Q&A DORA

Le présent Q&A DORA est destiné à compéter les réponses apportées fin 2024 à l'occasion du *Point sur la cybersécurité* organisé par l'AFG afin de répondre aux attentes de ses membres souhaitant bénéficier d'un éclairage sur certains points dans la perspective de l'entrée en vigueur de la réglementation DORA.

Incidents - 1 : Quels incidents notifier à l'AMF ? Toutes les tentatives de phishing reçues doivent-elle être qualifiées comme "incidents" et être notifiées, étant donné que des phishings peuvent être détectés et déjoués sans qu'il y ait d'« incident » impactant la société de gestion ?

Il convient de se référer à l'article 3.8 de DORA qui définit l'incident lié aux TIC comme « un événement ou une série d'événements liés entre eux que l'entité financière n'a pas prévu qui compromet la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'entité financière ». Dès lors sur la base de ce texte, la tentative n'apparait pas couverte par une obligation de déclaration.

Pour aller plus avant, on distingue deux catégories d''incidents :

- les incidents classés comme majeurs (RTS 2024 - 1772) à déclarer obligatoirement aux autorités nationales,
- les incidents non classés comme majeurs (par exemple tentatives échouées) dont la transmission n'est pas obligatoire mais encouragée, notamment en cas de répétitions.

A noter à titre illustratif, que des tentatives de phishing visant un même service, ou une même personne, même bloquées peuvent être annonciatrices d'une volonté de pénétrer une partie de l'organisation et donc porteuse d'un risque plus grand.

Beaucoup de systèmes automatiques dont on dispose aujourd'hui déjouent les tentatives de phishing génériques dont on ne verra pas la majeure partie. En revanche l'usurpation d'identité avérée d'un dirigeant ou d'un collaborateur est à signifier parce qu'annonciatrice d'une attaque potentielle plus sophistiquée.

Un incident cyber même non majeur ayant un impact opérationnel est à remonter.

On distingue 3 types d'incidents, comme le rappelle la synthèse des contrôle SPOT cybersécurité n°2 :

- Les tentatives de détournement d'authentifiants individuels ou phishing :
  Ces tentatives de phishing non ciblées cherchent à obtenir des premiers accès, ensuite exploités par d'autres : l'incident, de nature combinatoire, peut démarrer par un phishing large afin de pénétrer les messageries. L'attaque sera ensuite répétée, soit au sein de l'entité, soit en visant l'ensemble des contacts de la personne dont la boîte mail a été contaminée.
  A noter que ces attaques, lorsqu'elles se propagent sont de nature à engendrer un risque d'image, la victime étant amenée à prévenir tous ses contacts, ainsi qu'un risque technique de mise en quarantaine par les fournisseurs de services de lutte anti-spam en cas d'attaques répétées, l'adresse (assimilée à un bot frauduleux) se trouvant bloquée.

Les mesures de protection prennent différentes formes : authentification forte, revue régulière des règles de transfert automatique, vérification de l'authenticité des messages par rapport aux noms de domaine.

- Les tentatives de détournement de fonds
  Ce sont des attaques de plus en plus évoluées dans lesquelles les pirates parviennent à s'infiltrer sur des boites mails de personnes clés afin de glaner des informations sur les flux d'affaires, clients, montants d'affaires, dates et vont pouvoir déclencher une attaque, par exemple en tentant de s'interposer, via un IBAN frauduleux, sur un appel de fond.
- Les tentatives de récupération de données à caractère personnel commercial ou stratégique dans le but de les revendre, notamment sur le Darknet.
  A noter des cas d'attaques non techniques pouvant passer par des insiders (par exemple un stagiaire ou un prestataire externe disposant d'accès étendu) qui vont utiliser leurs accès pour télécharger des données et les transmettre par exemple vers un cloud externe. Il est possible de s'en protéger par des procédés techniques comme les DLP (*data loss prevention*) qui permettent d'identifier en amont des téléchargements ou des transferts de données massifs.

Incidents - 2 : Quel est le niveau de formalisme attendu en matière de remontée des incidents pour les SGP microentreprises ? Est-il possible d'utiliser un fichier Excel plutôt qu'un workflow tool dédié ?

La remontée des incidents majeurs est attendue de la part de l'ensemble des SGP. Dans un but de facilitation, les SGP pourront utiliser Excel via un outil de conversion disponible sur le site de l'EBA ou utiliser le format JSON.

Incidents – 3 : En cas sinistre important, lorsqu'il n'y a plus de système d'information, comment faire pour remonter l'incident ?

Il convient de contacter son correspondant usuel au sein de l'Autorité.

Incidents – 4 : Pour les SGP ayant une présence internationale et un système d'information centralisé, un incident majeur central peut impacter de nombreuses entités. La SGP peut-elle notifier uniquement au régulateur de l'entité centrale (pour diffusion « intra régulateurs ») ou doit-elle diffuser le même reporting à tous les régulateurs ?

Chaque succursale ou filiale de la SGP devra notifier à chacune des autorités compétentes locales.

C'est la préparation qui permet d'anticiper un mécanisme de diffusion adapté.

A noter que le RTS sur la classification des incidents comprend un critère qui concerne le nombre de pays impactés par l'incident.

Audit, contrôles et proportionnalité - 5 : Existe-t-il un corpus documentaire procédural attendu pour répondre aux exigences de la règlementation DORA ? Certains régulateurs à l'international commencent à solliciter les SGP sur divers éléments, quelle serait votre grille d'attente ?

Il n'y a pas de grille à plaquer indifféremment sur toute entité quelle que soit son organisation, sa date d'agrément, son activité. L'appréciation de la conformité à DORA va se faire en prenant en considération des risques, un contexte, une activité, une organisation et des moyens.

L'article 21 du RTS Risk Management Framework, qui vient préciser les éléments attendus a minima, mentionne un certain nombre de points à faire figurer dans le corps procédural (principes de sécurité, sécurité des réseaux, résilience opérationnelle, gestion des incidents d'origine cyber, charte informatique).

Il est attendu que la politique générale de sécurité de la SGP fixe les grands principes, mentionne les zones principales du système d'information que l'on sécurise, comment on les sécurise, qui les sécurise. Une charte informatique ayant pour finalité d'embarquer les collaborateurs derrière la notion de responsabilité de chacun, d'usage raisonnable et sécurisé du matériel informatique, une procédure de gestion des accès (qui les affecte, les valide, les contrôle, les supprime) est également à prévoir.

Les procédures doivent englober la gestion des incidents cyber et la gestion des changements informatiques. On peut également penser à une procédure d'exploitation informatique (incluant par exemple la sauvegarde et les tests de restauration), une procédure de sélection et de contrôle des prestataires informatiques, une procédure d'administration informatique. Des recoupements sont bien entendu possibles entre ces documents.

En matière de procédures attendues, on peut se référer utilement aux synthèses des contrôles SPOT AMF publiées en 2019, 2020 et 2023, accessibles sur le site internet de l'AMF.

Il est crucial que l'objectif de résilience prime sur une simple visée de conformité.

Audit, contrôles et proportionnalité - 7 : Quelle mise en œuvre en pratique pour les SGP du principe de proportionnalité mentionné à l'article 4 de DORA ?

Le principe de proportionnalité, consacré par l'article 4 de DORA, intègre les notions de taille, de profil, de risque global ainsi que la nature, de l'ampleur et la complexité des activités.

Toutefois les cyberattaques peuvent cibler à la fois grandes et petites SGP, avec des conséquences pouvant être désastreuses indépendamment de la taille de l'acteur, il convient donc que toutes les entités intègrent le risque cyber.

Un PCA bien fait, en intégrant les systèmes d'information internes et externes, prestataires informatiques, constitue une bonne base.

Dans cette approche, la cartographie des systèmes d'information des prestataires et des données sensibles est essentielle. Au regard des zones de risque identifiées comme plus importantes, la SGP va établir ses priorités en fonction des moyens dont elle dispose.

De manière pragmatique, il convient de ne pas plaquer aléatoirement de moyens en cybersécurité sans finalité précise : DORA demande d'identifier ce qu'on appelle les fonctions critiques ou importantes.

Prestataires TIC - 8 : L'AMF pourrait-elle apporter des précisions quant aux prestataires à inclure dans le scope des prestataires tiers de services TIC de DORA ?

a. Quid des dépositaires et valorisateurs (ex : dépositaire fournissant une interface numérique pour sa prestation de fund administration / dépositaire, comme OLIS) ?

b. Quid des fournisseurs de données (Morninstarg, Reuters, fournisseurs de données ESG …) ?

c. Quid du prime broker qui fournit une plateforme de réconciliation ?

d. Quid des OMS (Aladdin, Alto, etc) ?

L'ensemble des acteurs ci-dessus mentionnés sont inclus parmi les prestataires tiers de services TIC entrant dans le scope de DORA.

De façon pratique, il convient pour la SGP d'agir en 3 temps :

- En 1er lieu - Etablir une cartographie de ses prestataires informatiques (l'analyse faite dans le cadre du PCA constituant un bon point de départ.
- En 2ème - Vérifier les contrats existants.
- En 3ème - Si des clauses dans les contrats s'avèrent manquantes, ouvrir des négociations avec le prestataire.

Du point de vue du pilotage des prestataires informatiques, DORA ne révolutionne pas les choses par rapport à la règlementation domestique existante, elle fournit cependant une grille de travail permettant de mieux structurer les relations contractuelles.

L'AMF invite les SGP à entamer ces démarches en commençant par les plus sensibles, s'agissant d'un sujet épineux.

Si certains prestataires refusent d'intégrer ces clauses, il convient pour les SGP d'en informer son autorité de tutelle.

S'agissant des CTTP (*critical IT third-party providers*), DORA prévoit une supervision en direct par les ESAs.

Dora ne révolutionne pas les choses mais apporte une grille, une structuration permettant de mieux encadrer les relations contractuelles

Chaque SGP va ainsi, pour chacun de ses prestataires, identifier le caractère critique/important qu'il a ou non pour son activité, afin d'en tirer les conséquences qu'il convient

Il convient de bien distinguer :
- le prestataire important/critique du point de vue de la SGP
- du CTTP qui est un prestataire considéré comme critique d'un point de vue systémique et qui fera l'objet dans ce cadre d'une supervision directe par les ESAs.

Prestataires TIC - 9 : Quels seraient les critères à appliquer pour déterminer si des prestataires TIC sont critiques/ importants ?

a. Les grands acteurs US (Bloomberg…) auxquels recourent les SGP entrent-ils dans la catégorie des prestataires critiques ?

b. Un prestataire qui vend une solution critique est-il à considérer comme un prestataire critique (cf. revente de licences uniquement) ? Ou est-ce l'éditeur de la solution qui a qualité de prestataire critique ? Ou les 2 ?

c. Certains prestataires peuvent-ils être considérés comme critiques par certaines filiales d'un groupe financier, et non critiques par d'autres filiales ?

d. Un outil qui permet de gérer des reportings est-il critique (reporting EMIR…) ?

La question à se poser est la suivante : Ce prestataire est-il important/critique pour l'activité de ma SGP ainsi que pour la protection de la disponibilité, de l'intégrité, de la confidentialité et de la traçabilité des données de mon système d'information ?

Ce travail va déboucher sur une cartographie des prestataires importants et critiques, qui va permettre à la SGP de leur associer le dispositif de sécurité qui convient, en fonction de niveaux et des zones de risque.

En réponse à la question a) : Pour ce qui est des grands acteurs US auxquels recourent les SGP, typiquement les fournisseurs de données, la SGP doit se poser la question de savoir si elle peut continuer son activité sans eux.

En réponse à la question b) : S'agissant de la société qui ne fait que vendre une licence d'un logiciel qu'elle n'a pas développé, on pourrait considérer qu'il ne s'agit pas d'un prestataire critique.

L'article 31 de DORA fournit un certain nombre de critères d'identification des CTPP.

En réponse à la question d) : S'agissant des reportings EMIR, AIFM ou MMF, l'examen à faire par la SGP doit tenir compte du plus ou moins grand morcellement de la chaîne de production. Certaines chaînes sont très simples, passant par de l'Excel en interne, d'autres sont très morcelées : c'est à la SGP de distinguer, sur chacune des étapes de production des reporting, ce qui critique de ce qui ne l'est pas et mettre en regard les processus.

La période où le système d'information pourrait ne pas être opérationnel doit être anticipée au niveau du PCA. Ce dernier doit intégrer en effet le délai acceptable 1 d'interruption des outils utiles à la production des reportings. Ce délai est à évaluer par chaque SGP en fonction de ces moyens, de son appréciation du risque et des processus requis pour redémarrer.

Prestataires TIC - 10 : Quand la liste des CTPPs fera -t-elle l'objet d'une publication par les ESAs ?

Les ESAS vont effectuer un travail d'identification des CTPPs en s'appuyant sur les registres d'information qui seront remontés.

[1] *Recovery time objective* (RTO).

Pour l'identification des CTTPs qui feront l'objet d'une supervision, l'article 31-2 DORA donne un certain nombre d'éléments à prendre en considération. Ces éléments seront précisés dans le RTS *on subcontracting ICT services supporting critical or important functions* et dans l'ITS concernant le registre.

La date de publication de la liste des CTTPs par les ESAs n'est pas encore certaine, probablement 2025. A terme, la supervision directe des CTPP par les ESAs devrait constituer un atout pour les SGP dans la perspective de la mise en conformité avec DORA s'agissant du pilotage des prestataires.

Prestataires TIC - 11 : DORA prévoyant explicitement la fourniture de clauses types par les autorités, l'AMF pourrait-elle obtenir des instances européennes que soit ainsi facilitée l'appréhension par les petites SGP des liens contractuels à établir avec les prestataires de services TIC ?

L'AFG souligne qu'il serait souhaitable dans un but de facilitation de la mise en œuvre de DORA par les acteurs que la Commission européenne, comme elle a pu le faire pour un autre règlement européen (le RGPD), fournisse des clauses types aux acteurs pour DORA, l'article 30.4 de DORA faisant mention de clauses contractuelles type élaborée par les autorités publiques.

Face au refus de prestataires de voir figurer une clause DORA au contrat, les SGP pourront d'abord leur faire un rappel de l'article 30 de DORA, puis, dans un deuxième temps, notifier aux autorités nationales ceux de ses prestataires importants/critiques qui refusent. De même, en serait-il en cas de refus ultérieur de mise en œuvre de la clause.

On pourrait également envisager, pour contrebalancer l'effet pot de terre contre pot de fer, que plusieurs SGP utilisant le même service d'un même prestataire s'unissent pour demander ensemble un audit mutualisé du service du prestataire réalisé par un tiers qualifié indépendant, par exemple le biais d'une association professionnelle (refuser un audit collectif sera sans doute plus difficile pour un prestataire).

Mise en œuvre de la réglementation - 12 : Est-il exact que, s'agissant de DORA, à ce jour la Commission européenne a publié deux règlements délégués et trois RTS ITS et que six autres RTS ITS restent à être officiellement publiés, sachant que DORA entre en application le 17 janvier ?

C'est exact. Il convient de se référer au site webgate.ecec.europa.eu qui liste les textes qui ont été publiés.

Mise en œuvre de la réglementation - 13 : Est-il exact que les CIF n'entrent pas dans le périmètre de DORA ?

C'est exact, les CIF n'entrent pas dans le périmètre de DORA à l'exception des « CIF MiCA » (qui disposeront d'un agrément de PSAN de prestataire de services en actif numérique.

Mise en œuvre de la réglementation - 14 : Une SGP doit-elle nécessairement mettre en place des process dédiés et/ou prendre ceux du groupe auquel elle appartient (groupe bancaire) ?

Les SGP présentant des risques (notamment sur le périmètre de la cybersécurité) différents de ceux de leur société mère bancaire, il est attendu que le dispositif de sécurité du groupe bancaire soit a minima challengé par les décideurs de SGP pour décider ce qu'ils en retiennent et ce qu'ils ne retiennent pas en fonction des spécificités de l'activité.

Mise en œuvre de la réglementation - 15 : Comment articuler DORA avec la mise en application des Orientations ESMA sur les prestataires cloud ?

L'ESMA procède actuellement à une « gap analysis » entre les obligations liées à DORA et celles résultant des Orientations ESMA sur les prestataires cloud. Il convient de noter que la philosophie concernant les Orientations ESMA sur les prestataires cloud ne diffère pas de manière importante de celle de DORA. Les prestataires cloud étant un type de prestataire informatique, ceux-ci seront soumis de facto à DORA.

Mise en œuvre de la réglementation - 16 : Comment mettre en œuvre DORA au niveau d'une SGP dont la fonction IT/gestion du SII se trouve intégralement déléguée au niveau de la maison mère (service intragroupe) ?

DORA est clair sur la responsabilité des dirigeants de la société de gestion dans la validation de la stratégie de cybersécurité. Le dirigeant a pour responsabilité de s'enquérir sur la stratégie de cybersécurité proposée par la maison mère, de la challenger à l'aune de ses besoins et de sa cartographie des risques et ensuite de prévoir les adaptations nécessaires. La délégation n'exclut pas le contrôle.

En conclusion :

- **DORA est plus une évolution qu'une révolution.**
- **DORA n'invente rien mais a le mérite de structurer des règles de manière à en accroître la lisibilité pour l'ensemble des acteurs y compris les non spécialistes.**
- **On protège bien ce que on connaît bien : avant toute démarche, tout achat, tout test, la première étape la plus importante est de réaliser une cartographie du système d'information, des données sensibles et des prestataires informatiques. Il convient de poser les bases de ce que l'on souhaite protéger en priorité. Le PCA, obligation règlementaire, constitue dans ce cadre un bon point de départ.**
- **DORA doit conduire notamment à ce que les comités de direction s'approprient davantage des sujets qui étaient parfois enfouis dans l'organisation.**
- **En visant à améliorer le niveau de cybersécurité et de résilience de l'ensemble des SGP, il doit en résulter un bienfait pour la place financière européenne.**

L'Association Française de la Gestion financière (AFG) représente et promeut l'utilité de la gestion d'actifs pour l'avenir de notre pays. Elle regroupe **plus de 440 membres**, dont 340 sociétés de gestion, qui gèrent **90 % des encours sous gestion en France**.

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.

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

Site https://www.afg.asso.fr/fr/