DORA

Les 10 enjeux clés pour une mise en conformité réussie

De la gestion du risque informatique et cyber à la résilience opérationnelle numérique

Février 2023

pwc

Let’s Change the Way We See Risk

Remerciements

Les messages mentionnés dans ce document sont issus de la conférence « Règlement DORA : Décryptage, enjeux et partage d'expériences » organisée le 24 novembre 2022 par PwC France et Maghreb.

Nous tenons particulièrement à remercier les deux intervenantes à la table ronde :

Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management, AXA
Caroline Cerval, Chief Operating Officer, Head of Operations and Technology, LCH SA

Ce document a été rédigé grâce à la contribution des experts PwC sur le sujet :

Romain Camus, Associé gestion des risques technologiques, secteur Banque, PwC France et Maghreb
Karine Pariente, Associée gestion des risques technologiques, secteur Assurance, PwC France et Maghreb
Jamal Basrire, Associé en charge des activités cyber Intelligence, PwC France et Maghreb

Nous tenons également à remercier les membres du centre d'excellence réglementaire de PwC France et Maghreb pour leur apport d'expertise :

Monique Tavares, Directrice Banque
Olfa Ehrhard, Senior Manager Assurance

Sommaire

Qu'est-ce que DORA ?

Le « *Digital Operational Resilience Act* », communément appelé « DORA », est un règlement européen[1] qui a pour objectif de renforcer la résilience opérationnelle numérique du secteur financier dans un contexte de profonde transformation numérique des activités et de montée des risques cyber et informatiques. Entré en vigueur le 16 janvier 2023, il sera applicable à partir du 17 janvier 2025 par tous les États membres de l'UE.

L'enjeu de la résilience est absolument crucial pour les institutions financières, mais le sujet est aussi potentiellement systémique, compte tenu de l'augmentation du nombre de cyberattaques et de l'interdépendance croissante des réseaux et des infrastructures. « *Les banques et les compagnies d'assurance ont besoin d'accéder à un nombre croissant de données internes et externes. Elles sont aussi de plus en plus dépendantes des tiers informatiques. Les normalisateurs européens souhaitent donc s'assurer que le risque généré par ces évolutions est maîtrisé* », explique Karine Pariente, Associée PwC. L'augmentation de la consommation des technologies s'associe ainsi à l'augmentation de l'exposition au risque cyber et constitue donc autant de sources potentielles d'instabilité du secteur financier dans son ensemble, précise Jamal Basrire, Associé PwC.

Cela a amené les autorités de réglementation et de supervision, après avoir œuvré au renforcement de la résilience financière des institutions, à se focaliser sur leur résilience opérationnelle. Le règlement DORA crée un cadre réglementaire sur la résilience opérationnelle numérique en vertu duquel toutes les entités financières devront s'assurer qu'elles peuvent résister, répondre et se rétablir face à tous types de perturbations et de menaces liées aux technologies de l'information et de la communication (TIC).

Le concept de résilience opérationnelle met ainsi l'accent sur la nécessité de faire évoluer l'approche de gestion des risques opérationnels, d'une approche centrée sur la prévention des risques et la limitation des pertes vers une approche plus large et proactive, qui part du principe que les

incidents vont se produire et qu'il faut être prêt à les traiter et à assurer la continuité des activités et services critiques ou importants.

Ainsi, le règlement DORA identifie et propose des exigences relatives à 5 piliers essentiels que les institutions financières doivent mettre en œuvre, en particulier :

- la gestion des risques liés aux TIC,
- la gestion des incidents, avec notamment un reporting harmonisé et centralisé à destination des autorités compétentes,
- la conduite de tests réguliers de la résilience,
- la gestion du risque tiers avec la mise en place d'un mécanisme de surveillance direct des prestataires de services TIC critiques au niveau de l'UE,
- et le partage d'informations sur les cybermenaces.

1 Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier

Le règlement DORA va apporter, dans un seul acte législatif et pour la première fois au niveau de l'UE, un cadre détaillé et complet sur la résilience opérationnelle numérique pour les institutions financières.

Les 5 piliers à appréhender pour encadrer la résilience opérationnelle numérique

1. Le dispositif de gestion des risques liés aux TIC
2. La gestion, la classification et la notification des incidents TIC et des cybermenaces
3. La conduite des tests de la résilience opérationnelle numérique
4. La gestion des risques liés aux prestataires de services TIC
5. Le partage d'informations en matière de cybersécurité

Qu'est-ce que la résilience opérationnelle numérique ? Selon DORA :

« La capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant, directement ou indirectement, par le recours aux services fournis par des prestataires de services TIC, l'intégralité des capacités en matière de TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue des services financiers et leur qualité, y compris en cas de perturbations. »

Quel est le périmètre d'application de DORA ?

Le règlement DORA s'applique à un très large éventail d'entités financières du secteur financier ainsi qu'aux prestataires de services TIC qui opèrent au sein de l'Union européenne dans les services financiers.

Entités financières

- Établissements de crédit
- Établissements de paiement
- Établissements de monnaie électronique
- Entreprises d'investissement
- Sociétés de gestion et gestionnaires de FIA
- Prestataires de Services d'Information sur les comptes ou « agrégateur de comptes bancaires »
- Prestataires de services sur cryptoactifs agréés conformément à MiCA, émetteurs de jetons

- Entreprises d'assurance et de réassurance
- Intermédiaires de (ré)assurance, intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle

Nota : sous réserve des exclusions prévues en fonction de critères de taille

- Contreparties centrales
- Référentiels centraux
- Plates-formes de négociation
- Prestataires de service de communication de données
- Agences de notation de crédit, administrateurs d'indices de référence critiques
- Prestataires de services de crowdfunding

Prestataires de services TIC

Les entreprises qui fournissent de manière permanente des services numériques et de données par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes dont le matériel en tant que service et les services matériels qui englobent la fourniture d'assistance technique au moyen de mises à jour de logiciels ou de micrologiciels réalisées par le fournisseur de matériel, à l'exclusion des services de téléphonie analogique traditionnels.

Cadre de gestion des risques liés aux prestataires de services TIC

Sont considérés comme des tiers prestataires de services liés aux TIC :

- **Les prestataires de services TIC intra-groupe** qui fournissent des services de TIC principalement à leur entreprise mère, ou à des filiales ou des succursales de leur entreprise mère
- **Les entités financières qui fournissent des services de TIC à d'autres entités financières**
- **Les participants à l'écosystème des services de paiement**

Cadre de supervision UE

Prestataires de services TIC désignés comme « critiques » à l'exception des :

- **Entités financières qui fournissent des services de TIC à d'autres entités financières**
- **Prestataires de services TIC intra-groupe**
- **Prestataires de services TIC soumis** à des cadres de supervision établis en vue de soutenir les missions du système européen de banques centrales

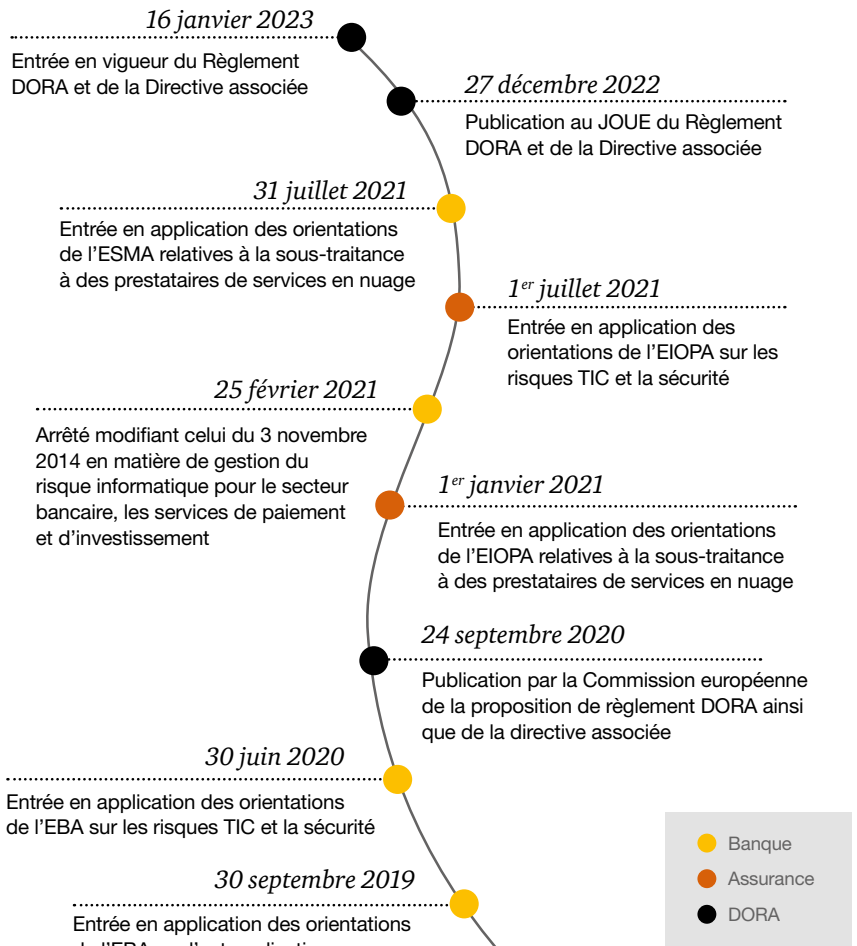
Enjeu 1 Comprendre l'approche retenue par le Régulateur

Si DORA s'inscrit dans la continuité de nombreux textes antérieurs, la nouvelle réglementation change la donne. Les attentes ont évolué et il faut bien les intégrer avant d'entrer dans le détail des changements nécessaires.

Dans le cadre existant, on peut citer concernant le secteur bancaire, les orientations de l'EBA sur l'externalisation et celles sur la gestion des risques liés aux TIC et à la sécurité ou encore, les orientations de l'ESMA sur la sous-traitance à des prestataires de services « Cloud ». Concernant les compagnies d'assurance, plusieurs textes en miroir de ceux qui affectent les banques, avec par exemple les orientations de l'EIOPA sur la sous-traitance ou encore celles sur la gestion des risques liés aux TIC et à la sécurité.

Autant de sujets liés aux risques et à la résilience opérationnelle numérique qui seront dorénavant sous une seule ombrelle : celle de DORA. « *Jusqu'à présent, le cadre réglementaire en vigueur était fragmenté et hétérogène. Il existait de nombreuses réglementations sectorielles, mais elles étaient de niveaux différents, et plus ou moins contraignantes. Cela crée aujourd'hui des chevauchements, des interprétations différentes selon les pays européens et, finalement, des coûts de conformité très importants. Les règles en matière de cybersécurité n'étaient pas harmonisées, et les obligations de reporting, de plus en plus importantes, ne permettaient pas d'assurer une surveillance adéquate au niveau européen. DORA va constituer un cadre unique, reprenant tout l'historique des orientations des autorités européennes de supervision, mais aussi les bonnes pratiques au niveau européen et international en matière de cyber-résilience et de gestion des risques liés aux TIC. Le nouveau texte va en quelque sorte mettre en cohérence tous les textes existants en matière de risque informatique, de cybersécurité, de gestion des tiers et de continuité d'activité* », explique Karine Pariente, Associée PwC.

Un renforcement et une harmonisation progressive des exigences sectorielles



A côté du règlement DORA, la directive associée[2] viendra également modifier les directives existantes afin de les mettre en cohérence avec les dispositions du règlement. Ainsi, par exemple, les établissements de crédit devront reporter au titre de DORA les incidents opérationnels ou liés à la sécurité des paiements - précédemment déclarés au titre de la directive DSP2. Entrée en vigueur le 16 janvier 2023, elle devra être transposée par les États membres d'ici le 17 janvier 2025.

La construction d'un cadre harmonisé en lien avec les autres réglementations

Au niveau du secteur financier de l'UE

1 Prise en compte des **orientations existantes des AES (EBA, EIOPA, ESMA) et des bonnes pratiques européennes et internationales** destinées à renforcer la cyber résilience et la résilience opérationnelle du secteur financier

2 Prise en compte des **exigences existantes relatives aux risques liés aux TIC réparties entre différentes directives** de manière implicite ou explicite

DORA

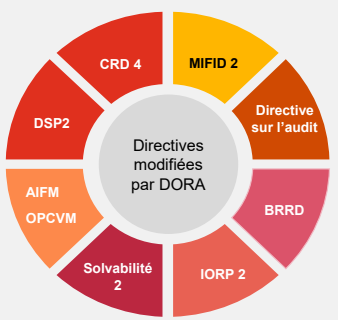
3 Mise en place d'un **cadre unique et commun en matière de résilience opérationnelle numérique** pour le secteur financier

4 **Mise en cohérence des directives existantes**

Règlement - DORA

- Règlement
- Actes délégués / RTS - ITS
- Orientations

Directive associée DORA



2 Directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022

Globalement, l'approche retenue par le Régulateur s'articule autour de trois grands principes :

1. La convergence

Pour la première fois en Europe, les régulateurs se mettent autour de la table pour traiter, de façon commune, des risques liés aux technologies de l'information et de la communication et poser des éléments permettant la maîtrise de ces enjeux opérationnels et informatiques.

« *Nous comptons sur DORA pour proposer un langage commun et un calendrier aligné, par opposition aux nombreuses exigences, divergentes, qui s'imposent aujourd'hui dans les pays où nous opérons* », explique Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA.

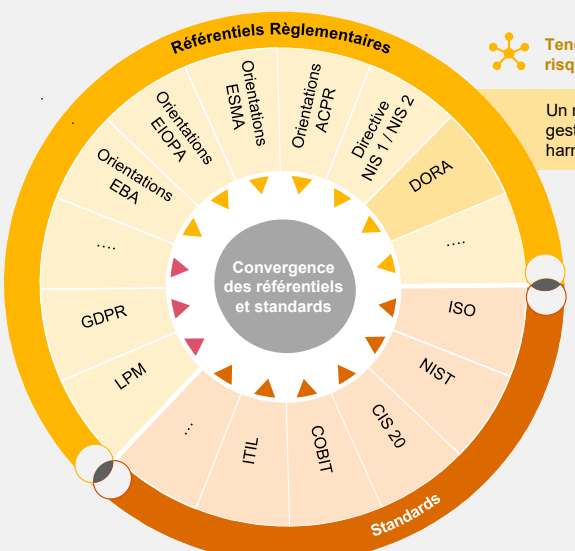
Mais encore faut-il que les institutions financières parviennent à s'appuyer sur l'ensemble des travaux déjà réalisés dans le cadre des différentes réglementations, que ce soit dans les domaines de la gestion des tiers, de la continuité d'activité, ou encore de la cybersécurité, et ne pas partir de la « feuille blanche »...

« *En matière de cybersécurité, par exemple, cela fait plusieurs années que notre stratégie est ambitieuse avec des vagues d'investissements importants et la mise en place de contrôles pour renforcer la sécurité de nos opérations. Encore récemment, nous avons mis à jour cette stratégie pour garantir une meilleure couverture de la surface d'attaque* », détaille Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA.

Cela passera également par une convergence de l'organisation et des approches de gestion des risques :

« *Convergence des textes, mais aussi des différentes approches de gestion des risques, qui sont souvent très fragmentées entre risques informatiques, cyber, continuité d'activité ou encore risques liés aux tiers* », explique Jamal Basrire, Associé PwC.

Capitaliser sur la convergence des textes et sur les efforts déjà entrepris



Tendances réglementaires: faire converger et harmoniser les référentiels règlementaires de gestion des risques liés aux TIC et à la sécurité.

Un nouveau référentiel réglementaire faisant converger les orientations de l'EBA, EIOPA et ESMA sur la gestion des risques liés aux TIC et à la sécurité, avec de nouvelles exigences visant à renforcer et harmoniser la gestion des risques liés aux TIC et à la sécurité pour l'ensemble du secteur financier.

Objectifs clés de la convergence

- **Simplifier la conformité** en consolidant dans un seul référentiel les exigences règlementaires applicables
- Construire un programme de transformation **solide, complet et conforme aux exigences** pour optimiser les efforts liés au processus de conformité
- **Faciliter le reporting** aux régulateurs et aux instances de direction
- Identifier les synergies avec les nouveaux cadres réglementaires et **anticiper la conformité** avec les nouvelles exigences supplémentaires

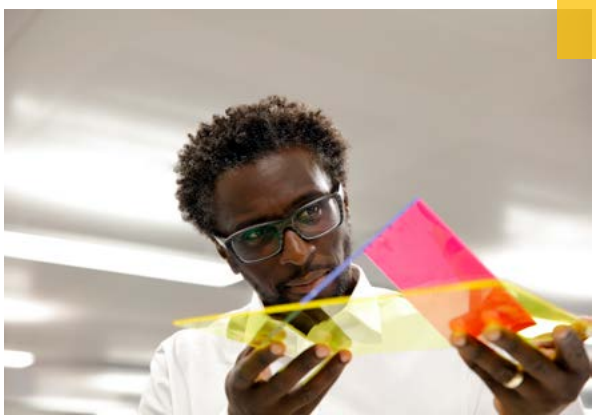
C'est en capitalisant sur leurs travaux passés que les institutions financières pourront parvenir à améliorer leur résilience sans compliquer leur organisation. « *On peut même espérer que, finalement, le texte simplifie la mise en conformité pour les institutions financières* », estime Romain Camus, Associé PwC.

2. La proportionnalité

Selon le principe de proportionnalité, les entités financières doivent mettre en œuvre les exigences en tenant compte de leur taille et de leur profil de risque global ainsi que de la nature, de l'ampleur et de la complexité de leurs services, activités et opérations. En effet : « *Compte tenu de la largeur du spectre de DORA, il est essentiel de calibrer ses efforts et le niveau de profondeur de ses actions au contexte de l'entreprise et aux risques auxquels elle est exposée* », explique Jamal Basrire, Associé PwC.

3. La promotion du principe général de « *security by design* »

Enfin, l'approche intègre le principe général de la « security by design », c'est-à-dire l'idée qu'il faut immédiatement penser sécurité, dès la conception des produits et services jusqu'à leur distribution aux clients et tout au long du cycle de vie, et en imposant cet enjeu au cœur de la gouvernance des institutions. Cela suppose aussi de développer une vision d'ensemble de la chaîne d'approvisionnement des TIC et d'évaluer sa résilience.



Enjeu 2 Démarrer au plus vite

Les entreprises ont deux ans pour se préparer à la nouvelle réglementation européenne. Un délai qui pourrait sembler suffisant... Mais, en réalité, les institutions financières qui ont déjà commencé à plancher sur le sujet se sont déjà rendues compte que cela nécessitera un travail non négligeable. « *Nous avons commencé à travailler sur DORA dès le début 2022. Il a d'abord fallu identifier et classifier les profils de risques des tiers avec lesquels nous travaillons. Puis travailler sur les interdépendances entre les systèmes d'information, les processus, les données, etc. La gestion des risques est au cœur de notre métier mais, dans le domaine cyber, cela nécessite une gestion du changement, et une appropriation des risques cyber par les métiers et par tous les niveaux managériaux.* », illustre ainsi Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA.

L'échéance du 17 janvier 2025 est d'autant plus proche qu'un certain nombre d'éléments, notamment sur les conditions de mise en place, doivent encore être précisés dans des textes à venir, dits « textes de niveau 2 ». Ils sont attendus au cours des 12 à 24 prochains mois.... « *Quand les textes détaillés seront publiés (RTS/ITS), il restera moins d'un an pour les mettre en œuvre : c'est vraiment très court en matière de risque technologique* », estime Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA, qui se dit prête à participer aux consultations de place, afin d'être le plus au fait possible de ce qui sera décidé.

Une entrée en application à partir du 17 janvier 2025

Les dates clés

Les AES devront soumettre à la Commission européenne des RTS/ITS dans les délais suivants et notamment sur les sujets cités ci-après :

- **Au plus tard le 17 janvier 2024** : Outils, méthodes, processus et politiques de gestion du risque lié aux TIC ; Cadre simplifié ; Classification des incidents et des cybermenaces ; Stratégie en matière de risques liés aux prestataires tiers de services TIC ; Modèles types aux fins du registre d'informations sur les prestataires TIC y compris les informations communes à tous les accords contractuels relatifs à l'utilisation de services TIC
- **Au plus tard le 17 juillet 2024** : Contenu et modèles des rapports de notification ; Tests avancés ; Sous-traitance de services TIC ; Supervision des prestataires de services TIC critiques

Reste que, même sans connaître le détail des textes de niveau 2, il faut avancer dans ses travaux... « *Cela peut être déstabilisant, mais beaucoup d'éléments des futurs textes sont connus et les règles actuelles peuvent déjà être source d'inspiration* », estime Karine Pariente, Associée PwC.

Les grandes étapes du plan de route sont déjà connues. « *Il est possible de travailler dès maintenant à l'analyse des écarts entre le dispositif mis en œuvre par l'entreprise et l'attendu décrit dans le règlement DORA.*

Il s'agit par ailleurs de définir son plan d'action au regard d'une analyse du contexte de l'entreprise (évolution du business model notamment dans le contexte de la digitalisation, présence géographique, interconnexions avec les tiers partenaires / fournisseurs / clients…) et de ses risques. Le principe de proportionnalité permet ensuite d'adapter le dispositif en place au regard du contexte de l'entreprise », explique Jamal Basrire, Associé PwC.

La mise en œuvre de ces travaux nécessite de s'assurer d'avoir mis en place une gouvernance forte.

Enjeu 3 Faire évoluer sa gouvernance et sensibiliser le Management

La gouvernance se pose en enjeu central de la nouvelle réglementation DORA : l'objectif est de développer une gouvernance globale des risques pour assurer la résilience opérationnelle numérique, nouveau paradigme amené par DORA. « *Il va falloir casser les silos entre gestion des risques informatiques, cyber, risques de tiers ou encore de continuité d'activité. Une révolution, ou presque, pour de nombreuses institutions financières : encore récemment, les « PCA » (plans de continuité d'activité) de nombreux établissements ne tenaient pas compte du risque cyber, alors même que les attaques par rançongiciel sont en 2022 l'une des menaces principales pouvant mettre à défaut la disponibilité des systèmes informatiques.* » explique Jamal Basrire, Associé PwC.

En pratique, les institutions financières doivent mettre en place ou poursuivre la mise en place de règles de gouvernance qui leur permettent de garantir une gestion efficace et prudente des risques liés aux TIC et d'atteindre un « niveau élevé » de résilience opérationnelle numérique.

Le Régulateur confie à l'organe de direction la responsabilité de la mise en œuvre du dispositif de gestion et de suivi des risques liés aux TIC. Il est chargé notamment de :

- la définition de la stratégie de résilience opérationnelle numérique, y compris la détermination du niveau de tolérance au risque lié aux TIC,
- l'approbation, la supervision et l'examen périodique de la politique de continuité des activités liées aux TIC et des plans de réponses et de rétablissements des TIC,
- l'approbation et l'examen des plans d'audits et des audits des TIC,
- la revue au moins des incidents majeurs liés aux TIC, de leur incidence et des mesures de réponse, de rétablissement et de remédiation mises en œuvre,
- l'approbation et la revue de la politique d'utilisation des services TIC fournis par des tiers et la revue des nouveaux contrats ou des modifications des contrats existants,
- et, bien sûr, l'allocation des ressources nécessaires.

En conséquence, il va falloir revoir la gouvernance de la gestion des risques pour intégrer le paradigme de la résilience opérationnelle numérique tout en préservant le modèle des trois lignes de défense, permettant notamment de challenger les dispositifs en place. En effet, les entités financières devront s'assurer d'une séparation adéquate des fonctions de gestion informatique, des fonctions de contrôle et des fonctions d'audit interne. Le dispositif de gestion des risques liés aux TIC devra être documenté et faire l'objet d'un réexamen, a minima une fois par an.

L'organe de direction doit disposer de compétences en cybersécurité

Pour cela, des efforts en matière de sensibilisation et de formation devront également être entrepris : « *La gouvernance des risques informatiques fait partie du mandat de nos Directeurs informatiques, et plus largement les sujets sur la connaissance du parc informatique ou la gestion de l'obsolescence sont abordés lors des Comités risques ou du Comité de Direction* », illustre Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. Il sera toutefois nécessaire en raison de l'évolution rapide des menaces de renforcer les compétences des membres de l'organe de direction pour accomplir leurs responsabilités : des compétences minimales et régulièrement actualisées en matière de risques cyber et informatique sont désormais attendues.

Enjeu 4 Identifier et impliquer les bons acteurs

Attention, DORA n'est pas qu'un sujet de cybersécurité ! Certes, le texte traite du risque cyber et de la sécurité des réseaux et des systèmes d'information, mais il relève de beaucoup d'autres domaines : risques de tiers, continuité d'activité, risques informatiques, etc. « *La résilience opérationnelle touche des sujets beaucoup plus larges que la seule sécurité informatique. En aucun cas, les projets de mise en conformité « DORA » ne peuvent être localisés uniquement au niveau de la Direction informatique* », estime Jamal Basrire, Associé PwC.

De fait, il s'agit d'un sujet stratégique, qui se doit d'être traité comme tel : à un niveau stratégique au niveau de l'organe de direction, avec le soutien du Management de l'entreprise. Au-delà des responsables IT et cyber, de nombreuses autres fonctions doivent être sensibilisées au sujet et impliquées dans le projet. Avec, en premier lieu, la Direction Générale. « *L'enjeu principal va être de coordonner les actions avec les principales parties prenantes concernées. Cela nécessite de renforcer la gouvernance et ne pourra se faire qu'en impliquant le top management* », souligne Karine Pariente, Associée PwC.

S'agissant d'un enjeu lié au risque opérationnel, la plupart des acteurs de la place ont généralement positionné le sujet au niveau de la Direction des Risques ou de la Conformité, avec des contributions fortes attendues de la Direction Informatique, des responsables Sécurité, des équipes de continuité d'activité, des directions des achats et du juridique (pour les contrats de service avec les tiers).

> La mise en conformité à DORA doit impliquer l'ensemble des acteurs de l'entreprise : métier, risque, opérations IT et cybersécurité

Enjeu 5 Faire le lien avec les évolutions réglementaires en cours ou à venir

Comme vu précédemment, les délais sont courts et il faut commencer dès maintenant à travailler à la mise en conformité au règlement et suivre les projets à venir de RTS/ITS. « *Il est aussi essentiel de considérer DORA dans l'écosystème réglementaire global avec notamment la nouvelle directive NIS 2*[3] *afin de prendre en compte l'ensemble des contraintes réglementaires avant de lancer une démarche de mise en conformité* », estime Jamal Basrire, Associé PwC.

En effet, le règlement DORA s'inscrit dans le cadre de la nouvelle directive NIS 2, entrée en vigueur le 16 janvier 2023, et qui définit le cadre horizontal des mesures minimales visant à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'UE. Le règlement DORA constitue la « lex specialis » pour le secteur financier en ce qui concernent notamment les mesures de gestion des risques de cybersécurité et les obligations de reporting des incidents liés aux TIC. Il sera d'autant plus nécessaire d'avoir une lecture d'ensemble des deux textes que le périmètre d'application de la directive NIS 2 est étendu à l'ensemble des entreprises de moyenne et de grande taille des secteurs d'activité couverts par la directive (« les entités essentielles et importantes »), et non plus aux seules entreprises désignées comme opérateurs de services essentiels (OSE). La directive NIS 2 devra être transposée par les États membres d'ici le 17 octobre 2024.

A côté de cette initiative, il sera également nécessaire de faire le lien avec d'autres initiatives législatives existantes ou en cours en matière de cybersécurité. Tout d'abord avec le règlement sur la cybersécurité en vigueur depuis 2019 : pour certaines catégories d'entités essentielles et importantes qui seront tenues, au titre de la directive NIS 2, de certifier certains produits, services ou processus TIC mis au point par les entités ou acquis auprès de tiers conformément à ce règlement. Il faudra également suivre la proposition de règlement « Cyber resilience act », publiée le 15 septembre 2022, et qui précisera les exigences en matière de cybersécurité applicables lors du développement ou de la mise sur le marché de produits et services comportant des éléments numériques.

L'ensemble de ces initiatives vise à renforcer la sécurité des actifs TIC mais aussi de l'ensemble de la chaîne d'approvisionnement des TIC.

3 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022

Enjeu 6 Capitaliser sur l'existant avec le prisme de la résilience

Pour les institutions financières les plus matures, qui ont déjà beaucoup travaillé sur les règles en vigueur actuellement autour de la gestion des risques informatiques, la cybersécurité ou la gestion des prestataires informatiques, il ne devrait y avoir que peu de changements dans la substance.

L'évolution portera sur le développement d'une vision holistique du sujet au travers notamment de la stratégie de résilience opérationnelle numérique et la prise en compte de la profondeur des exigences. L'évolution sera plus ou moins marquée suivant à quel point la gestion des risques est considérée avec le prisme de la résilience et la résilience intégrée dans les organes de gouvernance. « *Les approches de gestion des risques jusqu'ici fragmentées et silotées ont permis de monter en maturité sur ces différents sujets mais cela ne permet pas d'adresser aujourd'hui le nouveau paradigme qu'amène DORA* », souligne Jamal Basrire, Associé PwC.

Ainsi, si la convergence des textes permet de capitaliser sur les efforts déjà entrepris, « *il est nécessaire de rationaliser, homogénéiser et de transversaliser l'approche de résilience opérationnelle mise en œuvre* », estime Jamal Basrire, Associé PwC.

Pour les institutions financières moins matures, la nouvelle réglementation risque en revanche d'être un vrai défi. « *Le renforcement de la gestion de notre risque informatique va passer par une évolution de notre gouvernance et le renforcement de nos lignes de défense. Il va aussi nous falloir nous outiller pour suivre les risques de façon holistique, être en capacité de les monitorer et d'établir un reporting, tant stratégique que managérial* », explique ainsi Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA, qui se définit comme un acteur de « *taille mesurée* ».

> Il est nécessaire de transversaliser l'approche de résilience opérationnelle numérique au sein de l'organisation

Enjeu 7 Créer un cadre harmonisé et favorable aux partages d'information sur les incidents et les cybermenaces

Nous assistons aujourd'hui à un véritable « foisonnement de demandes de reporting d'incidents » indique Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. « *Si on veut vraiment réaliser les objectifs des reporting incidents, c'est-à-dire une réaction rapide si on est dans le cas d'un évènement systémique et ensuite une bonne compréhension a posteriori pour s'adapter aux menaces, il faut vraiment que le reporting soit harmonisé* » ajoute Céline Samain.

C'est un des objectifs du règlement DORA qui vise à harmoniser et à simplifier le processus de déclaration obligatoire des incidents majeurs liés aux TIC et à instaurer un signalement volontaire des cybermenaces importantes. Les textes de niveau 2 préciseront le seuil permettant de considérer un incident comme majeur ainsi que les délais de notification des incidents aux autorités compétentes.

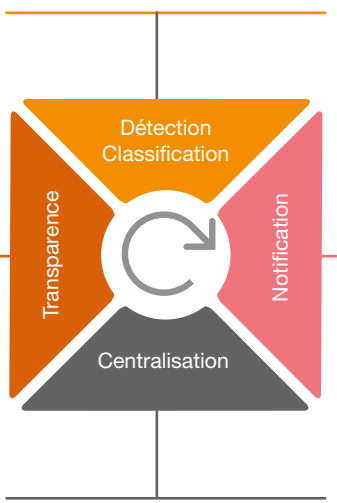
Le règlement DORA pose aussi un certain nombre de règles visant à favoriser le partage d'information entre les entités financières. « *Dans un objectif de place et afin d'améliorer la résilience de tous, il va falloir partager les menaces importantes*. » « *Bien sûr, il s'agit de données sensibles et il faudra créer pour ces échanges un cadre sécurisé, de confiance et informer les autorités des accords d'échanges d'informations conclus entre institutions financières, tiers, autorités, etc.*», ajoute Romain Camus.

Le règlement DORA encourage les entités financières à s'organiser mais aussi au niveau des autorités compétentes : le texte prévoit, à l'horizon de 2025, l'étude de la possibilité de centraliser les rapports sur les incidents liés aux TIC avec la mise en place d'une plateforme unique au niveau de l'UE.

La gestion, la classification et la notification des incidents

- Collecte de tous les incidents liés aux TIC et les cybermenaces significatives
- Classement des incidents TIC ainsi que des cybermenaces

- En cas de cybermenace significative, les entités financières informent, le cas échéant, leurs clients potentiellement affectés de toute mesure de protection appropriée que ces derniers peuvent envisager de prendre
- Publication chaque année par les AES d'un rapport anonymisé et agrégé sur les notifications des incidents majeurs liés aux TIC reçues des autorités compétentes



- Création d'un pôle européen en charge de la centralisation des notifications d'incidents majeurs TIC

- Notification au moins des incidents majeurs TIC aux membres de la direction concernée
- Communication à l'organe de direction des informations sur au moins les incidents majeurs TIC, expliquant leurs incidences, la réponse à leur apporter et les contrôles supplémentaires à mettre en place
- Notification à l'autorité compétente des incidents majeurs liés aux TIC dans des délais qui seront déterminés par les AES
- Notification, sur une base volontaire, des cybermenaces importantes à l'autorité compétente
- Les entités financières peuvent externaliser, conformément à la législation sectorielle nationale et européenne, les obligations de notification prévues auprès d'un prestataire de services tiers (dans la dernière version de la proposition DORA, plus d'obligation d'obtenir au préalable l'approbation de l'autorité compétente)

Enjeu 8 Saisir l'opportunité pour revoir ses relations avec les prestataires TIC

Force est de constater que, ces dernières années, les institutions financières ont fait de plus en plus appel à la sous-traitance informatique et massivement externalisé. Avec parfois un déséquilibre dans la relation contractuelle : les « petites banques » ou les institutions financières de taille modeste font face à des acteurs très importants, qui leur laissent peu de marges de négociation. Mais cela pourrait changer grâce à DORA. « *Le texte établit un cadre juridique de supervision des prestataires de services TIC critiques très clair et très sécurisant pour les institutions financières* », estime Romain Camus, Associé PwC.

La mise en place de clauses contractuelles types et notamment des clauses en matière de résiliation et de stratégies de sortie devrait permettre, à terme, une standardisation des contrats avec les prestataires de services TIC. « *DORA va nous aider à avoir un cadre homogène pour la gestion des tiers, dont nous sommes très dépendants* », explique ainsi Caroline Cerval, Chief Operating Officer, Head of Operations and Technology - LCH SA . « *DORA va donner une plus grande légitimité aux demandes que nous adressons à nos prestataires* », complète Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA .

En effet : « *pour que la résilience soit effective, il faut qu'elle se fasse des deux côtés de la relation et que l'intégralité de la chaîne de valeur se trouve renforcée* » ajoute Céline Samain

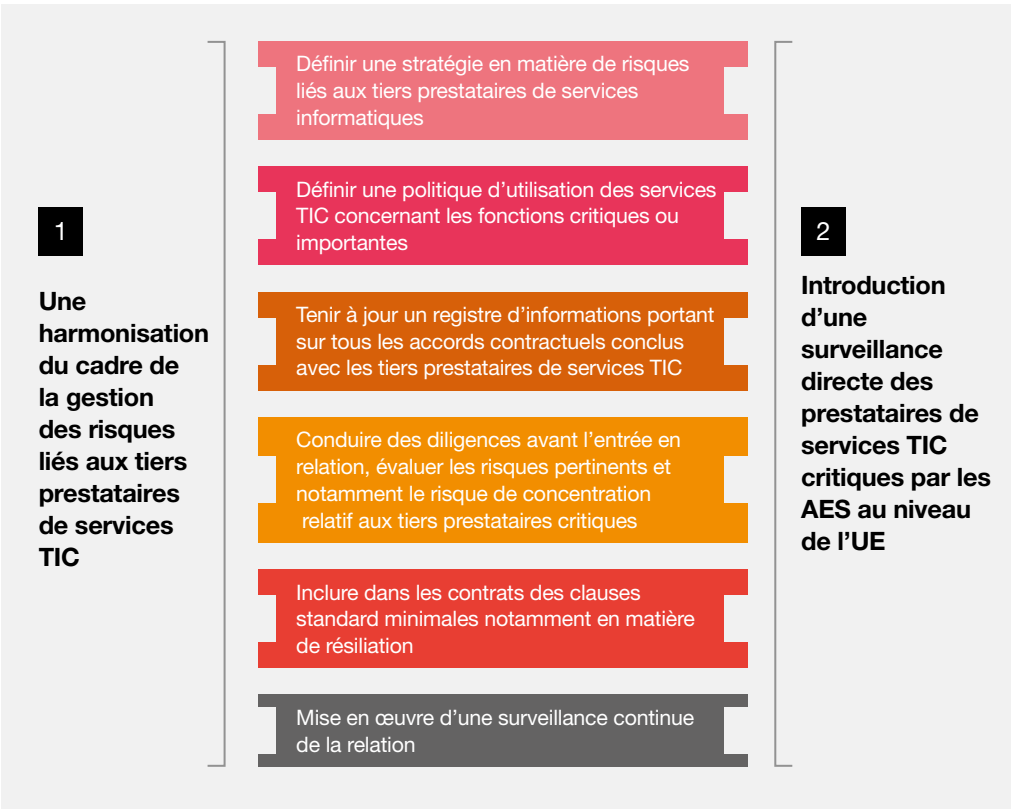
De quoi permettre un renforcement de toute la chaîne de valeur et donc une amélioration de la résilience globale du secteur financier. « *Les nouvelles exigences sur le risque lié aux tiers va contraindre les prestataires à fournir des informations à leurs clients. Avec également un droit de suite pour le superviseur : si les prestataires ne sont pas à la hauteur des attentes, les clients devront en changer. Il y aura donc un avantage concurrentiel à la conformité, ce qui devrait conduire à une amélioration globale des relations avec l'ensemble des acteurs de la place* », estime Romain Camus. Et, finalement, on peut espérer une

meilleure prise en compte des spécificités du secteur financier par les prestataires informatiques, des prestations plus adaptées et enfin davantage de réactivité.

Le principe de proportionnalité est également important dans la gestion du risque de tiers : « *Il va falloir déterminer les efforts à réaliser pour chaque prestataire de service, en fonction de critères variés. Ainsi, nous avons des cadres de contrôle de nos prestataires qui s'organisent autour d'un arbre de décision, qui en fonction des données, des connections, de la profondeur de la relation, etc. vont potentiellement évoluer, se renforcer ou voire s'alléger…* », explique Céline Samain.

Un mécanisme de supervision des prestataires TIC critiques plus sécurisant pour les institutions financières

La gestion des risques liés aux tiers prestataires de services TIC

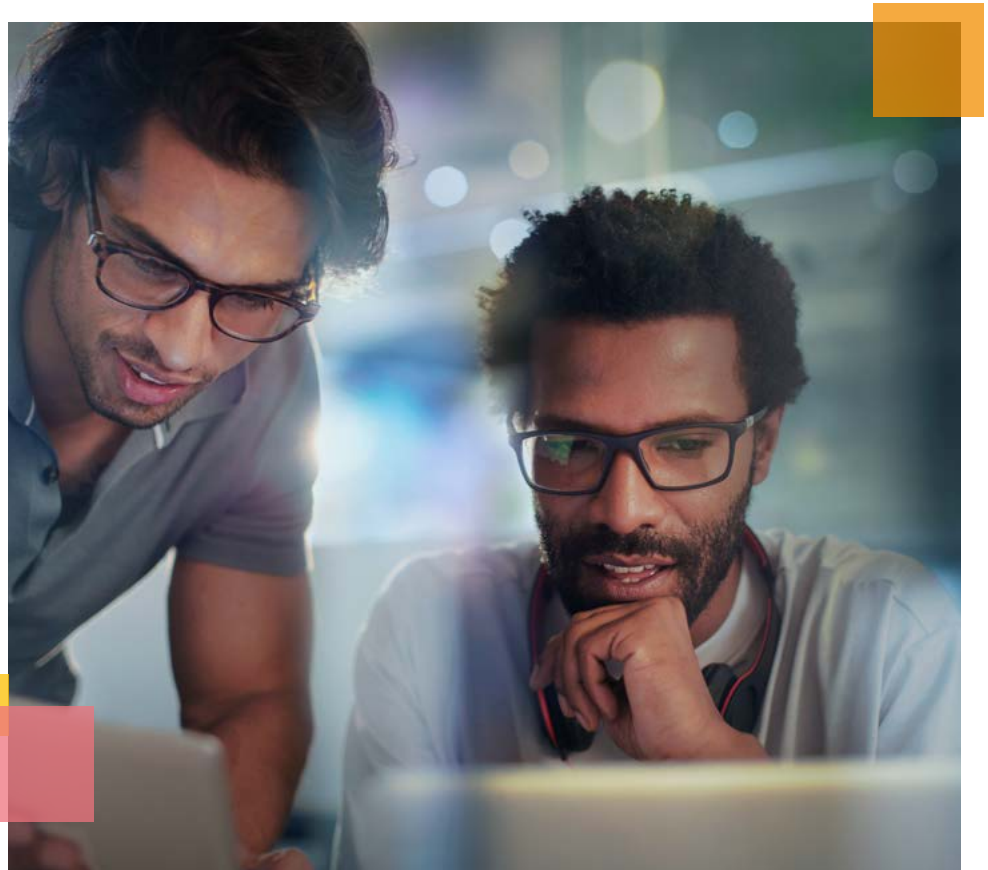


Enjeu 9 Mettre à l'épreuve régulièrement les capacités de résilience

Les capacités de résilience opérationnelle numérique doivent être confrontées à la réalité. Au moyen de tests réels destinés à les éprouver, à identifier les lacunes de réponse aux incidents et les défaillances éventuelles. « *DORA met un accent important sur les programmes de tests et sur la nécessité de se préparer opérationnellement, au-delà de ce qui est déjà fait aujourd'hui. Il va falloir mettre en place des exercices solides de simulation de crise* », détaille Karine Pariente, Associée PwC.

En effet, les entités financières autres que les microentreprises doivent élaborer, maintenir et réexaminer un programme solide et complet de tests de résilience opérationnelle numérique. Composante essentielle de la stratégie globale de résilience opérationnelle numérique et intégré au dispositif de gestion des risques liés aux TIC, il doit permettre d'évaluer régulièrement les capacités TIC et sécurité en cas de survenance d'incidents informatiques ou de cyberattaques.

Le règlement DORA prévoit une application proportionnée des exigences en matière de conduite de tests de résilience en fonction de la taille, de l'activité et du profil de risque des entités financières. Ainsi, si toutes les entités financières, y compris les microentreprises doivent tester leurs outils et systèmes de TIC, seules celles qui seront désignées par les autorités compétentes (sur la base des critères énoncés dans le règlement et précisés par les futurs textes de niveau 2) comme étant d'importance significative et cyber-matures seront tenues de procéder à des tests avancés (des tests de pénétration fondés sur la menace ou TLPT). « *Cela concerne les structures qui constituent un potentiel risque systémique au niveau de l'Union ou au niveau national. Elles devront tester tous les trois ans leurs fonctions critiques ou importantes, en s'appuyant sur des testeurs indépendants internes ou externes* », explique Jamal Basrire, Associé PwC. Le programme de tests doit être élaboré sur la base d'une approche fondée sur les risques.



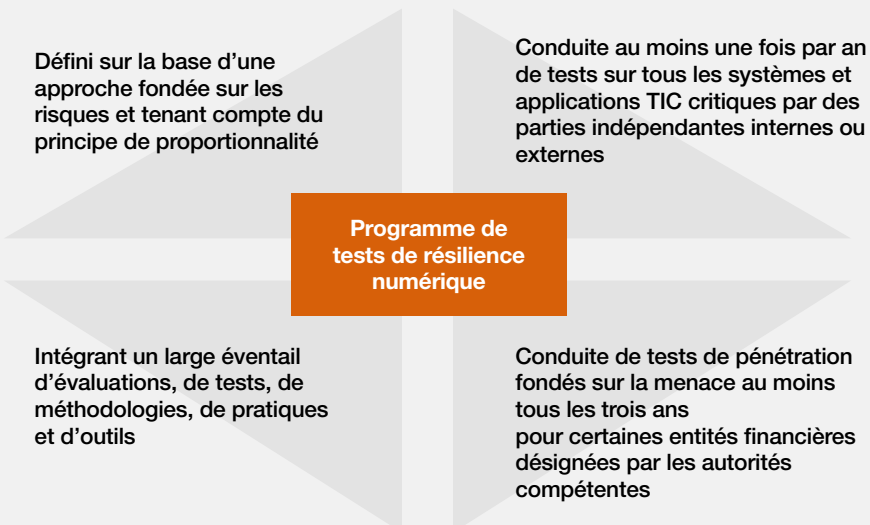
Le nouveau cadre de conduite des tests avancés apportera un avantage non négligeable : ces tests bénéficieront d'une reconnaissance mutuelle au niveau de l'UE. Toutefois, la conduite de ces derniers nécessitera des efforts plus importants en termes de préparation et de coordination.

A noter que les entités financières devront impliquer davantage les prestataires de services TIC intervenant au niveau des fonctions critiques ou importantes et inclure ces obligations de test renforcées dans leurs accords contractuels.

Enfin, via la conduite régulière de ces tests, c'est tout une dynamique qui doit se mettre en place et qui doit favoriser le développement d'une culture forte de la résilience opérationnelle numérique au sein de l'organisation.

Les tests de la résilience opérationnelle numérique

Établissement, maintien et réexamen d'un **programme de tests de résilience opérationnelle numérique** faisant partie intégrante du dispositif de gestion des risques liés aux TIC (pour les entités financières autres que les microentreprises)



Enjeu 10 Développer une véritable culture de la résilience opérationnelle numérique

Par-delà les détails, le principe de résilience opérationnelle numérique se pose véritablement en fil conducteur de DORA : pour garantir la solidité du système financier, il faut que les institutions soient capables de faire face à tous types d'incidents liés aux TIC. « *Beaucoup d'entreprises ont amélioré la gestion de leur risque cyber. C'est un point de départ très positif, mais cela ne suffit pas à adresser le nouveau paradigme de DORA : celui de la résilience opérationnelle numérique. Il faut aujourd'hui homogénéiser et travailler de façon transverse pour véritablement appréhender l'ensemble du sujet et développer une culture de la résilience opérationnelle* », insiste Jamal Basrire, Associé PwC.

Tout l'enjeu de la mise en place de DORA tient au basculement dans cette nouvelle culture de la résilience. Tirant les enseignements de leurs expériences récentes de gestion de crise lors de la pandémie de COVID-19 ou d'incidents cyber, certaines institutions financières ont fait évoluer leur culture en réponse aussi aux attentes de leurs clients.

« *La culture de la résilience opérationnelle est très importante pour nos clients. Nous nous sommes dotés d'une organisation spécifique pour la renforcer, à travers une analyse des ressources critiques, une gouvernance de crise et des plans de continuité d'activité régulièrement testés mais aussi éprouvés par de nombreux événements ces dernières années : mouvements sociaux, pandémie, ou guerre...* », illustre Céline Samain, Head of Operational & Information Risk, Internal Control and Standards Management - AXA. Pour d'autres institutions financières, le défi reste important.

Une culture de la résilience opérationnelle numérique doit être mise en place

Glossaire

EBA : The European Banking Authority ou Autorité bancaire européenne (ABE).

EIOPA : The European Insurance and Occupational Pensions Authority

AES : Autorités européennes de surveillance (ou European Supervisory Authorities)

ESMA : European Securities and Markets Authority

FIA : Fonds d'investissement alternatifs

MiCA : Proposition de règlement européen sur les crypto-actifs dit règlement « MiCA » (Markets in Crypto-Assets).

NIS : Directive dite « NIS » pour « Network and Information Security » relative à la sécurité des réseaux et des systèmes d'information

PCA : Plan de Continuité d'Activité

OSE : Opérateurs de services essentiels

TIC : Technologies de l'information et de la communication.

TLPT : Threat-Led Penetration Testing

Conclusion

Dans un contexte géopolitique incertain, de recrudescence des cyberattaques et d'enjeux forts de digitalisation du secteur financier, le règlement DORA établit un cadre unique et commun sur la résilience opérationnelle numérique pour les entités financières et les prestataires de services TIC qui opèrent au sein de l'Union européenne dans les services financiers.

Les enjeux à la fois stratégiques et opérationnels soulevés sont complexes et profonds et nécessitent l'implication de plusieurs fonctions en interne telles que la Direction des risques et de la Conformité, la Direction informatique, les responsables de la Sécurité, la Direction des achats, et plus particulièrement le sponsoring fort du Management dans l'établissement d'une gouvernance appropriée.

Les « dix enjeux clés » que nous avons recensés ici sont autant de pistes pour aider à la préparation de la mise en conformité, dans les meilleurs délais. Ils constituent des repères qu'il conviendra bien évidemment d'adapter à chaque environnement afin de faire de DORA non pas une contrainte règlementaire supplémentaire mais une opportunité pour les institutions financières de se différencier sur le marché en renforçant leur résilience opérationnelle sur les risques informatiques, de cybersécurité, de continuité d'activité et sur les risques liés aux tiers.

Contacts

Romain Camus
Associé
Gestion des risques technologiques,
secteur Banque
PwC France et Maghreb
06 75 75 51 94
romain.camus@pwc.com

Karine Pariente
Associée
Gestion des risques technologiques,
secteur Assurance
PwC France et Maghreb
06 11 15 84 91
karine.pariente@pwc.com

Jamal Basrire
Associé
Cyber
Intelligence
PwC France et Maghreb
06 43 31 86 31
jamal.basrire@pwc.com

pwc.fr