Ce que vous devriez retenir en priorité concernant DORA

Suite à sa publication en janvier 2023, les entités du secteur financier de l'Union Européenne disposent de deux ans pour se mettre en conformité avec le règlement DORA (*Digital Operational Resilience Act*) sur la résilience opérationnelle numérique. Mais agir dès maintenant présente des avantages non négligeables.

Si vous êtes responsable informatique d'une entité financière dans l'Union Européenne, vous connaissez certainement l'initiative réglementaire DORA. Ce règlement a été publié en décembre 2022 et est entré en vigueur en janvier 2023, à l'issue d'une période de révision débutée en septembre 2020. Toute entité du secteur financier de l'UE a désormais moins de 24 mois pour augmenter sa maturité en matière de cybersécurité et sa résilience face aux risques numériques, afin de se conformer à ces nouvelles dispositions[1] avant le 17 janvier 2025, date d'entrée en application de DORA.

Si vous siégez au conseil d'administration d'une entité financière ou si vous êtes membre du COMEX, vous n'avez peut-être pas prêté beaucoup d'attention à DORA. D'ailleurs pourquoi le feriez-vous ? Cela ne relève-t-il pas de l'IT ? La conformité et les tests ne sont-ils pas l'affaire de vos experts et autres techniciens ?

Vous pourriez raisonner ainsi. Mais compte tenu des origines et des ambitions du nouveau règlement il se peut que vous sous-estimiez les défis de taille posés par la mise en conformité avec DORA. Par ailleurs, vous pourriez manquer une opportunité unique de réhausser votre posture en matière cybersécurité en rapport avec l'évolution des menaces et d'améliorer votre gestion des risques numériques pourtant bénéfique à votre organisation. Car au-delà de renforcer la cybersécurité, DORA entend développer la résilience opérationnelle de l'entreprise dans son ensemble.

N'importe quel responsable IT vous dira à ce sujet : la cybersécurité et la résilience doivent faire partie intégrante du fonctionnement de votre organisation et de sa transformation numérique.

Un accent mis sur les TIC

Pour mieux comprendre, revenons à l'origine de DORA et à ses objectifs. Pendant des années, les organes gouvernementaux des membres de l'UE ont exercé un pouvoir discrétionnaire en matière de cybersécurité dans les services financiers. Cela a conduit à une multiplicité d'interprétation et de mise en oeuvre pour le signalement des incidents par exemple, renchérissant les coûts de conformité pour les organisations.[2]

DORA harmonise le cadre réglementaire et vise la cohérence à travers l'UE, pour garantir la résilience opérationnelle en cas de perturbation grave. Plus précisément, l'UE espère que cette nouvelle

réglementation aidera les entreprises du secteur financier à mieux résister, réagir et se remettre des menaces pesant sur les technologies numériques qu'elles utilisent. Compte tenu des impératifs commerciaux inhérents à son maintien, le règlement DORA entend renforcer la stabilité et la confiance au sein du système financier.[3]

Ses implications seront donc d'une grande portée. Nous répondons ici aux principales questions relatives à ce nouveau cadre réglementaire qui s'invite dans les agendas des dirigeants.

Q. En quoi le règlement DORA est-il différent de la réglementation à laquelle mon entreprise est actuellement soumise ?

A: Cela dépend de votre réglementation nationale. Mais il est important de savoir que le règlement DORA montre un interventionnisme inédit. Il est beaucoup plus normatif que tout ce qui a été publié précédemment. Car répétons-le : l'UE entend jouer un rôle central dans les technologies numériques du secteur financier. En effet, les failles et les vulnérabilités des infrastructures numériques ne sont pas seulement des problèmes informatiques, mais des problèmes affectant tout le fonctionnement du système financier. Adieu la « cyber conformité », pensez plutôt « cyber résilience ».

Q. Ne peut-on pas simplement attendre un an ou deux pour se mettre en ordre de marche ?

A. Vous le pourriez. Sauf qu'étant donné les enjeux de ce règlement, les sanctions et les conséquences attachées à son non-respect, les entreprises ont en réalité tout intérêt à prendre les devants. Les banques et les compagnies d'assurance ont déjà lancé des initiatives DORA cette année.[4] Si vous attendez et vous cantonnez à bricoler à la marge vos principales plates-formes, cela vous semblera moins perturbant mais vous devrez ajouter ensuite nombre d'infrastructures supplémentaires.

Q. Nous ne sommes pas une entité financière, mais travaillons avec. Le règlement DORA s'applique-t-il à nous ?

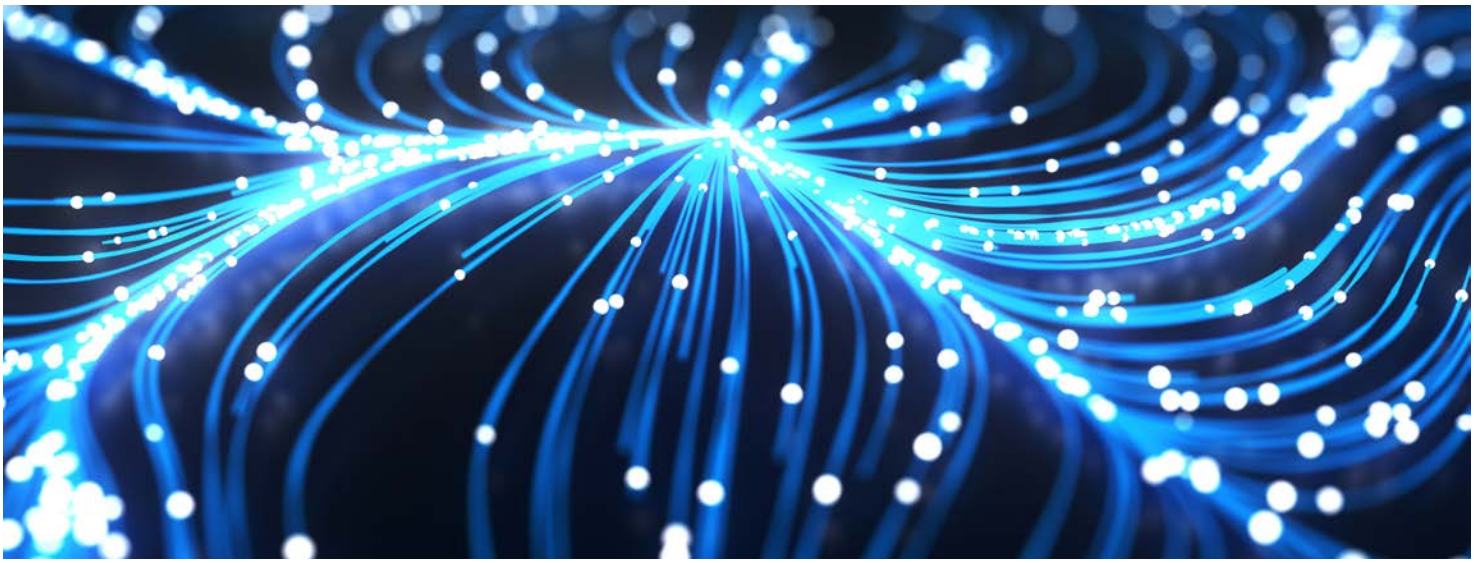
Par exemple, les tiers qui fournissent des services informatiques et numériques aux entreprises de services financiers, tels que des plateformes cloud ou des services d'analyse de données, doivent être conformes. Et le Conseil européen indique que « les fournisseurs de services numériques issus de pays tiers essentiels aux entités financières de l'UE seront tenus d'établir une filiale au sein de l'Union ».[5]

Q. Y a-t-il un point que je pourrais négliger lors de la mise en œuvre de DORA ?

A. Comme indiqué, DORA pose de nombreuses exigences dans tous les aspects de la résilience opérationnelle numérique. Par exemple, avez-vous réfléchi à votre communication de crise si vous subissez un incident cyber une fois le règlement en vigueur ? Celui-ci oblige à signaler tous les incidents. Et anticiper les choses atténue clairement le risque réputationnel.[6]

Q. Cinq piliers clés sont associés au règlement DORA (voir encadré). Lequel dois-je privilégier en premier ?

A. Les cinq piliers sont interdépendants et doivent être abordés conjointement. Par contrainte rédactionnelle, cet article ne présente que le pilier « tests de résilience opérationnelle numérique ». Des articles ultérieurs couvriront les quatre autres piliers.



Q. Très bien, alors parlez-moi des tests de résilience opérationnelle numérique.

A. Ce pilier obligera les entités financières à se soumettre à des tests réguliers effectués par des tiers indépendants. Les législateurs s'efforcent encore de clarifier la méthodologie des tests et la manière dont les différentes entités en reconnaîtront les résultats. Mais selon l'accord provisoire, les tests d'intrusion et "Red Team" sont basés sur des initiatives européennes existantes, comme TIBER-EU, un cadre qui « imite les tactiques, les techniques et les procédures d'attaquants réels, à partir de renseignements sur des menaces sur-mesure ».[7] Les tests sont personnalisés pour simuler une attaque sur les fonctions critiques d'une entité et ses systèmes sous-jacents.

Q. Maintenant que je connais le pilier « tests », quelle est la chose la plus importante à garder à l'esprit lors de l'exécution d'un programme de tests ?

A. Qu'il doit permettre de simuler une attaque qui correspond à l'état de l'art de la menace et d'identifier ainsi les faiblesses éventuelles de ses systèmes et les axes d'amélioration en matière de protection, de détection, de réaction et de gestions de crise.

Les cinq piliers de DORA*

— Test de résilience opérationnelle numérique

— Gestion des risques numériques

— Rapports d'incidents

— Partage d'informations et de renseignements

— Gestion des risques numériques pour les tiers

Source: https://reciprocity.com/blog/learn-about-the-digital-operational-resilience-act/

* FTI Consulting organise les exigences de DORA en cinq piliers clés ; d'autres sources peuvent les organiser différemment.

Pour en savoir plus

1 FTI Perspectives, “DORA Overview for Permanent TSB (FTI Perspectives,” April 2022, p. 3)

2 FTI Cybersecurity, “The Digital Operational Resilience Act (DORA): Key questions business leaders should be asking,” FTI Consulting, December 29, 2020, https://fticybersecurity.com/2020-12/the-digital-operational-resilience-act-dora-key-questions-business-leaders-should-be-asking/

3 Council of the EU, “Digital finance, provisional agreement reached on DORA,” May 11, 2022 https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

4 Lafarge, Joanna Grove “What firms can expect from DORA,” Global Risk Regulator,” February 4, 2021, https://www.globalriskregulator.com/Subjects/Reporting-and-Governance/What-firms-can-expect-from-DORA

5 Council of the EU, “Digital finance, provisional agreement reached on DORA,” May 11, 2022 https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

6 Moinuddin, Ali, “The Global Drive for Better Financial Sector Operational Resilience,” International Banker, June 7, 2022, https://internationalbanker.com/finance/the-global-drive-for-better-financial-sector-operational-resilience/

7 European Central Bank, “What is TIBER-EU,” https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html#:~:text=TIBER%2DEU%20is%20the%20European,carrying%20out%20a%20controlled%20cyberattack.

THOMAS HUTIN
Head of Cybersecurity
France