PAR NICOLAS VETRIAK, PRÉSIDENT FONDATEUR ET GEORGES CHAPPOTTEAU, DIRECTEUR DE LA DIVISION RISQUE ET CONTRÔLE. **NOVAMINDS**

DÉCIDEURS MAGAZINE

DORA ou la nécessité d'une gouvernance encore plus efficace pour la résilience opérationnelle

Le projet de règlement DORA[1] vise à établir un cadre juridique pour renforcer la résilience opérationnelle numérique du secteur financier à l'échelle européenne. Prévu pour fin 2022, ce texte a vocation à développer la finance numérique pour une meilleure compétitivité et innovation européenne, tout en renforçant la nécessité d'adresser les risques issus de la dépendance aux TIC[2]. Dans ce cadre, un des enjeux majeurs est la gouvernance et l'identification des acteurs responsables tant au niveau européen qu'au niveau même des établissements.

Nicolas Vetriak
Président Fondateur

Georges Chappotteau
Directeur de la division Risque et Contrôle

SUR LES AUTEURS

Nicolas Vetriak, Président Fondateur de Novaminds, est ingénieur et titulaire d'un MBA en Finance Internationale, diplômé de l'ENPC. Il dispose d'une longue expérience, d'abord dans des fonctions à responsabilités opérationnelles en Risk Management puis dans le conseil en Stratégie et Organisation, avec la donnée au cœur de ses interventions.

Georges Chappotteau, Directeur de la division Risque et Contrôle chez Novaminds et Maître de Conférences associé à l'IAE de Paris. Il exerce depuis de longues années des fonctions de conseil et de formation en Contrôle Interne et en gestion des Risques Opérationnels, et développe sa recherche autour de la prise de décision de la Gouvernance des organisations, en matière de risque.

LES POINTS CLÉS

- DORA[1] constitue une avancée majeure pour la résilience opérationnelle au travers de ses principes directeurs ;
- DORA se présente comme une opportunité pour la compétitivité, les coûts, la résilience ou encore le capital humain des établissements ;
- DORA s'appuie sur des dispositifs afférents à d'autres publications telles que les lignes directrices de l'ABE[5] ou encore les principes pour la résilience opérationnelle du BCBS[6] ;
- Un facteur clé réside dans la convergence, l'articulation et la coordination des dispositifs existants et non comme la création ex nihilo d'un dispositif supplémentaire.

En proposant des grands axes d'actions et de réflexions, le projet de règlement DORA s'inscrit dans la continuité des préoccupations européennes autour de la résilience opérationnelle. Plus précisément, DORA entend répondre à la problématique de la résilience opérationnelle numérique, c'est-à-dire la capacité pour les établissements financiers à renforcer et restaurer leur intégrité opérationnelle sur le plan technologique. Pour cela, à travers ses principes directeurs, ce projet de règlement vise à garantir, directement ou indirectement, au travers des fournisseurs liés aux TIC, la sécurité du réseau et des systèmes d'information utilisés par les établissements pour délivrer leurs services au niveau de qualité requis et ce, dans le cadre d'une gouvernance renforcée.

Pour assurer la résilience opérationnelle des institutions, DORA s'appuie sur différents principes. Le projet de règlement entend ainsi encadrer la gestion des risques et des incidents liés aux TIC, les tests de résilience opérationnelle numérique, la gestion des risques liés aux fournisseurs de services TIC et enfin le partage d'informations concernant les cybermenaces.

Cette gestion spécifique des risques informatiques liés aux TIC comprend notamment une identification et une classification de ces risques, des politiques de sauvegardes et des méthodes de restauration ainsi qu'une harmonisation des politiques.

> « À travers DORA, les établissements devront faire converger leurs dispositifs et leur gouvernance quels que soient les métiers et fonctions »

Le deuxième pilier de DORA se base sur la définition d'une stratégie et d'un cadre de gestion des risques des fournisseurs de services TIC. Cela entraîne la formalisation d'un processus de gestion des incidents, leur classification ainsi qu'une présentation de rapports anonymisés par les AES[3]. Un programme de tests doit être défini et réalisé de manière indépendante sur les applications et systèmes critiques au moins une fois par an. Ce dispositif de gestion des risques se décline ensuite à travers une politique et une supervision des prestataires critiques au niveau de l'Union européenne par les AES. Enfin, le partage d'informations liées aux cybermenaces doit être encadré par la notification des accords d'échanges aux autorités.

Quelles opportunités pour les établissements financiers ?

En plus d'être un élément de réponse à la problématique de la résilience opérationnelle, DORA représente aussi de nombreuses opportunités pour les établissements financiers.

Ce projet de règlement s'inscrit d'abord directement dans l'intérêt des établissements assujettis puisqu'il veille à garantir une meilleure compétitivité et innovation de ces derniers à l'échelle européenne. Son objectif est aussi de tirer profit de l'éventail d'opportunités offert par les nouvelles technologies.

Par ailleurs, DORA représente une opportunité économique pour les établissements puisqu'il permettra, à travers une approche uniformisée des tests de résilience opérationnelle numérique à l'échelle européenne et une rationalisation des coûts. De même, DORA en renforçant le cadre réglementaire de la gestion du risque opérationnel, vise la réduction des risques et des vulnérabilités des établissements dans leurs relations vis-à-vis des fournisseurs liés aux TIC. Ces éléments restent cependant une des difficultés majeures rencontrées par les établissements tant dans l'harmonisation de leurs référentiels que dans la consolidation des reportings. *In fine*, DORA peut contribuer à faire progresser les établissements sur ces sujets.

Enfin, DORA propose également une occasion d'améliorer le capital humain des établissements concernés. Il entend améliorer la formation du personnel sur la résilience opérationnelle numérique à travers des formations spécifiques des membres du Management. L'objectif est de maintenir à jour leurs compétences afin de mieux appréhender les risques informatiques et les impacts métiers associés.

Autant d'opportunités qui mettent en évidence la nécessité de mettre en place une gouvernance adaptée à ces nouveaux enjeux. De fait, à travers DORA, les établissements devront faire converger leurs dispositifs et leur gouvernance quels que soient les métiers, fonctions et zones géographiques.

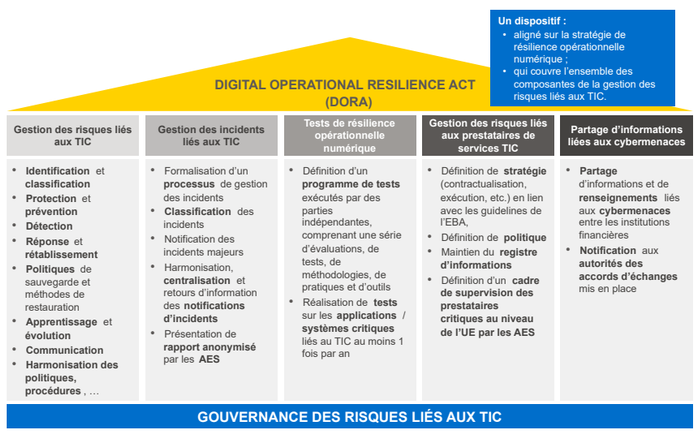
La mise en œuvre de DORA peut-elle capitaliser sur les dispositifs en place ?

DORA s'appuie sur de nombreuses consultations ou des principes qui traitent de la résilience dans le secteur financier, publiés par des instances telles que la BRI[4], l'ABE[5], ou encore la FED. En effet, bien que DORA aille plus loin, ce projet de règlement s'inscrit dans la continuité des orientations de l'ABE de 2019 sur la gestion des risques liés aux TIC et à la sécurité des établissements financiers, reprises par l'arrêté du 25 février 2021. Si cette gestion spécifique comprenant l'identification et la classification des risques ou encore une harmonisation des politiques et des procédures, elle est également une des recommandations de l'ABE à travers la maîtrise des risques ou encore l'établissement et la mise à jour d'une cartographie des fonctions et métiers.

Par ailleurs, ces thématiques adressées par DORA sont également reprises dans les principes pour une résilience opérationnelle publiés en mars 2021 par le BCBS[6]. En effet, DORA s'appuie sur des principes déjà existants, à l'image de l'accroissement du rôle et des responsabilités des instances de gouvernance, du renforcement de l'obligation de sensibilisation, notamment pour le top management, auquel s'ajoute la réalisation régulière de tests et des retours d'expérience, et enfin le renforcement de la gouvernance des tiers.

L'enjeu est double : (i) Au niveau européen savoir à qui reviendra le rôle d'encadrement et de supervision, et (ii) au niveau des organisations, la mise en place d'une gouvernance adaptée et transversale pour renforcer la mise en œuvre d'un dispositif avec de véritables convergences, voire des effets de mutualisation.

Au-delà de cette capitalisation, il reste que pour être efficient, les établissements se doivent de définir ces responsabilités. Ces nouveaux projets réglementaires constituent également une opportunité d'appréhender de manière transversale et coordonnée les enjeux afférents, par opposition aux approches traditionnelles en silo au sein d'une même organisation. ◆



[1] *DORA : Digital Operational Resilience Act*
[2] *TIC : Technologies de l'Information et de la Communication*
[3] *AES : Autorités Européennes de Surveillance*
[4] *BRI : Banque des Règlements Internationaux*
[5] *ABE : Autorité Bancaire Européenne*
[6] *BCBS : Basel Committee on Banking Supervision*