Forum Fintech ACPR AMF

Résilience opérationnelle numérique - état des lieux 9 mois après l'entrée en application de DORA

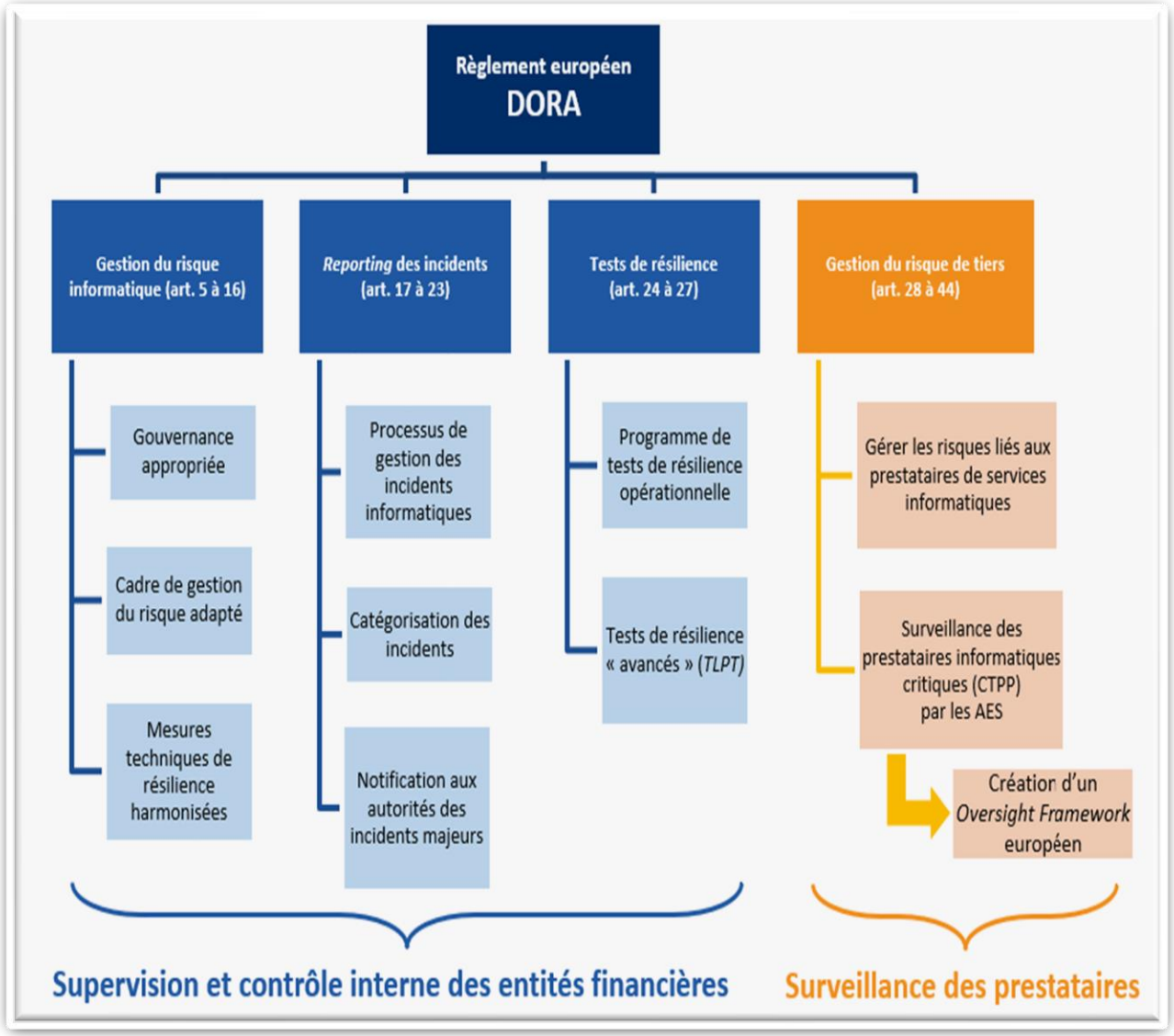
9 octobre 2025

1. Cadre règlementaire : quelques rappels
2. Premiers constats depuis l'entrée en application de DORA
3. Retour d'expérience en matière de supervision du risque cyber
4. Prochaines étapes

1

CADRE RÈGLEMENTAIRE : QUELQUES RAPPELS

- **DORA : « accélérateur » en faveur d'une résilience opérationnelle accrue**
  - Un cadre de gestion du risque informatique renforcé nécessitant une formalisation des politiques et procédures mises en place et une structuration de l'organisation de chaque entité financière
  - Un programme de test ambitieux et proportionné avec, pour les entités les plus importantes, un suivi par l'autorité compétente des tests d'intrusion fondés sur la menace (TLPT)
  - Une obligation de déclaration des incidents majeurs : incitation pour toutes les entités à mettre en place une un process efficace de détection des incidents ; permet une plus grande réactivité des autorités en cas d'incident critique
  - Un nouveau cadre de surveillance des fournisseurs de services TIC critiques: en assurant une plus grande résilience de ces tiers, ce cadre doit également accroitre la résilience des entités financières



- **DORA : un cadre qui simplifie et harmonise**
  - Ce règlement fixe des exigences communes à tout le secteur financier et s'applique à 20 catégories différentes d'entités et permet ainsi de limiter la « fragmentation » règlementaire dans le domaine de la résilience opérationnelle
  - DORA est *lex specialis* de NIS2 : étant donné que les dispositions de DORA ont un effet au moins équivalent à celle de NIS2, les entités essentielles et importantes au sens de NIS2 ne sont soumises qu'aux dispositions de DORA en matière de gestion du risque cyber et de notification des incidents
  - Des orientations ont été supprimées ou fortement réduites : par exemple, c'est le cas des lignes directrices de l'EIOPA et de l'ESMA sur la gestion du risque *Cloud* ou encore des lignes directrices de l'EBA et de l'EIOPA sur la gestion du risque TIC
  - La simplification de certaines orientations toujours en cours : les lignes directrice de l'EBA sur l'externalisation ou encoure les orientations de l'EBA sur le risque opérationnel des IORP.

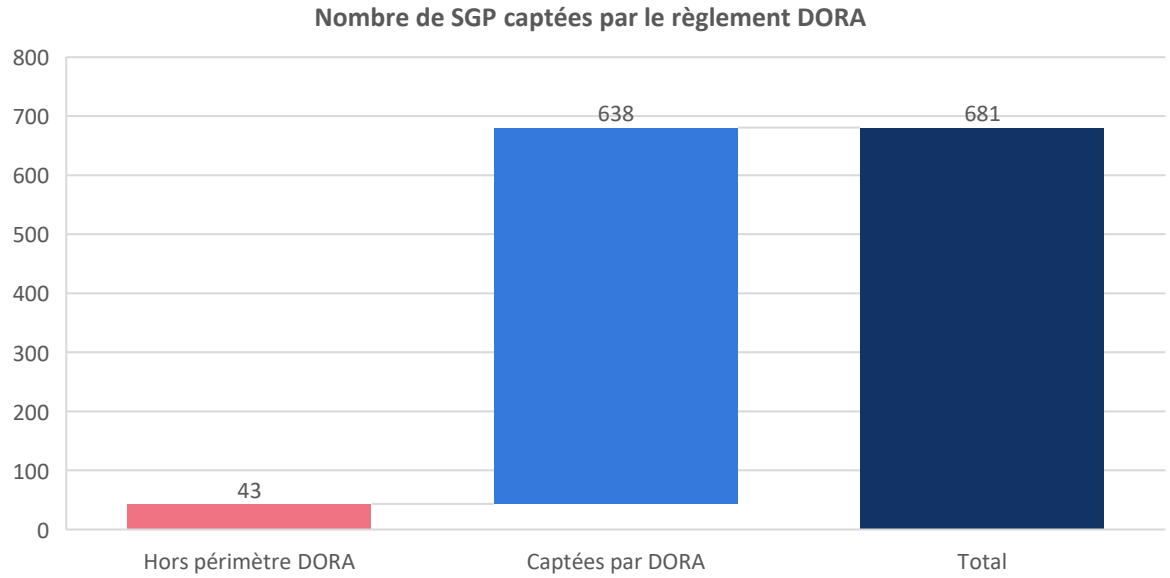
- **Finalisation du corpus règlementaire**
  - Niveau européen : malgré le retard, l'ensemble des textes de niveau 2 ont été adoptés. Le dernier texte adopté et entré en vigueur est le règlement délégué 2025/532 sur la sous-traitance. L'ensemble des textes est consultable sur Eurlex (ici). C'est une règlementation vivante qui fait également l'objet de plusieurs Q&A déjà adoptées ou en cours de finalisation. Une clause de revoyure au 17 janvier 2028
  - Niveau français (PJL Résilience) : Examen au Sénat: commission spéciale le 4 mars 2025 et en séance publique les 11 et 12 mars 2025. Examen à l'Assemblée nationale: une commission spéciale a eu lieu la semaine du 8 septembre et en séance publique la semaine du 22 septembre. L'adoption du texte ainsi que sa transposition au niveau réglementaire (ajustement à la marge de l'arrêté du 03/11/2014 sur le contrôle interne des entités du secteur « bancaire ») est attendue d'ici la fin de l'année

2

PREMIERS CONSTATS DEPUIS L'ENTRÉE EN APPLICATION DE DORA

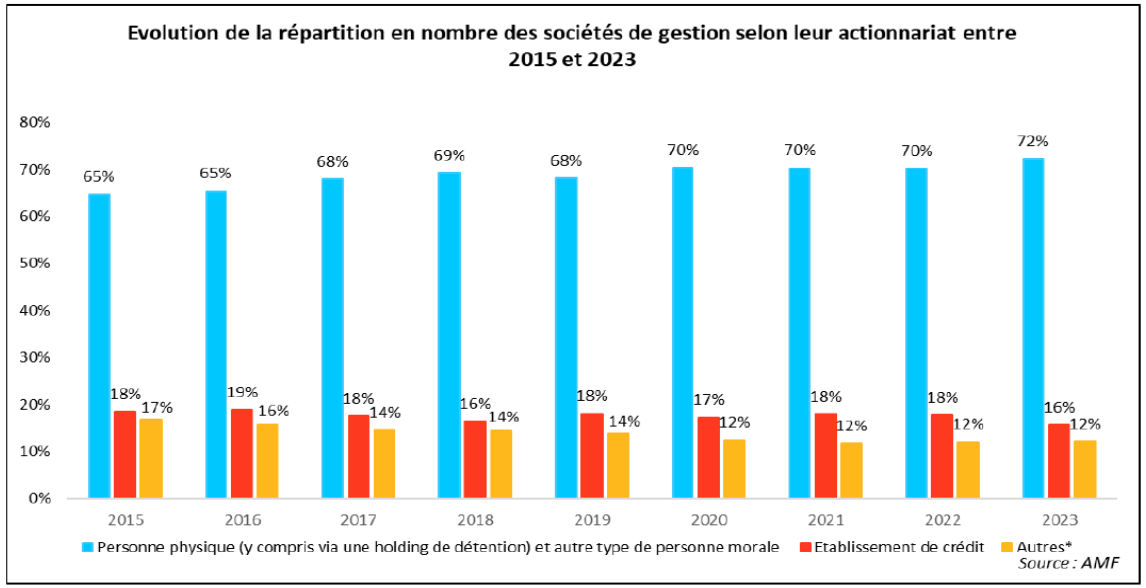
DORA – Etat des lieux de l'implémentation du règlement DORA

94% des SGP sont captées par DORA sachant que la grande majorité d'entre elles sont de taille entrepreneuriale. Malgré son exigence, DORA constitue un règlement utile pour le secteur de la gestion d'actifs



Source : Données AMF au 22/09/2025

Le paragraphe 3 de l'article 2 indique que DORA ne s'applique pas aux gestionnaires de FIA sous les seuils AIFM. **Toutefois, si un gestionnaire** avec des encours sous les seuils **a opté pour l'application intégrale de la Directive AIFM, il rentre dans le champ d'application de DORA**



* La catégorie « Autres » comprend les compagnies d'assurances et mutuelles et les prestataires de services d'investissement (hors établissements de crédit).

93% des SGP ayant des personnes physiques comme actionnaires présentent des effectifs inférieurs à 50 collaborateurs en 2023

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

DORA – Etat des lieux de l'implémentation du règlement DORA

- Les principales avancées portent sur l'évolution de la gouvernance et du cadre procédurale
- Les mesures de gestion des risques liés aux TIC sont encore en cours d'implémentation/finalisation
- Les principales difficultés portent sur le pilier relatif à la gestion des risques liés aux prestataires tiers de services TIC

Pilier	Description succincte du pilier	Constats
Gestion des risques liés aux TIC	• Cadre formalisé incluant des règles de gouvernance et de contrôle interne, une stratégie de résilience, une classification des risques, des mesures d'atténuation, etc. • Principe de proportionnalité introduit dans la mise en œuvre de ce cadre	• Gouvernance du cadre de gestion des risques liés aux TIC qui s'est mise en place avec une implication des dirigeants des SGP • Mise en place de formations • Renforcement du cadre procédural pour se conformer au règlement DORA • Actuellement, les efforts portent davantage sur la mise en place des mesures de gestion des risques
Gestion, classification et notification des incidents liés aux TIC	• La gestion des incidents doit notamment reposer sur des processus formalisés de surveillance (alertes et identification), de réponse et de communication (à la direction et aux parties concernées) • L'obligation de classification des incidents majeurs liés aux TIC et des cybermenaces • Déclaration obligatoire des incidents majeurs liés aux TIC et notification volontaire des cybermenaces importantes	• Pilier qui a suscité des interrogations de la part des SGP notamment sur la méthodologie de classification des incidents et sur le calendrier des déclarations • Déclaration des incidents majeurs en phase de rodage

Les services de l'AMF ont demandé aux SGP de répondre à questionnaire permettant d'évaluer leur niveau d'implémentation du règlement DORA. Le questionnaire doit être soumis à l'AMF au plus tard le 14 novembre 2025 ➔ L'Etat des lieux présenté dans cette slide sera affiné sur la base des réponses au questionnaire

DORA – Etat des lieux de l'implémentation du règlement DORA

- Les principales avancées portent sur l'évolution de la gouvernance et du cadre procédurale
- Les mesures de gestion des risques liés aux TIC sont encore en cours d'implémentation/finalisation
- Les principales difficultés portent sur le pilier relatif à la gestion des risques liés aux prestataires tiers de services TIC

Pilier	Description succincte du pilier	Constats

Tests de résilience opérationnelle	• 2 niveaux de tests
	  • Tests basiques de résilience opérationnelle pour toutes les entités financières
	  • Tests avancés de pénétration basés sur la menace pour les fonctions critiques ou importantes pour les entités « systémiques »
		• De la même façon que le pilier sur la gestion des risques aux TIC, la partie documentaire a avancé plus rapidement que la mise en œuvre opérationnelle

Gestion des risques liés aux prestataires tiers de services TIC	• Intégration des risques liés aux prestataires de services TIC avec l'instauration de règles de gouvernance, de sélection et d'évaluation des prestataires de services TIC • Evaluation des risques avant la conclusion de tout accord contractuel, intégration de clauses minimales, de stratégies de sortie • Tenue d'un registre d'informations des accords contractuels conclus avec ces prestataires (ROI)	• Certains prestataires refusent d'être déclarés comme TIC de manière à ne pas avoir à se conformer à DORA. • Difficultés dans l'intégration des clauses DORA au sein des contrats • Difficultés exprimées dans la transmission du ROI

Les services de l'AMF ont demandé aux SGP de répondre à questionnaire permettant d'évaluer leur niveau d'implémentation du règlement DORA. Le questionnaire doit être soumis à l'AMF au plus tard le 14 novembre 2025 ➔ L'Etat des lieux présenté dans cette slide sera affiné sur la base des réponses au questionnaire

Face à l'exigence du règlement, l'accompagnement de l'AMF a été renforcé

1 Accompagnement avant l'application du règlement DORA

- ✓ Accompagnement des SGP lorsqu'elles étaient victimes d'un incident cyber
- ✓ Formations biannuelles à destination des responsables de la conformité et du contrôle interne
- ✓ Contrôles SPOT (2019, 2020, 2023)
- ✓ Intervention à des événements externes (webinaires et forum)
- ✓ Publication sur le site internet de l'AMF d'une synthèse des principales exigences du règlement DORA
- ✓ Formation des collaborateurs en interne (Contexte DORA & processus de réaction face à une déclaration d'incident)

2 Accompagnement après l'application du règlement DORA

- ✓ Communication d'une nouvelle synthèse des obligations relatives au règlement DORA
- ✓ Formations biannuelles à destination des responsables de la conformité et du contrôle interne
- ✓ Webinaires avec les différentes associations professionnelles
- ✓ Accompagnement des SGP lors d'incidents majeurs et non majeurs
- ✓ S'agissant du ROI :
  - ✓ Présentation pédagogique lors de l'atelier data de la journée RCCI, détaillant les modalités de constitution du ROI
  - ✓ Webinaire spécifique sur les difficultés liées au ROI
  - ✓ Communication incluant les points d'attention, des liens ciblés sur les principaux documents mis à disposition par l'EBA, une FAQ spécifique AMF, une communication sur les principales erreurs rencontrées et leurs explications
- ✓ Réponses aux sollicitations des SGP pour leur mise en conformité

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

R.O.I. : UNE REMISE COMPLEXE QUI NÉCESSITE DE L'ANTICIPATION

- **84% des entités ont fait une remise sur Onegate mais pour seulement 39% d'entre elles le RoI a pu être traité au niveau européen**

- **Plusieurs facteurs peuvent contribuer à l'expliquer, à l'instar de :**
  - Un calendrier très resserré pour tous les acteurs
  - Des règles de validation non stabilisées et modifiées en cours de période de remise du côté des autorités compétentes ainsi qu'un volume inhabituellement élevé de sollicitations du support technique
  - Un format de remise inhabituel et nécessitant une appropriation parfois sous-estimée du côté des remettants (faible participation observée à l'exercice de dry-run, faible utilisation de l'environnement de test, défaut d'anticipation de l'ampleur de la gouvernance nécessaire en interne)

R.O.I. : UNE REMISE COMPLEXE QUI NÉCESSITE DE L'ANTICIPATION

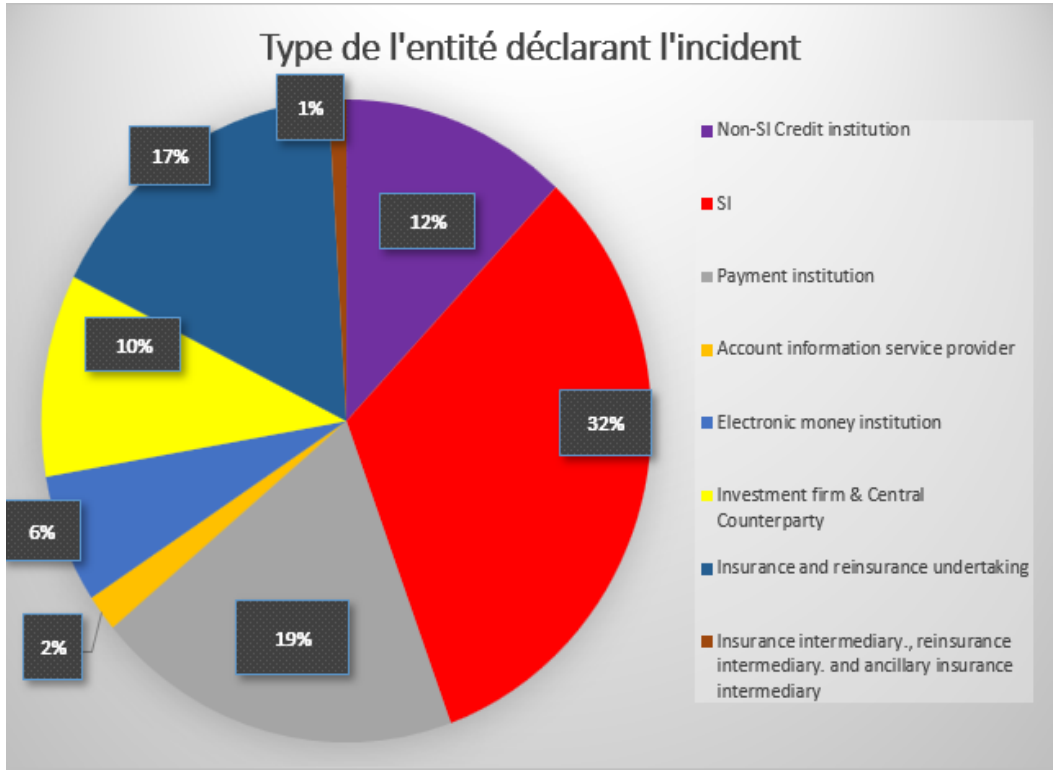
- **Et maintenant ? Les solutions**

  - En prévision de la prochaine remise, l'ACPR va accroitre ses efforts en termes de communication et d'accompagnement des remettants, de manière bilatérale chaque fois que nécessaire
  - Alignement des règles de validation Onegate avec celles des AES (à l'exception de la vérification de l'EUID lorsqu'il est utilisé par les entité). Une automatisation de la production et de la communication des CRT devraient être mises en place d'ici la fin de l'année.
  - Les entités remettantes sont, quant à elle, invitées à anticiper les prochaines remises, par exemple 1) en développant un outil interne ou en recourant à un accompagnement extérieur en se basant sur tous les éléments de validation et autres retours d'expériences déjà à disposition et 2) en procédant à des remises test sur l'espace homologation dans les mois précédents la période de remis

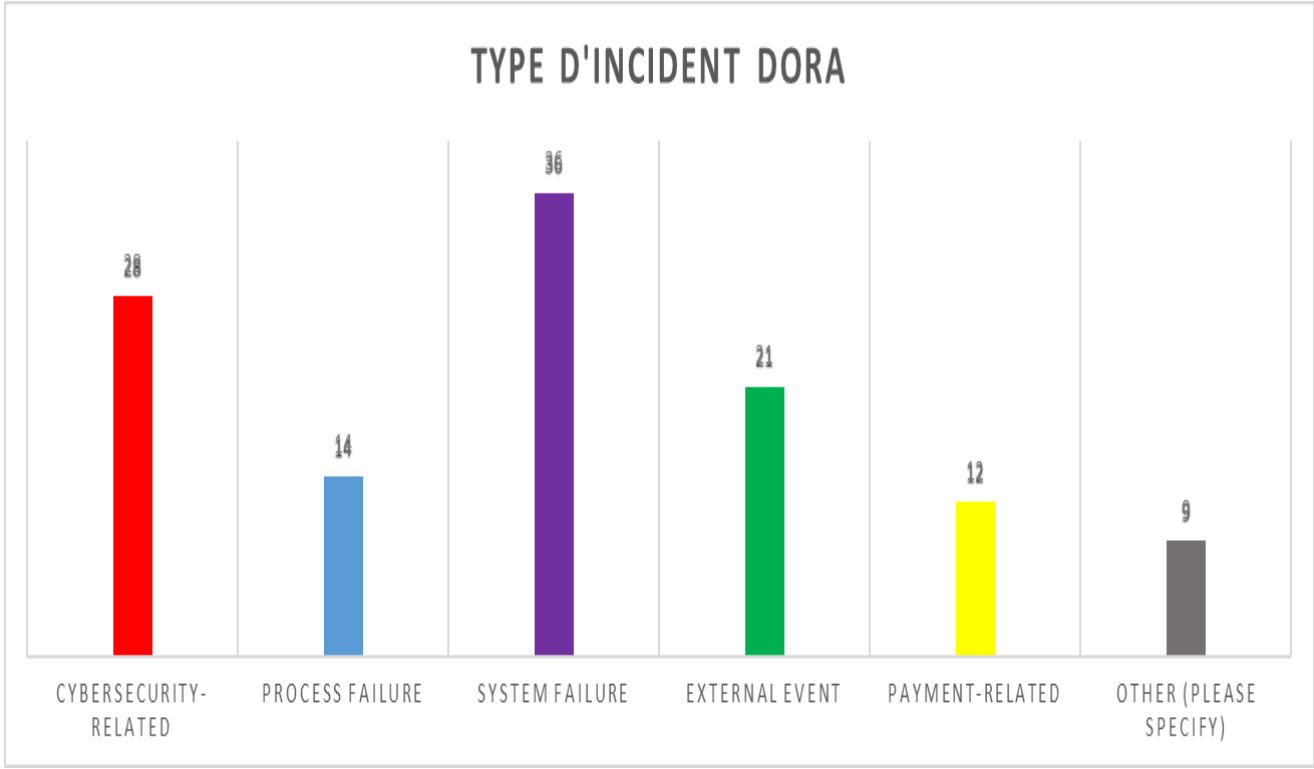
Plus globalement, le RoI doit être pleinement intégré dans le cadre de gestion du risque de tiers des entités (cf. slides 14 et 15)

INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

Entités notifiantes : majoritairement des EC et assurances



Type d'incidents : essentiellement des failles dans les SI. Le chiffre sur les incidents cyber est élevé du fait d'un incident ayant affecté plusieurs entités



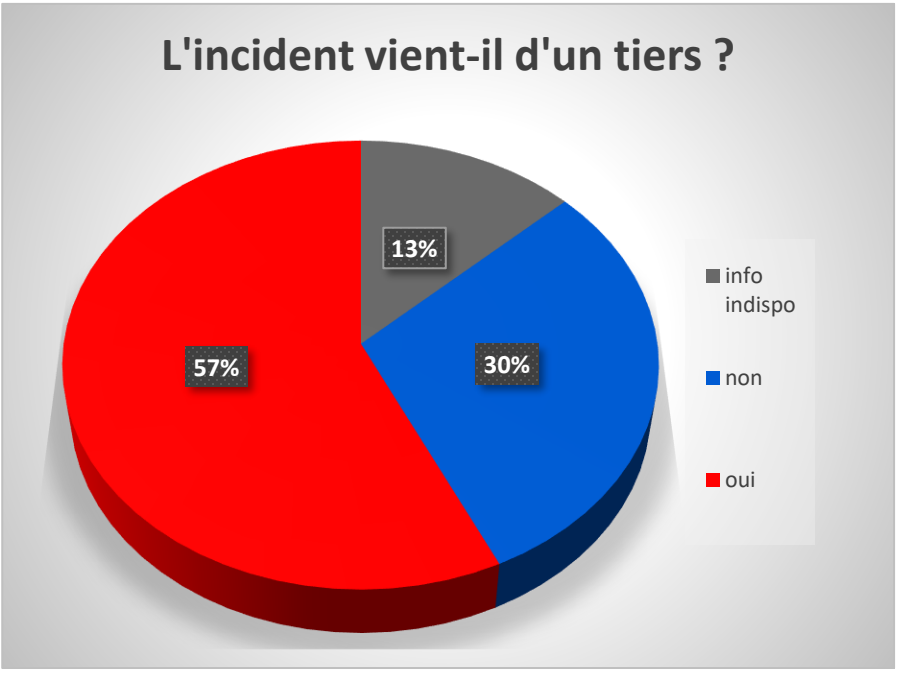
Chiffres au 23/08/2025

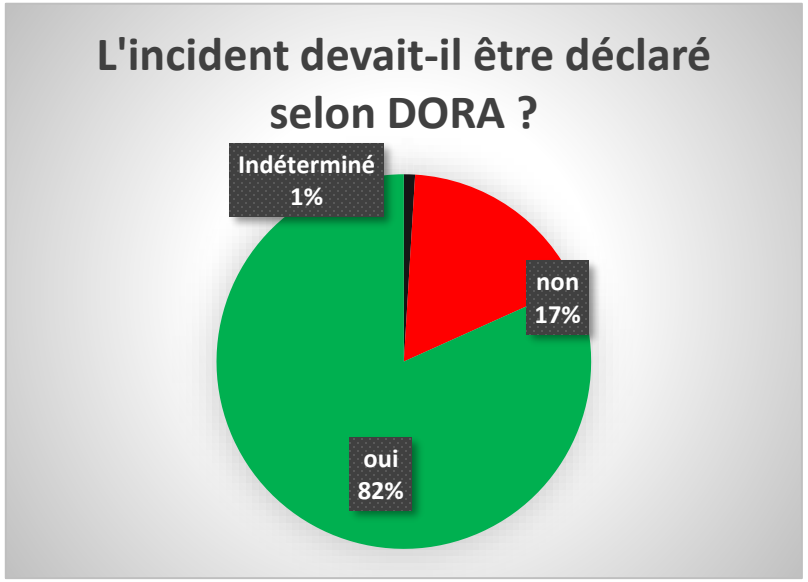
INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

- **Tiers impliqués : oui dans plus de la moitié des cas (impact important de l'incident Harvest)**

Dans près 60% des cas l'incident est déjà clos au moment de la notification initiale (les activités ont repris normalement et/ou l'analyse des causes a été terminée)

- **[analyse préliminaire] dans les majorités des cas les notifications sont justifiées**





INCIDENTS : UN NOMBRE IMPORTANT DE NOTIFICATIONS

- **Difficultés :**
  - Retard des remises : un incident doit être notifié maximum 4h après sa classification comme majeur, et maximum 24h après sa détection (art5 du règlement délégué (UR) 2025/301). Ces délais sont encore rarement respectés.
  - Le format .Json et les remises sur OneGate : des outils internes « artisanaux » ; manque d'anticipation sur les accréditations
  - Non-remplissage de certains champs obligatoires ou erreurs dans leur remplissage

La FAQ DORA de l'ACPR, avec la maquette annotée, est visible ici (partie B, Reporting). Il convient de la lire attentivement afin de disposer de toutes les informations nécessaires au reporting correct des incidents.

- Mécompréhension et/ou omission de certains critères de classification des incidents (règlement délégué (UE) 2024/1772)

Un incident est majeur dans 3 cas possibles :

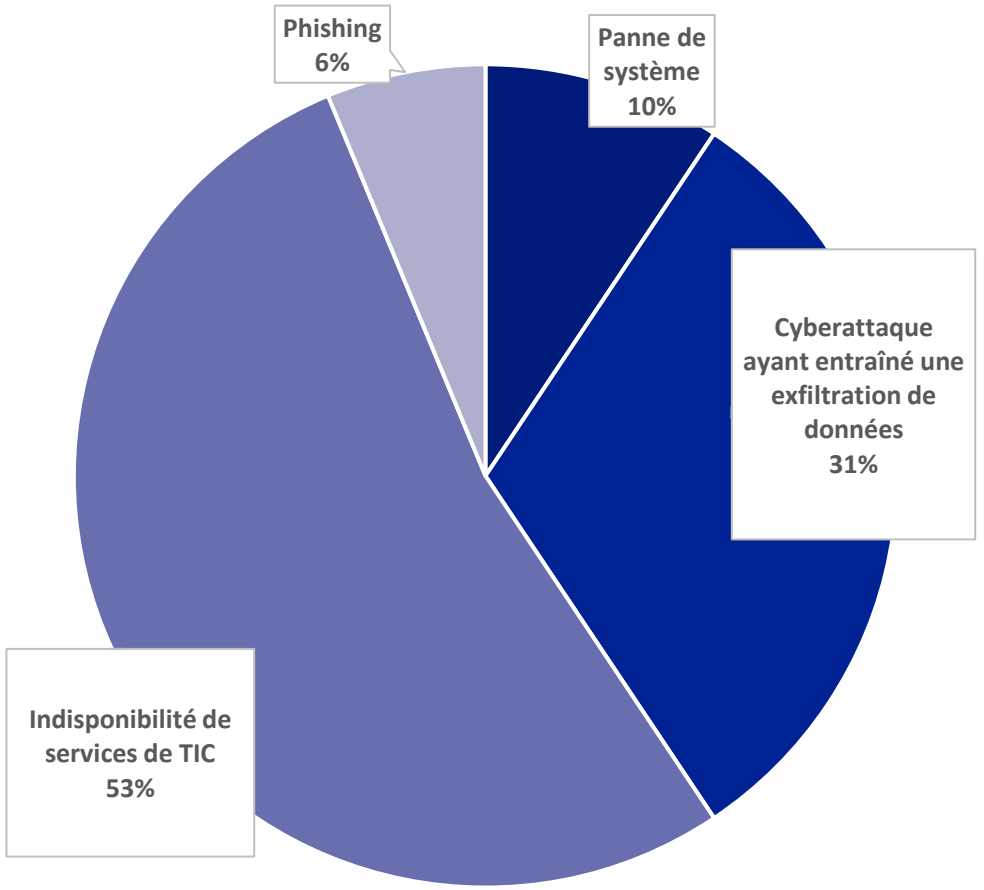
1) **L'incident est une cyberattaque (art6c + 9.5b)**
2) **L'incident touche ou a touché, quelle que soit l'ampleur de l'impact, des services TIC/réseaux/SI soutenant des FCI (critère primaire) + il remplit au moins 2 critères secondaires**
3) **L'incident touche ou a touché, quelle que soit l'ampleur de l'impact, des services financiers nécessitant un agrément, un enregistrement ou étant surveillés par l'ACPR (critère primaire) + il remplit au moins 2 critères secondaires**

- Prise en compte erronée des mesures compensatoires mises en place après détection d'un incident dans l'évaluation des critères de classification : un incident doit être classifié indépendamment de la mise en place d'éventuelles mesures compensatoires

Etat des lieux des incidents pour les SGP (1/3)

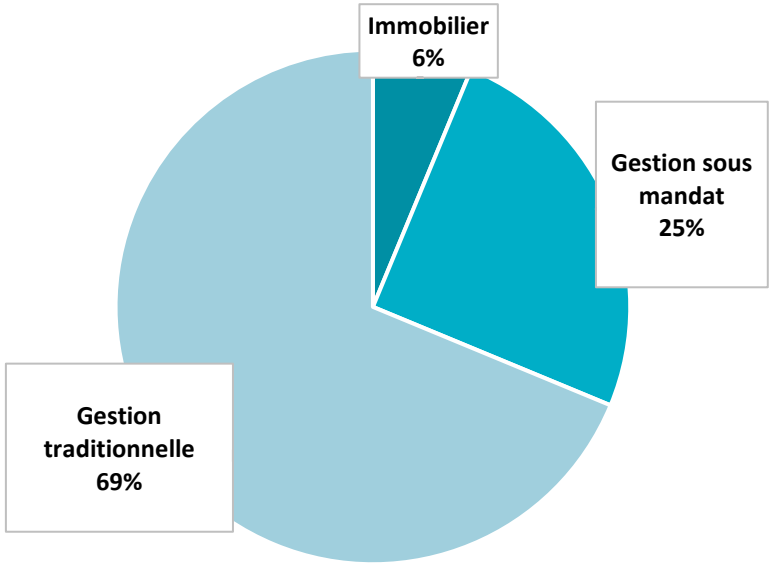
- **44 déclarations initiales d'incidents. 32 incidents confirmés majeurs suite aux échanges avec les SGP, déclinés ci-dessous**
  - → 17 incidents ayant été causés par une indisponibilité de services TIC
  - → 10 incidents ayant été causés par une exfiltration de données
  - → 3 incidents issus de panne dans le système d'information des SGP : erreur de code, erreur d'authentification
  - → 2 incidents de phishing

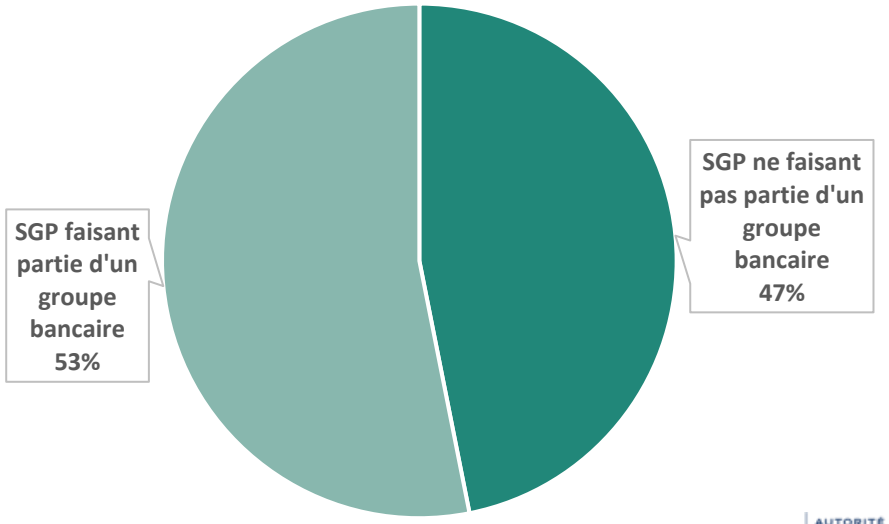
- **Fonctions critiques impactées :**
  - → Gestion (comprenant le passage d'ordres) ;
  - → Valorisations d'instruments financiers ;
  - → Conformité (entrée en relation, KYC, LCB-FT)



Etat des lieux des incidents pour les SGP (2/3)

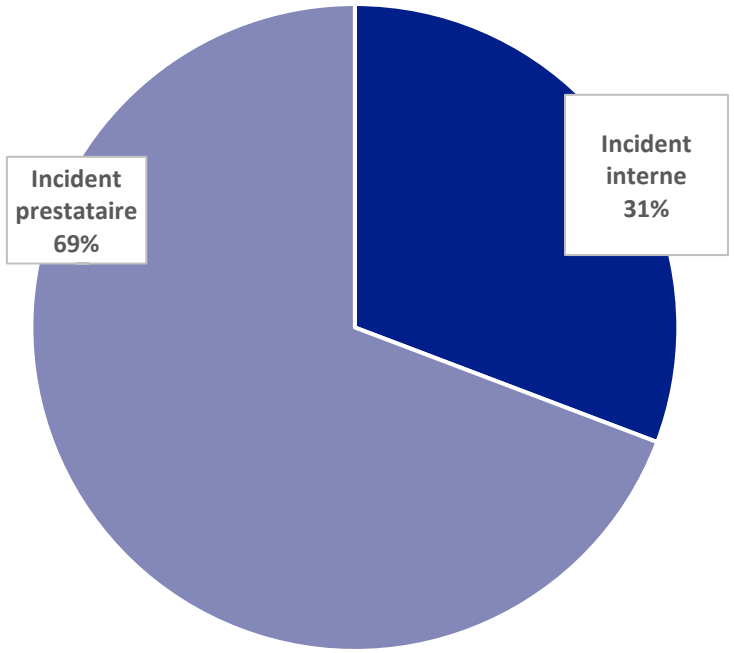
- **Des incidents concernant des SGP de tout type et de toute taille**
  - → De tout type : Gestion traditionnelle, sous mandat ou immobilière
  - → De toute taille : Encours de 40 millions d'euros à 250 milliards d'euros.
    - → Médiane : 3 milliards.
    - → Premier et troisième quartile : 600 millions et 50 milliards.
  - → Effectifs de 5 ETP à 1200 ETP



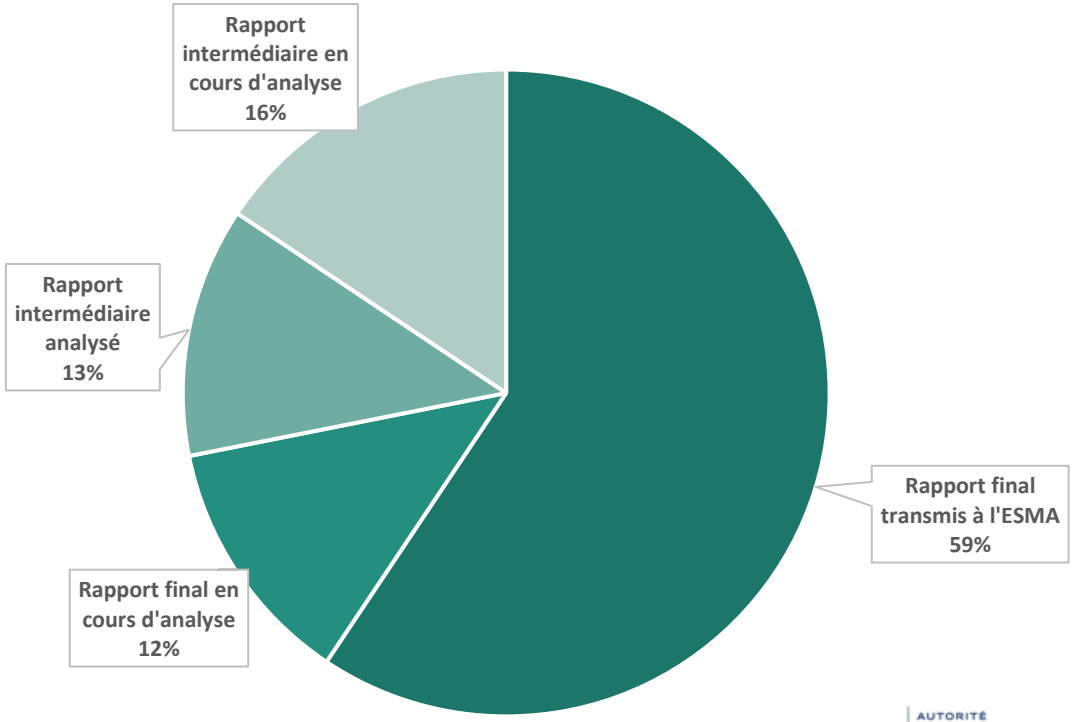


Etat des lieux des incidents pour les SGP (3/3)

- **Principalement des incidents concernant des prestataires des SGP**
  - → Sur les 32 incidents, 22 incidents concernent des prestataires
  - → Enseignement sur l'interconnexion des SGP par leurs services TIC



- **32 incidents traités depuis l'entrée en application de DORA**
  - → Analyses communes entre les chargés de portefeuille, les référents DORA et les services de cybersécurité de l'AMF
  - → 19 rapports finaux transmis à l'ESMA



3

RETOUR D'EXPÉRIENCE EN MATIÈRE DE SUPERVISION DU RISQUE CYBER

1. DÉROULÉ DES CONTRÔLES SUR PLACE – RELATIONS AVEC LES INTERLOCUTEURS

- **Les missions de contrôle couvrant le risque IT et la cybersécurité ont un scope allant au-delà des systèmes d'information :** Le système d'information supporte les fonctions métiers et transverses et celles-ci sont donc également impliquées par le contrôle.
- **Les contrôles nécessitent que des ressources soient mobilisées par l'établissement pour assurer sa fluidité :** les contrôleurs doivent avoir à leur disposition le personnel qualifié pour leur fournir les renseignements qu'ils jugent nécessaires.
- **Les échanges et demandes de pièces visent à donner une vision extensive de la manière dont l'IT est piloté et des risques afférents :** désigner une personne pour assurer la coordination des échanges avec la personne en charge de la conduite du contrôle sur place.

- **Quelques exemples** de sujets dépassant le périmètre IT:

✓ **Gouvernance et stratégie**

✓ **Organisation, politiques et procédures**

✓ **Résilience, continuité:** la résilience opérationnelle numérique promue par DORA s'inscrit dans le cadre plus large de la poursuite de l'activité et du respect des engagements

✓ **Données métiers:** la protection des actifs ne se limite pas aux seuls actifs informatiques

- Pour aller plus loin :

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

✓ **Charte de conduite d'une mission de contrôle sur place** publiée par l'ACPR et s'appuyant sur les dispositions du code monétaire et financier

2. 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 et ses clients, 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

3. PRESTATAIRES DE SERVICES TIC ET EXTERNALISATION

- **La règlementation DORA sur les prestataires de services TIC ne se substitue pas à la règlementation préexistante sur l'externalisation:** les exigences relatives à l'externalisation demeurent
- **Les prestataires de services informatiques jouent un rôle crucial dans les opérations des établissements assujettis.** Les fintechs peuvent évoluer des deux côtés de la chaîne de sous-traitance.
- **Si un prestataire (de services TIC ou non) ne dispose pas des mêmes normes de sécurité ou subit une violation, cela peut entraîner une fuite de données critiques.** La confiance des clients est primordiale et une faille de ce type peut avoir des conséquences majeures, 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**.

- **Le respect des différentes exigences relatives à l'externalisation et aux prestataires de service TIC nécessite une approche holistique et rigoureuse de l'identification des relations avec les tiers:** Toutes les prestations de services TIC doivent être identifiées et parmi elles celles qui sont essentielles. Elles sont ensuite typées (cloud). Les lignes directrices de l'EBA relatives à l'externalisation restent applicables.
- **Les processus de gestion de la relation et d'évaluation du risque informatique doivent couvrir la relation contractuelle de bout en bout**, impactant les deux parties, voire les sous-traitants (externalisation en cascade).
- **Vision complète de la chaîne de sous-traitance.**

✓ **Contrats avec des clauses solides et détaillées :** 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, la résiliation et la renégociation. Définir des attentes claires et mesurables (contrôlables) sur la performance, la sécurité, la gestion des données et la continuité de service.

✓ **Sélection rigoureuse et 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 30

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

- Mais aussi :

✓ **EBA guidelines EBA/GL/2019/02 on outsourcing arrangements**

4. RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE

- **Pour être opérationnelle la résilience doit s'appuyer doit impliquer les métiers:** La résilience doit s'appuyer sur une identification des fonctions et processus qui soit partagée par tous.
- **L'identification des actifs informatiques qui permettent les opérations, ainsi que leur documentation nécessitent rigueur, ressources et engagement de la gouvernance.** La fiabilisation des registres d'actifs nécessite engagement, ressources et coordination de tous les acteurs.
- **L'efficacité des processus de protection des actifs, de détection des menaces et des vulnérabilités, de réaction à incident et de résilience dépend de la qualité des processus amont**

- ✓ **La politique de sécurité des systèmes d'information est un document stratégique**. Son contenu fonde la démarche de sécurité de l'entreprise.
- ✓ **Les actions d'administration (y compris création et décommissionnement) des actifs informatiques sont des actions sensibles qu'il convient d'être capable de contrôler et suivre.**
- ✓ **L'identification et la documentation des actifs sont des processus continus; la CMDB est une base vivante.**
- ✓ **Identifier les sources de risque et complexité dans les activités et les processus** (ex: CI/CD et sécurité dans les développements informatiques, administration des services Cloud et de leur sécurité). Documenter les mesures de mitigation des risques mises en place.
- ✓ **Des ressources doivent pouvoir être mobilisées pour réaliser les différents tests attendus** (tests de sécurité (red team), tests des plans de continuité, tests des plans de reprise informatique, revues de code)

- Pour aller plus loin :
- ✓ **DORA Texte de niveau 1 (Règlement UE 2022/2554) :** Art. 5 à 8
- ✓ **DORA Texte de niveau 1 (Règlement UE 2022/2554) :** Art. 24 à 27
- ✓ **RTS on ICT Risk Management framework (Commission Delegated regulation - EU - 2024/1774 of 13 March 2024)**

Rappel concernant les contrôles à composante cyber de l’ AMF

Une démarche engagée dès 2019 sur la base de la réglementation existante (1/2) :

- 3 campagnes de contrôles SPOT menées sur un périmètre de 15 SGP

➢ Présentation ci-après des bonnes et mauvaises pratiques identifiées dans ce cadre

- 12 contrôles classiques incluant le thème cyber, menés sur 7 SGP, 3 CIF, 1 PSFP et 1 IM

➢ Un tiers de ces contrôles ont inclus la réalisation de tests techniques par un 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

Rappel concernant les contrôles à composante cyber de l' AMF

Une démarche engagée dès 2019 sur la base de la réglementation existante (2/2) :

- Thèmes standards :
  - organisation et la 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.

- 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 relatives aux *cloud service providers*.

Pilier DE DORA : Reporting des incidents (1/2)

Compréhension accrue du *business model* des SGP par les attaquants

☐ L'essentiel des incidents reportés font suite à une intrusion sur boîtes emails.

☐ Tentatives de détournement d'identifiants et de mots de passe individuels

→ Tentatives de détournement de fonds

→ Tentatives de récupération de données à caractère personnel ou stratégique

→ *Ransomware*.

☐ Attaques plus sophistiquées :

→ Intrusion sur une plateforme d'épargne salariale via le compte d'une entreprise cliente pour tenter de « vider » les comptes de plusieurs salariés;

→ Exfiltration massive de données confidentielles sur une opération d'investissement en cours par un stagiaire vers un cloud externe.

☐ Emergence de risques nouveaux liés à l'usage de moteur d'IA dans des outils de CRM ou de valorisation.

☐ Subsistance d'attaques « basiques » tel que le vol de matériel informatique (importance de l'inventaire)

☐ Structuration progressive du processus de collecte des incidents par l'AMF :

→ formation des chargés de portefeuille au traitement des remontées d'incidents cyber ;

→ formalisation plus fréquente du rapport d'incident ;

→ revue en interne des cas sérieux

Pilier DE DORA : Reporting des incidents (2/2)

Bonnes pratiques :

- 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 :

- Ne pas veiller à circonscrire les vulnérabilités usuelles :
  - Ports USB non bloqués,
  - 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 (1/3)

Relation avec les prestataires informatiques et les autres partenaires

☐ Phase de sélection : la moins maîtrisée

→ Piste d'audit partielle, voire opaque.

☐ Phase de contractualisation : absence récurrente de clauses importantes

→ 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 : Gestion des risques lies aux prestataires de services TIC (2/3)

Relation avec les prestataires informatiques et les autres partenaires

- ☐ Phase de contractualisation (suite) :
  - → absence de plusieurs clause dans les contrats signés avec les infogérants
    - ▪ Réduit la capacité de supervision de ces acteurs critiques, ainsi que la capacité de réaction en cas de crise ;
  - → difficulté à négocier des clauses d'audit avec des éditeurs de rayonnement mondial ;
  - → absence de plusieurs clauses dans les contrats des commissaires aux comptes, justifiées par l'usage de modèles de contrat standards
    - ▪ La négociation d'annexes *ad hoc* demeure toutefois possible.
- ☐ Phase de contrôle : la plus robuste à date
  - → Modalités nombreuses (réunions ponctuelles, comités périodiques, demandes d'information par courriel, grille d'évaluation, audit technique)
- ☐ Rappel : Les fournisseurs intra et extra-groupe doivent être traités avec la même rigueur du point de vue de leur pilotage et de l'évaluation régulière des services.

Pilier DE DORA : Gestion des risques lies aux prestataires de services TIC (3/3)

Bonnes pratiques :

- 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 :

- 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.

4 PROCHAINES ÉTAPES

DE L'ACCOMPAGNEMENT À UNE SUPERVISION RENFORCÉE

- **Un accompagnement de l'ensemble des entités financières en 2025**
  - De nombreuses présentations auprès des acteurs de la place depuis le mois d'octobre 2024
  - Un support technique sur le pont (plus de 700 questions auxquelles des réponses ont été apportées)
  - Organisation d'entretiens bilatéraux lorsque cela était nécessaire, incluant le support technique et les services de contrôle
  - La création d'une FAQ plusieurs fois mis à jour et mettant à disposition une documentation visant à faciliter la compréhension des attendus

- **Une supervision renforcée à compter de 2026**
  - Identification des priorités de contrôle sur la base : i) des ESR menés par les services de contrôle ; ii) des conclusions issues de l'analyse des réponses au questionnaire transsectoriel relatif à la mise en œuvre de DORA ; iii) la qualité des RoI et les premières conclusions issues d'analyses horizontales ; iv) les notifications d'incidents majeurs
  - Le lancement d'analyses transversales sectorielles et transsectorielles
  - Des contrôles sur place pour les entités les plus à risque

ACPR
BANQUE DE FRANCE

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

FORUM FINTECH

ACPR - AMF

9 octobre 2025

French FinTech Weeks