ensemble, s'investir pour demain.

AFG
Ensemble, s'investir pour demain

Publication réalisée par le département Expertises

- Valentine Bonnet, Directrice Gouvernement d'entreprise et Conformité
  v.bonnet@afg.asso.fr | 01 44 94 94 32

41 rue de la Bienfaisance | 75008 Paris | T : +33 (0)1 44 94 94 00
Avenue des Arts 44 | 1000 Bruxelles

www.afg.asso.fr