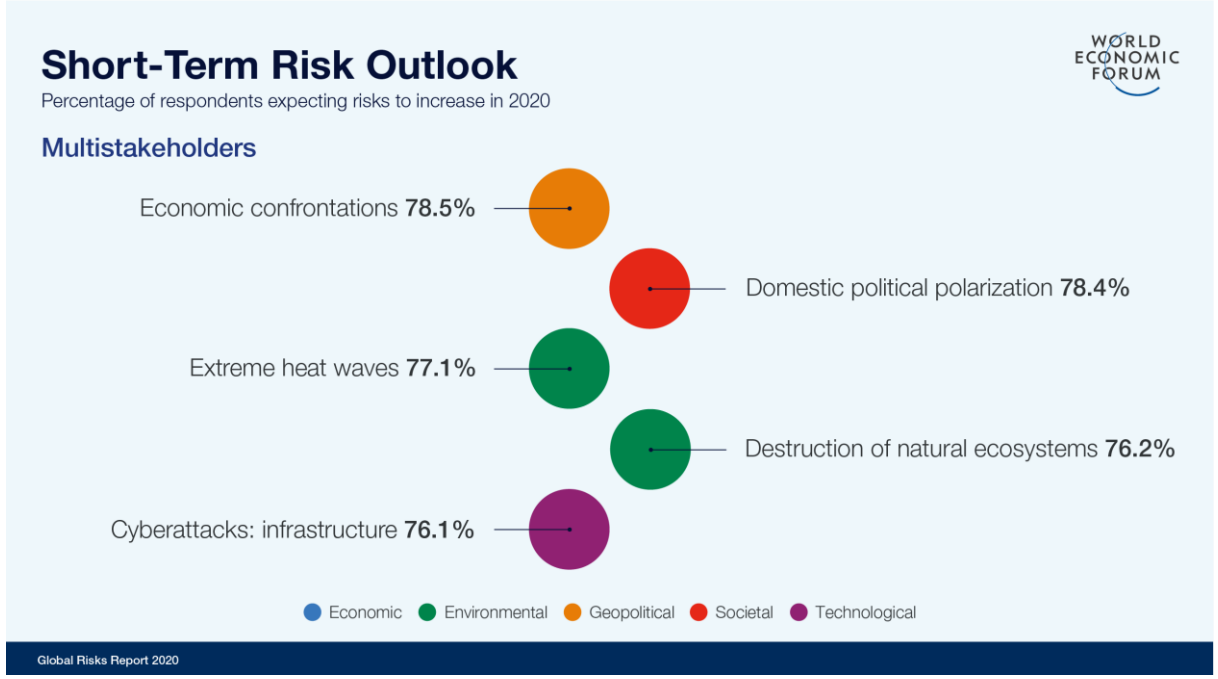
FORUM FINTECH ACPR-AMF

Cybersécurité et nouvelle réglementation du risque informatique : quelle application aux Fintech ?

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

- Le risque **« d'origine cyber »** devient prépondérant au point d'être classé par le Forum économique mondial comme **5e risque le plus probable et à l'impact le plus fort** à court terme



- https://www.weforum.org/reports/the-global-risks-report-2020
- https://reports.weforum.org/global-risks-report-2020/shareable-infographics/

- 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, l'un des **premiers documents** représentatifs de cette transformation est l'instruction **DOC-2019-24** qui 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**

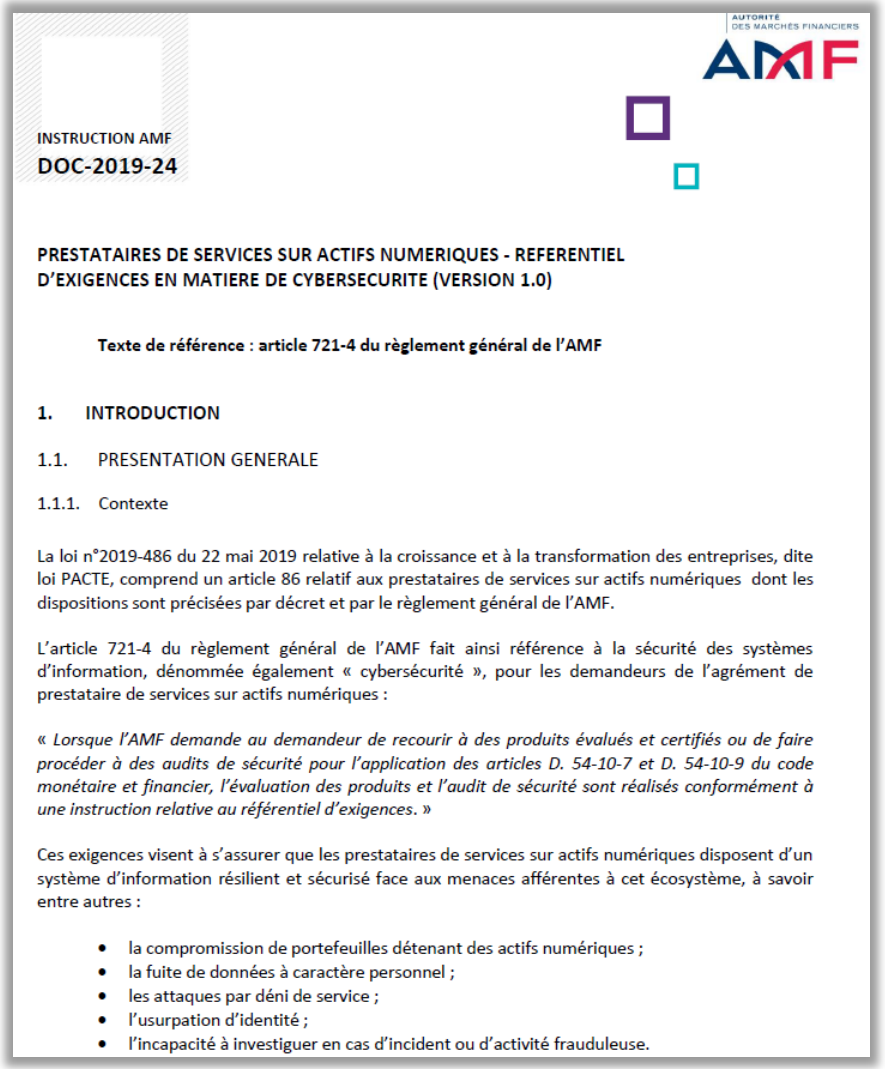
https://doctrine.amf-france.org/Reglementation/Doctrine/Doctrine-list/Doctrine?docId=workspace%3A%2F%2FSpacesStore%2F0a3bc47b-e103-4601-a9e4-9fda00b76784&category=III+-+Prestataires

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

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 (VERSION 1.0)

Texte de référence : article 721-4 du règlement général de l'AMF

1. INTRODUCTION

1.1. PRESENTATION GENERALE

1.1.1. Contexte

La loi n°2019-486 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, dite loi PACTE, comprend un article 86 relatif aux prestataires de services sur actifs numériques dont les dispositions sont précisées par décret et par le règlement général de l'AMF.

L'article 721-4 du règlement général de l'AMF fait ainsi référence à la sécurité des systèmes d'information, dénommée également « cybersécurité », pour les demandeurs de l'agrément de prestataire de services sur actifs numériques :

« *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 les prestataires de services sur actifs numériques disposent 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.

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

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**
- La méthode *EBIOS Risk Manager* **peut constituer une méthode** pour réaliser cette analyse (https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/)

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

- Cette analyse doit permettre d'évaluer le **niveau de risque** engendré par le traitement pour les droits et libertés des personnes physiques et prévoir les mesures appropriées pour atténuer ce risque
- La **CNIL** est l'autorité compétente sur ce sujet

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

Le programme de cybersécurité doit comprendre a minima ces axes

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

Les **mesures opérationnelles** à appliquer communément concernent :

- le **cloisonnement** appliqué aux systèmes et réseaux
- le **renforcement de la sécurité des configurations** des composants techniques (guides ANSSI, *CIS Benchmarks,* etc.)
- la **sécurisation dans les développements applicatifs** (*OWASP*, *CERT Securecoding,* etc.)
- la robustesse de **l'authentification** ainsi que le **chiffrement des flux et données**
- la norme **ISO 27002** constitue un recueil de bonnes pratiques sur ce volet

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 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 synthèse de la première série de **contrôles SPOT** réalisée en 2019 sur le dispositif de cybersécurité des **sociétés de gestion de portefeuille**

  ↗ 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

- **MINEFI :** arrêté du 18 septembre 2018 portant approbation du **cahier des clauses simplifiées de cybersécurité**

  ↗ https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037436658?r=vIDGZUD3g8

- **Conseil de stabilité financière (FSB) :** Recueil de bonnes pratiques en matière de **prévention, de gestion et de reprise face aux incidents de cybersécurité**

  ↗ https://www.fsb.org/2020/08/public-responses-to-consultation-on-effective-practices-for-cyber-incident-response-and-recovery/

- **Commission européenne :** 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