



FORUM FINTECH



French FinTech Weeks

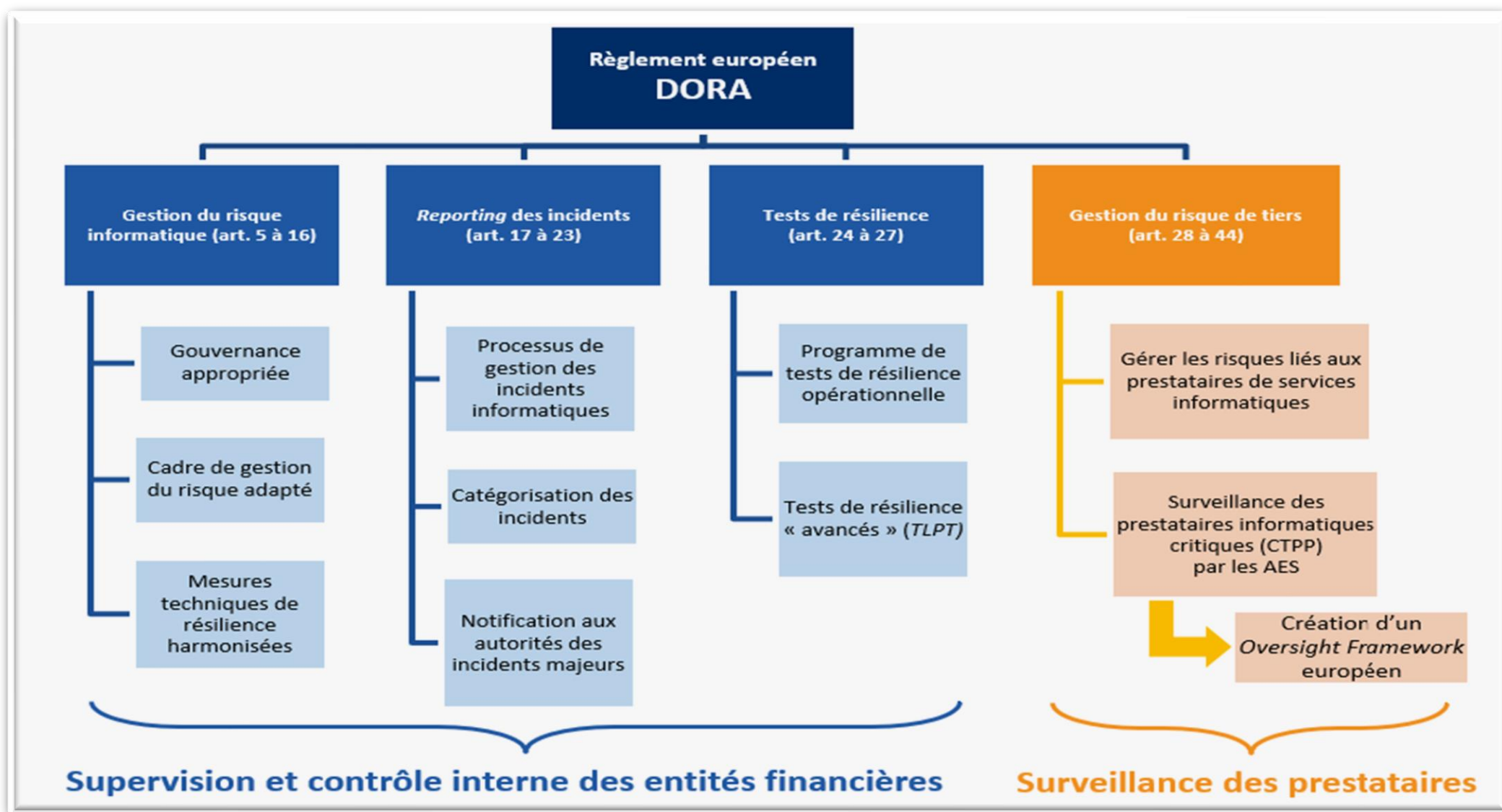
**La résilience opérationnelle numérique
un an après l'entrée en application de DORA
et à l'heure de l'IA de pointe (frontier)**

2 octobre 2026

- 1. Rappel du cadre réglementaire**
- 2. Bilan des notifications d'incidents majeurs**
- 3. Bilan de la seconde collecte du registre d'informations**
- 4. Risque cyber et modèles d'IA de pointe**
- 5. Retour d'expérience en matière de supervision du risque cyber**

1

RAPPEL DU CADRE RÈGLEMENTAIRE

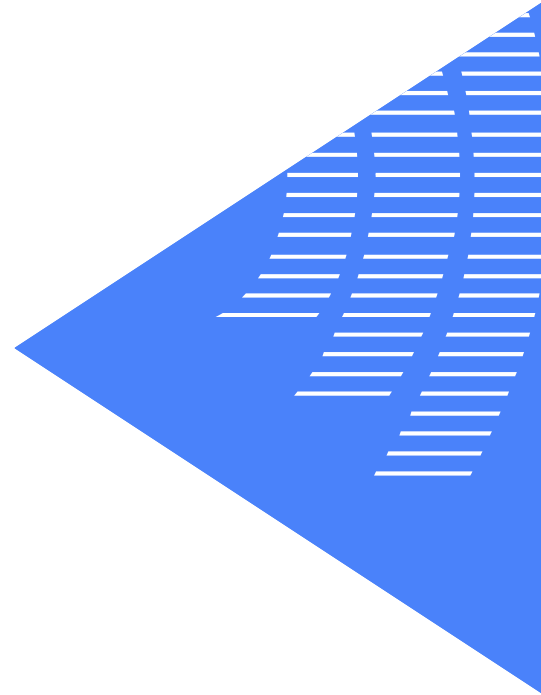


- DORA : « accélérateur » en faveur d'une résilience opérationnelle accrue

- DORA : un cadre qui simplifie et harmonise

2

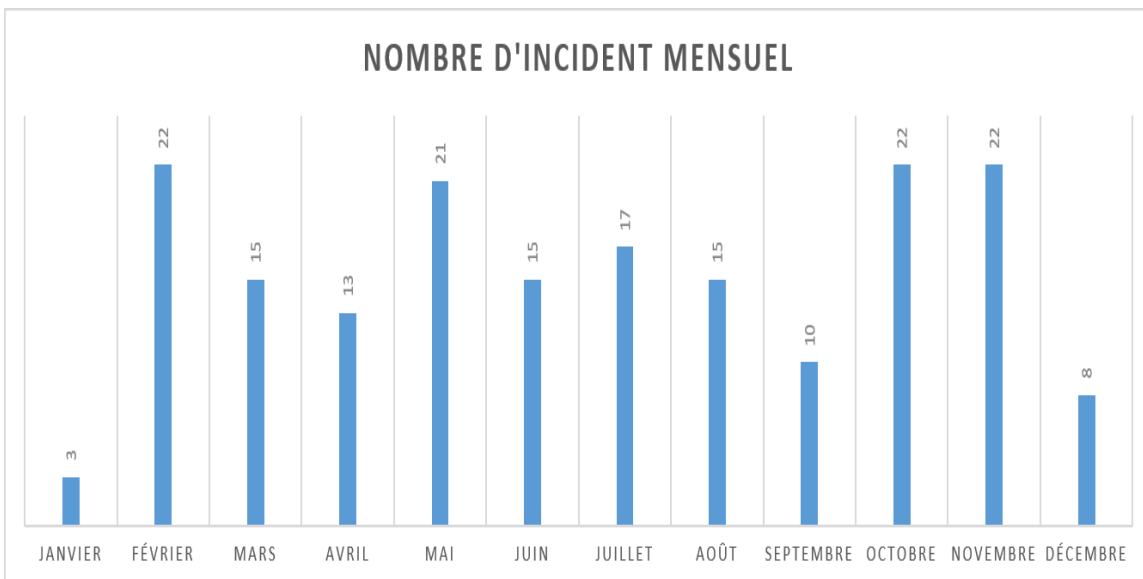
BILAN DES NOTIFICATIONS D'INCIDENTS MAJEURS



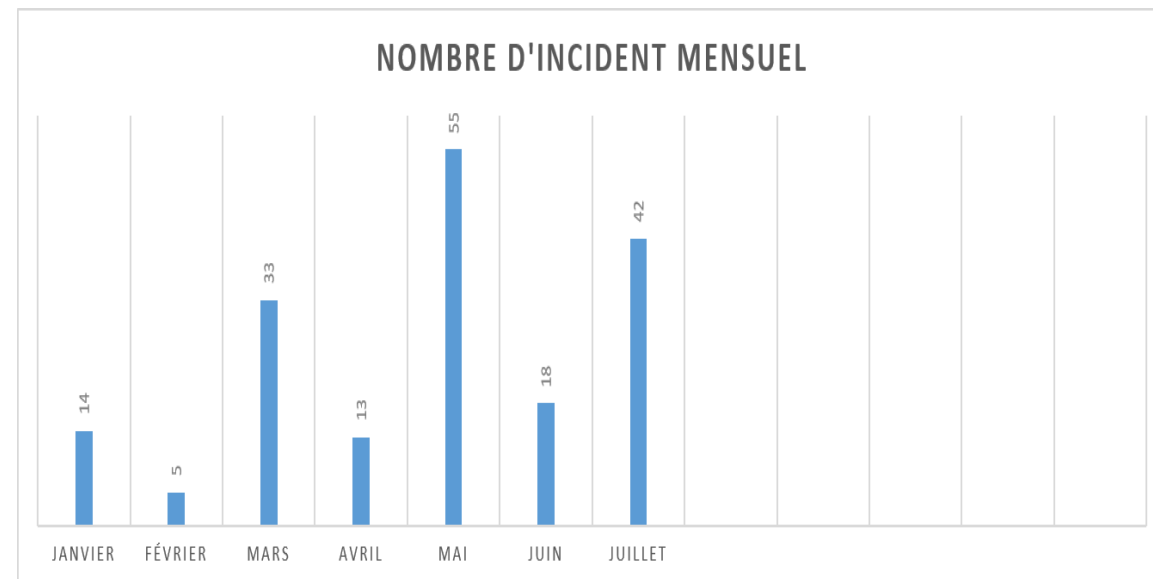


Bilan des notifications d'incidents majeurs

- **Constat n°1** : des incidents nombreux
- **Constat n°2** : absence de saisonnalité ou de régularité apparente
- **Constate n°3** : une augmentation des notification en 2026



2025 : 183 incidents

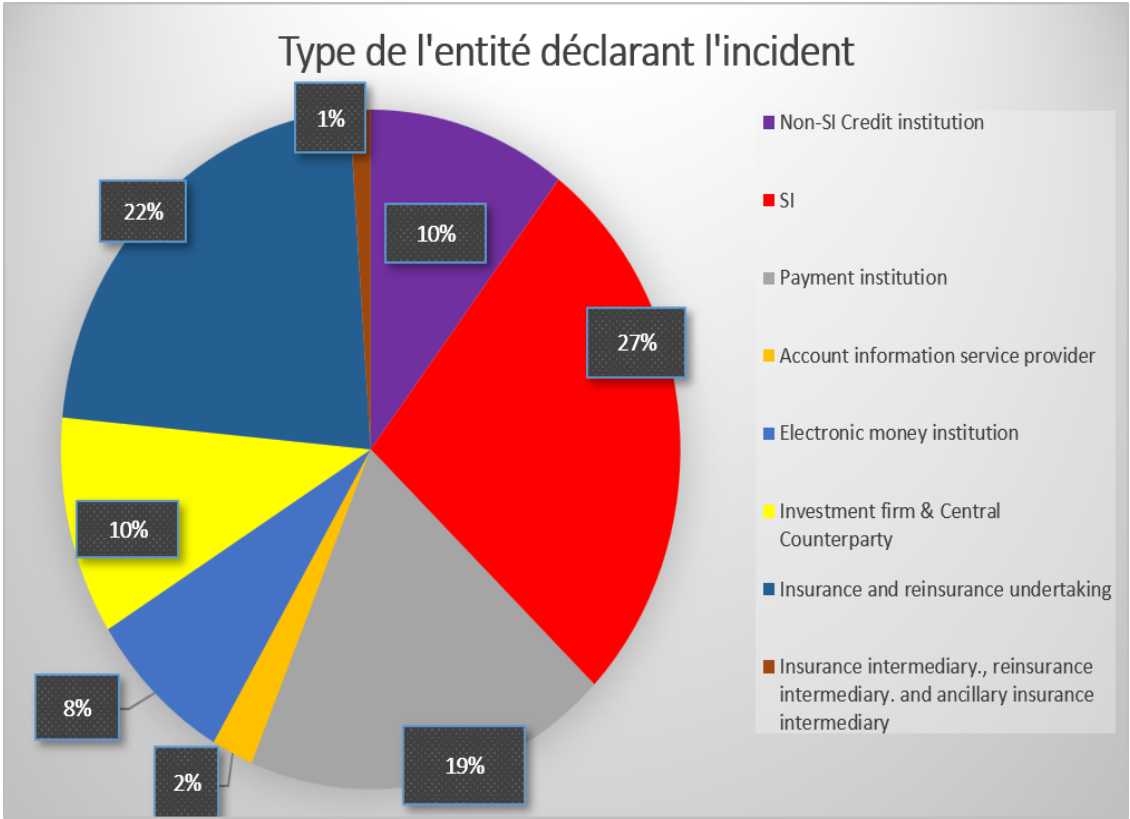


2026 (jusqu'à juillet) : 180 incidents

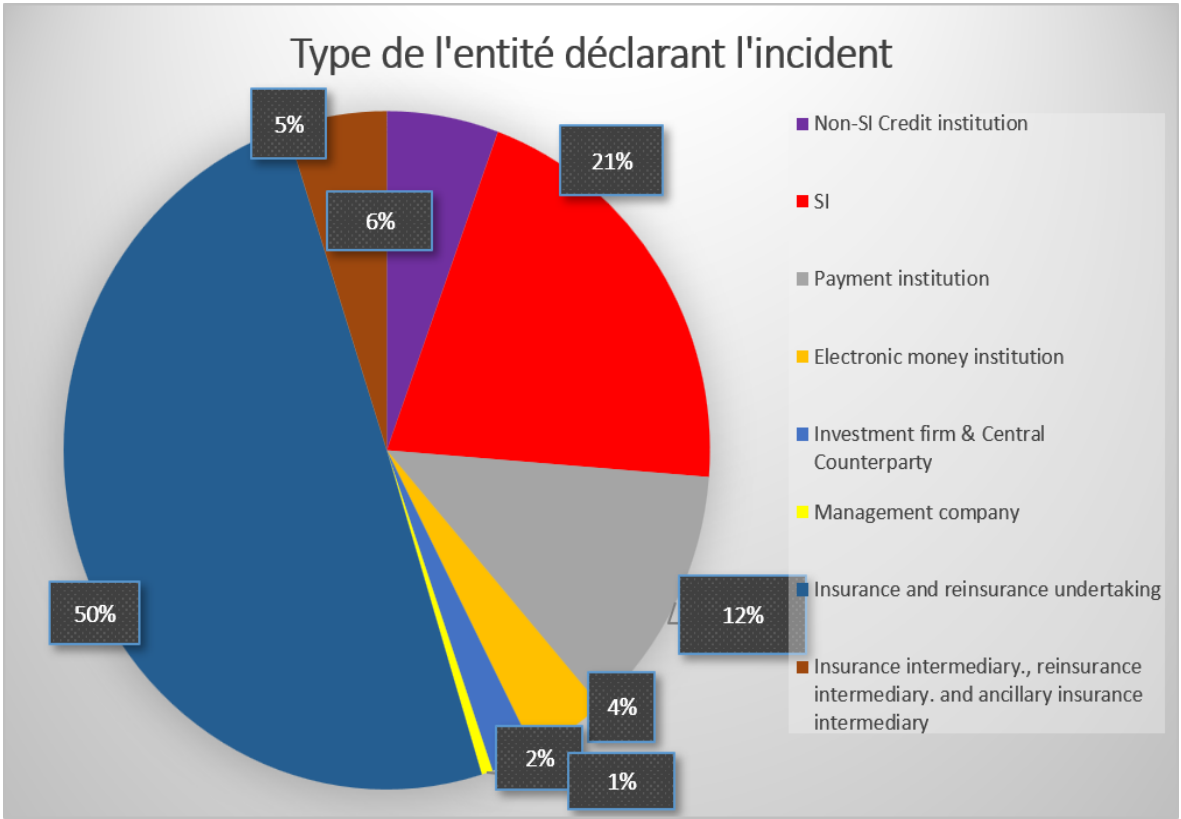


Bilan des notifications d'incidents majeurs

■ **Constat n°4** : baisse des notifications du secteur bancaire



2025

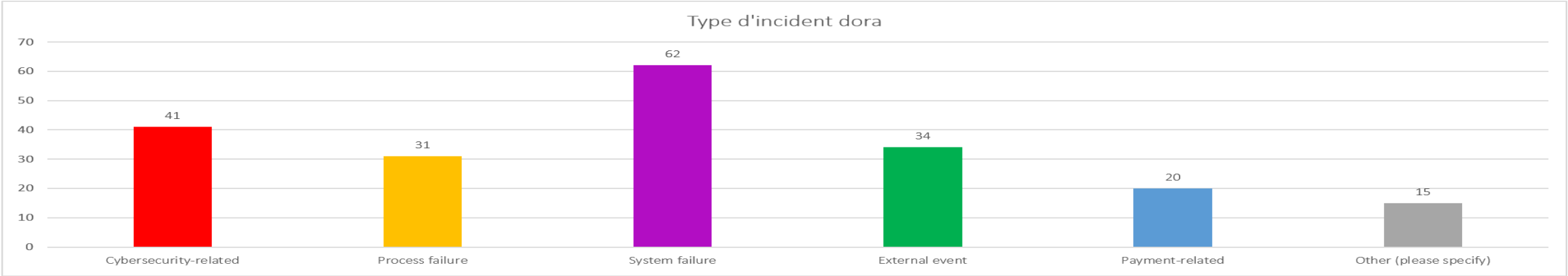


2026

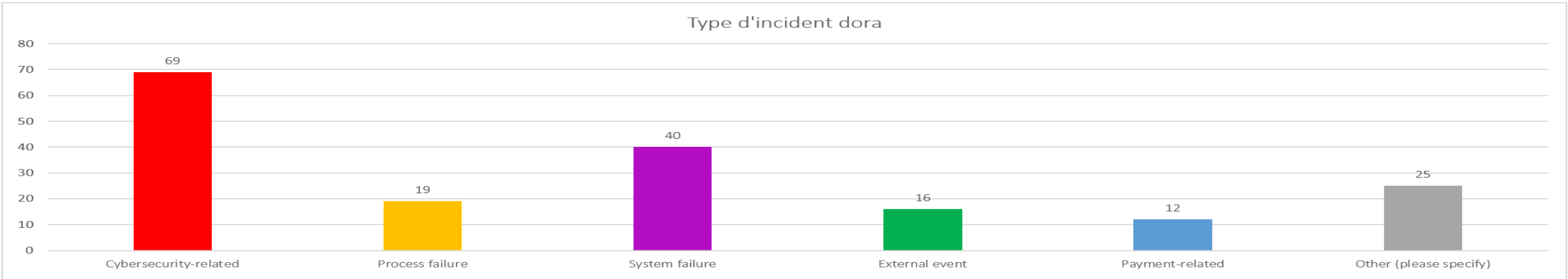


Bilan des notifications d'incidents majeurs

- **Constat n°5** : une augmentation des notifications d'incidents cyber
- **Constat n°6** : une part toujours importante des failles dans les systèmes



2025

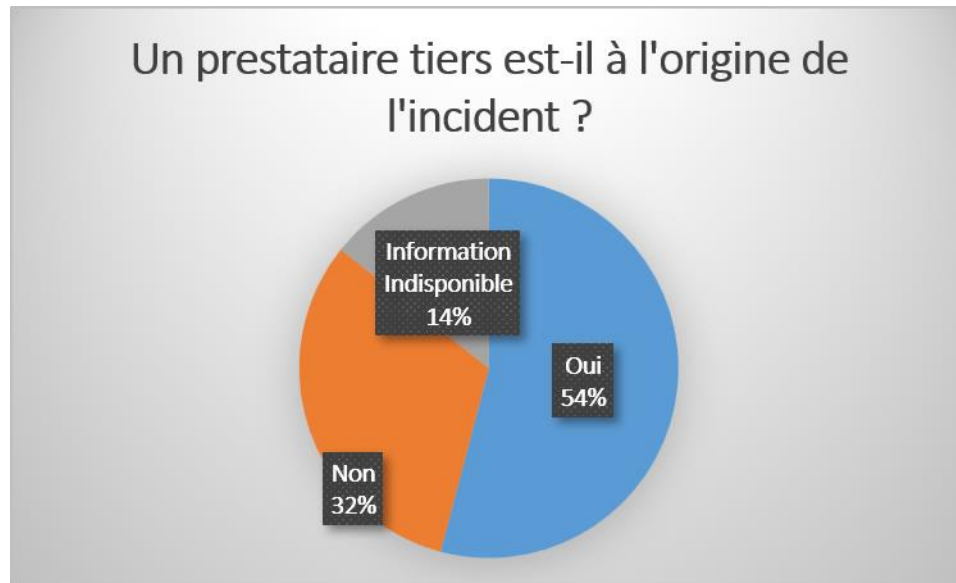


2026

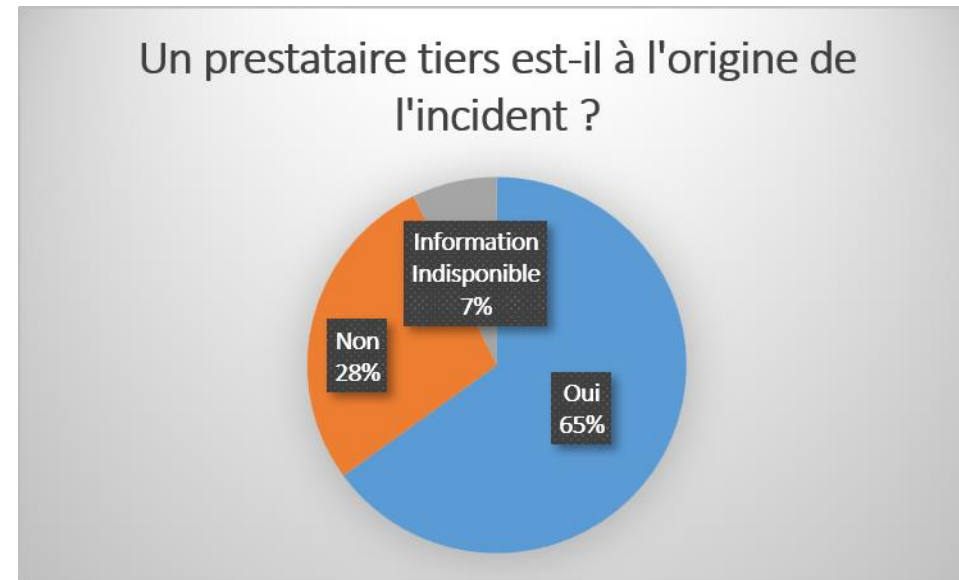


Bilan des notifications d'incidents majeurs

- **Constat n°7** : des tiers souvent impliqués dans les incidents notifiés



2025

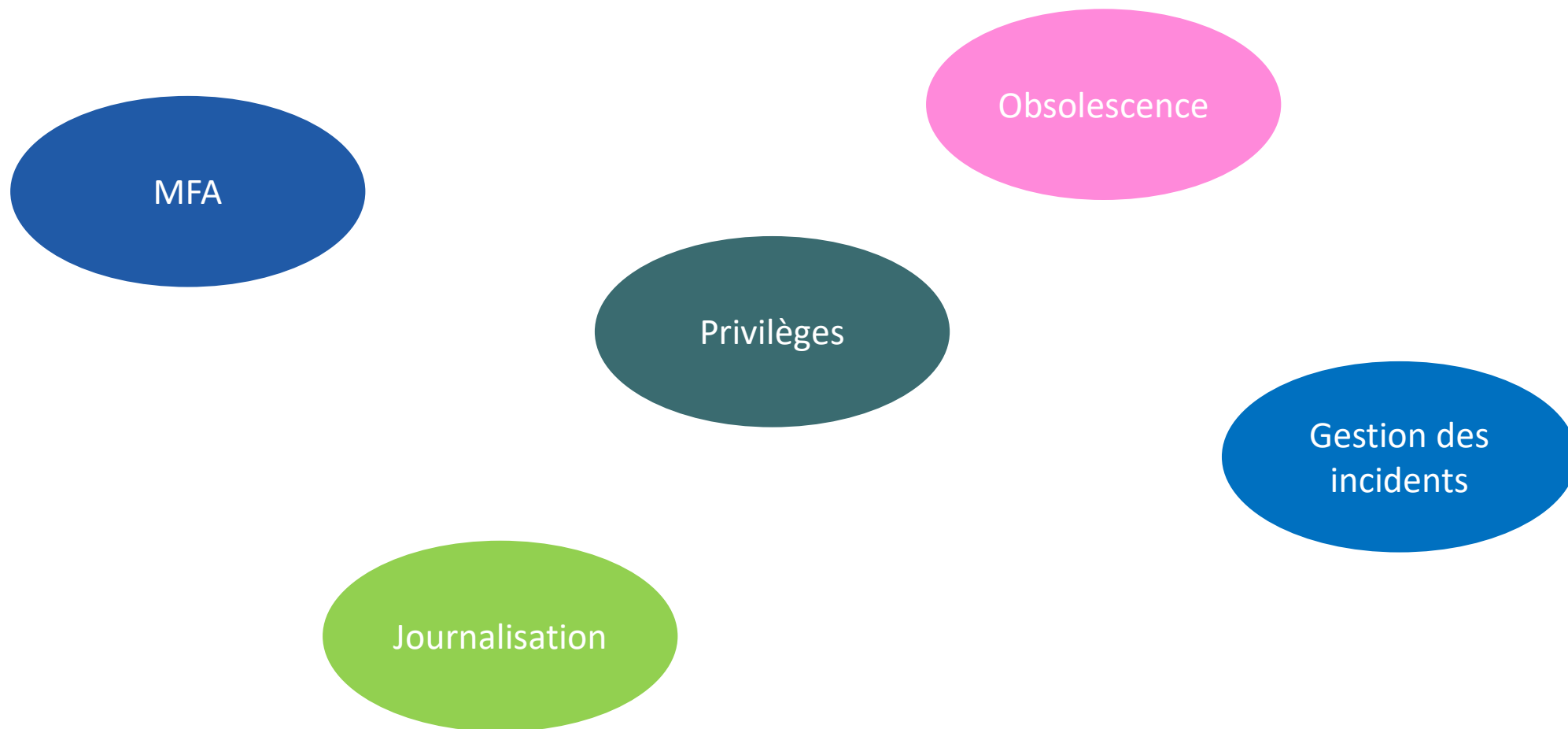


2026



Bilan des notifications d'incidents majeurs

- **Constat n°8** : des incidents attestant de faiblesses récurrentes et d'un niveau de conformité à DORA insatisfaisant



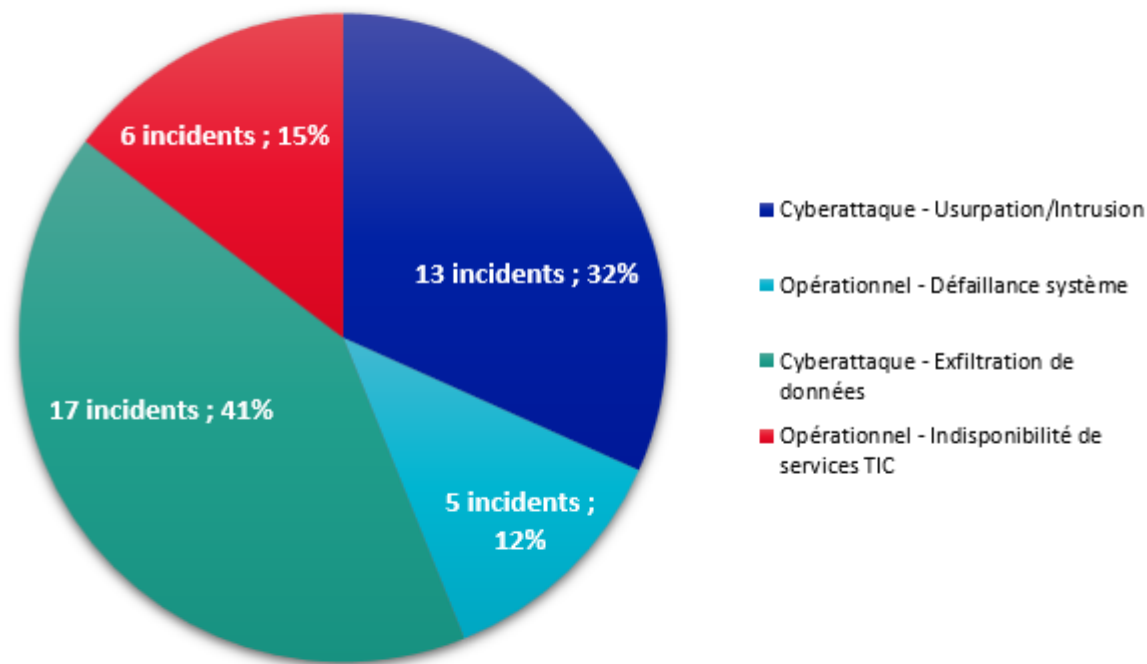
Etat des lieux des incidents pour les SGP – Synthèse

□ 61 déclarations initiales d'incidents depuis le 17 janvier 2025. 41 incidents confirmés majeurs suite aux échanges avec les SGP, déclinés ci-dessous

- 17 incidents ayant été causés par une cyberattaque – exfiltration de données
- 13 incidents ayant été causés par une cyberattaque – usurpation/intrusion
- 6 incidents ayant été causés par une indisponibilité de services TIC (opérationnel)
- 5 incidents ayant été causés par une défaillance système (opérationnel)

□ **Constat n°1** : La majorité des incidents majeurs subis par les SGP est causée par des cyberattaques de formes diverses (rançongiciel, ingénierie sociale, etc.) généralement subies par leurs prestataires

Répartition – Nature de l'incident



Etat des lieux des incidents pour les SGP – Origine de l'incident

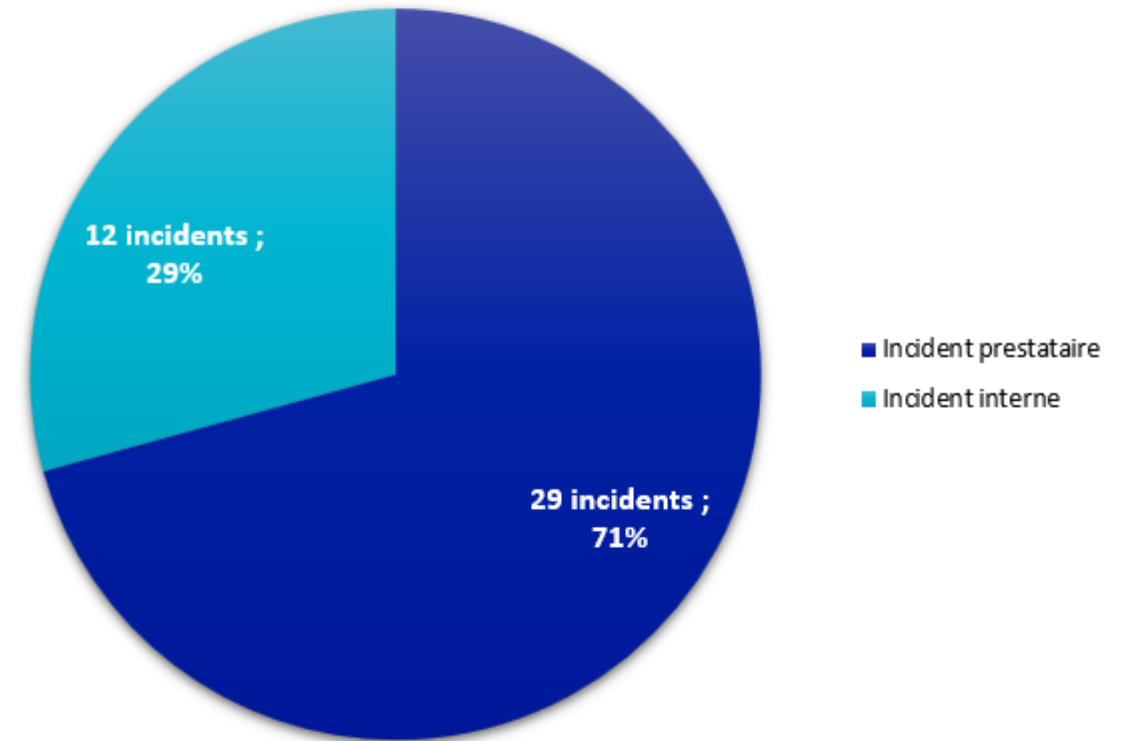
□ Constat n°2 : Principalement des incidents concernant des prestataires des SGP

- Sur les 41 incidents, 29 incidents concernant des prestataires
- Enseignement sur l'interconnexion des SGP par leurs services TIC

□ Ruissellement d'une cyberattaque sur un prestataire

- Industrialisation de la cybercriminalité, rapport annuel sur la cybercriminalité de 2025 du [Ministère de l'Intérieur](#)

Répartition – Incident interne ou prestataire



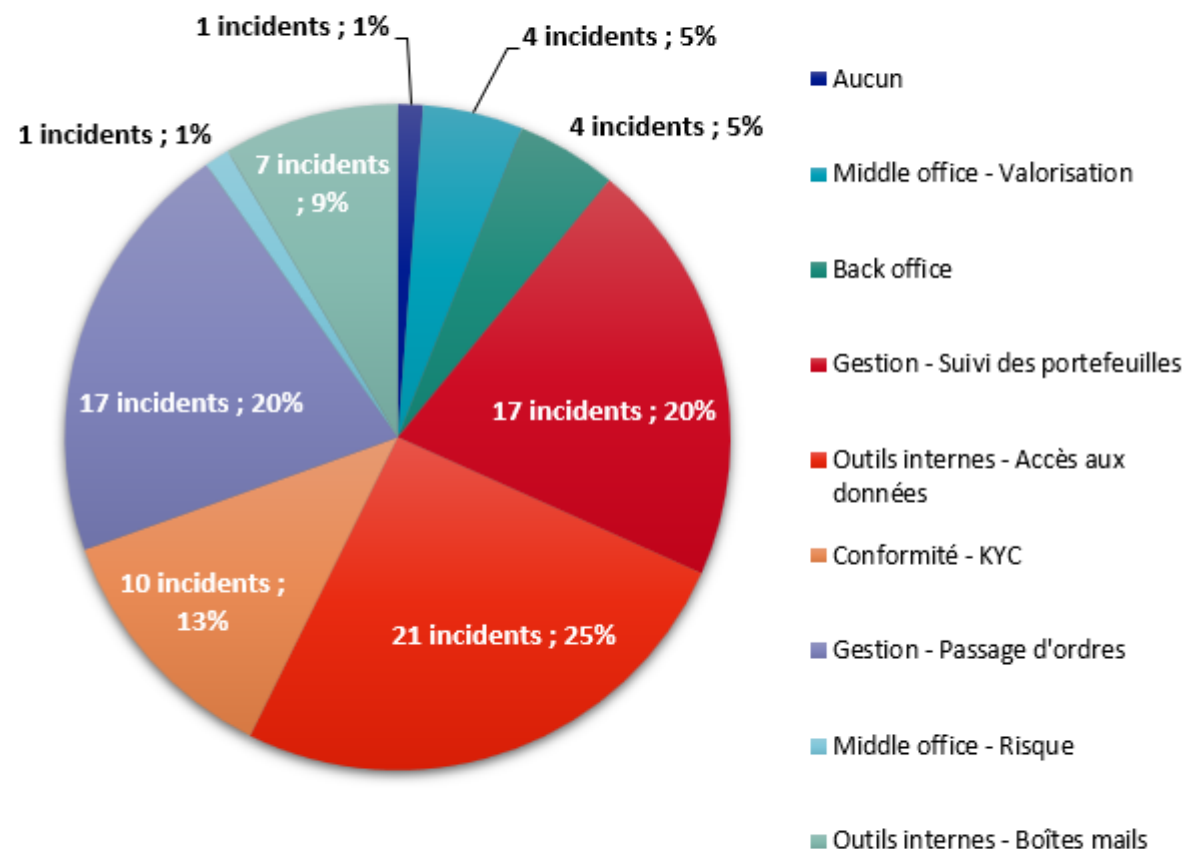
Etat des lieux des incidents pour les SGP – Impact de l'incident

□ Fonctions critiques impactées :

- gestion (comprenant le passage d'ordres) ;
- valorisations d'instruments financiers ;
- conformité (entrée en relation, KYC, LCB-FT) ;
- autres : accès aux données, *middle office*, *back office*.

□ Constat n°3 : Toute la chaîne de gestion peut être impactée

Répartition - Services Touchés

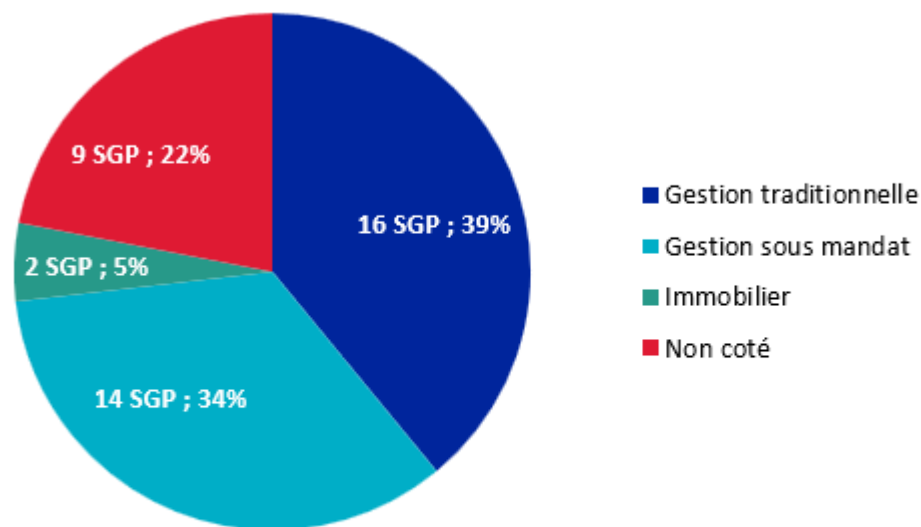


Etat des lieux des incidents pour les SGP – Nature des SGP et Critères

□ Constat n°4 : Des incidents concernant des SGP de tout type et de toute taille

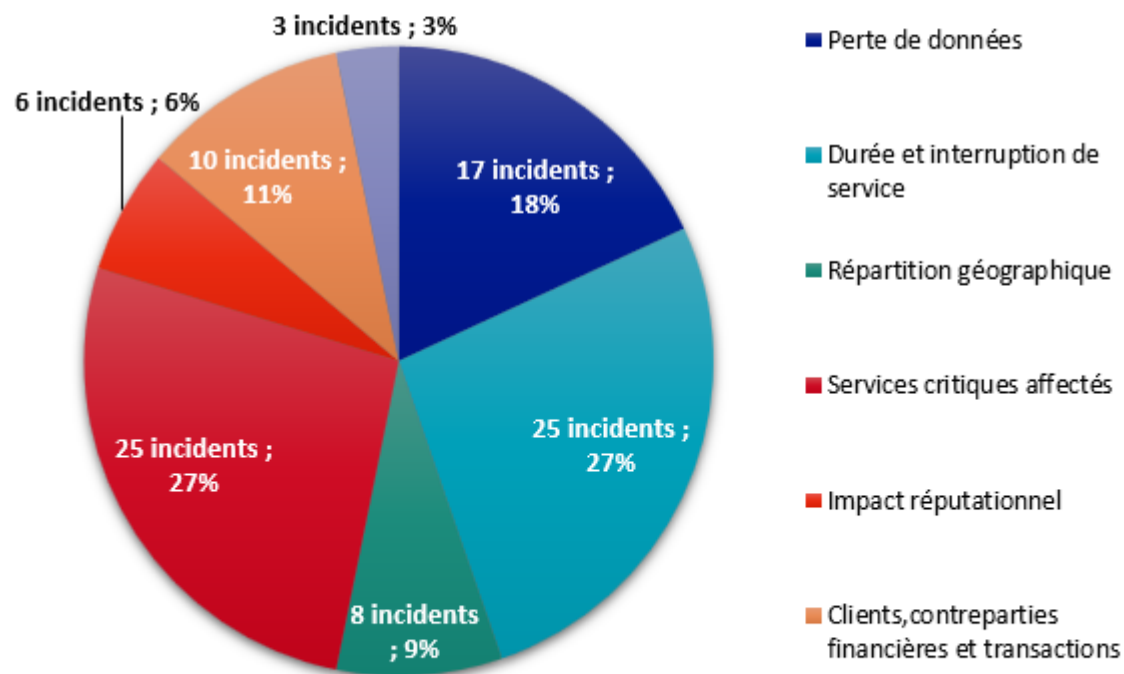
- De tout type : gestion traditionnelle, sous mandat ou immobilière
- De toute taille : encours de 40 millions d'euros à 250 milliards d'euros.
 - Médiane : 3 milliards
 - Premier et troisième quartile : 600 millions et 50 milliards.
- Effectifs de 5 ETP à 1 200 ETP

Répartition - Type de gestion



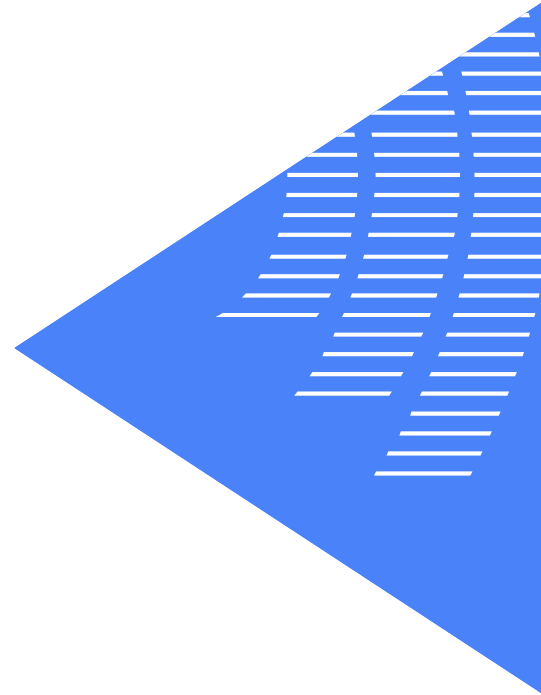
□ Constat n°5 : La gestion d'actifs constitue un secteur fortement exposé au risque cyber, classé 6ème risque le plus critique à court terme par le Forum économique mondial (2026)

Répartition - Critères de classification



3

BILAN DE LA SECONDE COLLECTE DU REGISTRE D'INFORMATIONS



Bilan et Orientation des ROIs

Les ROI

Un outil essentiel à la supervision des tiers.



Collecte 2026

Une meilleure préparation des entités, permettant la collecte d'un plus grand nombre de registres. Il est désormais important de mettre l'accent sur la qualité des données.



Les services utilisés

Le cloud reste le service le plus utilisé par l'ensemble des sociétés. La fourniture logicielle ainsi que la gestion des infrastructures TIC constituent également une part importante des contrats souscrits par les entités.



Un outil de surveillance

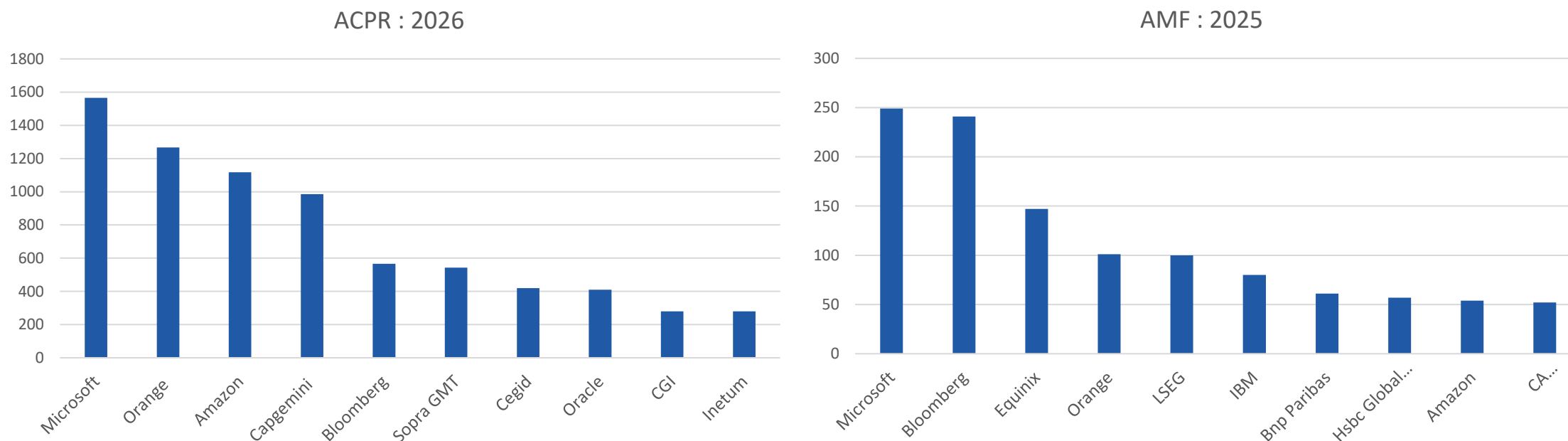
Les ROI permettent l'identification des principaux prestataires TIC au niveau national et européen. L'ACPR et l'AMF souhaitent accentuer ces travaux d'identification au niveau national afin notamment, de prévenir les incidents liés à la défaillance des prestataires.



Le registre 2027

Le calendrier sera similaire à celui de 2026 sans évolution de format. La collecte portera sur l'ensemble des acteurs soumis au registre.

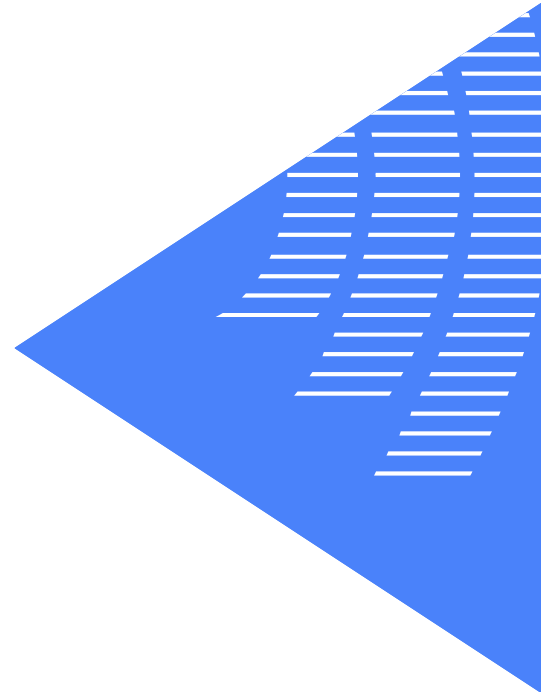
Principaux prestataires (en nombre de contrats)



- La collecte AMF de 2026 n'a portée que sur 70 sociétés et ne peut donc être comparée à celle de l'ACPR.
- Ce classement est cohérent avec les analyses faites par les AES en vue de l'identification des prestataires tiers critiques (CTTP) bien que certains prestataires identifiés soient spécifiques à la France.
- L'AMF et L'ACPR souhaite accentuer ses travaux sur l'identification de prestataires critiques au niveau national.

4

RISQUE CYBER ET MODÈLES D'IA DE POINTE





CONTEXTE (1/4)

Les modèles d'IA de pointe se multiplient rapidement et affichent désormais des capacités cyber avancées, notamment en matière d'identification de vulnérabilités, d'analyse de code et d'automatisation de tâches complexes.

Ces modèles sont progressivement mis à disposition d'un **nombre croissant d'acteurs** et leur diffusion continue de s'accélérer.

Ils sont également porteurs d'un **potentiel offensif significatif** en cas d'usage malveillant (enchaînement de tâches complexes, réduction du délai entre découverte et exploitation de vulnérabilités).

Les évaluations réalisées par différents organismes publics, industriels et académiques montrent que **plusieurs seuils de capacité ont été franchis** et que les performances continuent à progresser rapidement.

Ces évolutions marquent un changement structurel (« nouveau normal ») dans les domaines de la cybersécurité (attaques plus faciles et plus rapides) et du traitement des vulnérabilités (le modèle traditionnel de correction ne suffit plus et implique une compression des délais habituels de remédiation).

Les capacités cyber des modèles de pointe ne sont plus seulement prospectives : elles produisent déjà des **effets concrets** et des comportements inattendus ont été observés en environnement réel.

Une même capacité, deux types d'usage possibles

DÉFENSE

La diffusion progressive de tels outils pourrait **renforcer les capacités défensives des institutions financières**, car ils permettent de :

- Détecter des vulnérabilités
- Analyser plus vite les alertes
- Prioriser les correctifs
- Automatiser certaines réponses
- Renforcer le code avant déploiement

IA de pointe

ATTAQUE

L'IA de pointe est également **porteuse d'un potentiel offensif significatif en cas d'usage malveillant**, en permettant de :

- Accélérer la recherche des vulnérabilités
- Automatiser la reconnaissance
- Développer des exploits
- Enchaîner les tâches complexes avec moins d'intervention humaine
- Abaissement des compétences nécessaires

Ces développements requièrent une vigilance particulière de la part du secteur financier, avec 2 enjeux-clés à surveiller :

- 1) Augmentation du nombre de failles détectées et nécessitant un traitement rapide
- 2) Facilitation ou accélération des opérations malveillantes



CONTEXTE (3/4)

À mesure que l'IA accélère la découverte et l'exploitation des vulnérabilités, le facteur limitant pourrait se déplacer vers la capacité à les qualifier, les prioriser, les corriger et déployer les correctifs.

DÉFENSEUR



↑ Goulot d'étranglement potentiel : capacités humaines, techniques et organisationnelles

ATTAQUANT



CONTEXTE (4/4)

L'IA amplifie les techniques de cyberattaques existantes. Dans un système financier reposant sur des logiciels courants et des prestataires de services partagés, des risques systémiques liés à l'IA peuvent apparaître

FMI, "Financial Stability Risks Mount as Artificial Intelligence Fuels Cyberattacks"

Faible systémique découverte par l'IA

L'identification, par ces moyens, d'une vulnérabilité affectant un logiciel largement utilisé pourrait créer un risque systémique si elle était exploitée à grande échelle.

Concentration sur des fournisseurs d'IA

La concentration sur un petit nombre de fournisseurs d'IA amplifie les dépendances technologiques et l'impact des faiblesses exploitées.

Coupure d'accès à des fournisseurs d'IA

L'accès à un modèle peut être suspendu, notamment par son fournisseur, hors du contrôle de l'établissement utilisant l'IA.

IA et règlement DORA

Protection et prévention – Article 9

- Garantir, pour l'ensemble des actifs TIC la sécurité et la résilience dès la conception, la gestion des identités et des accès
- Processus de correction des vulnérabilités améliorés, tant en termes de rapidité que de complexité
 - **Cas d'usage** : Assistance dans la priorisation et déploiement des correctifs selon la criticité, en phase avec l'évolution des menaces

Détection – Article 10

- Renforcer la surveillance en imposant des délais de réaction plus stricts, par exemple en amélioration les capacités de détection
 - **Cas d'usage** : Mécanismes de détection des vulnérabilités et des comportements anormaux

Encadrement de l'intégration de l'IA

- Mise en place d'une gouvernance et d'un cadre d'utilisation de l'IA
- Former les collaborateurs à l'usage de l'IA et les sensibiliser aux risques
- Mettre à jour le dispositif de gestion des risques - En tant qu'actif de TIC, l'IA est captée par les obligations DORA, par exemple :
 - **Cadre de gestion du risque lié aux TIC** (identification, protection et prévention, détection, réponse et rétablissement, apprentissage et évolution, tests, etc.)
 - **Gestion des risques liés aux prestataires tiers de services TIC** (encadrement contractuel, évaluation du risque de concentration, etc.)
 - **Protection des données** (risques liés au lieu de stockage/traitement des données)



RECOMMANDATIONS DE L'ACPR ET L'AMF À DESTINATION DU SECTEUR FINANCIER

(1/3)

Pour répondre au **défi de la gestion des vulnérabilités**, les institutions financières sont invitées à :

Renforcer leurs capacités de veille

- Réalisation fréquente d'analyses (scans) de vulnérabilités ;
- Suivi régulier des alertes des CERT, éditeurs et bases de données spécialisées ;
- Participation à des dispositifs de partage d'information sectoriels.

Augmenter les capacités de correction des vulnérabilités, sans dégrader le niveau d'exigence en matière de qualité et de sécurité

- Mise en place de mécanismes de priorisation efficaces du traitement des vulnérabilités
- Identification de marges de manœuvre organisationnelles pour absorber les besoins de correction (patching) potentiellement plus fréquents et de raccourcir les délais de remédiation des vulnérabilités critiques



RECOMMANDATIONS DE L'ACPR ET L'AMF À DESTINATION DU SECTEUR FINANCIER

(2/3)

Pour répondre au **défi de la hausse de la menace cyber**, les institutions financières sont d'abord **encouragées à renforcer la défense périmétrique** :

Maitriser sa surface d'exposition

- Cartographier précisément les actifs numérisés
- Limiter les services accessibles depuis Internet
- Désactiver les ports non nécessaires

Sécuriser les accès

- Accélérer le déploiement des architectures de contrôle des accès et de la segmentation
- Généraliser l'authentification multi-facteurs
- Mettre en place des politiques robustes de gestion des mots de passe et des habilitations

Renforcer les capacités de détection rapide d'événements suspects

- Identifier au plus tôt toute compromission potentielle
- En limiter les impacts
- Engager un dialogue avec les prestataires à propos de leur capacité de détection et de remédiation

Se doter de capacités minimales de réponse à incident

- Déployer des mesures de confinement pour limiter la propagation
- Préparer des plans de continuité régulièrement éprouvés
- Prévoir des sauvegardes pour restaurer les systèmes en cas de compromission majeure

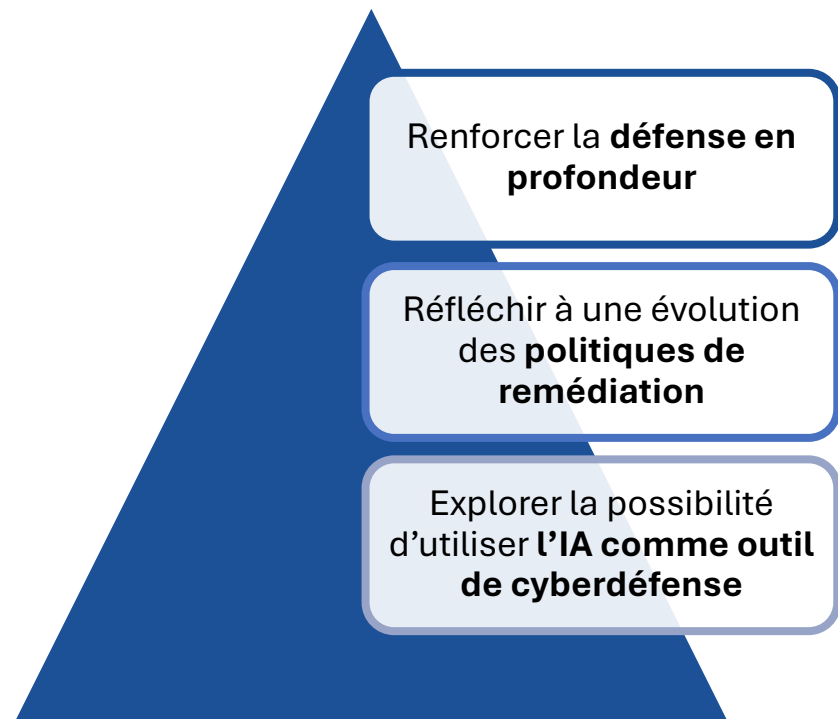


RECOMMANDATIONS DE L'ACPR ET L'AMF À DESTINATION DU SECTEUR FINANCIER

(3/3)

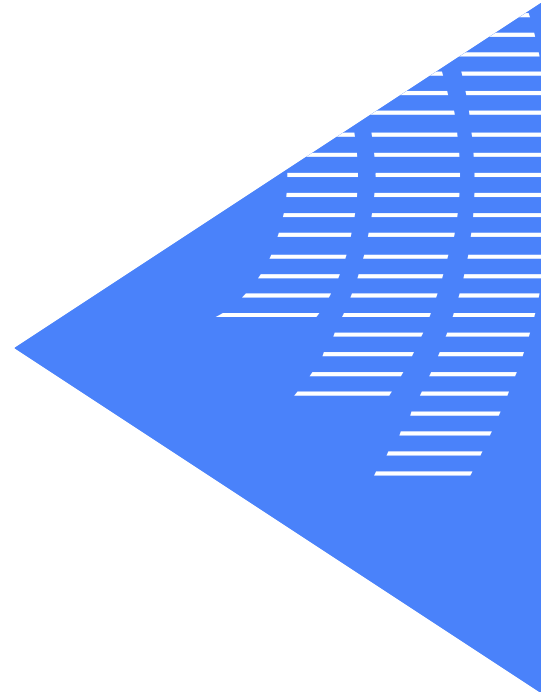
En complément, ces évolutions technologiques impliquent de :

- ☐ **Renforcer la gouvernance de l'IA au niveau des organes dirigeants**, avec supervision humaine effective, mécanismes d'arrêt d'urgence et contrôle des usages critiques
- ☐ **Maîtriser les risques de concentration, de dépendance technologique et de "shadow AI"**, grâce à une cartographie des tiers critiques et une surveillance spécifique des risques propres aux modèles
- ☐ **D'envisager une transformation plus profonde des approches de cybersécurité**



5

RETOUR D'EXPÉRIENCE EN MATIÈRE DE SUPERVISION DU RISQUE CYBER





ENSEIGNEMENTS DES PREMIERS CONTRÔLES SUR PLACE « DORA »

Des contrôles sur place, adaptés aux dispositions du nouveau cadre réglementaire DORA, ont été opérés sur différents périmètres des secteurs bancaire et assurantiel.

Périmètre d'intervention du secteur bancaire

- Principalement, de grands groupes bancaires (SI) présents au niveau international, couvrant des équipes IT de plusieurs milliers de personnes et un nombre d'assets de plusieurs milliers
- Dans une moindre mesure, des LSI (avec un fort taux d'externalisation)

Périmètre d'intervention du secteur assurantiel

- Quelques contrôles pré-entrée en vigueur/à portée pédagogique sur la préparation des entités à l'entrée en vigueur du cadre DORA
- Une large répartition des actions menées couvrant petits, moyens ou grands acteurs de l'assurance-vie, de la santé ou de la prévoyance.



PRINCIPAUX POINTS D'ATTENTION POUR LE SECTEUR BANCAIRE

Les points relatés ci-après ne constituent pas, en tant que tels, un baromètre de la santé cyber, Le propre du contrôle sur place n'est pas de donner des satisfecit mais de pointer avec acuité les lacunes ou insuffisances, Pour autant, il est précisé que les faiblesses relatées ci-après n'affectent pas de manière égale ou globale les différents acteurs visités. Ces derniers sont affectés à des degrés divers par tout ou partie des points relevés,

Gouvernance IT ayant mal anticipé les enjeux DORA

- Intégration tardive des exigences DORA avec des mesures correctives encore en cours de déploiement
- Implication insuffisante de l'organe de direction dans les sujets relatifs à l'IT, à la cybersécurité et à l'externalisation des services IT
- Stratégies IT/Cyber/Cloud insuffisamment matures, conduisant au maintien de SI fragmentés
- Budgets parfois mal calibrés
- Procédures, rôles et responsabilités manquant de clarté.

Faiblesses dans la mise en œuvre des mesures de sécurité

- Gestion des droits d'accès insuffisamment contrôlée
- Protection des réseaux insuffisante
- Administration des systèmes d'information insuffisamment maîtrisée
- Durcissement incomplet des équipements et patching défaillant / Obsolescence marquée de certaines briques
- Protection des données inadéquate
- Chiffrement au repos et en transit défaillant





PRINCIPAUX POINTS D'ATTENTION POUR LE SECTEUR BANCAIRE

Les sujets, d'une part, de gouvernance de déploiement des 3 lignes de défense, d'autre part, de mise en œuvre de la sécurité ou de pilotage des opérations IT, sont fréquemment entremêlés et interdépendants.

Maturité à renforcer de la gouvernance des risques SI/SSI

- Manque d'indépendance de la 2^{ème} ligne de défense dans le traitement des risques :
- Ressources insuffisantes en nombre et en compétences.
- Couverture des risques incomplète, notamment des risques liés à l'externalisation,
- Plans de contrôle cyber et risques tiers insuffisamment matures.

Faiblesses dans le pilotage des opérations IT

- Défaillances majeures et structurelles dans l'Inventaire des actifs (inventaire incomplet – carence récurrente-, manque de lien depuis les fonctions critiques ou importantes jusqu'aux actifs, manque d'automatisation).
- Dispositif de gestion de l'obsolescence et des changements insuffisamment structurés et contrôlés
- Pilotage des performances IT insuffisant
- Gestion des incidents (collecte, classification, priorisation, rapidité de traitement et contrôle) perfectible.





PRINCIPAUX POINTS D'ATTENTION POUR LE SECTEUR BANCAIRE

Ces deux derniers sujets sont tout aussi structurants, l'expérience nous ayant collectivement appris, d'une part, que les prestataires TIC constituent clairement un maillon sensible, exploité par les pirates, d'autre part qu'une faiblesse des dispositifs de continuité peut consister un risque existentiel pour les organismes.

Lenteur du déploiement des mesures de gestion du risque de tiers TIC

- Analyse des risques afférents aux prestataires TIC peu déployée
- Risque de concentration peu suivi
- Clauses contractuelles encore partiellement révisées et déployées (clause d'audit, de sortie)
- Carences dans le suivi et le pilotage des fournisseurs de services TIC.
- Registre d'information incomplet et identification des prestataires critiques imprécise

Faiblesses structurelles des dispositifs de continuité

- Les investigations réalisées jusqu'ici ont été limitées...
- ... mais les premiers travaux engagés révèlent un dispositif de résilience encore insuffisamment maîtrisé.



PRINCIPAUX POINTS D'ATTENTION POUR LE SECTEUR ASSURANTIEL

D'un point de vue thématique, il n'y a pas de différences fondamentales entre les sujets d'attention du secteur bancaire et du secteur assurantiel. Les points de divergence relative trouvent souvent leur origine dans les différences de marché : un plus grand nombre d'acteurs petits ou moyens pour l'assurance. Pour ces derniers, le degré médian de maturité SSI est plus bas et les faiblesses relevées témoignent plutôt d'une appropriation moindre de ces sujets.

Comparabilité globale sur les grands thèmes

- Implication de la gouvernance
- Approche par les risques du Top-management jusqu'aux risques SI-SSI
- Fonctionnement des 3 lignes de défense
- Sécurité en profondeur (inventaire, identification, détection et prévention)
- Gestion de la continuité (réponse, rétablissement, sauvegardes, restauration)
- Gestion des prestataires TIC.

Des sujets plus fondamentaux à approfondir

- *Gap Analysis* (avant/après DORA) rare ou insuffisamment approfondi
- Installation de la fonction de contrôle SSI absente ou insuffisante.
- Structuration non aboutie des politiques, procédures et processus.
- Identification à renforcer des FCI qui sous-tendent les actifs et fonctions TIC
- Faibles capacités de surveillance/détection, au-delà de la surveillance périmétrique (de ce qui vient de l'extérieur).



Rappels concernant les contrôles à composante cyber de l'AMF (1/3)

Une démarche engagée dès 2019 par l'AMF

- **3 campagnes de contrôles SPOT menées sur un périmètre de 15 SGP entre 2019 et 2022**
 - ✓ Chacune a fait l'objet d'une synthèse publiée sur le site internet de l'AMF, incluant des bonnes et mauvaises pratiques
- **14 contrôles classiques incluant le thème cyber, menés sur 9 SGP, 3 CIF, 1 PSFP et 1 IM**
 - ✓ Plus d'un tiers de ces contrôles ont inclus la réalisation de tests techniques par un PASSI qualifié par l'ANSSI.
- **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 et d'incident d'origine cyber avéré ayant compromis des données clients.
 - ✓ information des trois associations professionnelles de SGP par courrier en ce sens

Rappels concernant les contrôles à composante cyber de l' AMF (2/3)

Un programme de contrôle construit sur la base de la réglementation *ante* DORA, mais toujours pertinent post entrée en application de cette réglementation le 17 janvier 2025

■ Thèmes de travail :

- ✓ 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,
- ✓ volet informatique et cyber du plan de continuité d'activité,
- ✓ dispositif de contrôle interne appliqué aux systèmes d'information et au dispositif cyber.

■ Réglementation applicable (*ante* 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*.

Rappels concernant les contrôles à composante cyber de l'AMF (3/3)

Principaux constats consolidés issus des contrôles à composante cyber menés depuis 2019 : « seul ce qui est bien connu est bien protégé »

- ☐ **Prise en compte progressive** du sujet cyber dans les cartographies des risques et les plans de contrôle, avec délégation régulière de tests techniques (dont le ciblage demeure toutefois perfectible)
 - ☐ **Indépendance** de la fonction en charge du **pilotage de la cybersécurité**
 - ☐ Mise en place de **sensibilisation régulière de l'ensemble du personnel** (tests de *phishing*)
-
- ☐ **Défaut d'identification préalable des actifs critiques**, pouvant occasionner un **faux sentiment de sécurité**
 - ☐ **PCA** testé intensivement mais **omettant** le volet relatif à la **restauration des données**
 - ☐ **Pilotage et contrôle des fournisseurs IT critiques insuffisants**
 - ☐ Persistance de **défauts de sécurité standards** sur les ports UBS et les postes de travail
 - ☐ Absence d'**analyse de tendance des incidents d'origine cyber** (incluant les *near miss*)

Actualités concernant les contrôles à composante cyber de l'AMF

De premières difficultés rencontrées dans la réalisation des tests techniques (délégués) en situation de contrôle.

- Deux nouveaux contrôles classiques de SGP, achevés courant S1 2026, ont couvert le dispositif de cybersécurité de ces acteurs et inclus des tests techniques délégués à un PASSI :
 - ✓ L'éditeur extra-européen de l'une des applications visées par ces tests (et fournissant à cette dernière un service de *speech-to-text*) a refusé de se soumettre aux tests projetés, ce qui a conduit à qualifier un constat de manquement en l'absence de contrat conforme à DORA prévoyant cette option. La SGP concernée a résilié le contrat la liant à cet éditeur avant réception du rapport de contrôle.
 - ✓ C'est la deuxième fois depuis 2025 que la DC est confrontée à ce type de refus (le précédent ayant concerné une application de CRM) ;
 - ✓ Ces deux contrôles se sont conclus par une lettre de suites.
- Les méthodes des contrôles à composante cyber de l'AMF et de l'ACPR ont été présentées à l'ANSSI dans le cadre de sessions d'échanges menées en 2026 (cadrage, investigations, délégation des tests techniques, restitution, suivi des remédiations).

Perspectives des contrôles à composante cyber de l'AMF

Le thème de contrôle « cybersécurité » est devenu un standard, au même titre, par exemple, que les processus d'investissement ou de valorisation, ou le dispositif LCB-FT :

- Au moins un nouveau contrôle (classique) incluant une composante cyber est prévu d'ici la fin de l'exercice 2026.
- L'exploitation des RoI permet d'affermir la sélection des applicatifs sensibles pouvant faire l'objet de tests techniques en situation de contrôle.
- Jusqu'à présent, les outils informatiques utilisant des briques d'intelligence artificielle ont été contrôlés comme n'importe quel outil, sur la base de la réglementation DORA qui démontre ici sa pertinence.
- Des réflexions sont en cours pour approfondir les contrôles sur les usages et menaces liés à l'IA dans les années à venir. Dans ce cadre, le *Supervisory Toolkit for AI Use in Capital Markets* (publié en mai 2026) fait l'objet d'une lecture attentive des services.

Proposition de questions à destination de l'animateur

- Quel nombre de contrôle à composante cyber l'AMF vise-t'elle pour 2027?
- Toutes les sociétés supervisées par l'AMF sont-elles susceptibles d'un contrôle à composante cyber menés par l'autorité?
- Tous les contrôles à composante cyber de l'AMF incluent-ils des tests techniques tels que des test d'intrusion?
- Comment puis-je me préparer efficacement à un contrôle à composante cyber de l'AMF?
- Quels contrôles sont prévus sur l'IA dans les années à venir?



FORUM FINTECH



French FinTech Weeks

2 octobre 2026