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

Autorité des Marchés Financiers

DC – Division en charge du contrôle des SGP et des CIF

DRAI – Division Innovation & Finance Digitale (IFD)

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

SOMMAIRE

- 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
AMF

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

Contrôles SPOT / classiques menés de 2019 et 2020 sur les SGP et les IM

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

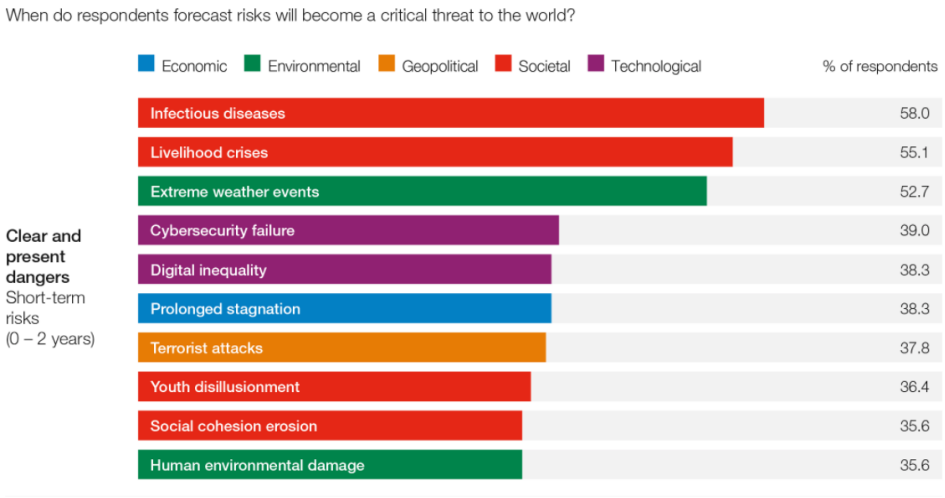
Rappel : définition du risque cyber

Un incident de cyber sécurité est une atteinte malveillante à l'une des caractéristiques-clé du SI d'une organisation :

- Sa **D**isponibilité,
- Son **I**ntégrité,
- La **C**onfidentialité des données qu'il contient,
  - incluant le processus d'**authentification** des utilisateurs
- La **T**raçabilité des actions qui y sont menées.
  - incluant la **non-répudiation** des actions des utilisateurs

Un risque « *d'origine cyber* » marquant l'actualité

- Le risque « d'origine cyber » est prépondérant au point d'être classé par le Forum économique mondial comme 4e risque le plus critique à court terme, et le 8ème à moyen terme



- https://www.weforum.org/reports/the-global-risks-report-2021
- http://reports.weforum.org/global-risks-report-2021/survey-results/global-risks-horizon

- Avec la **transformation numérique des services financiers**, ce risque doit ainsi être pris en compte par les **fournisseurs de services et solutions afin d'assurer la confiance et la résilience**, propriétés indispensables pour ce secteur d'activité

- Des **exigences de cybersécurité** sont de plus en plus formulées dans les **textes réglementaires**

- À l'échelle de **l'AMF**,

  - Des **contrôles** sur le **thème cyber** sont réalisés depuis **2019**

  - Une **instruction (DOC-2019-24)** sur le thème cyber existe depuis **2019** et précise les exigences en matière de cybersécurité que doivent respecter les **prestataires de services sur actifs numériques (PSAN)** dans le cadre d'une demande **d'agrément optionnel**

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Périmètre

Deux vagues de contrôles SPOT réalisées auprès de sociétés de gestion dans le cadre d'une priorité de supervision

☐ **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**

- https://www.amf-france.org/fr/actualites-publications/publications/syntheses-des-controles-spot/synthese-des-controles-spot-sur-le-dispositif-de-cybersecurite-des-societes-de-gestion-de

☐ **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**

- https://www.amf-france.org/fr/actualites-publications/publications/syntheses-des-controles-spot/synthese-des-controles-spot-sur-le-dispositif-de-cyber-securite-des-societes-de-gestion-de

Et également lors de contrôles « classiques »

☐ **Au total, 21 SGP contrôlées sur le thème cyber, avec des caractéristiques différentes :**

- **Encours :** de 500 millions à 20 milliards d'euros
- Appartenance ou non à un **groupe**
- **Tout type d'activité** : généraliste, *private equity*, gestion déléguée, immobilier

☐ **Ainsi que 3 CIF, 1 CIP et 1 infrastructure de marché**

Une troisième campagne de contrôles SPOT est actuellement en cours sur cette thématique. Elle cible le niveau de prise en compte des risques d'origine cyber dans le dispositif de sélection, contractualisation et contrôle des prestataires informatiques (ex : éditeurs, infogérants, « cloud service providers (CSP) ») et des partenaires de gestion (dépositaires, valorisateurs, TCC, distributeurs, CAC).

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Bonnes pratiques / Mauvaises pratiques (*) (1/5)

Organisation et gouvernance du dispositif cyber : *Bien que les risques d'origine cyber soient pris en compte dans les dispositifs existants, l'absence de réflexion ab initio quant aux zones de risques principales contribue au maintien d'un faux sentiment de sécurité.*

❑ Bonnes pratiques

- ❑ Assurer l'indépendance de la fonction RSSI par rapport à la DSI.
- ❑ Réaliser chaque année un test de « phishing ».
- ❑ Isoler, dans les dépenses informatiques, celles liées à la cyber sécurité.

❑ Mauvaises pratiques

- ❑ Déployer un dispositif cyber en l'absence d'identification préalable, de classification par niveau de criticité (DICT) et de revue régulière des données et des systèmes sensibles.
- ❑ N'appuyer le dispositif de cyber sécurité que sur la stratégie groupe.
- ❑ Cantonner l'analyse des risques d'origine cyber à leur seul impact opérationnel.
- ❑ Ne pas inclure les risques d'origine cyber dans les « reportings » aux dirigeants.
- ❑ Réduire les procédures de cyber sécurité à l'énoncé de principes généraux.

(*) Pour rappel, une bonne ou une mauvaise pratique correspond à un constat effectué par la mission de contrôle sur une fraction majoritaire du panel contrôlé lors des campagnes SPOT. Il ne s'agit pas d'un élément de doctrine.

Bonnes pratiques / Mauvaises pratiques (2/5)

Administration et surveillance des SI : *Le renforcement progressif des dispositifs d'administration et de surveillance demeure menacé par la persistance de vulnérabilités standards.*

❑ Bonnes pratiques

- ❑ Formaliser des procédures d'administration du matériel et des réseaux, incluant la gestion des versions de logiciels et celles des correctifs de sécurité.
- ❑ Mettre à jour régulièrement un inventaire des équipements du SI.
- ❑ Mettre en place un contrôle des connexions à Internet.
- ❑ Étendre la surveillance automatisée du SI au-delà des heures ouvrées.

❑ Mauvaises pratiques

- ❑ Ne pas assurer le blocage des ports USB des postes utilisateurs.
- ❑ Ne pas assurer le chiffrement des postes utilisateurs.
- ❑ Permettre aux utilisateurs d'être administrateur de leur poste.
- ❑ Maintenir une politique de construction des mots de passe non conforme aux recommandations de l'ANSSI/CNIL et de l'ISO 27002.

Bonnes pratiques / Mauvaises pratiques (3/5)

- Processus de collecte des incidents d'origine cyber : Les trois catégories d'incidents constatées sont les tentatives de détournement d'authentifiants individuels, de fonds ou de récupération de données à caractère personnel ou stratégique. Une compréhension accrue du « *business model* » des SGP est observée.

Bonnes pratiques

- Formaliser une procédure de gestion des incidents d'origine cyber.
- Prévoir la couverture des risques d'origine cyber dans les polices d'assurance négociées par les SGP pour leurs activités.

Mauvaises pratiques

- Ne pas identifier spécifiquement les incidents d'origine cyber dans le processus existant de collecte et gestion des incidents.

- L'essentiel des incidents reportés à ce stade à l'AMF sur le périmètre des SGP font suite à une intrusion sur les boîtes emails professionnelles des sociétés impactées.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Bonnes pratiques / Mauvaises pratiques (4/5)

Pilotage des prestataires informatiques : *Malgré l'intégration progressive des risques d'origine cyber dans les processus de sélection des prestataires informatiques, l'évaluation insuffisante des services rendus par ces derniers peut conduire certaines SGP à s'exonérer – à tort - du pilotage de ce type de risque.*

❑ Bonnes pratiques

- ❑ Faire réaliser régulièrement par un PASSI, certifié par l'ANSSI, un test d'intrusion sur le SI de la SGP.
- ❑ Formaliser une procédure de sélection et d'évaluation des prestataires informatiques.
- ❑ Procéder annuellement, à l'évaluation du niveau de cyber sécurité des services rendus par les éditeurs applicatifs.
- ❑ Demander aux prestataires et partenaires externes les rapports d'audit de sécurité ayant été menés sur la portion de leurs installations utilisées dans les services rendus.

❑ Mauvaises pratiques

- ❑ Ne pas inclure dans le contrat d'externalisation de l'administration informatique les mesures de cyber sécurité exigées de l'administrateur, ni le protocole de notification d'urgence, ni de clause d'audit.
- ❑ Ne pas maintenir à jour la liste des prestataires informatiques externes.
- ❑ Ne pas évaluer les prestations informatiques rendues par le groupe d'appartenance.

Les bonnes et mauvaises pratiques identifiées ici seront développées dans le cadre des conclusions de la campagne SPOT cyber sécurité n°3 en cours.

Bonnes pratiques / mauvaises pratiques (5/5)

Supervision des processus d'accès à distance au SI de la SGP : *Les risques associés aux flux d'échanges de données avec les systèmes des partenaires métier externes ne sont pas suffisamment pris en compte dans le dispositif de cyber sécurité.*

❑ Bonnes pratiques

- ❑ Encadrer les processus d'accès à distance par les collaborateurs au SI de la SGP par des contrôles à la fois préventifs et détectifs.

❑ Mauvaises pratiques

- ❑ Omettre de prendre en compte dans la cartographie des données sensibles les échanges informatisés de données opérés avec les partenaires de la SGP (ex : dépositaire, teneur de compte, délégataire comptable ou CAC).

Gestion de la continuité d'activité : *Les confinements 2020 et 2021 en ont permis le test intensif.*

❑ Bonnes pratiques

- ❑ Prendre en compte dans la stratégie de continuité les risques d'origine cyber pouvant impacter les installations de secours.
- ❑ Formaliser un plan de sauvegarde régulier des données informatiques, précisant le périmètre et la fréquence des opérations menées.

❑ Mauvaises pratiques

- ❑ Ne pas inclure dans le PCA de stratégie de continuité en cas (i) de coupure téléphonique et (ii) d'indisponibilité prolongée du DSI.
- ❑ Ne pas réaliser de tests de restauration périodiques des données sauvegardées.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Outils règlementaires

AMF

- Organisation générale (article 57 (1d) du règlement délégué (UE) n°231/2013, articles 321-23 et 321-25 du règlement général de l'AMF, article 21 (1) du règlement délégué (UE) n°2017/565)
- Procédures, description du processus de collecte des incidents dans les procédures (articles 61 (1) du règlement délégué (UE) n°231/2013, articles 318-4, 321-1, 321-30,du règlement général de l'AMF, article 22 (1) du règlement délégué (UE) n°2017/565)
- Contrôles de second niveau réalisés sur la cyber sécurité (article 61 (2) du règlement délégué (UE) n°231/2013, articles 318-4 et 321-31 du règlement général de l'AMF, article 22 (2) du règlement délégué (UE) n°2017/565)

AMF

- Contrôle périodique (article 62 du règlement délégué n°231/2013, articles 321-83 du règlement général de l'AMF et 24 du règlement délégué n°2017/565).
- Reportings aux dirigeants / système de reporting du risque cyber (article 60 (4) du règlement délégué (UE) n°231/2013, articles 318-6 et 321-36 du règlement général de l'AMF, article 22 (2c) du règlement délégué (UE) n°2017/565)
- Externalisation (article 318-93 à article 321-96 II 5) (OPCVM) et article 318-58 à article 318-61 II 5) (FIA) du RG AMF)
- Enregistrement (articles 321-24 du RG AMF (OPCVM), 57 2) du RD (UE) n°231/2013 (FIA) et 21 2) du règlement délégué n°2017/565)
- **Tronc commun cyber dans l'instruction DOC-2019-24 relative aux PSAN**

Commission européenne

- Les **orientations de l'ESMA** relatives à la **sous-traitance** à des **prestataires de services en nuage** sont **en cours d'analyse.**
- Avancement de la proposition de loi sur la **résilience opérationnelle numérique** (*Digital Operational Resilience Act*, *DORA*) **pour le secteur financier** (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:595:FIN)

SEC (Etats-Unis)

- La SEC a sanctionné en 2021 3 SGP (*) pour un niveau de protection insuffisant de leur système de messagerie professionnelle (ayant permis à des pirates l'accès aux informations confidentielles de plusieurs de leurs clients).

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

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

RÈGLEMENT DORA – CONTEXTE D'ADOPTION

- Degré croissant et caractère central de la **numérisation des services financiers** et de **l'utilisation de services de technologies de l'information et de la communication** (TIC) ;
- Rapport 2020 du Comité européen du risque systémique (CERS) sur le **risque de vulnérabilité systémique des systèmes d'information** des entités financières et des infrastructures de marchés financiers ;
- Constat par la Commission d'une nécessité de renforcer et d'harmoniser dans un même corpus les règles relatives la **résilience numérique opérationnelle** du secteur financier ;
- Publication du règlement DORA au Journal Officiel de l'Union européenne le **27 décembre 2022**.

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

RÈGLEMENT DORA – DÉFINITIONS

DORA définit plusieurs notions relatives à la résilience cyber des entités financières.

- **La résilience opérationnelle numérique** est *« la capacité d'une entité financière à **développer, garantir** et **réévaluer** son intégrité et sa fiabilité opérationnelles, **en assurant** directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, **l'intégralité des capacités liées aux TIC nécessaires** pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui **sous-tendent la fourniture continue de services financiers** et leur qualité, y compris en cas de perturbations » ;*

- **Les services TIC** sont *« les **services numériques** et de **données** fournis de manière permanente par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs »* ;

- **Le risque lié aux TIC** est *« toute circonstance raisonnablement identifiable liée à l'utilisation des réseaux et des systèmes d'information qui, si elle se concrétise, peut **compromettre la sécurité des réseaux et des systèmes d'information,** de tout outil ou processus dépendant de la technologie, du fonctionnement et des processus ou de la fourniture de services en produisant des effets préjudiciables dans l'environnement numérique ou physique; »*

RÈGLEMENT DORA – CHAMP D'APPLICATION ET PILIERS PRINCIPAUX (1/3)

☐ **Le cadre de résilience numérique introduit par DORA inclut pratiquement toutes les entités financières :**

→ Établissements de crédit, entreprises d'investissements, établissements de paiement, sociétés de gestion, entreprises d'assurance et de réassurance, CASPs agréés selon MiCA, plateformes de négociation, contreparties centrales, dépositaires centraux, prestataires de services de financement participatif, etc.

☐ **Certaines dispositions de DORA s'appliquent également aux prestataires tiers de services TIC :**

→ *Cloud computing services, software, data analytics* et *data centers, hardware*, etc.

☐ **Principe de proportionnalité sur l'application des exigences de DORA**

☐ **5 piliers principaux :**

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

RÈGLEMENT DORA – CHAMP D'APPLICATION ET PILIERS PRINCIPAUX (2/3)

Gestion des risques liés aux TIC

- Les entités financières assujetties sont tenues de mettre en place un **cadre de gestion des risques des incidents liés aux TIC** ;
- Ce cadre harmonisé doit notamment inclure des règles de gouvernance et de contrôle interne, une classification des risques, politiques de continuité d'activité ;
- **Cadre simplifié** pour certaines entreprises, notamment celles de plus petite taille.

Reporting des incidents liés aux TIC

- **2 niveaux de reporting à l'autorité compétente**
  - → Reporting **obligatoire** des incidents majeurs ;
  - → Reporting sur une **base volontaire** des cybermenaces.

Tests de résilience opérationnelle

- **2 niveaux de tests**
  - → Tests **basiques** ;
  - → Tests de **pénétration basés sur la menace** pour les fonctions critiques ou importantes de certaines entités financières.

RÈGLEMENT DORA – CHAMP D'APPLICATION ET PILIERS PRINCIPAUX (3/3)

Gestion des risques liés aux prestataires tiers de services TIC

- ☐ Instauration d'un **système de supervision européen** des prestataires tiers de services TIC considérés comme « **critiques** » ;
- ☐ Désignation selon les critères tels que :
  - → L'effet systémique sur la continuité de fourniture de services financiers ;
  - → L'importance systémique des entités financières dépendant des services TIC.
- ☐ Les autorités **compétentes européennes et nationales** disposent de certains pouvoirs tels que :
  - → **Pouvoirs de surveillance** (inspections sur place, enquêtes), **pouvoirs de sanction** (sanctions administratives), **exiger la résiliation** d'accords contractuels.

Partage d'informations et de renseignements

- ☐ **2 niveaux de partage d'informations et renseignements :**
  - → Entre les **entités financières sur une base volontaire** (tactiques, procédures, alertes, etc.) ;
  - → Entre les **autorités compétentes** (échanges d'informations pertinentes concernant les prestataires tiers critiques de services TIC, risques, approches, mesures adoptées, etc.).

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**.

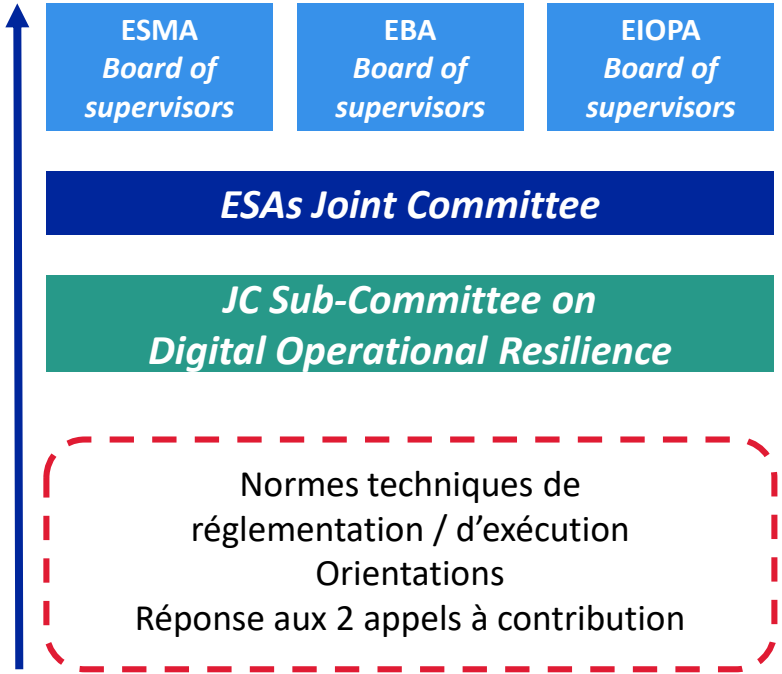
☐ L'AMF est également impliquée dans le **recensement des prestataires tiers de services TIC** qui pourraient être désignés comme « **critiques** », actuellement mené par les autorités de supervision européennes.

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).

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

CONSULTATION DE L'INDUSTRIE

- **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.
- Prochaine *public hearing* prévue après publication des prochaines consultations.
- Deux paquets de consultation :

1er paquet
(textes de niveau 2 et 3 avec une deadline réglementaire de 12 mois)

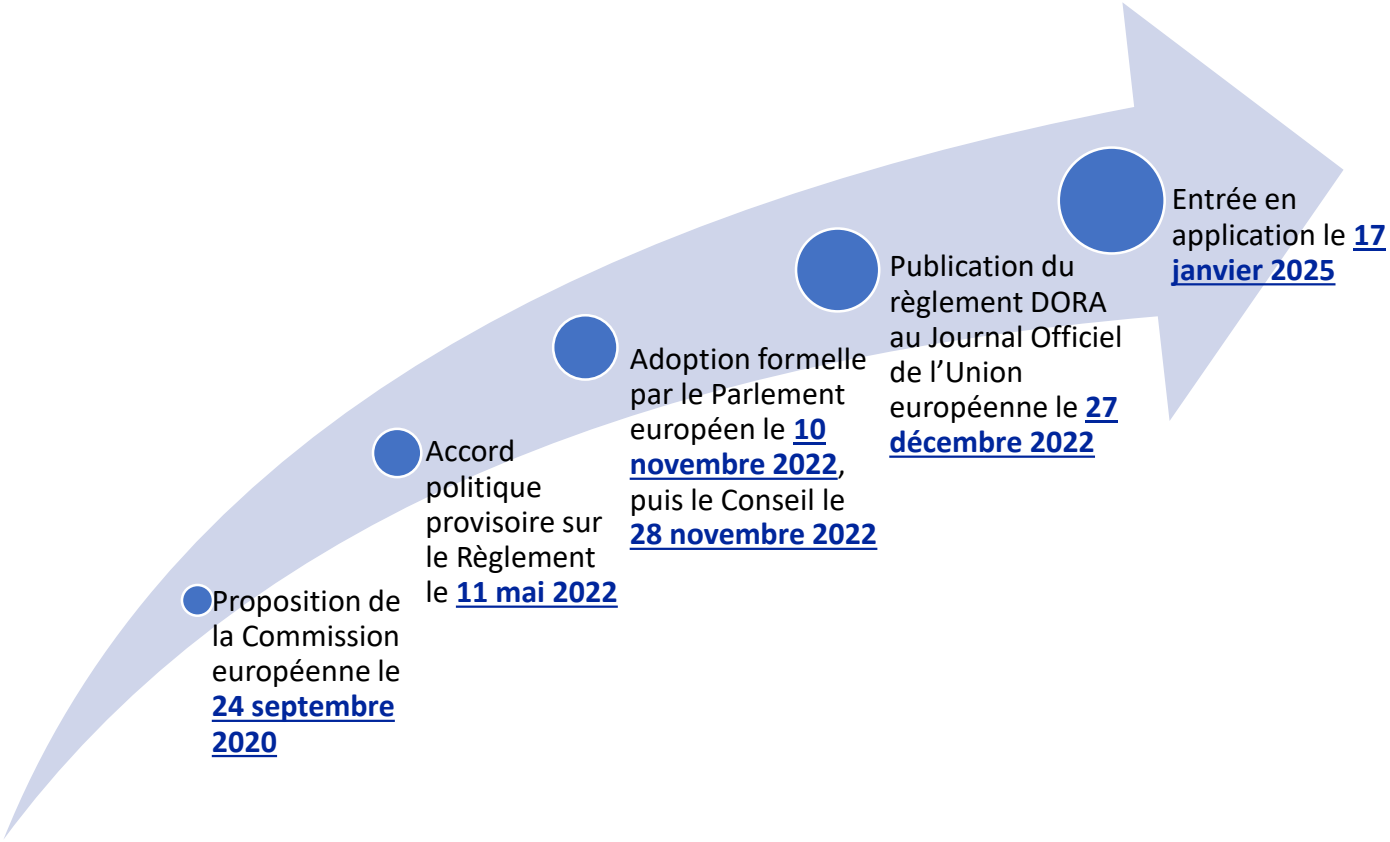
Consultation de mi-juin à mi-septembre

2nd paquet
(textes de niveau 2 et 3 avec une deadline réglementaire de 18 mois)

Consultation de novembre à février 2024 *(timing envisagé)*

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

RÈGLEMENT DORA – CALENDRIER D'ADOPTION DE DORA



Des questions ?

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

Autorité des Marchés Financiers

DC – Division en charge du contrôle des SGP et des CIF

DRAI – Division Innovation & Finance Digitale (IFD)

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

AUTORITÉ DES MARCHÉS FINANCIERS
AMF