AVIS D'EXPERT

REGLEMENT DORA, UNE OPPORTUNITE DANS UN CONTEXTE DE MENACES GRANDISSANTES

Le règlement européen DORA *(Digital Operational Resilience Act) sur la résilience opérationnelle numérique marque une étape importante dans la stratégie que la Commission Européenne déploie en matière de finance numérique. DORA vise en effet à établir un cadre harmonisant la réglementation existante et de renforcer la résilience opérationnelle des entités du secteur financier face à la recrudescence des risques auxquels elles sont confrontées, en particulier les risques cybernétiques.*

Si DORA ne modifie pas l'esprit des réglementations existantes (NIS2, Guidelines de l'EBA sur l'outsourcing), elle introduit cependant un certain nombre d'exigences plus précises ou approfondies. Les équipes spécialisées de Talan Consulting vous propose un décryptage de DORA à travers ses principaux enjeux et impacts opérationnels pour les acteurs du secteur financier.

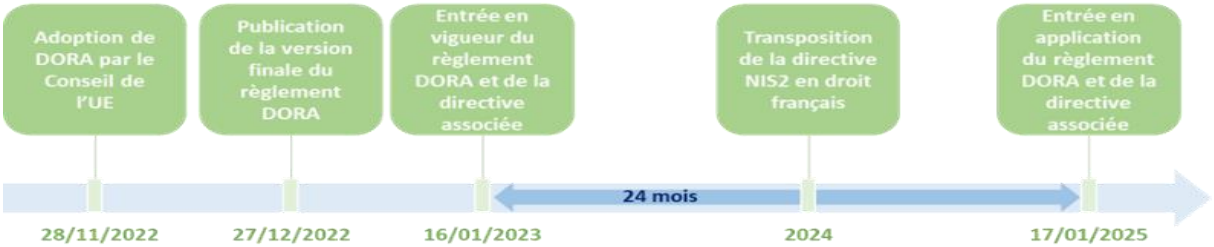
Contexte et calendrier

La cybercriminalité représente aujourd'hui une préoccupation grandissante pour les organismes financiers à travers le monde. Les avancées technologiques et l'interconnexion croissante ont ouvert de nouvelles possibilités aux cybercriminels susceptibles de mettre en péril non seulement la confidentialité des données sensibles, mais également la stabilité des organisations qu'ils attaquent. Depuis la crise sanitaire du COVID, l'avènement du télétravail et l'accélération de la digitalisation fragilisent davantage les organisations, notamment avec l'utilisation d'appareils personnels non sécurisés, ou encore l'accès à des réseaux Wi-Fi publics. Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la menace cybercriminelle, après une accalmie passagère au premier semestre 2022, a connu un regain d'activités fin 2022 avec la multiplication des attaques par rançongiciels.

Au-delà de l'uniformisation de la réglementation européenne, DORA a pour objectif d'instaurer sur le plan opérationnel une résilience nouvelle en imposant aux institutions financières et à leurs fournisseurs systémiques d'avoir la capacité de faire face à des crises majeures portant sur des activités critiques, en particulier celles impactant leurs clients.

Environ 20 000 organismes financiers en Europe sont concernés. Il s'agit notamment des établissements de crédit et de paiement ; des prestataires de services de cryptoactifs ; des sociétés de gestion ; des assureurs et réassureurs ; des organismes de retraite professionnelle mais également des prestataires de service de ces entités financières (art. 2 du Règlement). Tous doivent se préparer à adapter leurs opérations et leurs pratiques de gestion des risques afin de se conformer aux exigences de DORA et ainsi assurer la stabilité et la sécurité continues du secteur financier.

L'entrée en vigueur de DORA étant prévue le 17 janvier 2025, les acteurs du secteur financiers ont désormais moins de 8 mois pour mettre en application la règlementation et le faire dans la durée. En effet, les acteurs ont l'obligation de maintenir une gestion de la résilience en continue après la date butoir de transposition. Dans ce cadre, il convient de préciser que des normes techniques de réglementation et d'exécution, Regulatory Technical Standard (RTS) et Implementing Technical Standards (ITS) dites de niveau 2 seront publiées dans le courant de cette année afin de préciser certaines obligations issues du règlement DORA de niveau 1.



Les 4 thèmes couverts par le règlement DORA

Le règlement DORA s'articule autour de 4 grands thèmes que sont la gestion des risques entendue largement, la gestion et la communication des incidents, les tests de résilience et la gestion des tiers prestataires de services liés aux technologies de l'information et de la communication (TIC).

La gestion des risques liés aux TIC (articles 5 à 16). Cette gestion consiste en la mise en place d'une gouvernance à travers notamment un RACI dédié, des politiques, des procédures, des contrôles et une analyse des risques sur l'ensemble des systèmes et processus TIC pertinents. Une attention particulière est portée à l'implication des dirigeants dans ces activités ainsi qu'aux examens et mises à jour régulières de ce cadre de gestion.

La gestion et la notification des incidents liés aux TIC (articles 19 à 21). Le règlement DORA simplifie les exigences de reporting des incidents liés aux TIC dans une logique de partage efficace des informations entre les entités financières et les autorités compétentes. La règlementation doit permettre de mieux comprendre les menaces et de réagir à leurs évolutions en favorisant la collaboration entre les participants au marché. A ce titre, les acteurs financiers doivent signaler les incidents importants liés aux TIC à leurs autorités compétentes selon des délais impartis et un modèle unique que les autorités européennes de surveillance doivent préciser. Les acteurs doivent donc définir et mettre en œuvre un processus spécifique de gestion des incidents liés aux TIC allant de leur détection jusqu'à leur notification en passant par leur traitement à chaud.

Les tests de résilience opérationnelle numérique (articles 24 à 27). Le règlement prévoit que « les capacités et les fonctions intégrées dans le cadre de gestion des risques informatiques doivent être testées à intervalles réguliers afin de vérifier l'état de préparation aux risques et d'identifier les éventuelles faiblesses, défaillances ou lacunes, ainsi que de prendre rapidement des mesures correctives ». L'introduction de la notion de conduite de tests de résilience opérationnelle encourage ainsi les entités financières à continuellement évaluer et améliorer leur résilience opérationnelle numérique. Les tests réguliers de résilience opérationnelle numérique deviennent obligatoires tout comme les évaluations des vulnérabilités et des risques liés aux TIC et les tests de pénétration. Pour cela, DORA détaille une approche de mise à l'essai axée sur les risques, les systèmes, les processus et les données critiques. La règlementation recommande également un calendrier de tests réguliers avec la détermination d'un profil de risques de l'entité pour y indexer une fréquence et une intensité de test. Enfin, il convient de souligner que la participation d'experts externes indépendants et qualifiés est comprise dans le cadre de cette nouvelle exigence sans pour autant qu'elle soit obligatoire.

La gestion du risque lié aux prestataires tiers de services TIC (articles 28 à 39). Reconnaissant les risques associés à l'externalisation des fonctions essentielles à des tiers fournisseurs de services TIC, DORA met en œuvre un régime de surveillance les concernant. Celui-ci vient compléter les directives de l'Autorité Bancaire Européenne (EBA) sur l'Outsourcing, en vigueur depuis février 2019, en étendant le cadre de surveillance aux prestataires de service dit systémiques qui seront soumis à la supervision du régulateur local (ACPR pour la France) au même titre que les institutions financières.

Ainsi, la règlementation introduit un cadre solide de gestion des risques associés à l'externalisation vers des fournisseurs de services tiers. Ce cadre comprend à la fois un suivi accru de la performance et du profil de risques des prestataires, mais aussi une évaluation de leur résilience opérationnelle et leur capacité à respecter les obligations contractuelles.

Le cadre prévoit aussi la nécessité de s'assurer que des plans d'urgence sont en place pour maintenir la continuité opérationnelle en cas de perturbation des accords.

De manière plus spécifique, les banques qui se sont conformées aux directives de l'EBA de 2019 concernant l'externalisation, sont déjà dotées d'un cadre similaire en matière de gestion des risques liés aux tiers et devront ajuster leur dispositif à la marge. Ce qui n'est pas le cas pour les autres organismes financiers (Gestionnaires d'actifs, assureurs et réassureurs, etc.) qui doivent donc revoir leur dispositif de gestion et de suivi des prestations TIC externalisées sur les volets qualification, sélection, contractualisation, pilotage et contrôle avec leurs fournisseurs de services TIC.

L'évaluation précontractuelle des fournisseurs prévue par DORA pourrait s'avérer délicate. C'est notamment le cas des grandes institutions financières qui peineront à effectuer une évaluation approfondie pour tous leurs fournisseurs de services TIC compte tenu de leur nombre élevé et du temps imparti pour le faire. Par conséquent, il sera crucial d'établir une matrice de priorisation pour sélectionner les fournisseurs en fonction de critères préétablis. S'agissant des petites structures, elles sont susceptibles d'être confrontées à des fournisseurs informatiques de grande envergure et qui verront leur pouvoir de négociation réduit.

Quelles difficultés pour les acteurs financiers ?

Selon son degré de maturité, une organisation sera confrontée à plus ou moins de difficultés. Les plus matures pourront ainsi capitaliser sur des démarches déjà engagées alors que les moins avancées devront produire un effort substantiel nécessitant la mise en place d'un véritable programme. Cependant, au-delà de l'effort à produire, la mise en œuvre de DORA impliquera la nécessité de coordonner une multitude d'acteurs et de faire évoluer son approche de la gestion des risques opérationnels.

S'agissant des acteurs à mobiliser au sein des entreprises, il convient de souligner que DORA exige une forte implication des instances dirigeantes qui devront s'assurer que les dispositifs de résilience opérationnelle sont en place et en mesure de répondre à des menaces et des vulnérabilités évolutives.

L'un des premiers défis consistera donc à embarquer le top management dans l'initiative. Le pilotage de cette gestion des risques informatiques incombera à l'organe de direction qui sera responsable du suivi, de l'approbation, de la révision et de fixer le cap en termes de résilience opérationnelle (art. 5). L'implication des dirigeants est donc essentielle à la réussite d'un éventuel programme. Une acculturation et des formations « spécifiques proportionnées au risque lié aux TIC géré » du top management à ces sujets (cyber, risques IT, pilotage et suivi des tiers) seront nécessaires pour leur permettre de prendre les décisions éclairées en toute situation.

Au-delà de la Direction Générale, la mise en œuvre de la règlementation représente un véritable projet d'entreprise nécessitant la coordination de nombreux acteurs au titre desquels il convient de citer la Direction/Filière Résilience opérationnelle, sous réserve qu'elle existe, les directions spécialisées comme la DSI, la SSI, les directions supports mais également les directions métiers.

Au titre des fonctions supports/transverses, la Direction de la Conformité/Compliance sera nécessairement mobilisée tout comme la direction des Risques Opérationnels ou encore la Direction de l'Audit Interne. Plus spécifiquement, la direction des Achats devra contribuer aux travaux notamment dans les phases d'analyse des risques, de sélection et de contractualisation avec les tiers. La direction de la communication et la DRH devront aussi être associés aux travaux dans le cadre des actions de sensibilisation et de formation.

Enfin et s'agit là d'un point essentiel à souligner, si la survenance d'un risque informatique impacte nécessairement les équipes IT, leurs conséquences opérationnelles sont subies par les métiers. Il est donc indispensable d'associer étroitement les directions métiers aux travaux afin d'identifier avec elles les processus critiques pour l'entreprise et surtout les solutions devant être apportées pour assurer la résilience des activités correspondantes.

Quels sont les leviers à actionner ?

En fonction de la maturité de l'entreprise, l'organisation de cette mise en conformité peut se faire en mode programme ou en continuité des travaux de résilience opérationnelle déjà engagés. Le premier levier à actionner est de capitaliser au maximum sur les projets de conformité antérieurs (notamment par rapport aux réglementations NIS2, Guideline de l'EBA sur l'outsourcing, Solvency II, etc.).

En amont du lancement des travaux de mise en conformité, il est nécessaire que l'entreprise s'aligne sur des pratiques communes. En effet, elle doit, sur la base de tous les concepts clefs introduits par DORA, choisir les méthodes de travail adéquates afin d'identifier les fonctions critiques ou importantes ainsi que les risques auxquels elles sont exposées et de cadrer les travaux à mener sur les prestataires tiers de services TIC.

L'identification des fonctions critiques ou importantes et des risques est une phase à fort enjeu car elle va conditionner l'efficacité de la suite des travaux. En fonction de la nature et des niveaux de seuils retenus, une liste des fonctions critiques ou importantes sera à valider avec une gouvernance de gestion de la résilience qui lui sera associée. Une fois identifiés, les risques doivent être priorisés selon des critères à définir au préalable et les procédures en cas de survenance doivent être écrites et partagées.

Dora, plus qu'une contrainte, une réelle opportunité

Face à l'imprécision et à la diversité des règles de contrôle des risques sur le numérique, mais aussi en raison de la montée de la cybercriminalité, une règlementation européenne unifiée s'imposait.

Au-delà de ce constat général, force est de constater que la règlementation DORA répond à un besoin effectif. Face aux menaces grandissantes auxquelles ils sont exposés, les acteurs vont devoir s'appuyer sur ce nouveau socle règlementaire pour repenser leur stratégie de défense et non pas uniquement combler des écarts à la réglementation dans une logique de pure conformité ; le fond primant la forme.

Quel que soit votre secteur d'activité, bancaire ou assurantiel, les équipes Talan Consulting spécialisées en matière de conformité réglementaire vous accompagnent dans vos projets de mise en conformité de votre dispositif et d'élaboration d'une stratégie réglementaire à travers notamment l'analyse d'écart à la réglementation ; l'étude d'impacts et de risques ou encore le pilotage de programme portant sur la mise en œuvre du règlement DORA.

CONTACTS

José Dorrego,
jose.dorrego@talan.com
Partner

Taoufik Megzari,
taoufik.megzari@talan.com
Directeur

Frédéric Nguyen Kim,
frederic.nguyen-kim@talan.com
Senior Advisor