Le Règlement DORA: nouvelle étape de renforcement de la résilience opérationnelle informatique des acteurs financiers

- Matthieu Duponchel, Mazars

Le règlement européen sur la résilience opérationnelle numérique du secteur financier (Digital Operationnal Resilience Act ou Dora) s'inscrit dans un contexte d'accélération de la numérisation et de généralisation de l'interconnexion (recours à des sous-traitants). Dans les dernières années, des accidents visibles ou invisibles ont mis à jour des failles dans les dispositifs numériques. On avait jusqu'ici un patchwork de règles dans l'Union européenne: ce règlement n'en constitue pas une couche supplémentaire, mais au contraire un levier de simplification.

Le règlement a été adopté en novembre 2022, il est entrée en vigueur en janvier 2023 et entrera en application en janvier 2025. La publication des normes techniques réglementaires s'étalera jusqu'à la mi-2024.

L'ensemble du secteur financier – banques, gestionnaires d'actifs, observateurs (agences de notation, auditeurs…), prestataires - est concerné.

Cinq piliers

Le règlement repose sur cinq piliers.

Il établit un cadre de gestion des risques informatiques, qui vise une implication du top management, la mise en œuvre d'un cadre formel de gouvernance (politique de continuité des activités, plan de reprise d'activité…) et de gestion, la résilience du dispositif et non la seule maîtrise du risque opérationnel.

Le texte traite de la gestion des incidents en plusieurs étapes: identification, qualification et analyse d'impact, communication, notification aux autorités.

Le règlement se préoccupe du partage d'informations entre acteurs financiers. Ces échanges existent, mais ils n'étaient jusqu'ici pas formalisés.

Dora formalise le recours à des tests de résilience informatique qui, jusqu'ici, ressortaient de textes disparates. On dispose désormais d'un texte ombrelle, qui procède d'une vision holistique du risque numérique. Les acteurs financiers devront définir et décrire leur politique en matière de tests.

Dans son dernier pilier, celui de la gestion des risques de tiers prestataires, le règlement conforte les lignes directrices en la matière de l'Autorité bancaire européenne, par exemple le principe de proportionnalité dans la

gestion de ces risques.

Les facteurs clés

Pour relever les défis de Dora, les entreprises du secteur financier devraient adopter un mode projet (démarrer tôt, embarquer les bons acteurs…), disposer d'une stratégie globale, qui nécessite notamment que se répande une véritable culture du risque, porter attention à la gestion des tiers, consolider (ou abandonner) les dispositifs existants, effectuer une veille réglementaire de façon à disposer d'une vision d'ensemble des textes relatifs à la sûreté du numérique, et sensibiliser la direction générale. Il s'agit, en synthèse, de passer de la gestion du risque à la résilience opérationnelle.

- ## Aziza Halilem, Yann Marin, ACPR

Des cyberattaques de masse ont amené à considérer que le risque « cyber » n'était pas un risque opérationnel comme les autres. Il s'agit d'un risque à fort probabilité aux impacts très lourds. Grâce notamment aux travaux du Conseil de stabilité financière, les autorités de contrôle nationales disposent désormais d'un langage commun en la matière.

Dora renforce le versant numérique de la résilience opérationnelle par des meures sur la sécurité des réseaux et des systèmes d'information.

Le texte vise à ce que les préoccupations en matière de résilience numérique soient remontées au plus haut niveau de l'organigramme, une montée en charge des compétences en la matière, une systématisation du signalement des incidents afin de créer une base de données qui renforcera la compréhension des phénomènes, le recours à des tests plus harmonisés, et met en place un cadre de surveillance des tiers, avec l'objectif d'instaurer un plus haut niveau de confiance entre les acteurs.

La gestion des risques informatiques fait l'objet des articles 5 à 16, qui recouvrent les notions de bonne gouvernance et de cadre de gestion adapté et déclinent les mesures techniques harmonisées. La gestion des incidents est traitée par les articles 17 à 23, tandis que les tests de résilience, domaine dans lequel les exigences sont lourdes, font l'objet des articles 24 à 27.

La gestion des risques de tiers (gestion des risques, volet contractuel, surveillance des prestataires informatiques critiques par les autorités européennes de surveillance) est abordée aux articles 28 à 44. Des travaux sont en cours concernant la création d'un registre des prestataires et une définition de ce qu'est un prestataire critique. A noter : il n'y aura pas de règles spécifiques s'appliquant aux prestataires critiques, mais Dora ouvre la possibilité de les contrôler.

En matière de gestion des risques de tiers, Dora n'introduit aucun principe inédit. Comme sous l'ancien régime juridique, l'entité financière demeure responsable du risque - qui doit être géré de manière proportionnelle -, elle établit une stratégie spécifique en la matière ou encore signale aux autorités de contrôle les contrats portant

sur des fonctions critiques ou importantes. Par ailleurs, Dora réaffirme les bonnes pratiques contractuelles.
En synthèse, on a affaire à une harmonisation des termes (risque de tiers en lieu et place d'externalisation…), mais pas à une révolution des pratiques, et à un texte qui promeut une relation de confiance avec les autorités (notification volontaire des menaces, encouragement à utiliser des clauses types…).

Pour sa part, l'Autorité de contrôle prudentiel et de résolution (ACPR) participera aux travaux de niveau 2 jusqu'en 2024 (elle souhaite promouvoir l'efficacité et la qualité de la gouvernance et éviter le formalisme) et, d'ici à 2025, à la mise en œuvre de Dora avec les autorités européennes de surveillance et avec le mécanisme de surveillance unique.

En attendant, ses actions de supervision se poursuivent, avec, parmi ses priorités en matière de contrôle, le risque cyber. Pour connaître les attentes de l'ACPR en matière de bonnes pratiques, on se reportera à ses notices.

L'ACPR, par ailleurs, procèdent à des enquêtes régulières auprès des acteurs (qui s'autoévaluent) et en restituent les résultats auprès d'eux, mais aussi à des contrôles sur place, dont les résultats sont eux aussi restitués aux intéressés.

- ## Juliette Le Drogou, Charles Moussy, AMF

Les remontées d'expériences permettent de mettre en évidence plusieurs catégories de schémas d'attaque : détournement d'identifiant, usurpation d'identité, accès à des données professionnelles ou personnelles éventuellement divulguées, intrusion dans le système en vue, notamment, d'exiger une rançon.

L'équipe spécialisée de l'Autorité des marchés financiers (AMF) a déjà procédé à deux vagues de contrôle sur place. En 2019, étaient notamment examinés l'organisation du dispositif cyber, le contrôle interne, et en 2020, vague durant laquelle des tests techniques ont été effectués, la gestion des incidents ou encore le pilotage des fournisseurs critiques.

Les contrôles ont permis de mettre en évidence des points positifs comme l'introduction progressive de la cybersécurité dans les cartographies des risques, le fait que le pilotage cyber soit une fonction indépendante, ou encore la sensibilisation régulière de l'ensemble du personnel.

En revanche, les actifs critiques ne sont pas suffisamment identifiés, le pilotage et le contrôle des fournisseurs critiques sont nettement insuffisants et il n'y a pas d'analyse des attaques selon leur origine.

Impact sur les activité de supervision

Le règlement européen comporte cinq piliers: risques liés aux technologies de l'information et de la communication, déclaration des incidents, test de résilience opérationnelle, la grande nouveauté qu'est la gestion des risques liés aux prestataires, et le partage des informations sur une base volontaire qui permettra d'enrichir la connaissance des autorités de contrôle. Ces cinq piliers s'appliquent à presque tous les acteurs financiers, dont

de nouveaux comme les prestataires de services de financement participatif, et bientôt aux prestataires de services en cryptoactifs.

Pour l'AMF, l'application de Dora se manifestera par la vérification de sa bonne application et éventuellement par le prononcé de sanctions, la participation à la supervision des prestataires tiers critiques, en cours d'identification, et enfin par la réception et l'analyse des notifications d'incidents et des rapports d'entités ayant réalisé des tests d'intrusion.

Textes de niveaux 2 et 3 à venir

Certains de ces textes seront publiés avant l'entrée en application du règlement en janvier 2025. Le corpus sera rédigé par les trois autorités européennes de supervision réunies en un sous-comité ad hoc.

Seront publiées huit normes techniques de réglementation, juridiquement contraignantes et directement applicables, comme le seront les deux normes techniques d'application (sur les modèles de déclaration des incidents notamment).

S'y ajouteront deux orientations, non contraignantes mais dont les entités assujetties seraient bien avisées de s'inspirer, ainsi que deux actes délégués publiés par la Commission européenne.

Les acteurs seront consultés à propos de ces textes.

• Christophe Leblanc, responsable de la mission « Résilience opérationnelle », Société Générale

Le dossier de la résilience opérationnelle est en haut de la pile pour de bonnes raisons. La menace devient de plus en plus importante, avec des attaques invalidantes pour des établissements financiers ou leurs prestataires.

Selon le responsable des activités de marché de la Société générale, le risque principal n'a pas trait au crédit par exemple, mais aux attaques informatiques. Le risque cyber, par ailleurs, parce qu'il est potentiellement létal, est d'ordre systémique. Enfin, les services bancaires sont beaucoup plus numérisés et les clients de plus en plus exigeants quant à la continuité des opérations.

Au Royaume-Uni, le superviseur s'était déjà penché sur le risque cyber, demandant notamment aux établissements d'identifier leurs fonctions essentielles et de tester des scénarios extrêmes.

La résilience opérationnelle à la Société Générale

En matière de résilience opérationnelle, même si la prise de conscience et les dispositifs sont anciens, on assiste à une mue importante, en particulier en raison des enjeux qui se sont manifestés à l'occasion de la pandémie et des confinements.

Le programme de la banque consiste notamment à se doter d'outils de gestion des crises, à se donner les moyens de « survivre » durant la phase critique de l'immédiat après-attaque, ou encore à s'assurer qu'existe un capacité à reconstruire les systèmes (notamment dans les domaines complexes que sont les chaînes de paiement ou de traitement des titres financiers).

Le projet Dora

Sponsorisé au plus haut niveau, il implique les fonctions transversales (risques, sécurité informatique, juridique…), mais aussi les métiers, particulièrement quand des fonctions essentielles sont en jeu.

Le projet se décompose en quatre chapitres. Celui des déclarations, outre le fait qu'il existe déjà des processus dans la banque, ne semble pas le plus compliqué à mettre en œuvre. Les trois autres, plus délicats, ont trait au corpus de règles régissant la gestion des risques informatiques, les tests, et les prestataires (on assistera sans doute à un phénomène d'éviction de certains d'entre eux et/ou de certaines tâches, mais on ne peut se passer de certains prestataires, d'où la nécessité d'une exigence renforcée et de l'élaboration d'une stratégie).

Deux grandes étapes (en attendant la publication des textes de niveau 2) : diagnostic et établissement d'une feuille de route précise.

Parmi les tâches auxquelles la banque s'est attelée : formalisation des politiques de back-up ; revue des contrats avec les prestataires ; cartographie des systèmes (dont certains sont hérités d'acquisitions) ; tests, avec notamment la nouveauté qui consiste à systématiser les tests d'intrusion effectués par des tiers (est-ce vraiment plus efficace que ceux que réalisés avec les équipes de la banque ? ce n'est pas certain) et les tests liés à la reconstruction des systèmes, phase qui mobilise beaucoup de ressources ; détermination du périmètre pertinent.

• Laurent Briziou, CEO Exaegis

Fondée il y a douze ans, Exaegis s'est d'abord spécialisé dans la garantie de la disparition d'un prestataire de services informatiques (garantir le paiement du locataire). L'entreprise travaille avec des filiales de financement informatique de grands groupes bancaires.

Ce modèle d'affaires initial a ensuite été appliqué, il y a six ans, à la pérennité des contrats de location de logiciels (software as a service), dans le cas où le prestataire informatique réalise un chiffre d'affaires n'excédant pas 15 million d'euros.

L'entreprise compte actuellement 350 prestataires sous garantie. Depuis le démarrage de cette activité, il y a six ans, trente prestataires défaillants ont été « migrés ».

Il s'agit, en définitive, d'assurer la continuité du service, en garantissant les données, les sources ou encore les droits d'exploitation, mais aussi, par exemple, en lien avec le tribunal de commerce, en réglant les sous-traitants (notamment dans le domaine du cloud), et, par ailleurs, en identifiant des prestataires de secours.

Un audit de trois jours, qui permet de qualifier le risque opérationnel, mais aussi le risque financier, est réalisé en amont de la garantie.