Le règlement DORA et la mise en place d'un cadre de résilience opérationnelle numérique

- Retour sur les contrôles cyber menés par l'AMF
- Le règlement DORA et son impact sur les activités de supervision de l'AMF
- Les différents textes de niveau 2 et 3 à venir

Autorité des Marchés Financiers

Direction de la Régulation et des Affaires Internationales

Division Innovation & Finance Digitale (IFD)

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

RETOUR D'EXPÉRIENCE SUR LES CONTRÔLES CYBER MENÉS PAR l'AMF

Contrôles SPOT de 2019 et 2020 sur les SGP

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

UNE VINGTAINE D'INCIDENTS RAPPORTÉS DEPUIS 2020 (SGP)

Des schémas d'attaque récurrents pour des objectifs variés

- ☐ Détournement d'authentifiants individuels (par phishing ou autre vecteur)
  - → À partir du compte de messagerie Cloud d'une personne clé de l'entité (Président, DG, RCCI/RCSI)
  - → Suivi d'une tentative de phishing envoyée à tout le carnet de contacts de cette personne (dont l'AMF)
  - → Tentative de collecte des authentifiants des contacts de la personne piégée initialement
  - → Usage des données collectées pour insérer un logiciel malveillant sur le poste de travail et le SI des victimes
- ☐ Usurpation d'identité de personnes morales ou physiques
  - → Fraude auprès de /en tant que : personne clé de l'entité (client, fournisseur, dépositaire, conservateur)
  - → Exemple : via la création d'adresses email utilisant un nom de domaine visuellement proche de celui de l'entité légitime
- ☐ Accéder à, puis éventuellement divulguer, des informations professionnelles ou personnelles précises
  - → Exemple : mise en place, au sein de boites emails, de règles de redirections automatiques et silencieuses vers des adresses emails maitrisées par l'attaquant (actives pendant une période de plusieurs mois)
- ☐ Intrusion puis compromission du système d'information, puis par exemple exécution d'un rançongiciel
  - → Détournement de fonds, extorsion (Exemple : Interposition lors d'appels de fonds)

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

RETOUR D'EXPERIENCE SUR LES CONTRÔLES À COMPOSANTE CYBER MENÉS (SGP)

Deux vagues de contrôles SPOT réalisées auprès de SGP dans le cadre d'une priorité de supervision, avec le support de l'équipe cyber interne

☐ En 2019, sur les thèmes :

- → Organisation et gouvernance du dispositif cyber
- → Administration et surveillance du SI
- → Cartographie des données sensibles
- → PCA
- → Dispositif de contrôle interne
- → **Sans réalisation de tests techniques**

☐ En 2020, sur les thèmes :

- → Organisation et gouvernance du dispositif cyber
- → Gestion des incidents d'origine cyber
- → Pilotage des fournisseurs IT critiques
- → Processus d'accès à distance au SI (contexte covid)
- → **Avec réalisation de tests techniques délégués à un PASSI**

Et lors de contrôles classiques

☐ Au total, 14 sociétés contrôlées, avec des caractéristiques différentes :

- → Encours : de 500 millions à 20 milliards d'euros
- → Appartenance ou non à un groupe
- → Activité : généraliste, capital-investissement, immobilier

PRINCIPAUX CONSTATS DRESSES LORS DES CONTRÔLES À COMPOSANTE CYBER MENÉS

Points forts

- ☐ Prise en compte progressive du sujet cyber dans les cartographies des risques et les plans de contrôle, avec délégation régulière de tests techniques (dont le ciblage demeure toutefois perfectible).
- ☐ Indépendance de la fonction en charge du pilotage de la cyber sécurité
- ☐ Mise en place de sensibilisation régulière de l'ensemble du personnel (par exemple via test de phishing)

Points d'attention

- ☐ Défaut d'identification préalable des actifs critiques (données, applications, postes de travail, mobiles, installations et systèmes), pouvant occasionner un faux sentiment de sécurité
- ☐ PCA testé intensivement en période covid mais omettant le volet relatif à la restauration des données
- ☐ Pilotage et contrôle des fournisseurs IT critiques très nettement insuffisants
- ☐ Persistance de défauts de sécurisation communs, par exemple : pas de blocage des périphériques USB, postes de travail non chiffrés etc.
- ☐ Absence d'analyse de tendance des incidents d'origine cyber

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

LE RÈGLEMENT DORA ET SON IMPACT SUR LES ACTIVITÉS DE SUPERVISION DE L'AMF

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

LES CINQ PILIERS PRINCIPAUX DU RÈGLEMENT DORA

Gestion des risques liés aux TIC	Reporting des incidents liés aux TIC	Tests de résilience opérationnelle	Gestion des risques liés aux prestataires tiers de services TIC	Partage d'informations
Cadre harmonisé de gestion des risques liés aux TIC à mettre en place par les entités financières	Notification obligatoire des incidents majeurs liés aux TIC et facultative des cybermenaces aux autorités compétentes	Programme de tests de résilience opérationnelle numérique et tests avancés	Principes de gestion du risque lié au recours à des prestataires tiers & nouveau système de supervision européen des prestataires tiers critiques	Echanges volontaires d'informations entre les entités financières et entre les autorités compétentes

- Large champ d'application de DORA incluant un **très grand nombre d'entités financières**, supervisées par l'AMF et/ou l'ACPR
- Implication de l'AMF dans le cadre de chacun de ces piliers

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

LES IMPACTS SUR LES PRIORITÉS DE SUPERVISION DE L'AMF

☐ En termes d'impact sur les activités de l'AMF, le règlement DORA implique notamment que l'AMF :

→ Soit en charge de la **vérification du respect des obligations de DORA** par certaines entités financières, notamment l'élaboration d'un cadre de gestion des risques liées aux TIC. L'AMF devra pour ce faire assurer la supervision des entités financières dans son champ de compétence, réaliser des contrôles et le cas échéant prononcer des sanctions.

→ Participe à la **supervision des prestataires tiers critiques de services TIC** au niveau européen via le forum de supervision.

☐ Selon l'autorité compétente désignée, l'AMF pourra également être amenée à :

→ **Réceptionner et analyser les notifications d'incidents majeurs** liés aux TIC envoyées par certaines entités financières, ainsi que les déclarations volontaires de cyber-menaces ;

→ **Réceptionner et analyser les rapports** de certaines entités financières ayant réalisé **des tests de pénétration fondés sur la menace**.

☐ L'AMF est également impliquée dans le **recensement des prestataires tiers de services TIC** qui pourraient être désignés comme « **critiques** », actuellement mené par les autorités de supervision européennes.

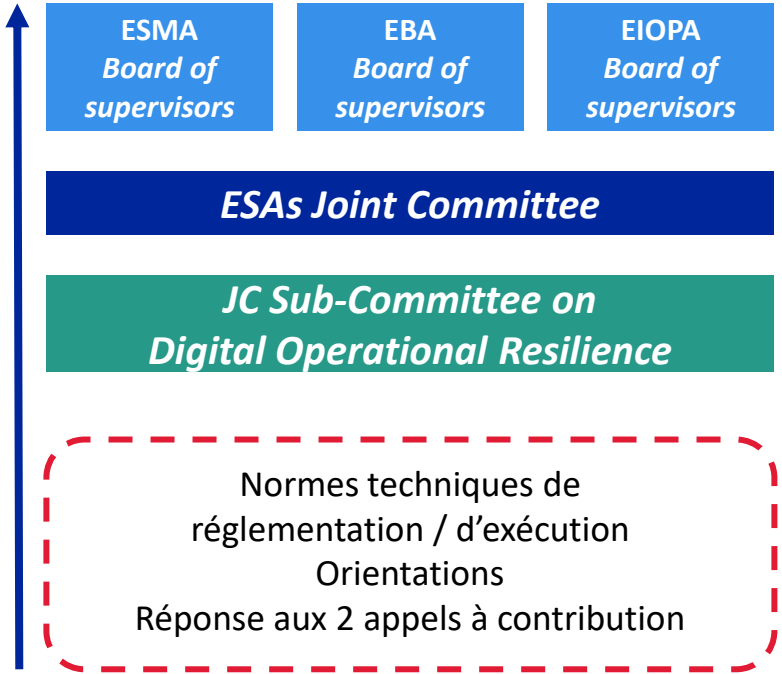
AUTORITÉ DES MARCHÉS FINANCIERS
AMF

DORA – LES DIFFÉRENTS TEXTES DE NIVEAU 2 ET 3 À VENIR

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

LE JC SC DOR – STRUCTURE AD-HOC EN CHARGE DES TRAVAUX DE NIVEAU 2 & 3



- Mise en place du ***Joint Committee Sub-Committee on Digital Operational Resilience*** (JC SC DOR)

- Un nombre important de **mesures de niveau 2 et 3** incluant ;
  - → 8 normes techniques de réglementation (RTS) ;
  - → 2 normes techniques d'exécution (ITS) ;
  - → 2 orientations ;
  - → 2 actes délégués de la Commission européenne (avec deux appels à contribution (*Call for advice)* aux autorités européennes).

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

LES DIFFERENTS TRAVAUX ET LES TIMELINES

Type de mesure	Sujet	Article	Deadline
Gestion du risque lié aux TIC			
RTS	Outils, méthodes, processus et politiques de gestion du risque lié aux TIC	Article 15	17 janvier 2024
RTS	Cadre simplifié de gestion des risques liés aux TIC	Article 16 (3)	17 janvier 2024
RTS	Tests de pénétration fondés sur la menace	Article 26 (11)	17 juillet 2024
RTS	Stratégie en matière de risques liés à l'utilisation de prestataires tiers de services TIC	Article 28 (10)	17 janvier 2024
RTS	Sous-traitance des services TIC pour des fonctions critiques ou importantes	Article 30 (5)	17 juillet 2024
Reporting des incidents liés aux TIC			
RTS	Critères de classification des incidents liés aux TIC	Article 18 (3)	17 janvier 2024
RTS	Notification des incidents majeurs liés aux TIC	Article 20 (a)	17 juillet 2024
ITS	Formulaires, les modèles et les procédures types pour notification des incidents	Article 20 (b)	17 juillet 2024
Guidelines	Estimation des coûts et pertes annuels causés par les incidents majeurs liés aux TIC	Article 11 (11)	17 juillet 2024
Rapport de faisabilité	Plateforme unique de l'Union pour la notification des incidents majeurs liés aux TIC	Article 21	17 janvier 2025
Structure de supervision			
ITS	Modèles types aux fins du registre d'informations	Article 28 (9)	17 janvier 2024
Guidelines	Coopération entre les ESAs et autorités nationales sur la structure de supervision	Article 32 (7)	17 juillet 2024
RTS	Supervision des prestataire tiers de services TIC	Article 41	17 juillet 2024
Acte délégué	Critères de désignation des prestataires tiers de services TIC critiques pour les entités financières	Article 31 (6)	17 juillet 2024
Acte délégué	Redevances de supervision	Article 42 (3)	17 juillet 2024

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

POINTS D'ATTENTION ET PROCHAINES ÉTAPES

☐ Entrée en application du texte **le 17 janvier 2025**

☐ Evènement public des autorités de supervision européennes sur DORA *(ESAs Joint event on DORA)* du 06 février 2023

→ Participation très forte de l'industrie (2000+ participants à l'évènement en ligne)

→ **Appel à la participation de l'industrie** dans le cadre des travaux de niveaux 2 et 3, autorités preneuses des commentaires des entités financières dans le processus de rédaction.

→ Prochaines *public hearings* prévues après les publications des différentes consultations.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Le règlement DORA et la mise en place d'un cadre de résilience opérationnelle numérique

Autorité des Marchés Financiers

Direction de la Régulation et des Affaires Internationales

Division Innovation & Finance Digitale (IFD)

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF