FORUM FINTECH 2022

CYBER SÉCURITÉ ET RISQUES INFORMATIQUES : LES POINTS D'ATTENTION DES AUTORITÉS

AZIZA HALILEM & DÉBORAH HADDAD (DIRECTION DES AFFAIRES INTERNATIONALES)
VALÉRIE PIQUET (DIRECTION DES CONTRÔLES SPÉCIALISÉS ET TRANSVERSAUX)
MARC ANDRIES (DÉLÉGATION AU CONTRÔLE SUR PLACE DES ÉTABLISSEMENTS DE CREDIT)

19 OCTOBRE 2022


ACPR
BANQUE DE FRANCE
AUTORITÉ
DES MARCHÉS FINANCIERS
AMF
FORUM FINTECH
ACPR - AMF
19 oct. 2022

SOMMAIRE

1. Le cadre européen DORA

2. État de préparation du marché :
   a. Les axes de progrès d'ici 2025
   b. Les points d'attention sur l'usage du *Cloud*

1. LE CADRE EUROPÉEN DORA

CONSIDERATIONS GÉNÉRALES SUR DORA : L'UNIFORMISATION DES REGLES POUR L'ENSEMBLE DES INSTITUTIONS FINANCIERES

- DORA vise à renforcer la cyber-résilience du secteur financier européen, dans un contexte où il est de plus en plus ciblé par les cyber attaques.

- La DORA devrait s'appliquer à pratiquement toutes les entités financières à compter du 1er janvier 2025. Il renforcera et harmonisera les règles de l'UE concernant :

Gestion des risques liés aux TIC - Les entités financières doivent mettre en place des mesures spécifiques concernant la gestion et la gouvernance des risques liés aux TIC, conformément aux orientations existantes
Incidents liés aux TIC - Les incidents majeurs et les cybermenaces importantes (sur une base volontaire) sont déclarés aux autorités compétentes au moyen de modèles communs
Test de résilience opérationnelle numérique - Utilisation des tests d'intrusion pour vérifier la résilience des systèmes, fournissant les exigences pour les tests de base et avancés
Gestion des risques liés aux tiers TIC, y compris un cadre de surveillance des prestataires de services critiques paneuropéens

ACPR
BANQUE DE FRANCE

PRINCIPAL ÉLÉMENT À RETENIR : DORA CONFORTE LES RÈGLES DE GOUVERNANCE EN VIGUEUR

- DORA renforce les exigences en matière de gestion des risques et de gouvernance liés aux TIC ; toutefois, la plupart des exigences figurent déjà dans les orientations actuelles et les pratiques prudentielles ne devraient pas être révolutionnées

  - Les entités financières soumises à la DORA sont **tenues de mettre en œuvre un cadre formel de gouvernance et de gestion des risques liés aux TIC. Toutefois, nombre de ces exigences de gouvernance figurent déjà** dans les orientations existantes (ABE/AEAPP) et sont déjà intégrées dans les pratiques prudentielles. Il s'agit plus d'une actualisation des méthodes existantes, avec un alignement à la hausse des exigences, que d'une véritable innovation.
  - **Il est demandé aux entités financières de mettre en place et de maintenir des systèmes** et outils de **TIC résilients** qui réduisent le plus possible l'impact des risques, d'identifier en permanence toutes les sources de risques, de mettre en place des mesures de protection et de prévention, de détecter rapidement toute activité anormale, de mettre en place des politiques de continuité des activités dédiées et exhaustives ainsi que des plans de secours et de rétablissement, ces éléments faisant partie intégrante de la politique de continuité opérationnelle.
  - L'organe de direction devra conserver un rôle actif essentiel dans la direction du cadre de gestion des risques liés aux TIC et maintenir une hygiène stricte en matière de cybersécurité. La **responsabilité pleine et entière de l'organe de direction** dans la gestion des risques liés aux TIC de l'entité financière sera un principe global qui devra être traduit plus avant en un ensemble d'exigences spécifiques.

PRINCIPAUX ÉLÉMENTS À RETENIR : DORA CRÉE UNE EXIGENCE EN MATIÈRE DE REPORTING DES INCIDENTS ET UNIFORMISE LA PRATIQUE DES TESTS

- DORA crée une exigence en matière de reporting des incidents liés aux TIC applicable à l'ensemble des institutions financières
  - Les IF seront soumis à une déclaration **obligatoire des principaux incidents liés aux TIC**, et à un **signalement volontaire des cybermenaces importantes**.
  - Les délais de notification et de soumission des notifications d'incidents à l'autorité compétente en vertu de la DORA **seront fixés dans les textes de niveau 2** et non de niveau 1, afin de permettre une plus grande flexibilité.
  - **La surveillance de ces incidents sera dévolue aux autorités de supervision.** Article 17, paragraphe 1, premier alinéa : "Les entités financières notifient les incidents majeurs liés aux TIC à l'autorité compétente concernée".
  - Il sera également nécessaire d'organiser la communication des notifications aux autorités européennes compétentes (ABE, AEAPP, AEMF, BCE ou CRU).

- DORA exige des entités financières qu'elles effectuent des tests de résilience opérationnelle et des tests d'intrusion
  - **Le suivi de la mise en œuvre et des résultats des tests de résilience opérationnelle** (articles 21 et 22) et des tests d'intrusion (tests d'intrusion fondés sur la menace ou TLPT - article 23) est une question importante, compte tenu de la complexité de ces tests.
  - Tout le monde devrait effectuer des tests de base: analyses, vulnérabilités, différentes analyses. Vérification de l'approche fondée sur les risques...
  - Certaines entités parmi les plus importantes seront désignées par le ou les ACN, qui effectueront le TLPT. Les autorités nationales compétentes auront un rôle important à jouer en **aidant les entités à réaliser les tests**.
  - En ce qui concerne les TLPT en particulier, les autorités compétentes devront décider quels assureurs devraient effectuer des TLPT ou modifier la fréquence triennale des TLPT.
  - Volonté de se diriger vers une reconnaissance mutuelle des tests.

PRINCIPAUX ÉLÉMENTS À RETENIR EN MATIÈRE DE GESTION DE TIERS

- Aucun des principes introduits par DORA n'est inédit
  - L'entité financière reste la **responsable** du risque
  - Le risque doit être géré de **manière proportionnelle**
  - Les entités financières doivent établir une **stratégie** relative au risque de tiers
  - Les entités financières doivent maintenir un **registre d'information** et **signaler** lorsqu'un contrat porte sur des fonctions critiques ou importantes
  - Étude **précontractuelle** des risques, sécurité et accès aux **données** et **stratégies de sortie**
- Les bonnes pratiques contractuelles sont réaffirmées
  - Clarté des obligations réciproques
  - Accords de niveau de service
  - Clauses de réversibilité…
- Mais DORA harmonise des termes, des périmètres et des pratiques
  - « risque de tiers » plutôt qu'« externalisation »
  - Une approche commune partagée avec les filiales et concurrents français et européens, des secteurs de la banque et de l'assurance…
- DORA va plus loin en organisant la surveillance des prestataires critiques au niveau européen

ACPR
BANQUE DE FRANCE

A VENIR : LE TRAVAIL DE POLICY AU NIVEAU EUROPEEN, UN CHANTIER ESSENTIEL

2022-2024 : Participer aux travaux sur les textes de niveau 2

8 RTS, 2 ITS (ci-après « actes délégués »), 2 orientations (sous 18 mois) et un rapport (sous 2 ans), soit un total de 13 textes, devront être adoptés par le Joint Committee des 3 AES (en lien éventuellement avec l'ENISA et/ou la BCE). La Commission adoptera en outre deux règlements délégués supplémentaires.

- ❑ Pilier Gestion des risques : concilier les exigences présentes dans les Guidelines et le texte DORA
- ❑ Pilier Reporting des incidents : les textes de niveau 2 préciseront le cadre de reporting des incidents (complétés par un rapport). Cohérence avec NIS.
- ❑ Pilier Test de résilience : L'essentiel des caractéristiques sont fixées au niveau 1, les textes de niveau 2 préciseront la méthodologie des tests d'intrusion (1 RTS).
- ❑ Pilier Externalisation et prestataires critiques : Le texte de niveau 1 établit clairement la mission du lead overseer : réaliser un assessment détaillé des règles et procédures mises en place par le prestataire pour réduire les risques informatiques qu'il fait peser aux entités financières clientes. La liste de ses pouvoirs est également définie de manière précise (accès à l'information, inspection…). Le RTS « on the conduct of oversight (art 36(1) » précisera certaines modalités de la surveillance qui sera effectuée sur les prestataires tiers critiques. En outre, le RTS précisera l'équilibre des rôles au sein des Joint Examination Teams (JET), avec un impact indirect sur la gouvernance du cadre de surveillance. Par ailleurs, la Commission a la responsabilité d'adopter le règlement délégué arrêtant la méthodologie de désignation des prestataires tiers critiques (art 28(3)). Sur la supervision existante du risque de tiers lié aux prestataires informatiques, des RTS devraient également apporter des compléments sur l'appréciation de ce risque par les IF.

2. ÉTAT DE PRÉPARATION DU MARCHÉ

LES AXES DE PROGRÈS D'ICI 2025

- Rappel : les références réglementaires actuelles
- La gouvernance et la gestion du risque cyber
- Les mesures de gestion opérationnelle : sécurité logique et continuité d'activité
- La gestion des risques liés aux TICS des tiers

LE CADRE DE RÉFÉRENCE

CADRE RÈGLEMENTAIRE BANCAIRE FRANÇAIS

Cadre européen harmonisé

ACPR déclarée conforme

- EBA/GL/2019/04 : orientations sur la gestion du risque et de la sécurité informatique (11/2019)
- EBA/GL/2021/05 : orientations sur la gouvernance interne (07/2021)
- EBA/GL/2019/02 : orientations sur l'externalisation (02/2019)

Cadre règlementaire

Conforme au cadre européen depuis fév. 2021

- Gouvernance / organisation du contrôle interne (titre 2, chapitre 1)
- Externalisation (titre 5, chapitre 2)
- Gestion de la continuité (article 215)
- Gestion du risque informatique (titre 6 bis)

Clarification du cadre règlementaire

Points de vigilance, bonnes pratiques

- Gouvernance et dispositif de gestion du risque informatique (section 1)
- Gestion des opérations informatiques (section 2)
- Gestion des projets informatiques et des changements (section 3)
- Sécurité du système d'information (section 4)
- Gestion de la continuité d'activité (section 5)

LE CADRE DE RÉFÉRENCE

CADRE RÈGLEMENTAIRE ASSURANCE FRANÇAIS

Règlement délégué Solvabilité II (UE) 2015/35 du 10 octobre 2014

Orientations AEAPP relatives à la sous-traitance à des prestataires en nuage (EIOPA-BoS-20-002)

Cadre européen harmonisé

Dispositions prudentielles d'application directe

ACPR déclarée conforme

- Dispositions d'ordre général sur la gouvernance, la gestion des risques et le contrôle interne, applicables y compris aux technologies de l'information et de la communication
- Politique de sous-traitance, évaluation des risques induits et surveillance, gouvernance, contractualisation et pilotage, notifications, documentation

Code des Assurances

Cadre règlementaire

Dispositions générales couvrant de fait la gestion des risques inhérents aux systèmes d'information

- Articles L. 354-1 à L. 354-3 : système de gouvernance, système de gestion des risques et système de contrôle interne, gestion de la sous-traitance, continuité d'activité

Notice ACPR

relative à la mise en œuvre des orientations AEAPP sur la gouvernance et la sécurité des TICs

Clarification du cadre règlementaire

Reprises des orientations (EIOPA-BoS-20/600)

- Proportionnalité, gouvernance et cadre de maitrise des risques (orientations 1 à 5)
- Gestion de la sécurité (orientations 6 à 13)
- Gestion des opérations et des incidents (orientations 14 et 15)
- Gestion des changements (orientations 16 à 18)
- Gestion de la continuité d'activité (orientations 19 à 24)
- Gestion de l'externalisation (orientation 25)

ACPR BANQUE DE FRANCE

LA GOUVERNANCE ET LA GESTION DU RISQUE CYBER

Carences constatées

- Dévoiement du principe de proportionnalité
- Manque d'implication des instances dirigeantes
- Insuffisante intégration du risque cyber dans l'univers des risques cartographié par les équipes de Gestion des risques et d'Audit interne

Références règlementaires

Secteur Banque

- Art. 12, 18, 24, 25, 100, 102, 270-1 et 270-2 de l'arrêté du 3 novembre 2014 sur le contrôle interne
- Section 1 de la Notice ACPR sur la gestion du risque informatique (07/2021)

Secteur Assurance

- Art. 258 – 261 bis, 266 – 273 du Règlement délégué SII
- Orientations 1 à 7 de la notice ACPR TICs 07/2021

Attentes du superviseur

- **Principe de proportionnalité : PROPORTIONNÉ AU RISQUE !** nécessité d'analyser et d'évaluer avant de décider dans une instance *ad hoc* des mesures proportionnées à mettre en œuvre (fonction de l'exposition objective au risque SSI et de la tolérance explicitée au risque SSI)
- **Implication des dirigeants effectifs et du conseil d'administration** dans les décisions structurantes (définition et suivi de la stratégie informatique et de sécurité, participation au processus de décision du recours à l'externalisation pour les prestations essentielles et importantes, décision et suivi des projets informatiques les plus importants y compris arbitrage en fonction des conclusions de l'analyse de sécurité IT, allocation des ressources en fonction du niveau de risque…)
- **Bonne organisation de la SSI :** les tâches opérationnelles de SSI sont gérées par un équipe spécialisée appartenant à la 1ère ligne de défense et répond aux préconisations et au contrôle d'une équipe disposant également de compétences en SSI située en 2ème ligne de défense. La 2LoD SSI est indépendante des fonctions opérationnelles. Elle accède aux instances et aux informations, interagit avec l'ensemble des lignes de défense et travaille en coordination étroite avec la Gestion des Risques et l'Audit interne
- Mise en place d'une **cartographie complète des risques tenant compte de toutes les dimensions du risque informatique dont la sécurité** et d'un **cadre de tolérance adapté et partagé** (limites du risque, indicateurs de suivi quantitatifs, processus prévu en cas de dépassement des limites, modalités de révision du cadre, …) **ainsi que de contrôles 1er et 2nd niveau intégrés au processus de contrôle permanent**
- Conception d'un scenario d'événement adverse pertinent et plausible étudié dans le cadre du PCA (adhérence avec l'ORSA - secteur assurance)

ACPR BANQUE DE FRANCE

LES MESURES DE GESTION OPÉRATIONNELLE : SÉCURITÉ LOGIQUE ET CONTINUITÉ D'ACTIVITÉ

Carences constatées

- Gestion des droits d'accès peu rigoureuse et revue irrégulière
- Inventaire des actifs incomplet et obsolète
- Tests de sécurité/d'intrusion incomplets/inadaptés
- Des tests de sauvegarde et de restauration pas encore systématiques
- Des PCA et PSI non testés / régulièrement

Références règlementaires

Secteur Banque

- Articles 270-3 et 215 de l'arrêté du 3 novembre 2014 sur le contrôle interne
- Sections 2, 4 et 5 de la Notice ACPR sur la gestion du risque informatique (07/2021)

Secteur Assurance

- Art. 258 (1 j) et 258 (3) du Règlement délégué SII
- Orientations 8, 12, 14 et 23 de la notice ACPR TICs 07/2021

Attentes du superviseur

- Formaliser et mettre en place un processus de gestion des droits d'accès (« principes ») et de revue annuelle
- **Actualiser au fil de l'eau un inventaire exhaustif des actifs informatiques** en indiquant notamment leur criticité, leur propriétaire, leur emplacement, leur classification de sécurité et en **incluant systématiquement le niveau de version** pour la bonne gestion des correctifs et des mises à jour qui pourront ainsi être déployés en temps utile
- Définir un cadre de tests de la sécurité du SI définissant une périodicité et prenant en compte « ses » particularités, en faisant évoluer les périmètres d'une fois sur l'autre en fonction de la criticité des TICs et idéalement de l'actualité des menaces
- Les procédures de sauvegarde et de restauration doivent être testées à intervalles réguliers et au moins annuellement
- Les PCA et PSI doivent être régulièrement testés en fonction du profil de risque des ressources TICs et leurs interdépendances (y compris de TICs de tiers)

LE CLOUD : AVANTAGES ET INCONVÉNIENTS

- Une technologie qui devient dominante
- Et qui présente des avantages:
  - Flexibilité du dimensionnement (virtualisation)
  - Facilité de mise à jour et de déploiement
  - Maîtrise de la configuration (Infrastructure as code)
  - Adaptation aux nouvelles technologies (IA, Big data)
  - Meilleure capacité technique du prestataire ?
  - Pouvant mener à une réduction des coûts?

- **L'enjeu principal: conserver la maîtrise de la prestation externalisée**
  - Implication des instances dirigeantes
  - Clauses contractuelles, droit d'audit
  - Niveaux de service (SLAs, pénalité)
  - Évaluation des risques et contrôles
  - Choix de configuration sécurisée
  - Gestion des incidents
- **4 points d'attention**:
  - Protection des données personnelles
    - Conformité au GDPR très difficile dans le cas des prestataires de cloud américains
  - Sécurité technique (chiffrement)
    - Quel contrôle des clés de chiffrement?
  - Résilience, continuité d'activité
    - Quelle maîtrise des Data centres utilisés?
    - Les environnements de cloud public n'offrent pas toujours un niveau de résilience égal à ce qui est requis par la réglementation bancaire
  - Difficulté de sortie de la prestation

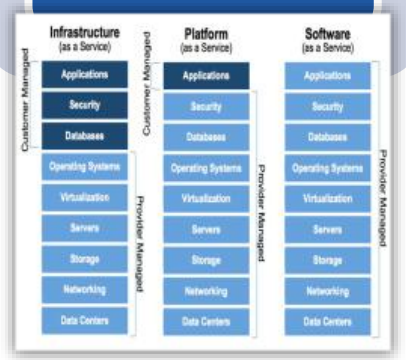
LE CLOUD, COMMENT MAÎTRISER ?

Maîtriser son environnement

Privilégier le cloud privé ou le cloud public de confiance pour des éléments sensibles

Maîtriser sa prestation

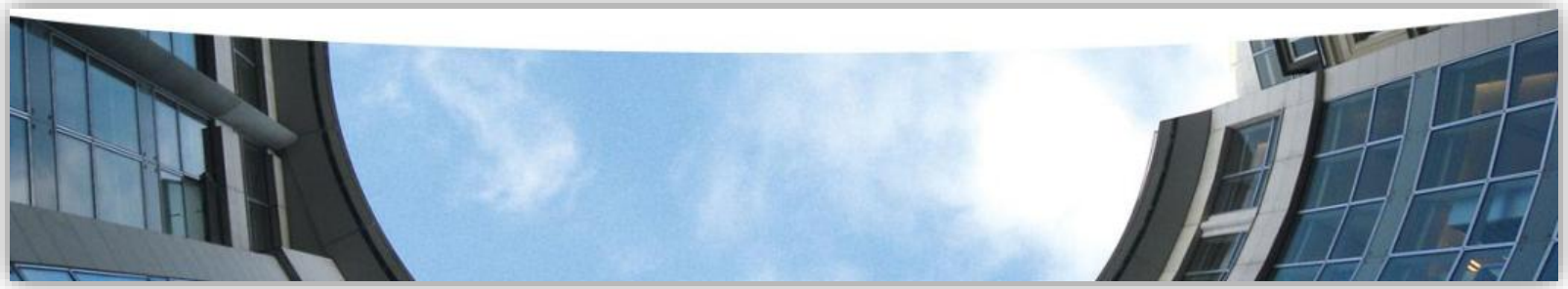
Le IaaS offre moins d'optimisation que le PaaS, mais permet de garder le contrôle de l'infrastructure



Maîtriser sa migration

Projets potentiellement complexes et ambitieux (coûts, délais, besoin d'expertise)

MERCI DE VOTRE ATTENTION




ACPR
BANQUE DE FRANCE
AUTORITÉ
DES MARCHÉS FINANCIERS
AMF
FORUM FINTECH
ACPR - AMF
19 oct. 2022

Forum Fintech ACPR-AMF 2022

Cybersecurité et risques informatiques les points d'attention des autorités

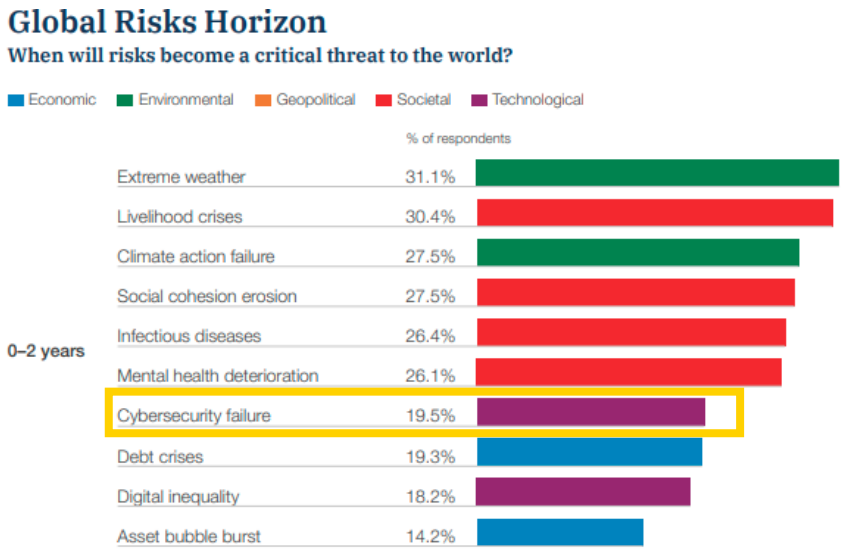
AUTORITÉ DES MARCHÉS FINANCIERS
AMF

ACPR
BANQUE DE FRANCE

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 **7eme risque le plus critique à court terme**, et le **8ème** à **moyen terme**

↗ https://www.weforum.org/reports/global-risks-report-2022/
↗ https://www.weforum.org/reports/global-risks-report-2022/data-on-global-risks-perceptions

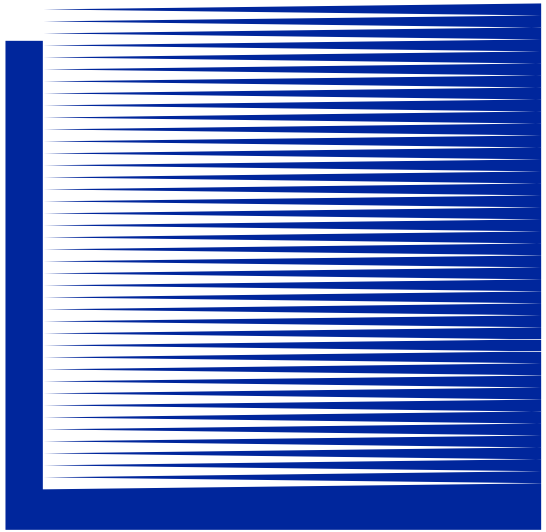


☐ Avec la **transformation numérique des services financiers**, ce risque doit ainsi être pris en compte par les **fournisseurs de services et solutions afin d'assurer la confiance et la résilience**, propriétés indispensables pour ce secteur d'activité

→ 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 incidents d’origine cyber observés

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

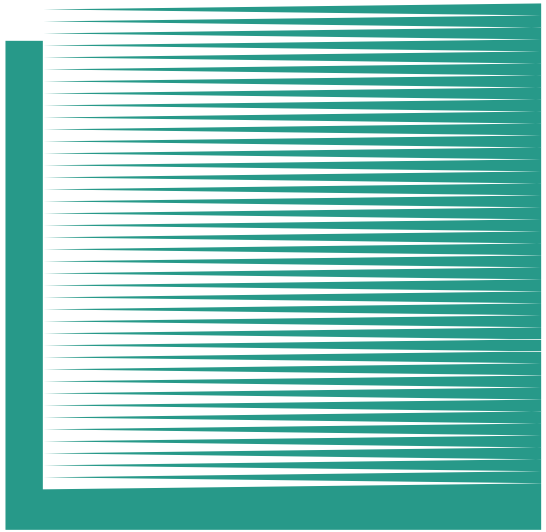
Une vingtaine d'incidents observés depuis 2020

Des schémas d'attaque récurrents

- **Détournement d'authentifiants individuels** (par *phishing* ou autre vecteur)
  - → Souvent, du **compte de messagerie Cloud** d'une personne clé de l'entité (Président, DG, RCCI/RCSI etc.) puis tentative de *phishing* envoyée à tout le carnet de contacts de cette personne…dont l'AMF
- **Usurpation d'identité** de personnes **morales** ou **physiques**
  - → Fraude auprès de /en tant que : **personne clé** de l'entité ; **client** ; **l'entité** ; **partenaire/fournisseur** de l'entité (dépositaire, conservateur, etc.)
  - → Par ex. via la création **d'adresses mail** avec des noms de domaine **visuellement proches** de l'entité légitime
- **Intrusion** puis **compromission du système d'information,** puis par exemple exécution d'un *rançongiciel*

Des objectifs et des impacts variés

- Tenter de **détourner les authentifiants** des **contacts** de la **personne piégée** initialement
- Piéger la victime afin **d'insérer un logiciel malveillant** sur son **poste de travail** et son **système d'information**
- **Accéder à, puis éventuellement divulguer, des informations professionnelles ou personnelles** plus ou moins **précises**, avec +/- de **discrétion** durant une période +/- **longue dans le temps** (jusqu'à quelques dizaines de mois)
  - → Dont par ex. le maintien au sein de boites mail, avec des **règles de redirections automatiques et silencieuses vers des adresses mail maitrisées par l'attaquant**
- Détournement de **fonds, extorsion**
  - → **Interposition** lors **d'appels de fonds, rançonnage,** etc.



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

AUTORITÉ DES MARCHÉS FINANCIERS

AMF

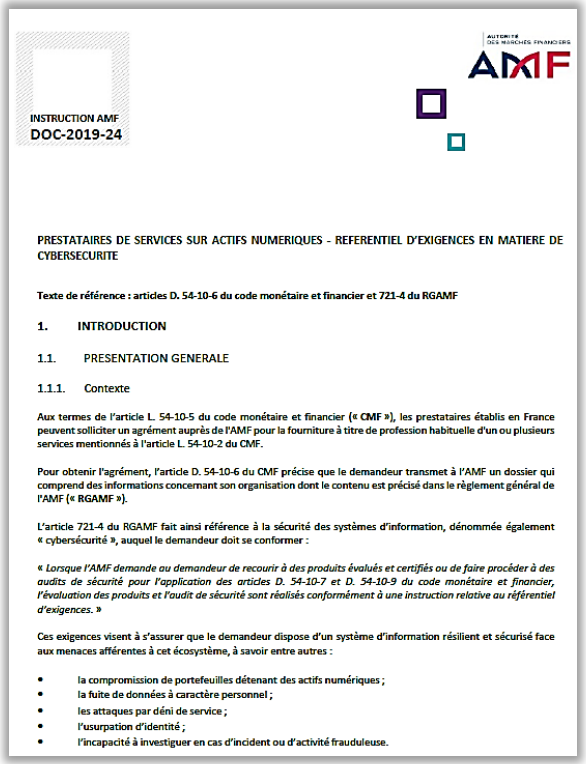
Structure de l'instruction DOC-2019-24 en matière de cybersécurité des prestataires de services sur actifs numériques (PSAN)

Cette instruction se divise en deux parties

- 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.)
- Mais surtout 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 !**

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



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 DOC-2019-24

Le programme de cybersécurité doit comprendre a minima ces 8 axes

1. L'identification des **risques d'origine cyber** pesant sur l'entreprise et leur **évaluation** en termes de **probabilité** et d'**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 DOC-2019-24

Le programme de cybersécurité doit comprendre a minima ces 8 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**

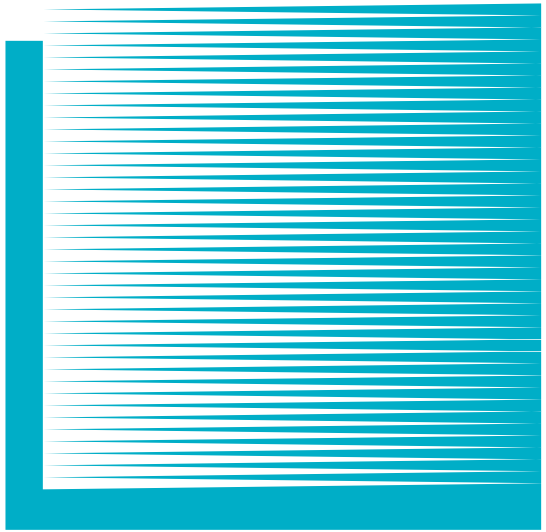
6 La gestion des **vulnérabilités** incluant une **veille sur les vulnérabilités techniques et menaces** pouvant apparaître ainsi que **l'application d'une politique** permettant leur **traitement**

→ 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, organisationnels 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

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

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

AMF

- **Poursuite** de la réalisation de **contrôles** à composante **cyber en 2023**
- **Généralisation** du processus de **collecte et traitement des incidents d’origine cyber** des assujettis
- **Appui** aux activités des **Autorités européennes de supervision (AES, *ESA*)** concernant **DORA**

Commission européenne

- Constitution du **comité joint** de supervision DORA par les **ESA** d’ici **fin 2022**
- Démarrage des travaux de formalisation des textes de **niveau 2** de DORA **début 2023**
- **Publication** estimée de **DORA** au JOUE d’ici le premier trimestre **2023, pour entrée en application** estimée **d’ici 2025**

ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

FORUM FINTECH

ACPR - AMF