AFG

LePointsur

Cybersécurité :

Règlement DORA : - de 100 jours avant l'échéance, l'AMF répond à vos questions

Vendredi 18 octobre 2024
9h00-11h00

AVERTISSEMENT

L’intervention des intervenants est proposée à titre d’information ou d’exemple pour présenter aux participants une pratique du marché applicable, une innovation en matière de technologie ou d’organisation. Cette présentation n’est pas une incitation pour les participants à utiliser les services des intervenants ou des sociétés pour lesquels ils travaillent, ni une offre commerciale.

L’AFG ne garantit pas la conformité règlementaire de cette proposition.

Aussi il appartient à chaque participant :

- de vérifier cette conformité au regard de sa situation propre
- de s’assurer que les propositions présentées sont adaptées à sa situation en vérifiant notamment si sur le marché d’autres offres sont plus pertinentes au regard de sa situation.

Cybersécurité : DORA : - de 100 jours avant l'échéance

AFG

LePointsur

Introduction

Laure Delahousse
Directrice générale de l'AFG

Cybersécurité - **DORA :**

- de 100 jours avant l'échéance, l'AMF répond à vos questions

René Amirkhanian
RSSI, DCNA Investment

Bruno Buresi
Adjoint à la Directrice des contrôles des SGP et des CIF de l'AMF

Valentine Bonnet
Directrice Gouvernement d'entreprise et Conformité, en charge du GT cybersécurité de l'AFG

Wilfried Lauber
Président du GT Cybersécurité de l'AFG et RSSI adjoint d'Amundi

Table ronde

AFG

LePointsur

Cybersécurité : DORA : - de 100 jours avant l'échéance

AFG

LePointsur

N'hésitez pas à poser vos questions aux orateurs sur la plateforme

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Incidents - QUESTION 1 :

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 n'y ait d' "incident" impactant la société de gestion ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Incidents - QUESTION 2 :

Quels sont les incidents que l'AMF s'attend à se voir notifier ?

TYPES D'INCIDENTS D'ORIGINE CYBER CONSTATÉS CHEZ LES SGP (SYNTHÈSE SPOT DE L'AMF, 2021) - 1/3

Tentative de détournement d'authentifiants individuels ou *phishing*

- Accès aux données des collaborateurs ciblés, puis usurpation de leur identité pour reproduction du scénario sur d'autres cibles
- Envoi d'un courriel infecté à l'ensemble des contacts de la cible initiale.
- Fort impact d'image car la victime est amenée à prévenir tous ses contacts de l'attaque réussie.
- Risque de mise en quarantaine (en cas d'attaques répétées) par les fournisseurs de services de lutte *anti spam*.
- Remédiation : authentification forte, revue des règles de transfert automatique, vérification de l'authenticité des messages/noms de domaine

TYPES D'INCIDENTS D'ORIGINE CYBER CONSTATÉS CHEZ LES SGP (SYNTHÈSE SPOT DE L'AMF, 2021) - 2/3

Tentatives de détournement de fonds

Nécessite une connaissance approfondie des flux d'affaires de la cible (afin de crédibiliser les conditions de l'attaque) passant par :

- une intrusion réussie sur une ou plusieurs boîtes emails internes stratégiques ainsi que par,
- une phase d'écoute de plusieurs mois des échanges transitant par ces boîtes.

Plusieurs typologies de fraudes constatées rappelant l'importance du contre-appel systématique

- au président
- au client
- au dépositaire (tentative d'interposition sur un appel de fonds)
- au teneur de compte conservateur

TYPES D'INCIDENTS D'ORIGINE CYBER CONSTATÉS CHEZ LES SGP (SYNTHÈSE SPOT DE L'AMF, 2021) - 3/3

Tentatives de récupération de données à caractère personnel, commercial ou stratégique

Intrusions au sein :

- de dépôts de code applicatif (ex : extranet) afin d'y identifier des vulnérabilités et de les exploiter ultérieurement,
- d'infrastructures cloud hébergeant les données ciblées, par exemple via la récupération d'identifiants techniques de service.

Objectifs : extorsion, usurpation d'identité, sabotage, revente de données, espionnage économique.

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Incidents - QUESTION 3 :

Quel est le niveau de formalisme attendu pour les SGP microentreprises en matière de remontée des incidents?

Est-il possible d'utiliser un fichier Excel plutôt qu'un *workflow tool* dédié ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Incidents - QUESTION 4 :

Pour les SGP avec 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-on diffuser le même reporting à tous les régulateurs ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Audit, contrôles et proportionnalité - QUESTION 5 :

Existe-t-il un corpus documentaire procédural attendu de l'AMF pour répondre aux exigences de la règlementation DORA ?

Certains régulateurs à l'international commencent à solliciter les SGP sur divers éléments : quelles serait votre grille d'audit ou d'attente ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Audit, contrôles et proportionnalité - QUESTION 6 :

Comment appliquerez-vous le principe de proportionnalité au sein des SGP lors de vos audits ou contrôles ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Audit, contrôles et proportionnalité - QUESTION 7 :

Quelle mise en œuvre en pratique pour les SGP du principe de proportionnalité mentionné à l'article 4 du règlement DORA?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Les prestataires TIC - QUESTION 8 :

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

Question 8 : L'AMF pourrait-elle apporter des précisions quant à la désignation de prestataires tiers de services TIC à inclure dans le scope 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, etc, données ESG?

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

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

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Les prestataires TIC - QUESTION 9 :

Quels seraient les critères à appliquer pour déterminer si des prestataires TIC sont critiques ou importants ?

Question 9 : Quels seraient les critères à appliquer pour déterminer si des prestataires TIC sont critiques ou importants ?

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

b. Est-ce qu'un prestataire qui vend une solution critique est considéré comme un prestataire critique (cf. revente de licences uniquement) ? Ou est-ce l'éditeur de la solution qui est prestataire critique ? Ou les 2 ?

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

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

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Les prestataires TIC - QUESTION 10 :

Quand la liste des CTPP fera-t-elle l'objet d'une publication par les ESAs ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Les prestataires TIC - QUESTION 11 :

DORA prévoit explicitement la fourniture de clauses types par les autorités, l'AMF peut-elle obtenir des ESAs que soit ainsi facilitée l'appréhension par les petites SGP des liens contractuels à établir avec les prestataires de services TIC ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Les prestataires TIC - QUESTION 12 :

Dans le cadre de refus d'audit d'un prestataire, que peut faire une SGP ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Mise en œuvre de la règlementation - QUESTION 13 :

Est-il exact que, s'agissant de DORA, à ce jour la Commission Européenne a publié 2 règlements délégués et 3 RTS/ITS, et que 6 autres RTS/ITS restent à être officiellement publiés pour rentrer en application ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

Mise en œuvre de la règlementation - QUESTION 14 :

Est-il exact que les CIF n'entrent pas dans le périmètre de DORA ?

CYBERSÉCURITÉ : DORA : - DE 100 JOURS AVANT L'ÉCHÉANCE

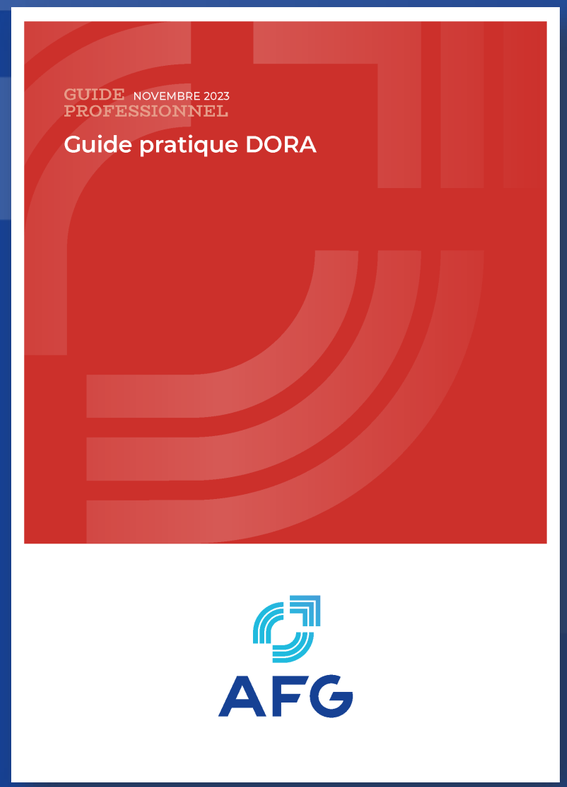
Mise en œuvre de la règlementation - QUESTION 15 :

Une SGP doit-elle nécessairement mettre en place des process dédiés et/ou prendre ceux du groupe auquel elle appartient (groupe bancaire) ?

Publications du GT cybersécurité AFG

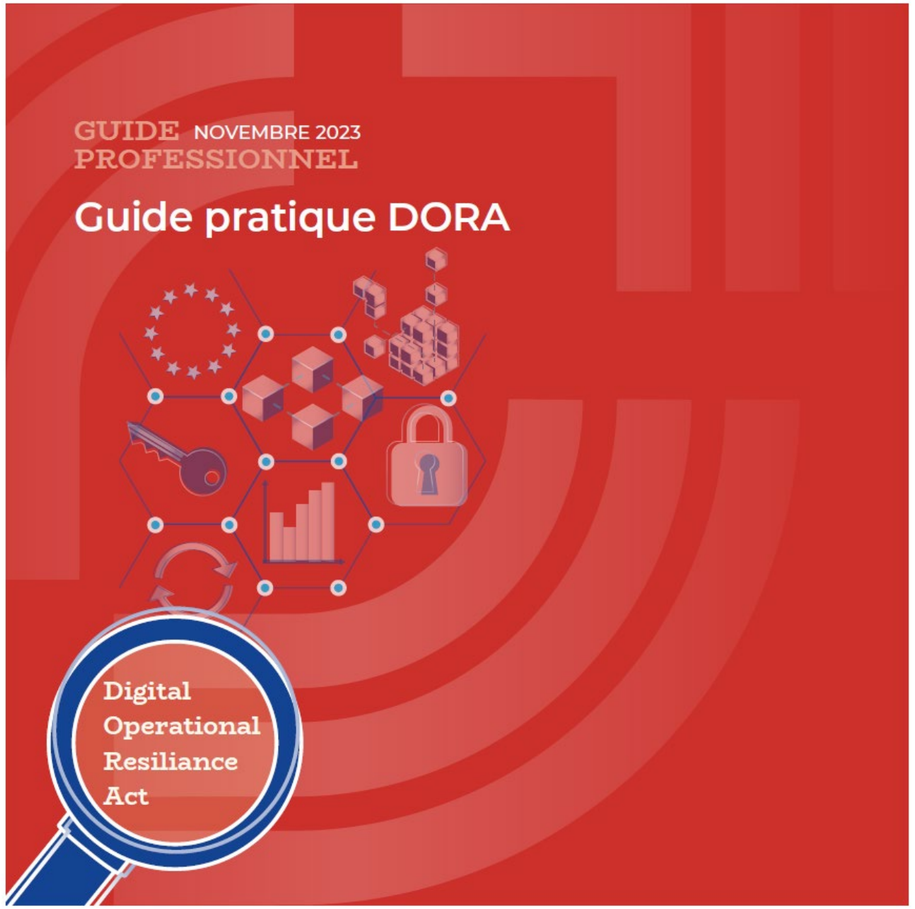
disponibles sur le site AFG

PUBLICATION 2023



AFG

STRUCTURE DU GUIDE



6 chapitres, 4 sections récurrentes

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 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 potentiellement longues ou complexes.

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".

AFG

Cybersécurité : DORA : - de 100 jours avant l'échéance

AFG

LePointsur

Rappel :

La vidéo de cette conférence, les slides et les documents cités seront disponibles prochainement sur le site de l'AFG

Ensemble,
s’investir pour demain

Merci !

AFG