

Le risque cyber

Le risque cyber est l'une des principales sources de risque opérationnel. Il fait l'objet d'une attention de plus en plus grande des régulateurs, compte tenu des conséquences potentielles très invalidantes pour les infrastructures d'un incident cyber majeur. Selon le [Rapport sur la cyber-résilience des infrastructures de marché](#), publié en novembre 2014 par la Banque des règlements internationaux (BRI), les cybermenaces sont définies comme « *une circonstance ou un événement pouvant potentiellement exploiter, de manière intentionnelle ou non, une ou plusieurs vulnérabilités des systèmes d'une infrastructure, se traduisant par une perte de confidentialité, d'intégrité ou de disponibilité des données* ».

Cadre de surveillance

Les cyberattaques, avec un risque extrême comme la corruption des données ou l'impossibilité d'accéder au système (*distributed denial of service – DDoS*) sont susceptibles de contraindre l'infrastructure à arrêter toute activité, l'empêchant de remplir son rôle crucial vis-à-vis de ses participants. Les cyberattaques de cette nature présentent un véritable défi pour les infrastructures en compliquant l'atteinte de l'objectif d'un retour à la normale des opérations (*return to operations – RTO*) dans un délai de deux heures, qui est un objectif général fixé par les [Principes pour les infrastructures de marchés financiers](#) (PFMI) de CPMI-IOSCO de 2012, compte tenu, par exemple dans le cas d'une corruption de données, de la nécessité : i) d'identifier un point de reprise possible ; ii) de restaurer les données saines avant ce point et iii) et de traiter à nouveau toutes les opérations arrivées dans le système après le point de reprise.

Pour décliner de façon plus détaillée les attentes en la matière, une [orientation sur la cyber-résilience des infrastructures de marché](#) a été publiée en 2016 par le CPMI et l'IOSCO (Organisation internationale des commissions de valeurs). Ils complètent ainsi les attentes générales sur la gestion du risque opérationnel (cf. PFMI publiés en 2012). L'Eurosystem, qui a un rôle majeur dans la surveillance des infrastructures de marché, a publié fin 2018 les [cyber resilience oversight expectations](#) (CROE), et défini trois niveaux de maturité en reprenant de façon plus opérationnelle l'ensemble des attentes de l'orientation CPMI-IOSCO de 2016. Plus une infrastructure de marché est systémique, plus le niveau de maturité attendu est élevé.

Ces préconisations pour la cyber-résilience des infrastructures des marchés financiers, se déclinent en neuf volets.

1. Gouvernance.
2. Identification des risques.
3. Protection.
4. Détection.
5. Rétablissement.
6. Tests.
7. Veille.
8. Apprentissage.
9. Évolution.

L'objectif est de fournir une démarche méthodologique et des outils pour permettre aux infrastructures des infrastructures des marchés financiers de renforcer leur résilience au regard des cybermenaces.

Enfin, le [règlement européen DORA](#) sur la résilience opérationnelle numérique du secteur financier, adopté fin 2022, et qui entrera en vigueur à partir de janvier 2025, vise à faire en sorte que pratiquement toutes les entités du secteur financier (banques, assurances, administrateurs des indices de référence, prestataires de services et émetteurs de crypto-actifs), mettent en place les garanties nécessaires pour atténuer les risques liés aux cyberattaques.

Le règlement vise notamment à imposer à toutes les entreprises de :

- mettre en place les mesures aptes à résister à tous les types de perturbations et de menaces liées aux technologies de l'information et de la communication (TIC) ;
- mettre en place un dispositif de gestion, de classification et de notification des incidents liés aux TIC ;
- conduire régulièrement, pour les entités les plus systémiques, des tests avancés d'outils, de systèmes et de processus de TIC sur la base de tests de pénétration fondés sur la menace (ou *red teaming*).

En complément, le règlement DORA instaure également un cadre de surveillance directe des prestataires informatiques critiques par les superviseurs financiers, y compris par exemple les prestataires de services d'informatique en « nuage » (prestataires de *cloud*).

TIBER-FR, pour renforcer la cybersécurité du secteur financier français

Au regard de l'exposition du secteur financier au risque de cyberattaques, la Banque de France et l'Autorité de contrôle prudentiel et de résolution (ACPR), ont conjointement opté dans le cadre de leurs missions de préservation de la stabilité du système financier, pour la mise en œuvre en France du cadre européen de cyberpiratage éthique contrôlé [TIBER-EU](#) (*Threat Intelligence-Based Ethical Red Teaming*). Cette déclinaison, dite « **TIBER-FR** », **s'accompagne de la publication d'un guide national d'implémentation.**

TIBER-FR est un référentiel de bonnes pratiques, basé sur le volontariat, qui offre un cadre de collaboration entre les autorités compétentes et les institutions financières nationales. Il s'agit de mettre en œuvre un programme de tests destiné à renforcer la cybersécurité de ces dernières et donc la résilience du secteur financier dans son ensemble. Plus largement TIBER-EU étant un cadre de tests répandu dans l'Union européenne cela facilite les tests d'entités transfrontières et la reconnaissance mutuelle entre juridictions.

Un test TIBER-FR est une tentative contrôlée de compromission de la sécurité du système d'information d'une entité financière (de ses fonctions critiques en production) en simulant les tactiques, techniques et procédures (TTPs) d'acteurs malveillants réels perçus comme représentant une menace pour l'entité testée. En adoptant le comportement d'attaquants réels de bout en bout de la *cyber kill chain* via du renseignement sur la menace, les tests TIBER sont vecteurs de plans de remédiation plus complets. Ce type de test est qualifié de TLPT (*Threat Led Penetration Testing* ou test d'intrusion fondé sur la menace) dans le règlement européen DORA (*Digital Operational Resilience Act*), dans lequel ils sont rendus obligatoires pour les institutions financières les plus critiques.

La cyber-résilience du secteur financier européen étant une priorité majeure, le législateur européen a édicté le règlement DORA définissant les obligations liées à la gestion des risques et à la sécurité informatique. Ce dernier définit, entre autres, un cadre de test TLPT, compatible avec TIBER-EU. Le cadre TIBER-EU, et par conséquent sa transposition nationale TIBER-FR, doivent donc être considérés comme apportant des compléments contextuels au règlement DORA et à ses standards techniques sur les TLPT.

Pour de plus amples informations sur TIBER-FR, nous contacter : TIBER-FR@banque-france.fr

Consulter le guide TIBER-FR

[TIBER-FR national implementation guide \(PDF - 417 Ko\)](#)

Pour aller plus loin

- [Conduite des activités de surveillance](#)
- [Composition du collège EMIR de LCH SA](#)
- [Suivi des évolutions des infrastructures de marché](#)