

La souveraineté numérique : un nouvel horizon pour la résilience des banques et assurances européennes à l'ère de DORA



Stéphane DANIEL

Sciences-Po Paris Consultant IT & Conformité (DORA, RGPD)

Introduction : DORA comme catalyseur d'une nouvelle souveraineté opérationnelle

L'entrée en vigueur du Digital Operational Resilience Act (DORA) marque un tournant majeur dans la régulation financière européenne.

Alors que le secteur financier est devenu l'un des plus numérisés au monde, sa dépendance envers des infrastructures technologiques mondialisées constitue aujourd'hui un risque systémique.

Face à cette réalité, l'Union européenne ne se contente plus de renforcer des exigences techniques : elle bâtit une **doctrine de souveraineté numérique appliquée à la stabilité financière**.

Cette souveraineté ne cherche pas à créer des champions européens du cloud ou de l'IA, mais à encadrer, superviser et maîtriser les dépendances qui structurent les infrastructures critiques des banques et assurances.

En cela, DORA n'est pas seulement un texte de conformité : c'est un **instrument stratégique de gouvernance des risques numériques**, qui rééquilibre le rapport de force entre l'Europe, ses institutions financières et les géants technologiques mondiaux.

L'enjeu est clair : **une Europe qui n'est pas souveraine numériquement ne peut pas être résiliente.**

1. La souveraineté numérique comme nouvelle exigence prudentielle

Le fonctionnement quotidien des institutions financières repose de plus en plus sur des services technologiques essentiels : clouds publics, infrastructures de stockage, gestion des identités, cryptographie, annuaires, réseaux mondiaux, services API, plateformes de transfert sécurisé, solutions DevOps et IA intégrée.

Ces briques critiques sont opérées par quelques grandes entreprises internationales, principalement américaines.

Cette dépendance massive ne relève plus seulement d'un enjeu opérationnel.

Elle touche au cœur même de la **stabilité du système financier**.

Les établissements financiers, pourtant très régulés, reposent sur des technologies très peu régulées.



Ce déséquilibre structurel crée un risque prudentiel inédit :

- si un fournisseur technologique tombe,
- si un service cloud devient indisponible,
- si une technologie critique devient vulnérable,
- ou si un acteur dominé par une juridiction extracommunautaire subit une contrainte légale étrangère,

alors une partie du système financier européen peut être fragilisée.

La souveraineté numérique, dans ce contexte, n'est plus un sujet géopolitique abstrait : c'est une **condition de stabilité**, de continuité de service et de maîtrise des risques.

Elle implique la capacité de l'Europe à :

- comprendre ses dépendances technologiques ;
- en cartographier les risques ;
- auditer les prestataires critiques ;
- contrôler leurs pratiques ;
- exiger des correctifs ;
- prévoir des plans de bascule réalistes ;
- éviter les situations de dépendance unique non réversible.

Longtemps considérée comme une préoccupation de DSI ou de RSSI, la souveraineté numérique devient ainsi un **enjeu prudentiel** au même titre que la solvabilité ou la liquidité.

2. DORA : la souveraineté par la résilience

Entré en application le 17 janvier 2025, DORA harmonise la résilience opérationnelle de plus de vingt catégories d'entités financières.

Mais son ambition dépasse largement l'harmonisation : il opère un changement profond de doctrine.

DORA introduit l'idée que la **résilience numérique est une composante de la souveraineté**. Une banque dépendante d'un acteur technologique qu'elle ne maîtrise pas ne peut pas garantir la continuité de ses services essentiels.

Un assureur incapable de basculer son système d'information vers une solution alternative ne peut pas prétendre être résilient.

DORA impose ainsi :

- une gouvernance renforcée de la résilience numérique ;
- une articulation claire entre direction générale, DSI, RSSI, risques et conformité ;
- des analyses d'impact BIA transverses ;
- des tests réguliers de continuité ;
- une gestion de crise plus structurée ;
- un suivi exigeant des incidents majeurs ;
- une capacité de bascule et de réversibilité documentée ;
- un **registre des TIC** permettant de cartographier précisément les dépendances aux prestataires.

Avec DORA, l'autorité de contrôle ne se limite plus à l'analyse prudentielle classique : elle devient garante de la **solidité numérique** du secteur financier.

La résilience technologique devient une dimension indispensable de la résilience financière.

3. Encadrement des prestataires critiques : un tournant stratégique pour la résilience européenne

Lors de la conférence de l'ACPR du 25 novembre 2025, un message fort a été réaffirmé : DORA change l'équation en permettant enfin à l'Europe de superviser directement les prestataires TIC critiques qui structurent l'écosystème financier. Pour les autorités de contrôle, il s'agit d'un **levier décisif** pour maîtriser les risques systémiques liés à la concentration technologique.

Le 18 novembre 2025, les Autorités européennes de surveillance ont publié **la liste des 19 Critical ICT Third-Party Providers**. Cette désignation, fondée sur l'analyse des registres d'information, des contrats transmis par les entités financières et des critères réglementaires, couvre l'ensemble des infrastructures essentielles : cloud, data centers, télécommunications et logiciels.

Dès 2026, des équipes conjointes basées à Paris et Francfort mèneront les premières investigations en coordination avec les 27 autorités nationales. L'enjeu n'est pas de limiter l'usage de ces acteurs, mais **d'obtenir un niveau de résilience**, de transparence et de gouvernance conforme aux attentes européennes. Ce cadre constitue une opportunité unique : sécuriser les dépendances critiques tout en renforçant la capacité des organisations à piloter leurs risques.

Il s'agit d'une souveraineté qui s'exerce par l'encadrement et la capacité à piloter les risques, plutôt que par la création d'alternatives technologiques ; une souveraineté d'influence, structurée autour d'une gouvernance renforcée.

4. 2025–2026 : la fin de l'accompagnement de l'autorité de contrôle, le début des sanctions

L'année 2025 a été celle de l'accompagnement. L'autorité de contrôle a multiplié :

- les échanges bilatéraux,
- les sessions d'assistance,
- l'interprétation des exigences,
- les communications pédagogiques,
- les réponses aux sollicitations des établissements.

En revanche, **2026 marque un changement profond de doctrine** : l'autorité passe désormais à une supervision renforcée.

Ce changement se matérialise par l'utilisation systématique d'un outil majeur : **les questionnaires DORA** adressés aux établissements.

4.1 Le déclenchement : la transmission du questionnaire comme début du contrôle sur pièces

Au cours du second semestre, les banques et les assurances ont dû transmettre un questionnaire. Il permet de savoir le niveau de maturité.

4.2 Analyse des réponses : un croisement systématique des informations

L'autorité ne s'appuie plus uniquement sur les déclarations des établissements. Elle réalise désormais un **croisement consolidé** des données grâce à l'IA :

- registres des TIC,
- notifications d'incidents,
- réponses au questionnaire,
- échanges bilatéraux antérieurs,
- analyses sectorielles et transverses.

Ce croisement permet d'obtenir une vision fiable de la maturité réelle, au-delà de ce qui est déclaré.

L'autorité peut facilement détecter :

- des incohérences entre registre des TIC et PRA,
- des dépendances mal documentées,
- des fragilités organisationnelles,
- des zones d'exposition technologique,
- une absence de bascule réaliste,
- une gouvernance insuffisante.

4.3 Décision : une approche graduée et proportionnée

À l'issue de cette analyse consolidée, l'autorité peut décider :

- de **clôturer** le pré-contrôle ;
- de formuler des **observations** et exiger un plan d'action ;
- de diligenter un **contrôle sur place** ;
- de recourir à des **mesures contraignantes** lorsqu'un risque critique menace la continuité des services essentiels.



4.4 2026 : l'entrée dans la supervision opérationnelle

Les échanges informels avec les autorités de contrôle indiquent clairement que **l'année 2025 a été celle de l'accompagnement ; l'année 2026 sera celle de la supervision renforcée. Les priorités de contrôle seront fixées en croisant les entretiens, le registre des TIC, les notifications d'incidents et les questionnaires reçus. Les entités les plus à risque feront l'objet de contrôles sur place.**

Nous entrons ainsi dans un modèle de supervision :

- plus analytique,-
- plus comparatif,
- plus exigeant,
- plus structurant.

DORA devient une régulation vivante, pilotée en continu par l'autorité.

5. Gouverner la dépendance : la nouvelle discipline prudentielle

Pour être conforme à DORA, un établissement doit démontrer qu'il maîtrise **la totalité de sa chaîne de dépendances technologiques**. Cela implique :

a) Une cartographie exhaustive des dépendances critiques

Avec un registre des TIC structuré, actualisé et gouverné.

b) Des scénarios de bascule réalistes

Pas théoriques, mais opérationnellement crédibles.

c) Des tests réguliers

PRA, BIA, exercices de crise, Red Team, TIBER, table-top multi-entités.

d) Une gouvernance unifiée

Associer direction générale, risques, DSI, RSSI, conformité, juridique.

Il s'agit d'un véritable **changement de modèle** : on passe d'un système où l'IT soutient la stratégie, à un système où l'IT **conditionne** la continuité, donc la stratégie elle-même.

Conclusion : une souveraineté d'encadrement du numérique, pas de substitution

Avec DORA, l'Union européenne se dote d'une véritable doctrine de souveraineté numérique appliquée au secteur financier.

Il ne s'agit pas de créer artificiellement des substituts européens aux géants technologiques mondiaux, mais de **reprendre le contrôle** sur les dépendances critiques.

La solidité d'un établissement dépend désormais autant de sa **maîtrise des risques numériques que de son bilan ou de ses ratios prudentiels**.

La souveraineté numérique devient un **nouveau pilier de stabilité financière**, et DORA en est la pierre angulaire.

Si l'Union européenne n'est pas productrice de ces technologies, elle en devient l'architecte prudentiel pour en assurer la résilience, lieu d'expression d'une souveraineté renouvelée. ■

