Digital Operational Resilience Act « DORA »

protiviti®
Global Business Consulting

Version Août 2023

La règlementation européenne évolue régulièrement pour s'adapter aux nouveaux enjeux et défis du numérique. Face à la hausse constante des cyberattaques visant les institutions financières et à la dépendance croissante de ces dernières à la technologie, les institutions financières doivent entreprendre des projets de transformation et des initiatives de remédiation pour se conformer aux nouvelles règlementations. C'est le cas avec le règlement européen DORA(1) – Digital Operational Resilience Act – qui a été publié et approuvé en novembre 2022. Son objectif est de renforcer et harmoniser la "résilience opérationnelle" du secteur financier au sein de l'Union Européenne.

Qu'est-ce que DORA ?

Digital Operational Resilience Act ou DORA est un nouveau règlement adopté par le Parlement européen et applicable au secteur financier. Il prévoit un ensemble d'exigences ayant pour objectif de renforcer le niveau de résilience opérationnelle numérique des institutions financières au sein de l'Union européenne, et ce, en proposant une approche harmonisée des règles déjà existantes en la matière. Ces exigences sont organisées autour de cinq piliers clé :

1 Gestion des risques liés aux TIC

- **La responsabilité de l'organe de direction est renforcée, celui-ci devra assumer la "responsabilité ultime" de la gestion des risques liés aux TIC**, ce dernier devra bénéficier des formations obligatoires sur les aspects de résiliences, en plus de l'ensemble du personnel.
- L'organe devra définir et approuver sa stratégie de résilience opérationnelle numérique ainsi que la politique de l'entreprise en matière d'utilisation des fournisseurs tiers de TIC.
- Les entreprises devront identifier leur tolérance au risque TIC.
- Elles devront mettre en place un cadre de gestion des risques basés sur les fonctions critiques et importantes (CIF - Critical or Important Functions), identifier la tolérance aux risques TIC et réaliser des analyses d'impacts basés sur des scénarios de perturbation grave des activités.

2 Gestion et signalement des incidents liés aux TIC

- Le règlement vise à rationaliser les exigences européennes existantes en matière de notification des incidents à travers une **méthodologie standard et harmonisée de classification des incidents avec un ensemble de critères et seuils spécifiques** qui seront clarifiés à travers la publication des RTS(2).
- Selon cette méthodologie, les incidents classés comme majeurs devront être signalés à l'autorité de régulation locale dans le même jour ouvrable, selon un modèle défini.
- Des rapports de suivi anonymisés seront communiqués régulièrement à l'ensemble de la communauté.

3 Tests de résilience opérationnelle numérique

- Les institutions financières établiront et maintiendront en fonction de leur taille, de leur activité et de leur profil de risque, **un programme complet de tests de résilience opérationnelle** numérique selon une approche fondée sur les risques et en se focalisant sur leurs systèmes et applications TIC jugés critiques.
- Certaines institutions financières identifiées comme importantes par les autorités compétentes via les RTS, devront effectuer des tests de pénétration approfondis fondés sur la menace (TLPT – Threat Led Penetration Testing à fréquence tri-annuelle par des testeurs indépendants (conformément au cadre TIBER-EU - Threat Intelligence-based Ethical Red Teaming - existant de la BCE).

4 Gestion des risques liés aux tiers prestataires de services informatiques

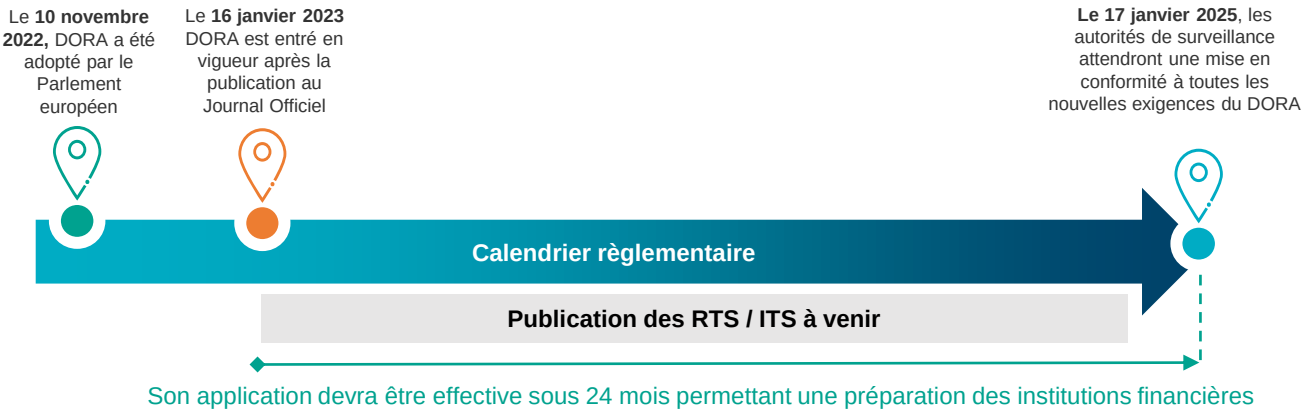
- Les institutions financières devront disposer d'une stratégie et politique définies en matière de risque de tiers pour les TIC et devront établir et tenir à jour un registre standard d'informations contenant la vue complète de leurs prestataires tiers TIC et situations des fonctions qu'ils sous-tendent.
- Elles devront procéder à des **évaluations du risque de concentration** pour tous les contrats d'externalisation qui contribuent à l'exécution des CIF ainsi que réaliser des évaluations précontractuelles selon certains critères et définir une stratégie de sortie en cas de défaillance d'un prestataire.
- Les prestataires tiers essentiels feront l'objet d'évaluations annuelles au regard de certaines exigences de résilience. Ces évaluations seront effectuées directement par le régulateur et donneront lieu à des sanctions en cas de non-conformité.

5 Partage d'informations et de renseignements liés aux cybermenaces

- Le règlement introduit des lignes directrices sur la **mise en place d'accords de partage d'informations entre les différentes institutions financières de l'UE relatifs les cybermenaces** ainsi que la nécessité d'informer l'autorité de régulation.

Dates clés et corpus accompagnant le règlement DORA

Entré en vigueur le 16 janvier 2023, les institutions financières disposent d'un délai d'environ 24 mois pour se conformer au règlement DORA. Durant cette période, celui-ci sera complété de plusieurs RTS (Regulatory Technical Standards) / ITS (Implementing Technical Standards) élaborés par les autorités européennes de surveillance, celles-ci détailleront les attendus pour la mise en œuvre technique de certaines exigences du règlement.



Gestion du risque	Gestion des incidents	Test de résilience	Risque de tiers
• RTS sur le cadre de gestion des risques liés aux TIC **(31/12/2023)** • RTS sur le cadre simplifié de gestion des risques liés aux TIC **(31/12/2023)**	• RTS sur les critères de classification des incidents liés aux TIC **(31/12/2023)** • RTS sur la notification des incidents majeurs liés aux TIC **(30/06/2024)** • ITS pour établir le rapport sur les incidents majeurs liés aux TIC **(30/06/2024)** • Agrégation des coûts/pertes causés par des incidents majeurs liés aux TIC **(30/06/2024)**	• RTS pour spécifier les aspects des tests de pénétration basés sur la menace **(30/06/2024)**	• RTS pour spécifier la politique sur les services TIC **(31/12/2023)** • ITS pour établir les modèles pour le registre d'information **(31/12/2023)** • RTS sur la sous-traitance de fonctions critiques ou importantes **(30/06/2024)** • Règlement général sur la structure du contrôle **(date à venir)** • RTS pour spécifier les informations sur la conduite de la supervision **(30/06/2024)**

Enjeux et apports clés

Une stratégie de résilience opérationnelle informatique robuste pour chaque institution financière portée par les organes de direction

Un référentiel de règles harmonisées (gouvernance, reporting, tests, risques liés au tiers...) pour toutes les institutions financières de l'UE

Un cadre juridique clarifié ainsi qu'un cadre de surveillance européen des prestataires critiques permettant de limiter le risque systémique et renforcer la confiance

Se préparer à la mise en conformité DORA

L'étendue des efforts à fournir pour être conforme à ce règlement dépend du niveau de maturité des organisations sur l'ensemble des aspects en rapport avec la gouvernance, le risque et la conformité autour des fonctions TIC, cyber et TPRM (Third Party Risk Management) ainsi que des travaux de suivis périodiques permettant de remédier aux vulnérabilités opérationnelles identifiées. Les institutions financières doivent donc procéder, dans un premier temps, à une analyse des écarts sur la base des exigences du règlement DORA, puis l'actualiser en tenant compte des exigences des RTS/ITS au fur et à mesure de leur publication. Cette phase préliminaire permettrait d'identifier les potentiels écarts existants vis-à-vis du règlement qui devront être remédiés au cours de la période de mise en œuvre de 24 mois.

➢ PROTIVITI vous accompagne dans votre démarche de mise en conformité

- PROTIVITI vous assiste sur l'ensemble de la démarche de mise en conformité DORA. Nous avons conçu des outils permettant d'analyser et évaluer votre niveau de maturité actuel, d'identifier les principaux axes d'améliorations sur chacun des chapitres puis de proposer des mesures spécifiques vous permettant de répondre aux exigences réglementaires, tout en adaptant notre plan de remédiation à votre environnement.
- Notre accompagnement vous permettra de vous situer par rapport aux exigences du règlement et in-fine d'améliorer vos capacités et de préparer votre établissement à une mise en conformité réussie.
- Les équipes de Protiviti disposent d'un ensemble de compétences, de connaissances et d'expériences spécialisées pour vous accompagner dans cette démarche de mise en conformité d'une importance cruciale. Elles bénéficient ainsi de formations continues et capitalisent sur les activités et missions qu'elles réalisent dans ce domaine. En outre, elles détiennent des certifications professionnelles pertinentes et reconnues en audit informatique, cybersécurité et gestion de projets, telles que : **CISA, CISM, CISSP, ISO 27001, ISO 22301, TOGAF, ITIL, PMP, Scrum Master, OneTrust, etc.** Ces certifications témoignent de notre engagement à maintenir un niveau élevé de compétence et à offrir à nos clients des services de la plus haute qualité.

DORA(1) – ***Nom complet du règlement****: Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 (Texte présentant de l'intérêt pour l'EEE)*

RTS(2) – *Regulatory Technical Standards*

Pour en savoir plus, contactez-nous ici : Contact us | Protiviti

Nous contacter

Bernard DRUI
Country Market Leader
bernard.drui@protiviti.fr

Lyes OUSSADIT
Senior Manager
lyes.oussadit@protiviti.fr

Loïck LATIFI
Manager
loick.latifi@protiviti.fr