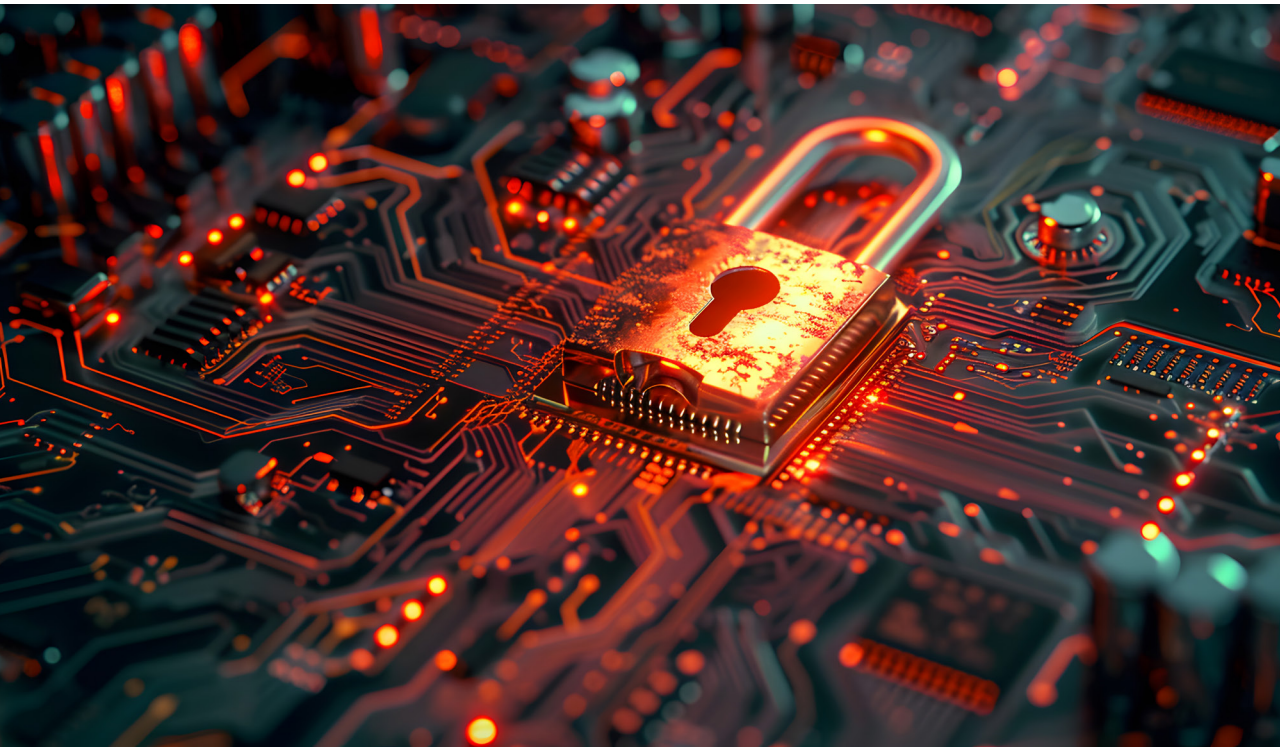
Guide pratique

# Gérer les risques informatiques dans le secteur financier

## Mettre en œuvre la réglementation DORA



Fabrice Rosa

L'ARGUS de l'assurance ÉDITIONS

# Sommaire

**Chapitre 4 - La gestion des systèmes d'information, clé de voûte**



**Chapitre 5 - Les impacts de DORA sur votre gestion des achats**



**Chapitre 6 - Le fonctionnement des autorités de surveillance**

Chapitre 1

# Pour comprendre DORA dans son ensemble

1. Historique
2. Les objectifs par piliers
3. Les élus et les exclus de DORA
4. Le principe de proportionnalité
5. Gouvernance et organisation à mettre en œuvre

L'historique a pour objectif de se représenter DORA dans ses principales étapes. Dans un deuxième temps, les dispositions générales de la réglementation DORA seront étudiées afin d'en exposer l'objet général et le champ d'application, à travers l'identification des entreprises concernées. Enfin, le principe de proportionnalité de la réglementation sera abordé, ainsi que les modalités de gouvernance et d'organisation à mettre en œuvre. Nous utiliserons dans les développements suivants les termes tels qu'ils sont définis à l'article 3 du règlement DORA (V. l'ensemble de ces définitions en Annexe).

Ce chapitre s'adresse à l'ensemble des interlocuteurs. Toutefois, dans le cadre de la prise de connaissance des informations liées à la gouvernance, les directions générales, éventuellement élargies aux comités de direction, se doivent de prendre en compte un certain nombre de points que la réglementation impose dans l'objectif de les approuver au niveau de l'entreprise.

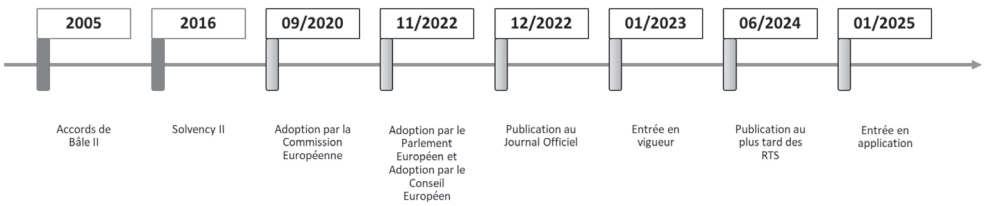
V. le règlement DORA, art. 1 à 5.

# 1. Historique

Le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique (dit règlement DORA) prend sa place dans la lignée des accords de « Bâle II » mis en œuvre en 2005 et de la réglementation « Solvabilité II » (ou Solvency II) mise en œuvre en 2016. Sans ces deux textes et leurs retours d'expériences, le Digital Operational Resilience Act n'existerait pas encore (voir liens en Annexe).

La frise chronologique présente de manière synthétique le calendrier de la réglementation DORA.

**Figure 1 – La réglementation DORA en dates**




De fait, les premiers travaux concernant DORA ont commencé à partir de l'année 2020 par l'intermédiaire de la Commission européenne, qui en adoptant une proposition de projet de régulation de la résilience opérationnelle du numérique du secteur financier a lancé le début de cette réglementation.

Le Parlement européen et le Conseil européen ont adopté le 14 décembre 2022 le règlement (UE) 2022/2554 DORA et la directive associée (UE) 2022/2556, pour une entrée en vigueur au 16 janvier 2023. Le règlement vise à consolider et à mettre à niveau les exigences en matière de risque lié aux technologies de l'information et de la communication (TIC) pour renforcer et harmoniser la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne ; la directive associée a elle pour objectif de modifier les directives existantes (Solvabilité 2, MiFID 2, AIFM), pour les aligner aux dispositions du règlement DORA.

Enfin, les RTS (Regulatory Technical Standards) qui sont les « normes techniques réglementaires », publiées en juillet 2024, sont venues compléter la réglementation pour préciser certains articles.

**C'est à partir du 17 janvier 2025, cela pour toutes les entreprises concernées, que la réglementation DORA (avec ses sanctions) sera mise en application.**

Les Systèmes d'Information (SI) sont la colonne vertébrale de tous les systèmes financiers du monde. Les cyberattaques sur des systèmes mutualisés, les détériorations ou les interruptions de service peuvent augmenter de manière conséquente, et subséquemment la gestion des risques informatiques en devient de plus en plus complexe.

De surcroît, le recours à des prestataires de services génère des risques par les actions opérées sur des environnements mutualisés, où se retrouvent plusieurs applications, infrastructures ou services utilisés par de nombreuses entreprises qui pourraient se faire contaminer par suite d'un incident.

Cette agora stratégique des Systèmes d'Information dans le fonctionnement des entreprises financières expose ; si elle n'est pas maîtrisée, elle peut affaiblir la résilience opérationnelle de l'entreprise tout entière.

Ainsi, on peut admettre que pour partie du risque IT (Information Technology), DORA est une évolution de la réglementation afin de mieux maîtriser ces risques.

# 2. Les objectifs par piliers

Pour chaque acteur concerné par la réglementation, l'objectif est d'atteindre « un niveau commun élevé de résilience opérationnel numérique ».

Dans un premier temps, il est essentiel de bien comprendre ce qu'est la « résilience opérationnelle numérique » que la réglementation définit comme tel :

> *« la capacité d'une entreprise à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou par le recours de prestataire de services, l'intégralité des capacités nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité. »*

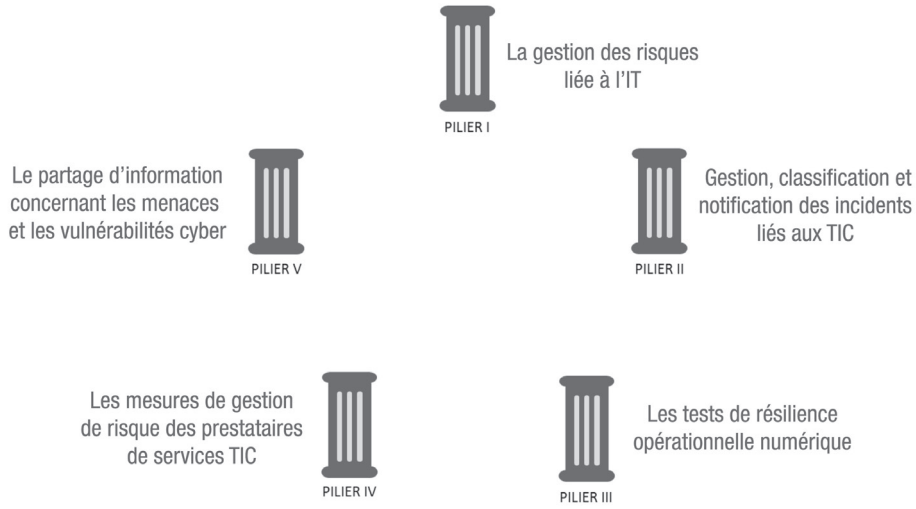
Les exigences générales de la réglementation sont énumérées et concernent le périmètre de sécurité des réseaux et des systèmes d'information sous-tendant les processus opérationnels.

DORA vous impose ainsi de prendre en compte 4 types d'exigences, indiquées comme obligatoires pour chaque entreprise et qui concernent :

– L'entreprise elle-même ;
– Les accords contractuels conclus avec des prestataires de services IT ;
– Les règles relatives à l'établissement du cadre de supervision applicable aux prestataires critiques de services IT ;
– Les règles relatives à la coopération entre les autorités incluant les règles relatives à la surveillance et à l'exécution.

Les 4 types d'exigences listés ci-dessus s'appliquent sur les différents périmètres suivants qui font référence aux 5 piliers de DORA :

**Figure 2 – Les 5 piliers de la réglementation DORA**




Alors que nous allons parcourir tout au long de cet ouvrage ces cinq piliers, nous pouvons dès maintenant résumer chacun en quelques mots :

– la **gestion des risques liée à l'IT** a pour objectif principal d'assurer la sécurité, la fiabilité et la disponibilité de votre informatique tout en contrôlant ses risques. La mise en place d'un cadre de gestion du risque IT en est l'enjeu principal ;
– la **gestion, classification et notification des incidents liés à l'IT** a pour objectif de mettre en œuvre une traçabilité, une catégorisation et une communication pour l'ensemble des incidents informatiques. L'enjeu de ce pilier est principalement la mise en place d'un processus de gestion des incidents enrichi d'exigences propres à DORA, notamment dans le cadre des communications, de l'estimation d'impact ou bien de l'analyse de risque ;
– les **tests de résilience opérationnelle numérique** ont pour objectif de mettre à l'épreuve la stratégie de résilience que vous avez définie dans le cadre de votre gestion de risque. L'enjeu de ses tests est de s'intégrer dans un processus d'amélioration continue de votre stratégie de résilience.
– les **mesures de gestion de risque des prestataires de services IT** ont pour objectif d'évaluer vos différents niveaux de risques auprès de vos prestataires. L'enjeu étant de posséder un niveau de risque acceptable selon vos activités vis-à-vis de ces services nécessaires mais externalisés ;
– le **partage d'information concernant les menaces et les vulnérabilités cyber** vise à mettre en œuvre un dispositif pour l'ensemble des acteurs (entreprise financière, prestataire, institution publique) afin de collaborer sur les cybermenaces. L'enjeu étant de renforcer la résilience du secteur financier.

Guide pratique

# Gérer les risques informatiques dans le secteur financier

**Fabrice Rosa**
Après un début de carrière dans les années 2000, il a exercé ces dernières années des fonctions de directeur de projet et de DSI pour plusieurs banques et mutuelles d'assurance, dont BNP, la MACIF et Garance Mutuelle. Il a également développé des compétences sur la mise en œuvre de réglementation comptable, fiscale et juridique. Il exerce aujourd'hui en tant que consultant et manager de transition auprès de directions évoluant dans les secteurs de l'assurance et de la prestation de conseil ou de services informatiques.

*Préface de* Nordine Benhatta*, avocat au barreau de Paris, réseau Laurence Lautrette et associés*

À partir du 17 janvier 2025, la réglementation DORA (*Digital Operational Resilience Act*) s'appliquera à l'ensemble des acteurs du secteur financier et assurantiel en Europe. Ce cadre juridique vise à renforcer et harmoniser la gestion des risques liés aux technologies de l'information et de la communication (TIC), ainsi qu'à la sécurité des réseaux et des systèmes d'information. Les entités financières devront prouver leur capacité à résister, répondre et se rétablir face à toute perturbation opérationnelle.

Ce livre offre une feuille de route pratique pour chaque direction fonctionnelle afin de se conformer au règlement DORA. Il fournit des clés pour améliorer la résilience opérationnelle face aux risques informatiques et de cybersécurité, en abordant des questions essentielles, telles que :

- Quelles sont les nouvelles obligations de sécurité ?
- Comment établir un plan d'action pour la mise en conformité ?
- Quelles mesures techniques et opérationnelles doivent être mises en œuvre ?
- Comment réagir en cas de cyberattaque ?
- Comment gérer, classifier et notifier les incidents IT ?

Que vous soyez dirigeant, DSI ou responsable des risques, cet ouvrage est conçu pour vous aider à répondre aux exigences de la réglementation DORA à tous les niveaux de votre entreprise. Vous y trouverez des conseils opérationnels et des actions concrètes pour vous assurer de la conformité de l'entité financière et des sous-traitants à cette réglementation.

ISBN 978-2-35474-526-4