Forum Fintech ACPR AMF

Atelier « Cybersécurité et risques informatiques : ce que DORA va changer »

14 octobre 2024

Intervenants

- **Déborah Haddad** – ACPR – Direction des affaires internationales de l'ACPR – Banques
- **Gauthier Villerabel** – ACPR – Direction du contrôle des banques
- **Eric Ly** – ACPR – Contrôle sur place – Banques
- **Thomas Debize** – AMF – Direction cybersécurité, sûreté et risques
- **Bruno Buresi** – AMF – Direction des contrôles

Déroulé de l'atelier

- Les temps forts :
  - → Première partie (ACPR) :
    - Le cadre européen DORA
    - Modalités de reporting (incidents & RoI)
    - Retours d'expérience en matière de supervision du risque cyber
  - → Seconde partie (AMF) :
    - Retour d'expérience sur les contrôles cyber
    - L'approche future de l'AMF concernant le risque d'origine cyber des assujettis

PREMIÈRE PARTIE : ACPR

1. Le cadre européen DORA
2. Modalités de reporting (incidents & RoI)
3. Retours d'expérience en matière de supervision du risque cyber

1. LE CADRE EUROPÉEN DORA

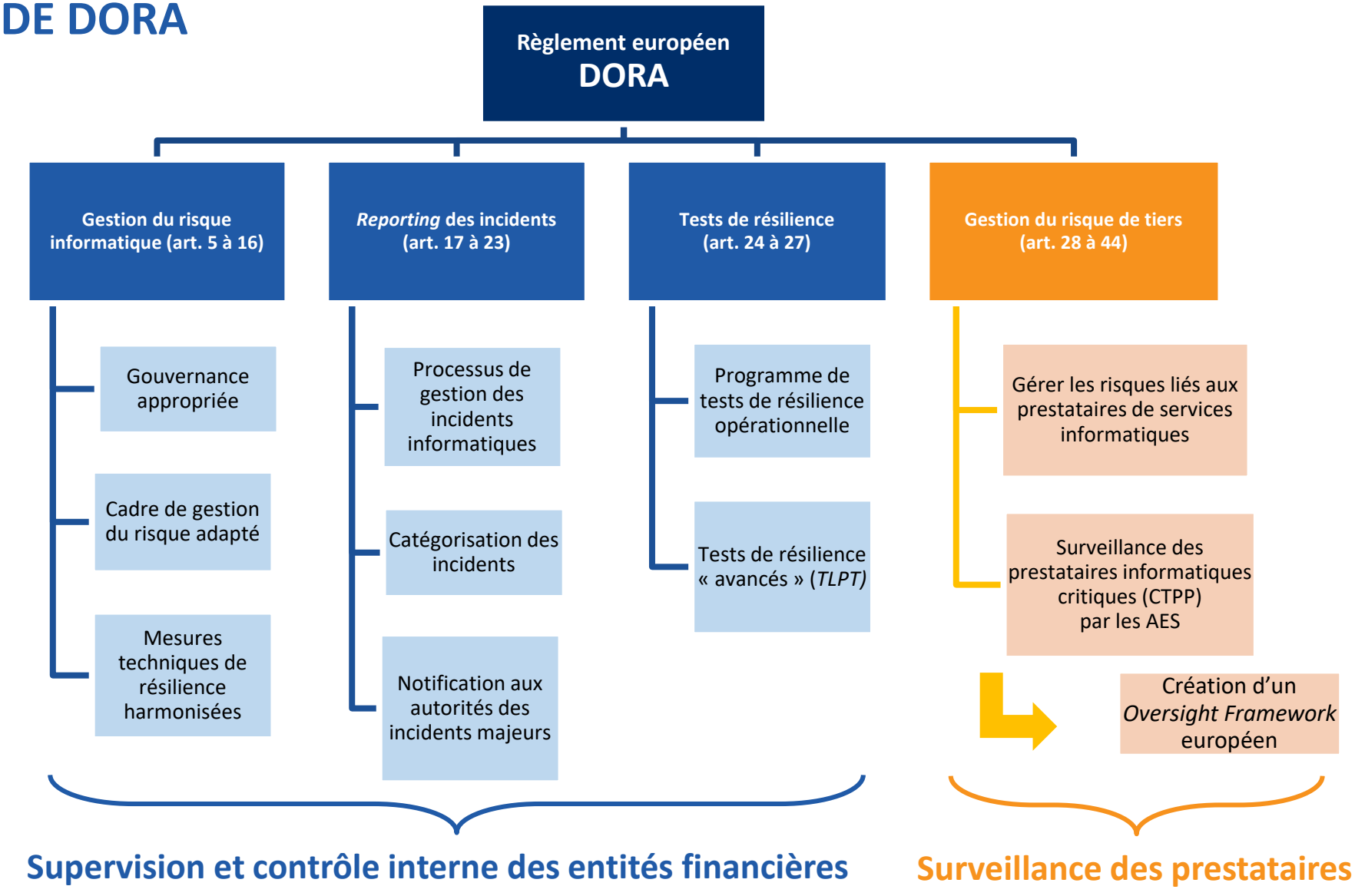
1. PROPOS INTRODUCTIF

- DORA c'est un règlement, une directive, 9 RTS, 2 ITS, 2 *guidelines* et un *call for advice*
- Via un champ d'application particulièrement large, DORA met fin à la fragmentation actuelle (sectorielle), à certaines lacunes dans la règlementation voire à une absence de réglementation
- Entrée en application : 17 janvier 2025
- 3 notions au cœur de DORA :
  - La résilience opérationnelle numérique qui va au-delà de la sécurité des systèmes d'information
  - Les fonctions critiques ou importantes :
    - Art3(22) : « une fonction dont la perturbation est susceptible de nuire sérieusement à la performance financière d'une entité financière, ou à la solidité ou à la continuité de ses services et activités, ou une interruption, une anomalie ou une défaillance de l'exécution de cette fonction est susceptible de nuire sérieusement à la capacité d'une entité financière de respecter en permanence les conditions et obligations de son agrément, ou ses autres obligations découlant des dispositions applicables du droit relatif aux services financiers »
    - Il appartient aux entités financières d'établir des critères de criticité tout en s'assurant que les évaluations restent appropriées et proportionnées à leurs spécificités
  - La proportionnalité (article 4 de DORA)
- Le règlement ne se concentre pas uniquement sur la conformité aux exigences réglementaires
- DORA est *lex specialis* de la directive NIS et de sa révision NIS2

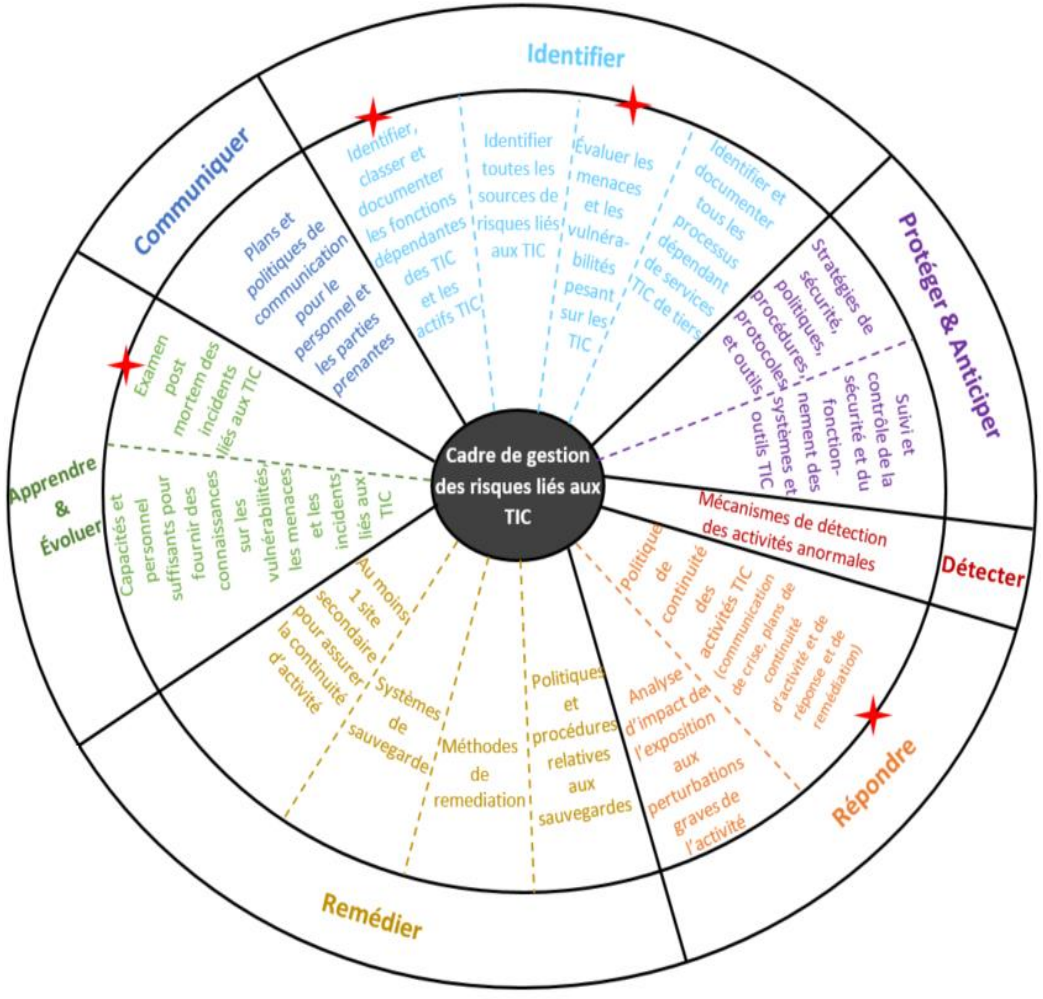
2. ACTEURS ET CHAMPS DE COMPÉTENCE
LES FINTECHS SONT CONCERNÉES

<table>
<tr><th>Compétence ACPR
– secteur assurance</th><th>Compétence ACPR
– secteur bancaire</th><th>Compétence AMF</th><th>Compétence Banque de France</th></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">Contrepartie centrale</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
(pour les compétences ne relevant pas de la BCE au titre du MSU)</td><td colspan="2">Dépositaires centraux de titres</td></tr>
<tr><td rowspan="2">Institutions de retraite professionnelle (sauf < à 15 adhérents)</td><td>Entreprises d’investissement
(sauf si exemptées à l’article 2 ou 3 de MiFID)</td><td>Sociétés de gestion</td><td rowspan="6"></td></tr>
<tr><td colspan="2">Plateformes de négociation
(MR, OTF, MTF)</td></tr>
<tr><td rowspan="4"></td><td>Établissements de monnaie électronique</td><td>Gestionnaires de fonds d’investissement alternatifs
(sauf petits & moyens)</td></tr>
<tr><td>Établissements de paiement</td><td rowspan="2">Prestataires de services de financement participatif</td></tr>
<tr><td>Prestataires de services d’information sur les comptes</td></tr>
<tr><td colspan="2">Prestataires de services sur crypto-actifs
Émetteurs de jetons se référant à des actifs (ART)</td></tr>
</table>

3. PILIERS DE DORA



4. CADRE DE GESTION DES RISQUES LIÉS AUX TIC
A. STRUCTURE GLOBALE



- DORA définit un cadre de gestion des risques à destination de l'ensemble des entités financières, et un régime simplifié à l'égard d'un nombre limité d'entités
- Le cadre recouvre les dispositions contenues dans le Règlement et le RTS *Risk Management Framework* (RMF)
- Importance de la phase d'identification : aboutir à une cartographie complète des services critiques et importants
- Proportionnalité : exigences globalement élevées mais adaptées à l'entité.

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

4. CADRE DE GESTION DES RISQUES LIÉS AUX TIC
B. CADRE FORMEL DE GESTION DES RISQUES

- Les entités financières soumises à DORA sont tenues de mettre en œuvre un **cadre formel** de gouvernance et de gestion des risques liés aux TIC
  - Documents, politiques écrites et procédures, outils et méthodes (déclinaison notamment du RTS RMF)
    - Politiques (notamment liées aux actifs informatiques, chiffrement, opérations, contrôle d'accès, etc.. et procédures (Gestion des capacités et des performances, sécurité des données, etc..)
    - Mesures de sécurité (journalisation, gestion de la sécurité des réseaux, sécurisation des informations en transit)
    - Gestion des projets et des modifications
    - Politiques de continuité des activités informatiques et plans de réponse et de rétablissement informatiques
  - Augmentation des livrables à traiter remis par les entités financières

5. TESTS DE RÉSILIENCE

- L'article 24 de DORA impose aux entités financières de son champ d'application la définition d'un **programme de tests de sécurité**
  - Selon une approche par les risques
  - Partie intégrante du cadre de gestion des risques
  - L'article 25 reconnait une pluralité de types de tests pertinents (scans, tests d'intrusion, etc.).
- Si des TLPT internes sont prévus dans le programme d'une entité elle-même soumise aux TLPT DORA, ils ne pourront les remplacer

→ Pour tout savoir sur les TLPT, un webinaire est organisé le 15 octobre par la TCT-FR

6. GESTION DU RISQUE DE TIERS
A. PRINCIPES GÉNÉRAUX

- Le règlement DORA aborde le **risque de tiers** selon deux volets :

  – Pour l'**entité financière** : la stratégie de gestion du risque lié aux prestataires de services aux Technologies de l'Information et de la Communication (TIC)

  – Pour les **prestataires critiques** de **services TIC** : un cadre de surveillance par les trois Autorités Européennes de Surveillance (AES)

  DORA confirme dans ses textes de niveau 1 et 2 :

  ✓ la **responsabilité ultime** de l'entité financière en cas d'externalisation
  ✓ l'obligation d'**enregistrer** tous les **contrats** de prestations TIC externalisés
  ✓ l'application d'un **cadre de gestion** du **risque d'externalisation** de service TIC portant sur des fonctions métier critiques ou importantes
  ✓ L'obligation de disposer d'une **stratégie** en matière de risques liés aux prestataires tiers de services TIC et une **politique** liée aux services TIC supportés par des tiers portant sur des fonctions critiques ou importantes

6. GESTION DU RISQUE DE TIERS

B. IDENTIFICATION DES PRESTATAIRES ET DES SERVICES INFORMATIQUES EXTERNALISÉS

- Obligation de maintenir à jour un **registre d'information** *(RoI)* sur base individuelle, sous-consolidée et consolidée
- Pour l'identification, les types de services TIC ont été listés dans l'annexe 3 de l'ITS sur le registre :

Type of ICT services
ICT project management
ICT development
ICT help desk and first level support
ICT security management services
Provision of data
Data analysis
ICT, facilities and hosting services (excluding Cloud services)
Computation
Non-Cloud data storage
Telecom carrier
Network infrastructure
Hardware and physical devices
Software licencing (excluding SaaS)
ICT operation management (including maintenance)
ICT consulting
ICT risk management
Cloud services : IaaS
Cloud services : PaaS
Cloud services : SaaS

2. MODALITÉS DE REPORTING

1. REPORTING DES INCIDENTS

A. INCIDENTS MAJEURS LIÉS AUX TIC

- Les entités financières doivent notifier à leur autorité compétente les incidents majeurs liés aux TIC.
  - Toutes les entités financières de son périmètre, *Significant Institutions* incluses, doivent transmettre leurs reportings d'incidents liés aux TIC majeurs à l'ACPR qui se chargera de la transmission aux AES et à la BCE
  - Les critères de classification d'un incident comme majeur ou non sont prévus par un règlement délégué de DORA
  - La notification initiale doit se faire dans les **4 h** après classification de l'incident comme majeur et sous **24 h** après sa détection. Un rapport intermédiaire doit être envoyé au plus tard **72 h** après la notification initiale, puis le rapport final au plus tard **1 mois** après le dernier rapport intermédiaire

1. REPORTING DES INCIDENTS

A. INCIDENTS MAJEURS LIÉS AUX TIC

Services TIC ou réseaux et systèmes d'information qui soutiennent des fonctions critiques ou importantes affectés

OU

Services financiers qui requièrent une autorisation, un enregistrement ou qui sont supervisés par des autorités compétentes

OU

Accès réussi, malveillant et non autorisé au réseau et aux systèmes d'information de l'entité financière

+

Au moins 2 parmi :

① Clients, contreparties financières, transactions
Nombre de clients affectés > 10% ou à 100 000
Nombre de contreparties financières affectées > 30%
Nombre/montant de transactions affectées > 10% du nombre/montant quotidien moyen
② Impact réputationnel : média, plaintes, etc.
③ Durée incident > 24h ou indisponibilité service TIC soutenant fcts critiques/importantes > 2h
④ Impact dans au moins 2 États membres
⑤ Impact sur la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui a une incidence sur la mise en œuvre des objectifs commerciaux ou sur le respect des exigences réglementaires
⑥ Coût & pertes > 100K€

OU

Tout accès réussi, malveillant et non autorisé au réseau et aux systèmes d'information qui peut entraîner une perte de données

1. REPORTING DES INCIDENTS MAJEURS
B. INCIDENTS MAJEURS LIÉS AU PAIEMENT

- La notification des incidents majeurs liés au paiement, actuellement issue de la DSP2, fait désormais partie du champ de DORA
- Le reporting des incidents opérationnels ou de sécurité liés au paiement utilise le même format (templates) que pour les incidents liés aux TIC
- Les critères de classification comme majeur d'un incident lié au paiement sont toujours définis dans les Orientations EBA 2021/03
- **Les rapports d'incident majeur lié au paiement devront être envoyés à l'ACPR, qu'il s'agisse d'un incident opérationnel ou de sécurité**
- La transposition en droit français des modalités de reporting est en cours

1. REPORTING DES INCIDENTS MAJEURS
C. CYBER-MENACES IMPORTANTES

- Le reporting des cyber-menaces importantes se fait sur la base du **volontariat** (alignement avec l'article 30 de la Directive NIS2) et du template prévu par DORA
- Le caractère volontaire du reporting des cyber-menaces pourra être réexaminé lors de la revue de DORA d'ici à janvier 2028, cf. art. 58(1)(b)
- Par ce reporting, les établissements peuvent contribuer à la résilience du secteur financier national/UE aux cyberattaques :
  - En assurant une meilleure connaissance du paysage des cybermenaces au superviseur
  - En lui permettant de faire des recoupements avec d'autres menaces ou incidents cyber majeurs notifies par d'autres établissements
  - Dans certains cas, en lui permettant d'alerter les membres du Groupe de Place Robustesse, du protocole de gestion de crise cyber ACPR

1. REPORTING DES INCIDENTS MAJEURS
D. MODALITÉS DE TRANSMISSION

- Pour toutes les entités assujetties (ACPR et BCE):
  - Canal : transmission de **tous les incidents majeurs** (liés aux TIC et liés au paiement) et **cyber-menaces importantes** à **l'ACPR** via le portail **ONEGATE**, qui se chargera de transmettre aux autorités pertinentes.
    - Décommissionnement à partir du 17 janvier 2025 du canal Sharebox de la Banque de France, aujourd'hui utilisé pour les incidents de sécurité liés au paiement
  - Template: prévu par l'ITS sur le reporting des incidents majeurs
  - Format: .JSON (à confirmer)
  - Reporting selon ces nouvelles modalités dès l'entrée en application de DORA le 17 janvier 2025

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Remise annuelle à l'autorité compétente qui transmettra aux AES** et obligation de fournir ponctuellement un RoI à jour sur demande.

  – L'échéance de la première remise collective est en cours de définition au niveau des autorités européennes. L'information sera communiquée une fois confirmée.

→ Un corpus d'aide à la préparation du RoI est mis à disposition par les autorités européennes

https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Niveau de remise pour le reporting annuel des RoI: réduire le nombre de remises pour les groupes**

Entités (liste de cas non exhaustive)	Niveau de remise
Entités financières **qui ne font pas partie d'un groupe financier**	Remise **à l'ACPR**, **sur base individuelle**.
Groupes avec une tête de groupe **EC SI***	Remise **à la BCE**, **au plus haut niveau de consolidation**, **sur base consolidée.** ***Sauf*** *entités financières qui ne sont pas incluses dans le périmètre de consolidation prudentielle et organismes d'assurance : remise distincte sur base individuelle à l'autorité compétente.*
Groupes avec une tête de groupe **EC LSI***	Remise **à l'ACPR, au plus haut niveau de consolidation**, **sur base consolidée** (yc les organismes d'assurance FR). ***Sauf*** *entités financières qui ne sont pas incluses dans le périmètre de consolidation prudentielle : remise distincte sur base individuelle à l'autorité compétente.*
Groupes avec une tête de groupe **organisme d'assurance***	Remise **à l'ACPR, au plus haut niveau de consolidation**, **sur base consolidée.** ***Sauf*** *entités financières hors supervision de l'ACPR: remise distincte sur base individuelle à l'autorité compétente.*
Entités financières établies en FR **appartenant à un groupe de pays-tiers**, sans entreprise-mère établie dans l'UE:	Remise **à l'ACPR, sur base individuelle**.

** Uniquement si cette tête de groupe en FR est également la tête de groupe dans l'UE. Si l'entité au plus haut niveau de consolidation du groupe est située dans un autre Etat membre, la remise consolidée sera effectuée par cette entité à l'autorité compétente.*

2. DÉCLARATION DES SERVICES INFORMATIQUES EXTERNALISÉS

- **Modalités de remise des registres d'information (RoI) :**
  - Pour les établissements de crédit considérés comme importants (*Significant Institutions*):
    - Canal : transmission des RoI à la BCE via CASPER
    - Template: prévu par l'ITS sur le registre d'information (a priori extrêmement proche de celui utilisé pour le *dry run*)
    - Format: Excel
    - La BCE procédera aux vérifications et à l'envoi à l'EBA
  - Pour toutes les entités financières relevant de la compétence de l'ACPR:
    - Canal: transmission des RoI à l'ACPR via le portail ONEGATE (et non plus Sharebox lors du *dry run*)
    - Template: prévu par l'ITS sur le registre d'information
    - Format: Plain CSV (format attendu par les AES). L'outil de conversion (Excel -> Plain CSV) mis à disposition par les AES lors du *dry run* ne sera plus disponible
    - L'ACPR procédera aux vérifications et à l'envoi aux AES
- **Date** de la première remise : en cours de discussion au niveau des autorités européennes

3. RETOUR D'EXPÉRIENCE EN MATIÈRE DE SUPERVISION DU RISQUE CYBER

1. GESTION DES RISQUES LIÉS AUX TIC

- **Les fintechs sont particulièrement exposées à plusieurs risques en matière de cybersécurité**, en raison de la sensibilité des données qu'elles manipulent (ex : informations bancaires, historiques de transactions, identités personnelles) et de leur dépendance aux technologies.
- **Une seule faille dans le système de sécurité d'une fintech peut permettre des attaques majeures** telles que le vol, la corruption et la destruction des données, la fraude bancaire, ou encore le piratage de comptes.
- **Les conséquences peuvent être désastreuses** pour l'établissement, notamment aux plans juridique (manquement aux obligations réglementaires) et financier (réparation des dommages, sanction), ainsi qu'en termes de réputation.

- **Quelques exemples** de mesures pour une protection des données :

✓ **Chiffrement des données :** Utiliser des algorithmes de chiffrement robustes pour protéger les données sensibles, tant au repos qu'en transit. Cela garantit que même si des données sont interceptées, elles ne pourront pas être lues sans la clé de déchiffrement appropriée.

✓ **Contrôle d'accès strict :** Implémenter des politiques de contrôle d'accès basées sur les rôles (RBAC) et le principe du moindre privilège, limitant l'accès aux données sensibles uniquement aux employés ou systèmes qui en ont absolument besoin. L'authentification multi-facteurs (MFA) doit également être utilisée pour renforcer la sécurité des comptes.

✓ **Sauvegarde et restauration :** Mettre en place des solutions de sauvegarde régulières, automatiques et sécurisées pour garantir que toutes les données critiques puissent être récupérées en cas de défaillance, d'attaque (comme un ransomware) ou de perte de données. De plus, des tests périodiques de restauration doivent être effectués pour s'assurer que les données peuvent être récupérées rapidement et de manière fiable en cas de besoin.

- Pour aller plus loin :

✓ **DORA Texte de niveau 1 (Règlement UE 2022/2554) :** Art. 5 à 16

✓ **RTS on ICT Risk Management framework (Commission Delegated regulation - EU - 2024/1774 of 13 March 2024) :** Art. 15

2. GESTION DES RISQUES LIÉS AUX PRESTATAIRES TIERS DE SERVICES TIC

- **Les prestataires de services informatiques jouent un rôle crucial dans les opérations des fintechs.** Si cela permet à une fintech de se concentrer sur son cœur de métier, elle expose également l'entreprise à plusieurs risques majeurs.
- **Si un prestataire ne dispose pas des mêmes normes de sécurité ou subit une violation, cela peut entraîner une fuite de données critiques.** Pour une fintech, où la confiance des clients est primordiale, une faille de ce type peut avoir des conséquences dévastatrices, tant sur le plan financier que sur celui de la réputation.
- **Externaliser des fonctions critiques peut créer une dépendance excessive à l'égard d'un prestataire.** Si ce dernier rencontre des difficultés ou décide de modifier ses conditions contractuelles, cela peut affecter directement l'activité de la fintech.

- **Quelques exemples** de mesures pour une gestion des risques liés aux prestataires tiers de services TIC :

✓ **Évaluation rigoureuse des prestataires :** Analyser notamment en profondeur la sécurité, les conflits d'intérêt, et la solidité financière de chaque prestataire avant de les choisir.

✓ **Contrats avec des clauses solides et détaillés :** Intégrer notamment dans les contrats des dispositions précises sur la protection des données, la disponibilité, l'intégrité, la confidentialité, le droit d'audit, la gestion des incidents et de droit de résiliation. Assurez-vous que les prestataires s'engagent à respecter des mesures de sécurité robustes et définissez clairement les responsabilités en cas de violation des données. Définir des attentes claires et mesurables sur la performance, la sécurité, la gestion des données et la continuité de service.

✓ **Surveillance continue :** Mettre en place une surveillance continue des prestataires pour évaluer leur conformité aux exigences de qualité, de sécurité et de continuité, par exemple.

✓ **Réversibilité :** Élaborer des plans de reprise après sinistre et des stratégies de sortie afin de minimiser l'impact en cas de défaillance du prestataire.

- Pour aller plus loin :

✓ **DORA Texte de niveau 1 (Règlement UE 2022/2554) :** Art. 28 à 44

✓ **RTS on ICT services provided by ICT third party policy (Commission Delegated Regulation - EU - 2024/1773 of 13 March 2024) :** Art. 28.10

Forum Fintech ACPR-AMF 2024

Cybersécurité et risques informatiques – 2ème partie

Bruno BURESI - Direction des Contrôles - Adjoint à la directrice en charge des contrôles des SGP et des CIF

Thomas DEBIZE – Direction Cybersécurité, Sûreté et Risques

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

Retour d’expérience sur les contrôles cyber

Une démarche engagée dès 2019 sur la base de la réglementation existante

- **3** campagnes de **contrôles SPOT** menées sur un périmètre de **15** Sociétés de Gestion de Portefeuille (SGP)
  → Présentation ci-après des **bonnes et mauvaises pratiques** identifiées dans ce cadre au regard des « piliers DORA »

- **11 contrôles classiques** incluant le thème cyber menés sur :
  → **6** SGP
  → **3** Conseillers en Investissement Financiers (CIF)
  → **1** Prestataire de Services de Financement Participatif (PSFP)
  → **1** Infrastructure de Marché (IM)
  ➔ **Un tiers** de ces contrôles ont inclus la réalisation de tests techniques, notamment des **tests d'intrusion** et **revues de configuration**, par un prestataire d'audit de cybersécurité **qualifié PASSI**

- **Pas de sanctions prononcées à date** pour des **manquements** relatifs à la **cybersécurité** mais :
  → **Possibilité de sanctions dès à présent** en cas d'identification de dispositif cyber défaillant
  → **Information des trois associations professionnelles** de SGP par courrier en ce sens

- Egalement depuis 2019, une **instruction DOC-2019-24** (révisée en 2023), précisant les **exigences en matière de cybersécurité pour les prestataires de services sur actifs numériques (PSAN)**

Une démarche engagée dès 2019 sur la base de la réglementation existante

- **Des thèmes standards de cybersécurité faisant l'objet de contrôles :**
  - → Organisation et gouvernance du dispositif cyber
  - → Administration et surveillance du SI
  - → Cartographie des données et systèmes sensibles
  - → Sélection, contractualisation et contrôle :
    - Des prestataires informatiques sensibles
    - Et des canaux de communication existants avec les autres partenaires
  - → Gestion des incidents d'origine cyber
  - → Plan de continuité d'activité
  - → Dispositif de contrôle interne

- **Sur la réglementation applicable avant DORA :**
  - ↗ Le Code Monétaire et Financier (CMF) ;
  - ↗ Le Règlement Général de l'AMF (RG AMF) ;
  - ↗ Le règlement délégué (UE) (RD) n° 231/2013 « RD AIFM »;
  - ↗ Le règlement délégué (UE) (RD) n°2017/565 « RD MIF II » ;
  - ↗ La position AMF DOC-2021-05 concernant la sous-traitance auprès de prestataires de services Cloud

Pilier de DORA : Gestion des risques liés aux technologies de l'information et de la communication (TIC)

- **Bonnes pratiques identifiées :**
  - → Assurer l'indépendance de la fonction RSSI par rapport à la DSI
  - → Sensibiliser les collaborateurs via l'usage de tests de phishing
  - → Différencier les responsabilités respectives du DSI et du RSSI dans des fiches de poste dédiées
  - → Faire valider la stratégie de cyber sécurité par les dirigeants responsables
  - → Permettre l'identification des dépenses liées à la cybersécurité au sein de celles liées à l'informatiques

- **Mauvaises pratiques identifiées :**
  - → Ne pas assurer de reporting réguliers des risques d'origine cyber aux dirigeants responsables
  - → Pour les filiales de groupes, n'appuyer le dispositif cyber que sur la stratégie de ce dernier
  - → Limiter les procédures de sécurité des systèmes d'information à l'énumération de principes génériques

Pilier de DORA : Gestion des risques liés aux technologies de l'information et de la communication (TIC)

Focus sur la résilience

- **Bonnes pratiques identifiées :**
  - → Vérifier régulièrement les capacités de travail à distance des équipes ainsi que le niveau de sécurité des installations de secours
  - → Formaliser un plan de sauvegarde/restauration régulier des données informatiques, précisant le périmètre et la fréquence des opérations menées

- **Mauvaises pratiques identifiées :**
  - → 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

Pilier de DORA : Reporting des incidents

- **Bonnes pratiques identifiées :**
  - → Compléter les cartographies internes du SI d'un dossier d'architecture technique explicitant le processus de supervision opéré par l'administrateur
  - → Formaliser et mettre à jour un inventaire complet des équipements informatiques
  - → Formaliser une procédure de gestion des incidents d'origine cyber
  - → Étendre la surveillance automatisée du SI au-delà des heures ouvrées

- **Mauvaises pratiques identifiées :**
  - → Ne pas veiller à circonscrire les vulnérabilités usuelles :
    - Ports USB non restreints
    - Utilisateurs standards administrateurs de leurs postes de travail
    - Postes de travail et messageries non chiffrés
    - Règles de construction des mots de passe non conformes aux critères de l'ANSSI
    - Absence de double authentification pour accéder à la messagerie
  - → Ne pas distinguer les incidents d'origine cyber des incidents opérationnels.

Pilier de DORA : Gestion des risques lies aux prestataires de services TIC (1/2)

- **Bonnes pratiques identifiées :**
  - → Prise en compte des risques d'origine cyber et de continuité dans la sélection et l'évaluation des prestataires
  - → Cartographier l'ensemble des prestataires informatiques interne et externes
  - → Demander aux prestataires/partenaires externes clés la communication des rapports d'audit de sécurité ayant été menés en leur sein

- **Mauvaises pratiques identifiées :**
  - → Ne pas réduire le niveau de visibilité sur internet des interfaces d'administration externes du SI
  - → Ne pas faire état dans le contrat de l'administrateur informatique externe des mesures de cyber sécurité exigées pour son activité
  - → Ne pas définir, ni suivre, d'indicateurs de pilotage des prestations informatiques ou de cyber sécurité délivrées par le groupe d'appartenance

Pilier de DORA : Gestion des risques lies aux prestataires de services TIC (2/2)

- **Clauses standards contrôlées :**
  - → Autorisation (et conditions d'exécution) d'une éventuelle sous-traitance de la prestation
  - → Localisation géographique des serveurs du prestataire
  - → Droit d'audit
  - → Mode de protection des informations confidentielles (incluant les données personnelles)
  - → Modalités d'information de la SGP en cas de dysfonctionnement
  - → Plan d'urgence permettant le rétablissement du service externalisé en cas de sinistre
  - → Accès (par la SGP et l'autorité de tutelle) aux données externalisées et aux locaux professionnels du prestataire
  - → Réversibilité de la prestation (modalités et conditions de résiliation du contrat d'externalisation)
  - → Stratégie globale de sortie

Pilier de DORA : Tests de résilience opérationnelle numérique

- **Bonnes pratiques identifiées :**

  → Faire réaliser régulièrement, par un prestataire externe spécialisé, un test d'intrusion sur le SI de la SGP, notamment sur les ressources critiques ou importantes pour l'activité de l'entreprise

- **Mauvaises pratiques identifiées :**

  → Déployer un dispositif de cyber sécurité en l'absence d'une cartographie structurée des données et des systèmes sensibles

L’approche future de l’AMF concernant le risque d’origine cyber des assujettis

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

L’approche future de l’AMF concernant le risque d’origine cyber des assujettis

- Avec la **transformation numérique** des services financiers et **l’application du Règlement DORA**, le **risque d’origine cyber** doit ainsi être **pris en compte au plus haut niveau** par les entités financières et leurs prestataires afin d’assurer **confiance et résilience**, qui sont des **propriétés indispensables pour le secteur financier**

- **L’outillage** n’est pas la finalité :

  → **L’approche de mise en conformité** doit certes être **globale et outillée**…

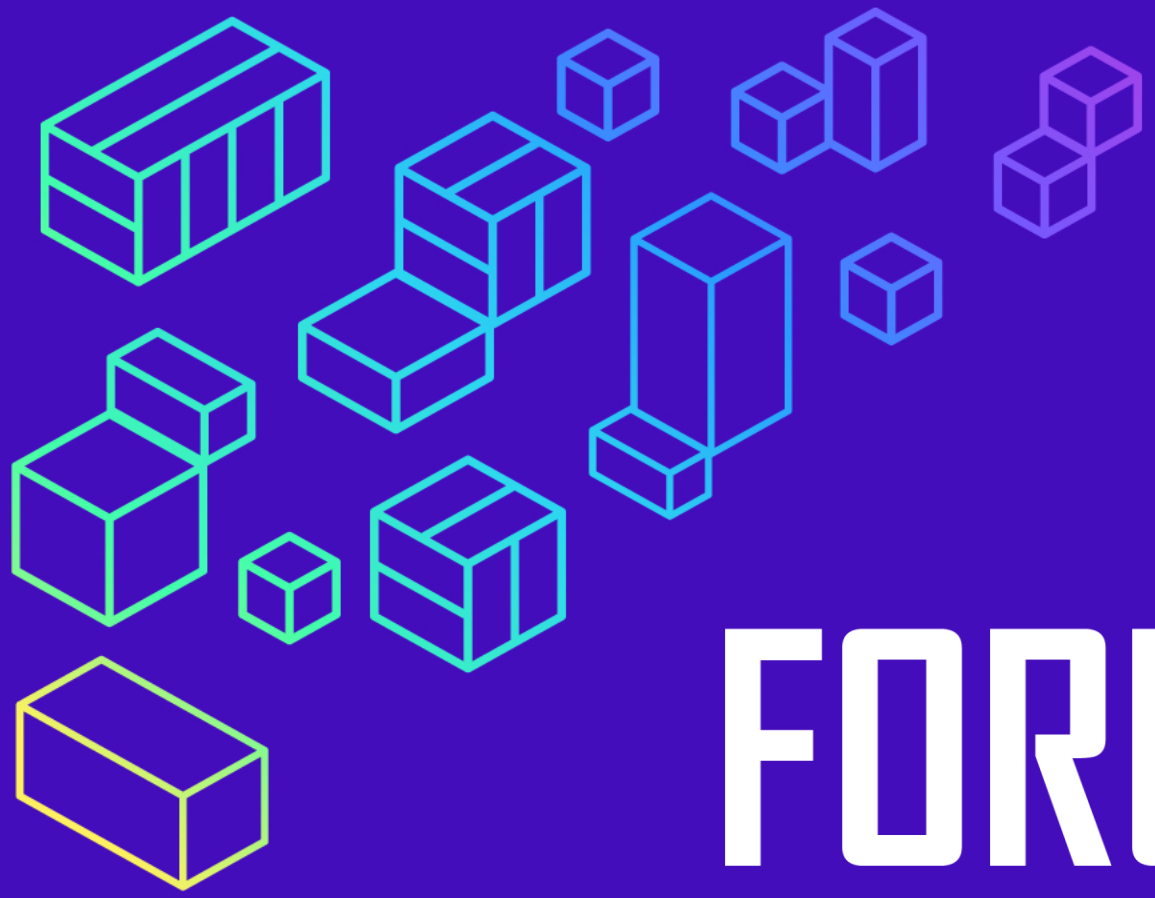
  → …mais doit **commencer par la mise en œuvre d’une gouvernance cybersécurité claire et adaptée au contexte de l’entité financière**

- Au-delà de la **déclaration obligatoire des incidents majeurs prévue dans DORA**, les entités sont invitées à également nous communiquer sur base volontaire les **incidents significatifs**

  → Une tentative d’attaque ou attaque échouée dans votre contexte…peut malheureusement aboutir dans un autre contexte

- Après une **phase pédagogique initiée en 2019** sur la **gestion du risque cyber par les entités financières,** et dans le cadre de **l’application de DORA au 17/01/2025**, des **sanctions répressives** pourront désormais être prononcées pour les **situations qui le méritent.**

Merci pour votre attention!



ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

FORUM FINTECH

ACPR - AMF

14 octobre 2024