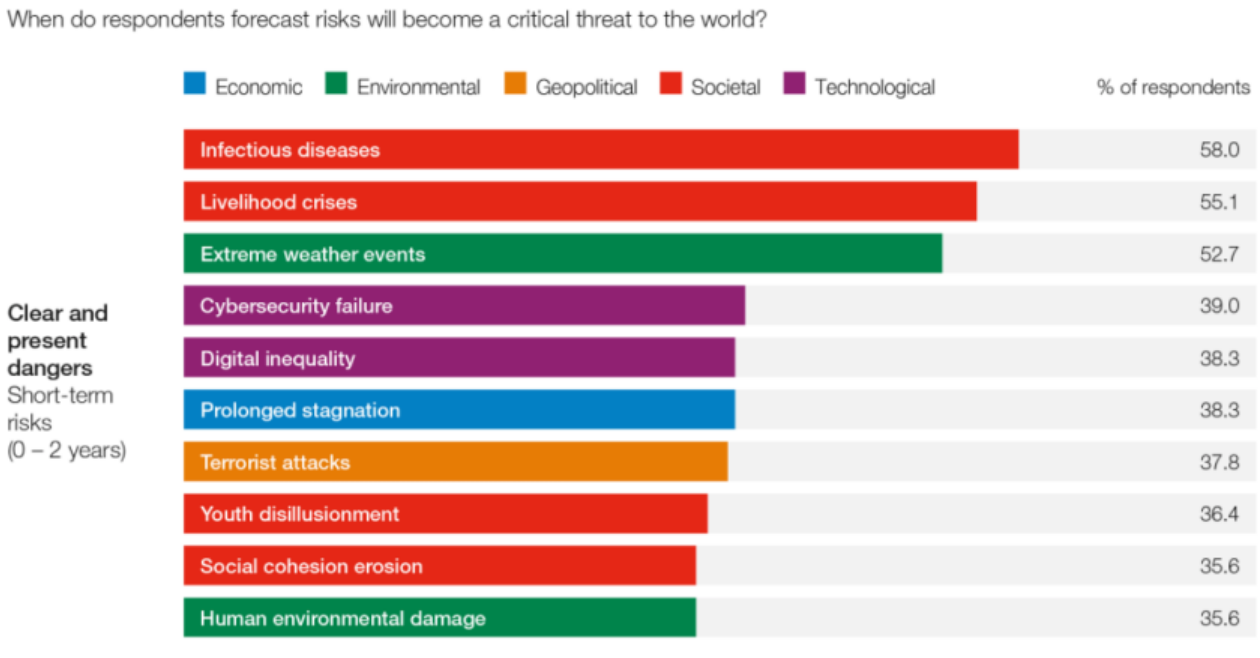
FORUM FINTECH ACPR-AMF

Cyber-sécurité et risque informatique : le point sur la nouvelle réglementation appliquée aux Fintechs

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**

RETOUR D'EXPÉRIENCE SUR LES CONTRÔLES CYBER

Retour d'expérience sur les contrôles cyber

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, 14 sociétés contrôlées, 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

Retour d'expérience sur les contrôles cyber

Principaux constats dressés lors des deux campagnes et des contrôles classiques

- **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 cybersécurité**
- Mise en place de **sensibilisation régulière de l'ensemble du personnel** (par exemple via test de *phishing*)

- **Défaut d'identification préalable des actifs (*) critiques**, 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**

(*) Données, applications, postes de travail, mobiles, installations et systèmes.

LE TRONC COMMUN DE CYBERSÉCURITÉ REQUIS DANS L'INSTRUCTION DOC-2019-24

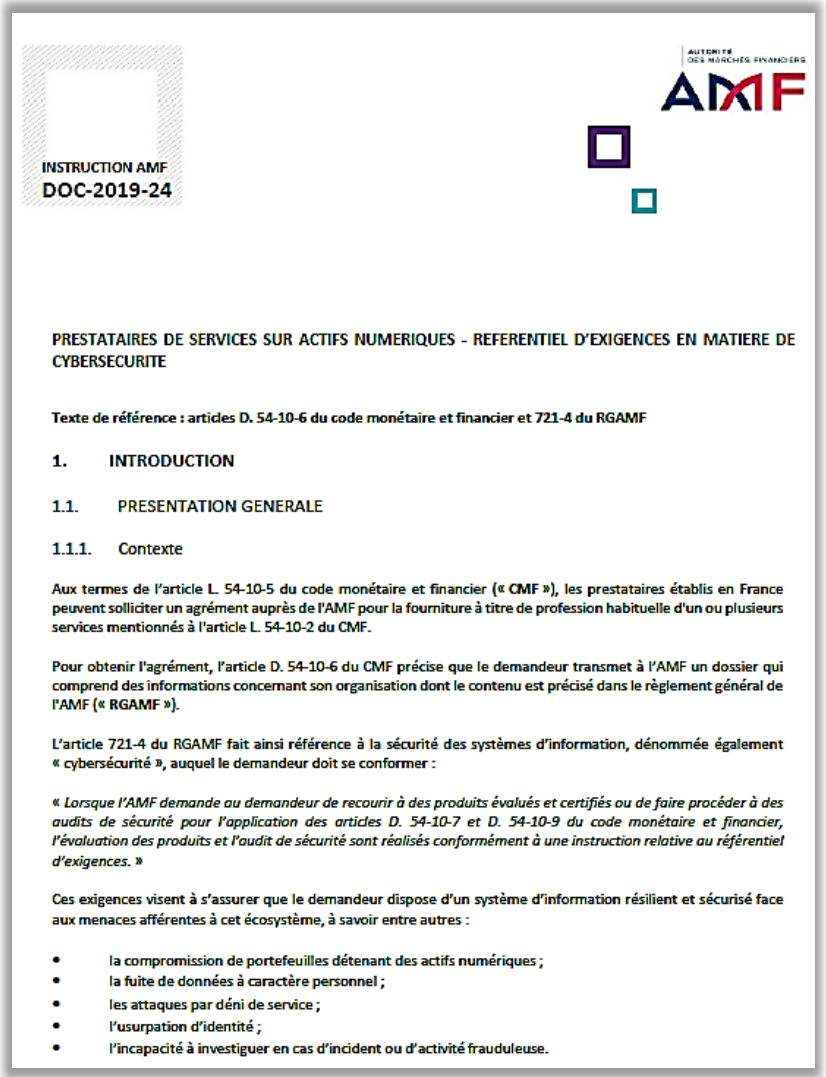
Structure de l'instruction DOC-2019-24 en matière de cybersécurité des PSAN

↗ https://www.amf-france.org/fr/reglementation/doctrine/doc-2019-24

Cette instruction se divise en deux parties

- **1.** Des **exigences spécifiques** au contexte des **PSAN** (conservation, types de portefeuilles électroniques, dispositif d'enregistrement électronique partagé, signature de transactions, journalisation dans le cadre de lutte anti-blanchiment, etc.)
- **2.** Mais surtout avant ces exigences spécifiques, un **tronc commun de cybersécurité**

  ↗ **Ce tronc commun, détaillé ci-après, peut être suivi et appliqué de manière transverse à toute activité relative au secteur des Fintech afin d'initier une démarche de cybersécurité !**



INSTRUCTION AMF
DOC-2019-24

PRESTATAIRES DE SERVICES SUR ACTIFS NUMERIQUES - REFERENTIEL D'EXIGENCES EN MATIERE DE CYBERSECURITE

Texte de référence : articles D. 54-10-6 du code monétaire et financier et 721-4 du RGAMF

1. INTRODUCTION

1.1. PRESENTATION GENERALE

1.1.1. Contexte

Aux termes de l'article L. 54-10-5 du code monétaire et financier (« CMF »), les prestataires établis en France peuvent solliciter un agrément auprès de l'AMF pour la fourniture à titre de profession habituelle d'un ou plusieurs services mentionnés à l'article L. 54-10-2 du CMF.

Pour obtenir l'agrément, l'article D. 54-10-6 du CMF précise que le demandeur transmet à l'AMF un dossier qui comprend des informations concernant son organisation dont le contenu est précisé dans le règlement général de l'AMF (« RGAMF »).

L'article 721-4 du RGAMF fait ainsi référence à la sécurité des systèmes d'information, dénommée également « cybersécurité », auquel le demandeur doit se conformer :

« Lorsque l'AMF demande au demandeur de recourir à des produits évalués et certifiés ou de faire procéder à des audits de sécurité pour l'application des articles D. 54-10-7 et D. 54-10-9 du code monétaire et financier, l'évaluation des produits et l'audit de sécurité sont réalisés conformément à une instruction relative au référentiel d'exigences. »

Ces exigences visent à s'assurer que le demandeur dispose d'un système d'information résilient et sécurisé face aux menaces afférentes à cet écosystème, à savoir entre autres :

- la compromission de portefeuilles détenant des actifs numériques ;
- la fuite de données à caractère personnel ;
- les attaques par déni de service ;
- l'usurpation d'identité ;
- l'incapacité à investiguer en cas d'incident ou d'activité frauduleuse.

Tronc commun de cybersécurité requis dans l'instruction DOC-2019-24

Le programme de cybersécurité doit comprendre a minima ces axes

1. **L'identification des risques d'origine cyber pesant sur l'entreprise et leur évaluation en terme de probabilité et impact sur les critères de disponibilité, intégrité, confidentialité et traçabilité (DICT)**

   - Les **données et systèmes jugés critiques** pour l'activité doivent être formellement **identifiés** pour **concentrer les efforts** de **sécurisation** et de **maintien en conditions de sécurité**

2. **L'analyse d'impact relative à la protection des données à caractère personnel (AIPD) pour les services fournis**

3. **La mise en œuvre de moyens humains, organisationnels et techniques permettant de maîtriser les risques identifiés et de répondre aux exigences de disponibilité, d'intégrité, de confidentialité et de traçabilité définies**

4. **Les dispositifs de contrôle de la présence et de l'efficacité des mesures de sécurité identifiées lors de l'analyse de risques**

   - Le référentiel des **prestataires d'audit en sécurité des systèmes d'information (PASSI) de l'ANSSI** est un **label de qualité** pour le choix de fournisseurs à même de réaliser des contrôles **organisationnels et techniques**

Tronc commun de cybersécurité requis dans l'instruction DOC-2019-24

Le programme de cybersécurité doit comprendre a minima ces axes

5 **Les procédures de revue régulière des comptes et des droits d'accès sur les systèmes d'information, notamment ceux identifiés comme critiques pour l'activité**

6 **La gestion des vulnérabilités incluant une veille sur les vulnérabilités techniques et menaces pouvant apparaître ainsi que l'application d'une politique permettant leur traitement**

- Une source de référence pour la centralisation des **bulletins de vulnérabilité**, celui du **CERT-FR** de l'ANSSI (https://www.cert.ssi.gouv.fr/)

7 **Les moyens humains et techniques permettant la détection d'intrusion ou plus généralement d'évènements redoutés sur les systèmes d'information listés précédemment**

8 **Les procédures de réponse aux incidents de sécurité et la reprise de l'activité nominale**

- En incluant notamment les volets de notification d'incident aux régulateurs ainsi que la communication auprès des utilisateurs et médias

L'ACTUALITÉ RÉCENTE, EN COURS ET FUTURE SUR LE VOLET DE LA RÉGLEMENTATION

L'actualité récente, en cours et future sur le volet de la réglementation

AMF

- La cybersécurité fait désormais partie des **thèmes potentiels de contrôles classiques**
- Un **processus de collecte et traitement des incidents d'origine cyber** des assujettis est en cours de **structuration**
- Les **orientations de l'ESMA** relatives à la **sous-traitance** à des **prestataires de services en nuage** sont **en cours de prise en compte**

Commission européenne

- 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