Nicolas Vetriak, Jean-Denis Pesty (Novaminds) : "Quelle responsabilité de l'organe de direction à l'aune du règlement européen DORA ?"

PAROLES D'EXPERTS . 16 SEPTEMBRE 2024

La mise en application du règlement européen DORA met en exergue de nombreux enjeux et défis à relever par les établissements financiers, avec les travaux de mise en conformité. Les organes de direction sont au cœur du dispositif de résilience opérationnelle numérique organisé par le législateur européen et une attention particulière doit être accordée à leur sensibilisation, information et formation en matière de risque lié aux TIC (Technologies de l'Information et de la Communication).

À l'instar des règlements européens récents, la responsabilité ultime du respect des exigences formulées échoit aux organes de direction (le conseil d'administration ou le conseil de surveillance, le directoire comme la direction générale).

Concernant la définition des organes de direction, la lecture des directives mentionnées par le règlement DORA (2014/65/UE, 2013/36/UE, 2009/65/CE, etc.) permet de poser les contours d'une définition concrète. Est un organe de direction – au sens du règlement DORA – l'organe ou les organes d'un établissement qui sont désignés conformément au droit national, qui sont compétents pour définir la stratégie, les objectifs et la direction globale de l'établissement et qui assurent la supervision et le suivi des décisions prises en matière de gestion et, en ce compris, les personnes qui dirigent effectivement les activités de l'établissement.

> *"Pour relever le défi d'une gouvernance TIC renforcée, les administrateurs disposent de plusieurs leviers."*

Pour assurer la concordance et la cohérence globale entre les stratégies des établissements et la mise en œuvre de la gestion du risque lié aux TIC, l'approche adoptée par les organes de direction doit être axée sur les moyens de garantir la résilience des systèmes de TIC. Le capital humain et l'ensemble des processus sont couverts au travers d'un corpus de politiques et de procédures.

Les établissements mobilisent ainsi des moyens financiers liés aux TIC avec un budget global adapté pour atteindre un niveau élevé de résilience opérationnelle numérique. Cette implication va de pair avec la définition d'une approche stratégique du risque lié aux prestataires tiers de services TIC et d'une analyse continue de toutes les relations de dépendance à l'égard de ces prestataires, incluant l'examen des modalités d'utilisation des services TIC fournis pas des prestataires tiers à l'établissement.

Renforcement de l'organe de direction à l'aune de DORA

Pour relever le défi d'une gouvernance TIC renforcée, les administrateurs disposent de plusieurs leviers. En ce sens, les administrateurs ne sont pas des spécialistes des risques liés aux TIC mais ils disposent du recul conjugué à une vision globale avec les compétences en matière de gouvernance, de délégations de pouvoir et, de fait, en gestion. Les administrateurs bénéficient d'expériences diverses, exécutives ou d'autres mandats d'administrateurs, dans des secteurs d'activités similaires ou différents.

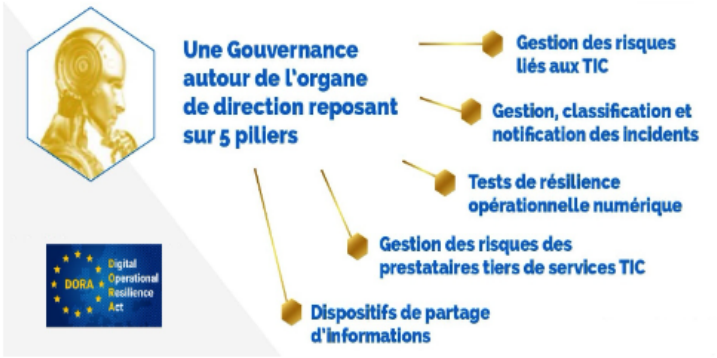
La mise en conformité s'accompagne d'une réflexion sur la structuration et les compétences au sein du conseil et des comités spécialisés. D'une part, il convient de se questionner sur la structuration du Conseil à l'aune de DORA ; Quels rôles ? Quelle gouvernance ? Un administrateur référent sur le sujet des risques liés aux TIC doit-il être nommé ? Quid de l'intégration d'un nouvel administrateur spécialisé ? Un comité existant peut-il être renforcé ou étendu pour satisfaire aux nouvelles obligations de DORA ou alors peut-on envisager la création d'un comité *ad hoc* couvrant les thématiques de la résilience opérationnelle numérique, du digital, l'IA…?

La mise en conformité avec les exigences de DORA implique aussi un renforcement de la formation des administrateurs. Cette réflexion peut amener une évolution du règlement intérieur du conseil (composition des comités, portée des missions du Conseil et des Comités spécialisés, fonctionnement de la gouvernance…).

Nous le constatons au regard des éléments susmentionnés, il convient de veiller à la bonne intégration de la gestion des risques liés aux TIC dans la gouvernance d'entreprise, en premier lieu au sein du conseil et des comités spécialisés. Cela suppose de placer le sujet à l'ordre du jour des séances de travail et de s'assurer que l'exécutif collabore efficacement tout en challengeant les différentes parties prenantes. Cela suppose également d'alimenter la direction avec les informations remontées par chaque acteur de la gouvernance d'entreprise ; l'enjeu étant d'éclairer, de co-piloter et d'orienter la direction pour toute prise de décision.

L'organe de direction est donc décisif dans le cadre de la gestion des risques TIC. Le point essentiel est la responsabilité ultime lui incombant et la définition claire des rôles et responsabilités de toutes les fonctions liées aux TIC. À l'instar de la gestion des risques existante au sein des entités financières, il convient de définir des stratégies adaptées et de déterminer un niveau approprié de tolérance aux risques liés aux TIC. La politique de continuité des activités de TIC, ainsi que les plans de réponse et de rétablissement des TIC doivent être approuvés, supervisés et examinés régulièrement. Enfin, des canaux de notification doivent être établis de manière à informer régulièrement l'organe de direction des accords conclus avec les prestataires tiers de services TIC, des changements significatifs et des incidences potentielles de ces changements sur les fonctions critiques ou importantes.

Eu égard à la responsabilité des membres du conseil d'administration dans les dispositifs de contrôle interne des entités, le règlement DORA emporte un rôle renforcé des instances de gouvernance dans la définition et le suivi de leur politique globale de maîtrise des risques.



La responsabilité ultime (et protéiforme) des organes de direction

La responsabilité des administrateurs pour faute de gestion pourra être invoquée en raison de la méconnaissance de cette nouvelle réglementation. Les administrateurs et dirigeants n'ont pas le choix et doivent inclure ce nouveau rôle dans leur champ de responsabilité et de compétence. En effet, concernant les sanctions, l'article 50 mentionne en son 5e paragraphe : *« Les États membres confèrent aux autorités compétentes le pouvoir d'appliquer les sanctions administratives et les mesures correctives prévues [...] aux membres de l'organe de direction, ainsi qu'aux autres personnes responsables de la violation au sens du droit national. »*

De quoi parlons-nous en matière de sanctions ?

- **Amendes administratives** : les entités financières peuvent se voir infliger une amende chiffrée en millions d'euros ou un pourcentage de leur chiffre d'affaires annuel total, le montant le plus élevé étant retenu, en cas d'infraction grave au règlement.
- **Mesures correctives** : les autorités de surveillance peuvent exiger des entités financières qu'elles prennent des mesures correctives pour remédier aux faiblesses ou aux défaillances de leur résilience numérique opérationnelle.
- **Réprimandes publiques** : les autorités de surveillance peuvent adresser un blâme public aux entités financières qui ne se conforment pas aux exigences du règlement.
- **Retrait de l'agrément** : les autorités de surveillance peuvent retirer l'agrément aux entités financières qui, de manière répétée, ne se conforment pas aux exigences du règlement.
- **Indemnisation des dommages** : les entités financières peuvent être tenues d'indemniser les clients ou les tiers pour tout dommage résultant d'un manquement aux exigences du règlement.
- **Sanctions pénales :** l'article 52 du règlement DORA institue cette possibilité pour les violations audit règlement.

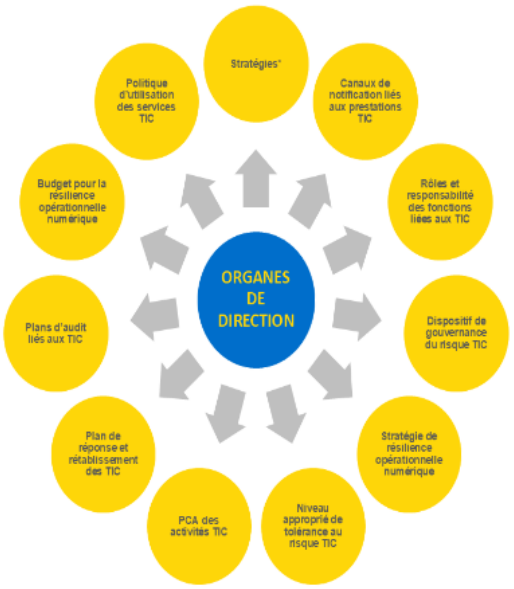
Outre ces sanctions, l'Autorité peut requérir une exigence additionnelle de fonds propres pour couvrir les risques liés aux TIC.

En conclusion, le règlement DORA place les organes de direction au premier plan de son dispositif de résilience opérationnelle numérique. Leur rôle va bien au-delà de la simple supervision, avec la définition stratégique et la mise en œuvre effective des politiques de résilience numérique. Les sanctions prévues en cas de non-conformité, qu'elles soient financières ou disciplinaires, soulignent l'importance de cette responsabilité. Les administrateurs doivent donc pleinement intégrer ces nouvelles obligations dans leur champ de compétences pour garantir la continuité d'exploitation et la sécurité des opérations des entités, et au-delà, la stabilité financière et l'intégrité du marché à l'ère numérique. Enfin, il convient de ne pas sous-estimer l'impact réputationnel qui découlerait d'un désengagement des organes de direction concernant les risques inhérents aux TIC. En effet, en cas d'incident grave, c'est la viabilité du marché unique européen qui peut être affectée et la confiance des clients rompue.

LES POINTS CLÉS :

Les organes de direction doivent s'impliquer dans la gestion des risques TIC au travers d'une revue de leur pilotage stratégique. Les enjeux directs sont notamment :

- comprendre et appréhender les défis et conséquences de cette nouvelle réglementation ;
- piloter la mise en conformité de leurs entités ;
- s'assurer que les dispositifs opérationnels de résilience numérique sont en place et en mesure de répondre à des menaces et vulnérabilités évolutives ;
- prendre des décisions d'investissements pour renforcer la résilience de leur entreprise sur le long terme ;
- approuver la stratégie de résilience numérique de l'entreprise.



Les 11 chantiers prioritaires des organes de direction à l'aune du règlement DORA

* Stratégies en matière de disponibilité, authenticité, intégrité et confidentialité des données.

Nicolas Vetriak et Jean-Denis Pesty

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 cybersécurité et résilience puis dans le conseil en stratégie et organisation, avec la donnée et l'IA au cœur de ses interventions.

Jean-Denis Pesty, manager, est titulaire du certificat d'aptitude à la profession d'Avocat et diplômé en droit des affaires de l'université de Paris Nanterre et de l'ESSEC Business School. Il est le référent DORA et IA Act au sein du cabinet.