Forum Fintech ACPR AMF

Atelier « Cybersécurité et risques informatiques »

16 octobre 2023

Intervenants

- **Thomas Debize**, responsable sécurité de l'information, direction Ressources, support et transformation, AMF
- **Déborah Haddad**, experte en risque cyber, direction des Affaires internationales, ACPR
- **Eric Ly**, contrôleur sur place IT et cyber, Délégation au contrôle sur place des établissements de crédit, ACPR

Cyber-sécurité et risques informatiques

1ère partie

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

ACPR
BANQUE DE FRANCE

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

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 **8eme risque le plus critique à court et long terme**

↗ https://www.weforum.org/reports/global-risks-report-2023
↗ https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Global risks ranked by severity over the short and long term

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period"

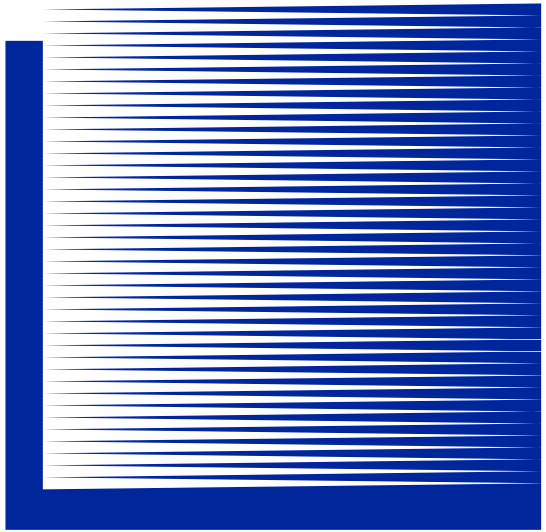
	2 years		10 years
1	Cost-of-living crisis	1	Failure to mitigate climate change
2	Natural disasters and extreme weather events	2	Failure of climate-change adaptation
3	Geoeconomic confrontation	3	Natural disasters and extreme weather events
4	Failure to mitigate climate change	4	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	5	Large-scale involuntary migration
6	Large-scale environmental damage incidents	6	Natural resource crises
7	Failure of climate change adaptation	7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	8	Widespread cybercrime and cyber insecurity

☐ 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, révisée en 2023**, et précise les exigences en matière de cybersécurité que doivent respecter les **prestataires de services sur actifs numériques (PSAN)** dans le cadre d'un **enregistrement renforcé ou agrément optionnel**



Retour d’expérience sur les incidents d’origine cyber observés

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

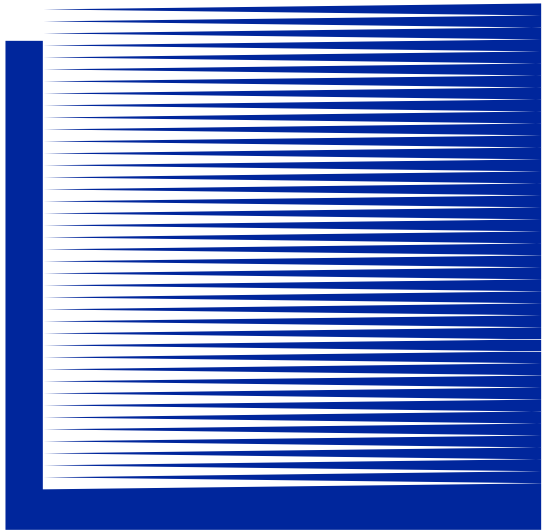
Une vingtaine d'incidents observés depuis 2020

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

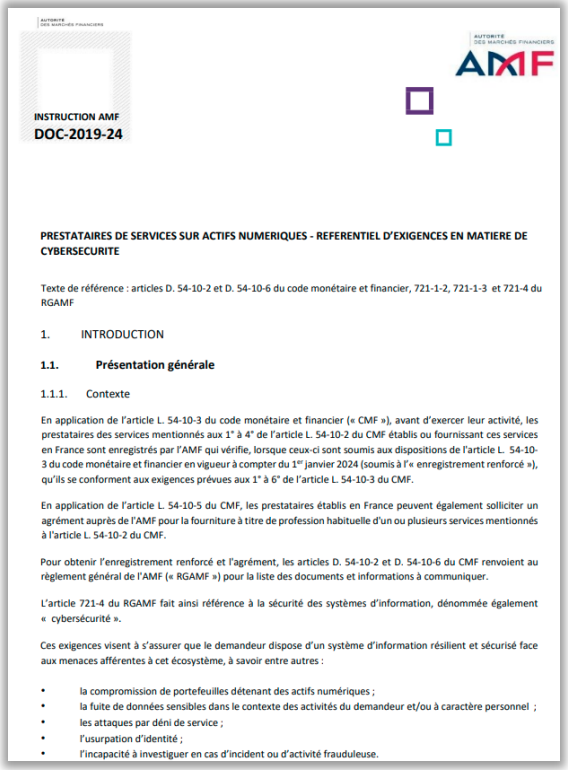
Structure de l'instruction DOC-2019-24 en matière de cybersécurité des prestataires de services sur actifs numériques (PSAN)

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. 54-10-2 et D. 54-10-6 du code monétaire et financier, 721-1-2, 721-1-3 et 721-4 du RGAMF

1. INTRODUCTION

1.1. Présentation générale

1.1.1. Contexte

En application de l'article L. 54-10-3 du code monétaire et financier (« CMF »), avant d'exercer leur activité, les prestataires des services mentionnés aux 1° à 4° de l'article L. 54-10-2 du CMF établis ou fournissant ces services en France sont enregistrés par l'AMF qui vérifie, lorsque ceux-ci sont soumis aux dispositions de l'article L. 54-10-3 du code monétaire et financier en vigueur à compter du 1er janvier 2024 (soumis à l'« enregistrement renforcé »), qu'ils se conforment aux exigences prévues aux 1° à 6° de l'article L. 54-10-3 du CMF.

En application de l'article L. 54-10-5 du CMF, les prestataires établis en France peuvent également 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'enregistrement renforcé et l'agrément, les articles D. 54-10-2 et D. 54-10-6 du CMF renvoient au règlement général de l'AMF (« RGAMF ») pour la liste des documents et informations à communiquer.

L'article 721-4 du RGAMF fait ainsi référence à la sécurité des systèmes d'information, dénommée également « cybersécurité ».

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 sensibles dans le contexte des activités du demandeur et/ou 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**

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

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**

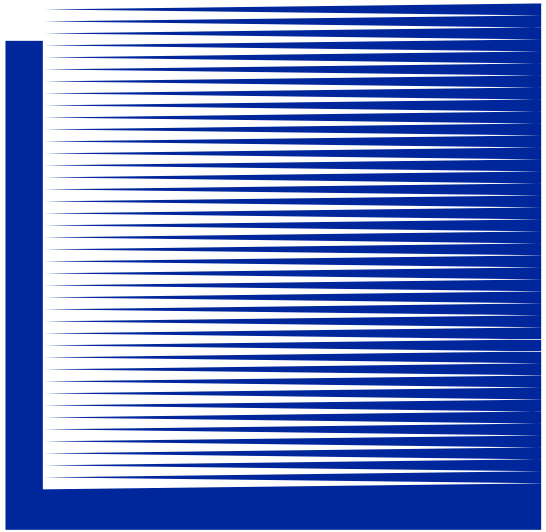
6 La gestion des **vulnérabilités** incluant une **veille sur les vulnérabilités techniques et menaces** pouvant apparaître ainsi que **l'application d'une politique** permettant leur **traitement**

→ 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** incluant une **composante cyber**
- ☐ **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 à travers la participation au comité joint de supervision**

Commission européenne : DORA

- ☐ Pour le **premier** lot de **projets de standards techniques** (RTS, ITS)
  - → **Consultation publique** entre **juin 2023 et septembre 2023**
  - → **Fin janvier 2024** : soumission à la **Commission européenne**
- ☐ Pour le **second** lot de **projets de standards techniques**
  - → **D’ici novembre 2023**, finalisation des projets
  - → **Consultation publique entre novembre 2023 et février 2024**
  - → **Fin juin 2024**, soumission à la Commission européenne
- ☐ **Entrée en application de DORA le 17 janvier 2025**

FORUM FINTECH 2023

CYBER-SÉCURITÉ ET RISQUES INFORMATIQUES

2ÈME PARTIE

16 OCTOBRE 2023

SOMMAIRE

1. Le cadre européen DORA

2. L'importance de la continuité informatique pour les Fintech et les attentes des superviseurs

1. LE CADRE EUROPÉEN DORA

CONTEXTE : UNE HAUSSE DE LA MENACE CYBER

- DORA s'inscrit dans un contexte de **hausse de la menace cyber**, qui n'épargne pas le secteur financier et les Fintech
- Vols de fonds, dont les plateformes d'échange de crypto-actifs et de finance décentralisée sont particulièrement la cible
  - *Ex : CoinsPaid (Juill 2023), BitBrowser (Sept 2023)*
- Attaques à visée d'extorsion, *via* l'usage ou non de rançongiciel
  - *Ex : attaque par le rançongiciel Lockbit contre ION Group (Févr 2023)*
- Exfiltration de données
  - *Ex : compromission d'au moins 30 000 données clients de Revolut (Sept 2022)*
- *Supply-chain attacks*
  - *Ex : compromission de MoveIT et atteinte aux données de ses clients, parmi lesquelles des Fintech (Mai 2023)*

CONTEXTE : L'ASSURANCE CYBER, L'UN DES LEVIERS DU RENFORCEMENT DE LA RÉSILIENCE CYBER

- La hausse de la menace (via notamment l'essor des rançongiciels) a accru le **niveau de sinistralité** à partir de 2019
- L'**assurabilité du risque cyber** est rendue complexe par l'évolution rapide de ce risque (évolution des TTPs et des cibles)
- Le potentiel de croissance du marché reste élevé, en particulier, la couverture des PME en assurance cyber reste améliorable
- Tendances actuelles du développement : coassurance et captives en essor, assurance des gros risques par strates
- Enjeux :
  - Pour le superviseur :
    - Stabilité financière (gestion du risque assuranciel, notamment couvertures implicites et reporting)
    - Protection de la clientèle (travaux sur la clarté des contrats)
    - LCBFT (dans le cadre de paiement de rançons)
  - Pour les assureurs, la maîtrise du risque passe par les autres actions des assureurs:
    - Les actions de préventions, auprès des assurés
    - Les formations de gestionnaires de sinistres et les procédures de prise en charge (gestion de crise dans le premiers jours suivant l'attaque)

INTRODUCTION À DORA

Finalité de DORA : renforcer le **versant numérique de la résilience opérationnelle** du secteur financier

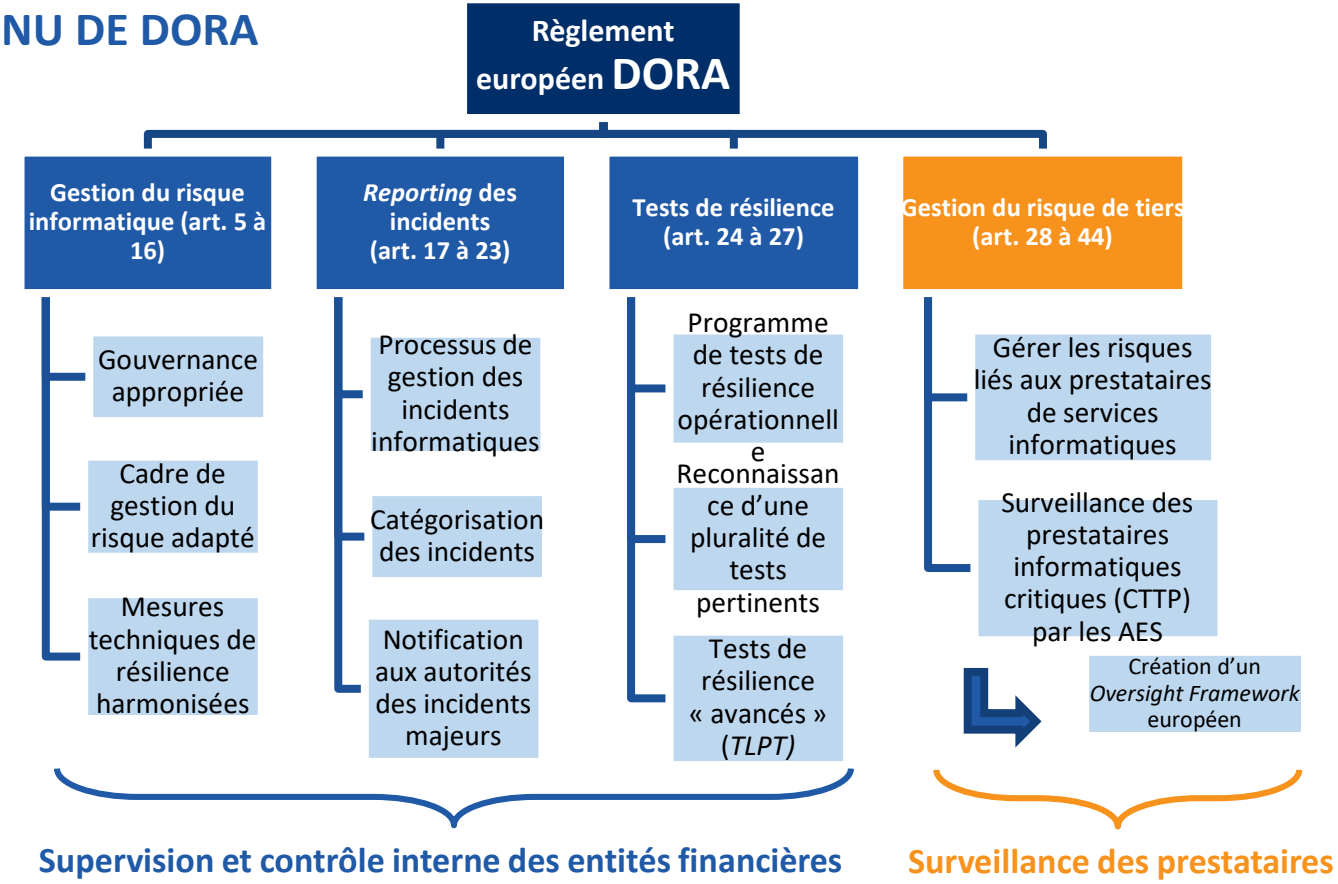
- DORA est la principale perspective réglementaire en matière de résilience IT/cyber dans le secteur financier d'ici 2025
- Un des éléments de la stratégie de l'UE en matière de finance numérique
- Adoption en décembre 2022 et **entrée en application en janvier 2025**
- C'est un règlement + une directive
- DORA est *lex specialis* de la directive *NIS2*
- Objectif : via un champ d'application particulièrement large, mettre fin à la fragmentation actuelle et à certaines lacunes dans la règlementation (en matière de gestion du risque cyber de tiers et de concentration des prestataires par exemple)
- Principe de **proportionnalité**

CHAMPS D'APPLICATION : LES FINTECH SONT CONCERNÉES

<table>
<tr><th>Compétence ACPR
– secteur assurance</th><th>Compétence ACPR
– secteur bancaire</th><th>Compétence AMF</th><th>Compétence Banque de France</th><th>Compétence ESMA</th></tr>
<tr><td>Organismes d'assurance et de réassurance (sauf les organismes écartés du périmètre de Solvabilité II en raison de leur taille)</td><td colspan="3">Contreparties centrales</td><td>Agences de notation de crédit</td></tr>
<tr><td>Intermédiaires d'assurance et de réassurance et intermédiaires d'assurance à titre accessoire (sauf si micro-entreprises ou PME, cf seuils fixés par DORA)</td><td>Établissements de crédit (sauf offices des chèques postaux)</td><td colspan="2">Dépositaires centraux de titres</td><td>Administrateurs d'indices de référence critiques</td></tr>
<tr><td>Institutions de retraite professionnelle (sauf < à 15 adhérents)</td><td colspan="2">Entreprises d'investissement
(sauf si exemptées à l'article 2 ou 3 de MiFID)</td><td rowspan="6"></td><td>Référentiels centraux</td></tr>
<tr><td rowspan="5"></td><td colspan="2">Prestataires de service en actifs numériques, tel que définis par le futur règlement MICA et émetteurs de jetons indexés sur des actifs.</td><td>Référentiels centraux de titrisation</td></tr>
<tr><td colspan="2">Plateformes de négociation
(MR, OTF, MTF)</td><td rowspan="3">Prestataires de services de communication de données</td></tr>
<tr><td>Établissements de monnaie électronique</td><td>Prestataires de services de financement participatif</td></tr>
<tr><td>Prestataires de services d'information sur les comptes</td><td>Sociétés de gestion</td></tr>
<tr><td>Établissements de paiement</td><td>Gestionnaires de fonds d'investissement alternatifs (sauf petits</td></tr>
</table>

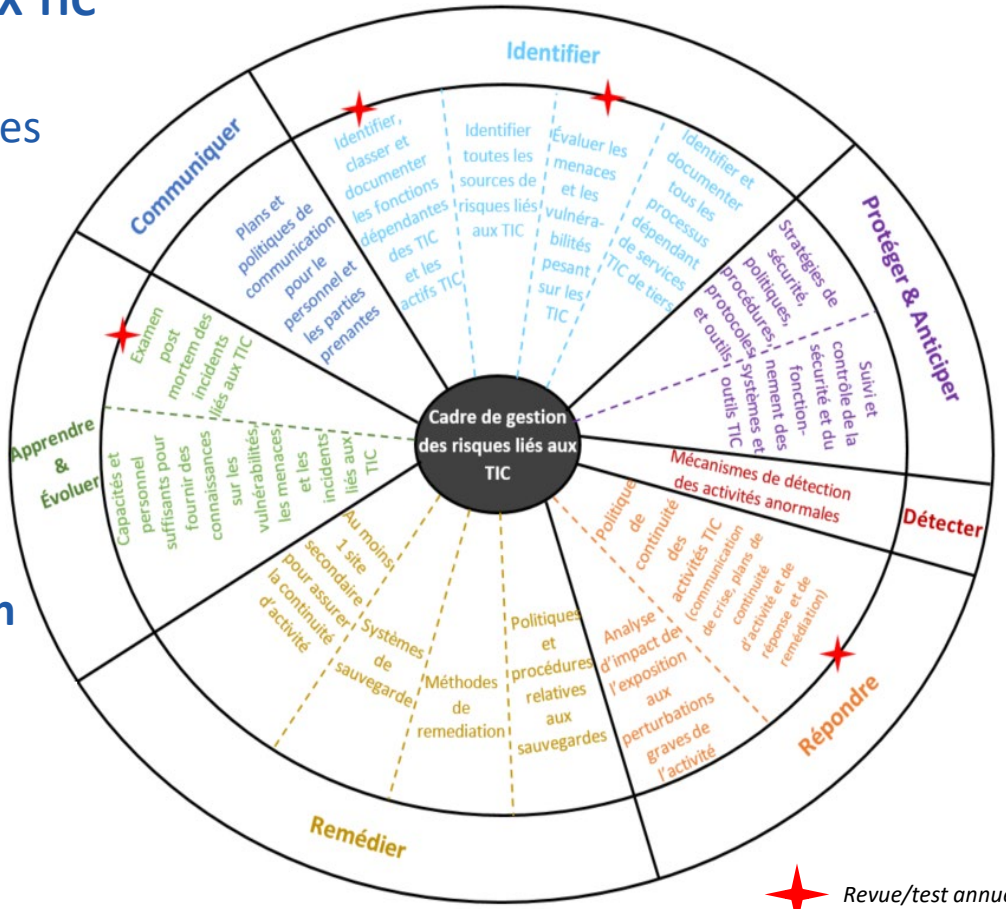
ACPR
BANQUE DE FRANCE

LE CONTENU DE DORA



CADRE DE GESTION DU RISQUE LIÉ AUX TIC

- Alignement à la hausse des exigences existantes (ABE/AEAPP) *via* la mise **en œuvre d'un cadre formel de gouvernance et de gestion du risque informatique**
- Régime simplifié à l'égard d'un nombre limité d'entités financières
- Gouvernance : **l'organe de direction est responsable** du cadre de gestion du risque informatique



REPORTING DES INCIDENTS

- **Déclaration obligatoire** pour toutes les entités financières des **incidents classifiés comme majeurs** selon des critères définis dans le RTS dédié
- Types d'incidents :
  - De paiement d'origine opérationnelle ou de sécurité (⇔ DSP2)
  - Liés aux TIC, c'est-à-dire liés à la compromission de la SSI au sens de l'art 3(8) de DORA
- En outre, reporting de remontée des cyber-menaces majeures sur base volontaire
- En l'attente du template DORA, un template de déclaration des incidents cyber sur base volontaire a été mis en place par l'ACPR à l'intention des établissements qu'elle supervise (hors MSU)

GESTION DU RISQUE DE TIERS

- Approche de la gestion de tiers plus large que l'externalisation.
- Avant DORA, le suivi des contrats avec des prestataires tiers de services TIC n'était pas pleinement consacré dans le droit de l'UE. Avec DORA :

Analyse précontractuelle (Art 28.4, 28.5, 29)	Clauses dans tous les contrats (Art 28.7, 30.2)	Pour les fonctions importantes (Art 30.3)
• Standards du prestataire en matière de sécurité informatique. • Évaluation des risques, y compris le risque de concentration. • Éventuels conflits d'intérêts.	• Description des services fournis. • Lieux des services fournis. • Disponibilité, confidentialité et sécurité des données. • Accès et restitution des données. • Niveaux de services. • Obligation d'assister le client. • Obligation de coopérer avec les autorités. • Contribution à la sensibilisation et la formation du client. • Droit de résiliation et préavis.	• Objectifs de performance du prestataire. • Délais de préavis. • Mise en œuvre et tests de plans d'urgence. • Participation du prestataire à la réalisation de tests d'intrusion du client. • Droit illimité du client à demander des documents et auditer. • Précisions sur la portée et la fréquence des audits et inspections. • Établissement d'une stratégie de sortie.

- Les entités financières sont **responsables** de l'exécution des contrats avec les prestataires.
  - Elles élaborent une **stratégie** dédiée.
  - Elles tiennent à jour et remettent au moins une fois par an un **registre**.

GESTION DU RISQUE DE TIERS : ILLUSTRATION AVEC LE CLOUD

- Les Fintech misent sur le Cloud
  - Tous les acteurs du marché financier utilisent au moins un service Cloud avec les avantages suivants :
    - Coûts d'investissement et d'exploitation réduits ;
    - Technologies et services avancés disponibles ;
    - Haute disponibilité des systèmes ;
    - Capacité d'adapter en temps réel les ressources informatiques aux besoins ;
    - Certains services apportent un premier niveau de sécurité.
  - Les assurtech s'appuient sur des nouveaux services offerts par les technologies Cloud pour inventer des services innovants et disruptifs :
    - Nouveau produit d'assurance (paramétrique) ;
    - Utilisation de l'IA pour un meilleur service personnalisé ;
    - Un parcours client simplifié et amélioré en particulier pour les PME et TPE.

GESTION DU RISQUE DE TIERS : ILLUSTRATION AVEC LE CLOUD

- Le transfert de l'exploitation de l'infrastructure, des applications et des données vers un tiers expose les souscripteurs aux risques suivants :
  - L'indisponibilité à fournir le service ;
  - La compromission des systèmes d'information ;
  - Le risque de fuite ou de perte de données ;
  - Risque d'accès aux données hébergées chez les Cloud Service Provider (CSP) qui sont soumis à l'extra-territorialité de certains droits (ex : « CLOUD ACT ») ;
  - Situation de forte dépendance vis à vis du fournisseur en cas de non prise en compte de la réversibilité.
- Les plateformes de Cloud ne sont pas immunisées contre les incidents

GESTION DU RISQUE DE TIERS : ILLUSTRATION AVEC LE CLOUD

- Maîtrise du risque lié au Cloud :
  - Pan réglementaire :
    - Renforcement contractuel
    - Cadre de gestion du risque de tiers
    - Référence en vigueur en l'attente de DORA : guidelines EBA/EIOPA, notice ACPR
  - Pan opérationnel :
    - Chiffrement spécifique des données ;
    - Solution complémentaire de sécurité :
      - Solution anti-DDoS ;
      - CASB (Cloud Access Security Broker) ;
      - Renforcement d'authentification ;
      - Approche 0 trust ;
      - Audit de tous les environnements virtualisés ;
      - CSPM (Cloud Security Posture Management).

CONCLUSION : LISTE DES ATTENDUS DE DORA

Nom de l'attendu (document, livrable, stratégie, politique interne)	Référence	Dispenses éventuelles
Cadre de gouvernance et de contrôle interne du risque ICT	Article 5.1	Les entités soumises au cadre simplifié de l'article 16.
Stratégies garantissant des normes élevées de disponibilité, authenticité, intégrité et confidentialité des données	Article 5.2.b	
Plan d'audit des TIC	Article 5.2.f	
Politique concernant les services TIC fournis par des prestataires tiers	Article 5.2.h	
Cadre de gestion du risque TIC (inclut : stratégie de résilience opérationnelle)	Articles 6.1 et 6.8	
Rapport sur le réexamen du cadre de gestion du risque TIC (sur demande de l'autorité compétente)	Article 6.5	
Stratégie globale multifournisseurs (facultatif)	Article 6.9	
Inventaires des risques ICT sur les fonctions métiers	Article 8.6	
Politique de la sécurité de l'information	Article 9.4.a	
Politiques qui limitent l'accès physique ou logique aux actifs ICT	Article 9.4.c	
Politiques et protocoles d'authentification forte	Article 9.4.d	
Politiques sur la gestion du changement ICT	Article 9.4.e	
Stratégies en matière de mises à jour et correctifs	Article 9.4.f	
Politique de continuité des activités de TIC	Article 11.1	
Plan de réponse et de rétablissement des TIC	Article 11.3	
Registre des activités lors de l'activation de PCA / plan de réponse	Article 11.8	
Estimation du coût annuel des incidents majeurs	Article 11.10	
Politiques et procédures de sauvegarde	Article 12.1.a	
Procédures et méthodes de restauration et rétablissement	Article 12.1.b	
Examens post-incident	Article 13.2	
Programmes de sensibilisation et formation du personnel	Article 13.6	
Plan de communication	Article 14.1	
Processus de gestion des incidents	Article 17.1	
Rapport d'incident initial	Article 19.4.a	
Rapport d'incident intermédiaire	Article 19.4.b	
Rapport d'incident final	Article 19.4.c	
Programme de tests de résilience	Article 24.1	Les microentreprises sont dispensées.
Procédures et stratégies pour traiter les problèmes identifiés par les tests	Article 24.5	Les microentreprises sont dispensées.
Plans de mesures correctives	Article 26.5	Les microentreprises sont dispensées.
Stratégie en matière de risques liés aux prestataires TIC tiers (inclut une politique sur l'externalisation des fonctions critiques et importantes)	Article 28.2	
Registre d'information sur tous les contrats d'externalisation TIC	Article 28.3	
Information sur tous les projets d'accord contractuel portant sur une externalisation TIC	Article 28.3	
Stratégies de sortie	Article 28.8	
Plans de transition	Article 28.8	
Mesures d'urgence lors de l'activation de la stratégie de sortie	Article 28.8	

COMMENT LES FINTECH PEUVENT-ELLES SE PRÉPARER À L'ARRIVÉE DE DORA ?

- Participer à la nouvelle consultation publique qui sera lancée fin 2023.
- Prendre connaissance des projets de standards techniques qui seront publiés début 2024, puis mi-2024.
- Identifier les livrables attendus dans le contexte du cadre de gestion du risque IT posé par DORA (plan d'audit, de communication, politique de sauvegarde, etc.).
- Mettre en place les canaux de communication pour informer en continu l'organe de direction de ces enjeux.
- Passer en revue tous les contrats de prestation informatique et s'assurer de leur conformité avec DORA.
- Lancer dès que possible les développements informatiques nécessaires aux nouvelles collectes de données qui seront conduites.

➡ Viser la ***résilience*** **opérationnelle** et non la seule maîtrise du *risque* opérationnel

2. IMPORTANCE DE LA CONTINUITÉ INFORMATIQUE POUR LES FINTECH & LES ATTENTES DES SUPERVISEURS

POURQUOI LA CONTINUITÉ INFORMATIQUE EST-ELLE IMPORTANTE POUR LES FINTECH ?

- Aujourd'hui, les Fintech sont des acteurs clés du secteur financier et ont une responsabilité de maintien de la stabilité, de la sécurité et de la confiance au sein de celui-ci.
- Les Fintech doivent faire face à des défis parmi lesquels la continuité informatique occupe une place centrale ; d'autant plus qu'elles se reposent en grande partie sur des systèmes d'information (SI).
- L'indisponibilité du SI peut entrainer des impacts importants pour les clients (ex : fonds bloqués, transactions suspendues), pour l'établissement lui-même (ex : pertes bases clients, perte de réputation) et la stabilité globale (ex : risque de contagion).
- Le règlement DORA prévoit des obligations relatives à la continuité informatique (articles 11 et 12).

QU'EST-CE QUE LA CONTINUITÉ INFORMATIQUE ?

- La continuité informatique désigne les mesures et moyens mis en œuvre pour garantir la disponibilité du système d'information selon les besoins exprimés par les utilisateurs.
- Les principales origines d'indisponibilités informatiques sont :
  - Mauvaise organisation de la continuité
  - Insuffisance dans l'identification des scénarios d'indisponibilité
  - Non-alignement de la continuité informatique avec la continuité métier
  - Protection insuffisante des moyens de production et de secours contre les accidents
  - Insuffisance des dispositifs de continuité
  - Tests insuffisants

QUELLES SONT LES ATTENTES DES SUPERVISEURS ? (1/4)

- **Les établissements doivent s'être organisés pour gérer leur dispositif de continuité d'activité, qui répond à des obligations réglementaires.**
  - La continuité d'activité s'appuie sur des politiques et des procédures formalisées.
  - Les rôles et les responsabilités pour les situations de gestion de crise sont clairement définis.
  - Les dirigeants doivent être impliqués.
  - Une méthodologie, une structure de gestion de crise efficace et une politique de communication adaptée sont nécessaires.
  - Un plan de continuité doit comporter un plan de secours informatique (PSI).
- **Les plans de continuité sont fondés sur des scénarios de perte de ressources, comprenant des dysfonctionnements de systèmes et de réseaux pour des durées plus ou moins longues.**
  - Analyses d'impact pour les métiers utilisateurs selon différents scénarios d'indisponibilité des locaux, des systèmes d'information, du personnel, de l'énergie et des télécommunications et des fournisseurs clés etc.

QUELLES SONT LES ATTENTES DES SUPERVISEURS ? (2/4)

- **Le PSI décrit les modalités de continuité pour la production informatique.**
  - Se base sur les analyses d'impact sur les métiers utilisateurs et les délais de rétablissement du service (exprimés en RTO et RPO).
  - Les écarts qui résulteraient d'une incapacité connue des moyens de secours doivent être portés à la connaissance des instances dirigeantes pour un éventuel arbitrage sur les besoins utilisateurs ou l'allocation de moyens supplémentaires.
- **Les centres informatiques sont particulièrement exposés aux accidents et détériorations pouvant affecter le matériel et ainsi provoquer des perturbations pour le bon fonctionnement du système d'information.**
  - Le choix des emplacements pour leurs centres informatiques est crucial, en évitant toute zone exposée à des risques naturels (zone inondable ou sismique par exemple) ou de voisinage (aéroport, site chimique, etc.).

QUELLES SONT LES ATTENTES DES SUPERVISEURS ? (3/4)

- **L'établissement doit pouvoir basculer l'exploitation de son système d'information sur une infrastructure de secours lorsque son système principal est indisponible.**
  - Les infrastructures doivent être opérationnelles pour faciliter le basculement de la production dans des délais réduits correspondants aux exigences des utilisateurs (RTO et RPO).
  - Les sauvegardes doivent être suffisamment fréquentes et protégées.
  - Si l'exploitation est répartie sur au moins deux sites fonctionnant en partage de charge (mode « actif-actif »), il importe que chacun des sites puisse supporter la charge totale de fonctionnement en cas d'indisponibilité d'un ou de plusieurs sites.
  - Les désastres régionaux doivent être pris en compte, en particulier par des distances suffisantes entre environnement de production et environnement de secours. Un troisième site est parfois nécessaire.

QUELLES SONT LES ATTENTES DES SUPERVISEURS ? (4/4)

- **L'efficacité et la pertinence des plans de continuité métiers et de secours informatique dépendent de tests de mise en œuvre suffisamment réguliers.**
  - Les plans de continuité sont testés sur un périmètre exhaustif à l'aide d'une méthodologie éprouvée.
  - La pertinence des tests de secours n'est démontrée que lorsque ceux-ci incluent le basculement de la production de l'environnement principal vers l'environnement de secours.
  - Cet environnement de secours doit ainsi être utilisé en situation réelle par les équipes métiers pendant une période suffisamment significative et sur un périmètre représentatif de leurs activités critiques.

MERCI DE VOTRE ATTENTION