

01

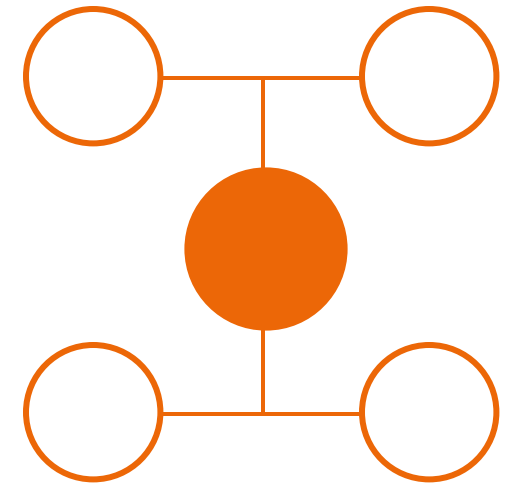
Banque – Finance :
La dépendance
technologique est
un risque
stratégique



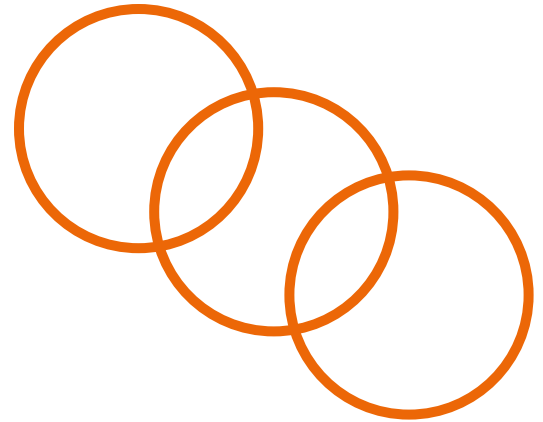
Et si votre principal fournisseur cloud cessait demain de vous servir, combien de temps votre banque pourrait-elle continuer à fonctionner ?

Dans le contexte géopolitique que nous connaissons aujourd'hui, la question des dépendances technologiques, et par extension celle de la souveraineté numérique, est plus que jamais d'actualité.

Paiement instantanés, banque mobile, automatisations des processus... En à peine une décennie, les métiers de la banque-finance ont profondément évolué grâce à la numérisation massive du secteur. Cette transformation n'est pas sans risque, portée par le fait qu'elle repose sur un nombre restreint d'acteurs souvent nord-américains et accentuée par l'usage démocratisée de l'intelligence artificielle.



Dans ce décor qui mêle à la fois risque cyber et risques portés par les dépendances technologiques, une question paraît primordiale : **les établissements bancaires maîtrisent-ils encore leurs infrastructures numériques critiques ?**



Comprendre ce double-risque, en mesurer les implications et engager des actions concrètes qui correspondent aux besoins : tel est désormais l'enjeu pour les établissements bancaires.

L'essentiel :

1

La dépendance technologique est devenue un risque stratégique.

Les banques dépendent de quelques fournisseurs, souvent américains, soumis à des lois extraterritoriales, et l'IA générative accentue ce risque en exposant leurs données et leur savoir-faire.

2

La souveraineté numérique, c'est garder la maîtrise.

Il ne s'agit pas de tout internaliser, mais de pouvoir décider, auditer et reprendre la main, comme l'exigent DORA, le Data Act et l'AI Act.

3

La maîtrise des accès est un levier clé de souveraineté.

Sécuriser les accès à privilèges (moindre privilège, MFA, coffre-fort, traçabilité) réduit la surface d'attaque, conformément aux recommandations de l'ACPR.

Pourquoi le secteur bancaire est-il particulièrement concerné par la dépendance technologique ?

Longtemps perçu comme un simple risque technique, les établissements bancaires doivent désormais envisager leurs dépendances technologiques sous le prisme du stratégique.

Ce sujet ne relève plus aujourd'hui de l'unique responsabilité du DSI ou du RSSI, mais aussi de celle de la direction générale et du conseil d'administration, tant les conséquences peuvent être sévères pour ces infrastructures.

Ces quarante dernières années, le secteur de la banque et de la finance a saisi toutes les innovations technologiques, en s'appuyant sur un nombre restreint d'acteurs, souvent américains.

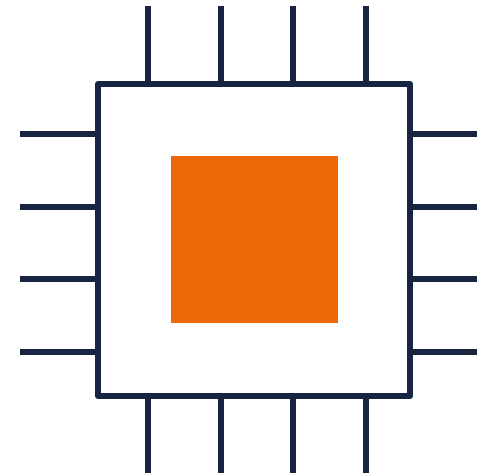
Ces derniers sont soumis à des législations extraterritoriales, comme le Cloud Act ou la section 702 du FISA, qui peuvent permettre à des autorités étrangères d'obtenir l'accès à des données qu'ils hébergent, y compris si elles sont stockées en Europe.

En quoi la démocratisation de l'intelligence artificielle a-t-il renforcé la dépendance technologique du secteur bancaire ?

L'adoption de l'intelligence artificielle a amplifié le côté stratégique de ce risque porté par les dépendances.

Avec l'usage de l'IA générative, le « capital informationnel » des banques (ses données clients, ses modèles de risque, ses processus internes, ses savoir-faire métier) circule vers des fournisseurs tiers par le biais de requêtes, de documents uploadés, d'intégrations dans les outils de travail ou d'usage non encadré (« shadow AI »).

C'est bel et bien une nouvelle dimension de la dépendance : il ne s'agit plus de louer de la puissance de calcul, mais de confier une partie de son intelligence métier à des modèles qu'on ne maîtrise pas.

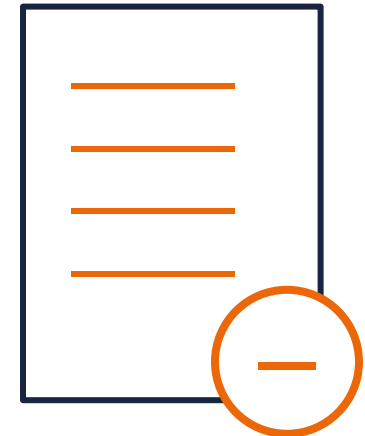


Celle-ci a un impact sur la confidentialité et la conformité, mais peut aussi créer une perte d'avantage concurrentiel sur le long terme.

Le risque de dépendance technologique est-il pris en compte dans la régulation ?

Les régulateurs ont pris très au sérieux ces nouveaux risques.

Applicable depuis 2025, le règlement européen DORA crée un régime de supervision directe des prestataires informatiques jugés critiques par les autorités européennes de surveillance. C'est une nouveauté législative : le régulateur s'intéresse donc directement aux fournisseurs, et plus seulement aux banques. Du côté du Data Act européen, celui-ci prévoit des obligations facilitant le changement de fournisseur cloud et la suppression progressive des frais de changement.





Cela s'oppose à une stratégie de « vendor lock-in » mis en place par certains acteurs pour conserver leurs clients coûte que coûte (retenir le client en lui imposant des coûts de sortie élevés, en réduisant son pouvoir de négociation au fil des ans ou en créant une forte intégration entre tous les services du fournisseurs).

Enfin, l'AI Act encadre progressivement les usages de l'IA, y compris certains cas d'usage bancaires comme l'évaluation de la solvabilité. Le régulateur ne demande pas aux banques de tout internaliser, il leur demande de rester maîtres de leurs choix.

Doit-on couper tout lien avec les fournisseurs étrangers pour gagner en souveraineté ?

Une vision simpliste de la souveraineté consisterait à couper tout lien avec des fournisseurs étrangers et à tout internaliser, mais ce n'est pas une solution viable pour les établissements bancaires. Être souverain réside avant tout dans la capacité de décider, de vérifier et de reprendre la main tout en étant en ligne avec ses enjeux.

C'est d'ailleurs cela que l'on peut relever dans le règlement DORA, puisque le texte législatif a pour objectif de rappeler que la responsabilité ne se délègue pas. Ainsi, une banque qui externalise ses infrastructures garde la responsabilité de ses activités.

**L'important est que le système puisse être audité,
quelle que soit sa localisation, preuve qu'on le
maîtrise vraiment.**

La maîtrise des accès est un enjeu de souveraineté

La souveraineté du système d'information passe aussi par la maîtrise des accès : qui peut accéder à quoi, et quand ? Les établissements bancaires sont administrés par des humains, mais aussi de plus en plus par des machines, qui peuvent accéder à ses ressources et conduire des actions.

Les accès à privilèges sont un peu comme les « clés du coffre-fort » : ils permettent à ceux qui en ont les droits de modifier, d'extraire ou de supprimer des données et des configurations critiques.

Ils doivent être contrôlés et protégés, car ils suscitent l'intérêt des attaquants qui, s'ils parviennent à compromettre un compte administrateur, peuvent contourner une grande partie des protections du système.



Plus il y a d'accès actifs, plus la surface d'exposition est étendue.

Comment mieux maîtriser ses accès ?

L'ACPR abonde en ce sens : elle insiste fortement sur l'importance de sécuriser ses accès et réduire la surface d'exposition. Elle traduit cela en plusieurs bonnes pratiques :

- 1 Appliquer le principe du moindre privilège : chacun n'a que les droits nécessaires à sa mission ;
- 2 Privilégier des accès temporaires (« juste à temps ») plutôt que permanents ;
- 3 Imposer une authentification forte (« MFA ») pour tout accès sensible ;

Comment mieux maîtriser ses accès ?

Parmi la liste des bonnes pratiques de l'ACPR, quatre d'entre elles correspondent particulièrement à la gestion des accès privilégiés (PAM) :

Supprimer les mots de passe partagés ou connus des utilisateurs et les gérer dans un coffre-fort ;

Centraliser les accès dans un point de passage unique et contrôlé ;

Tracer et enregistrer les sessions sur les systèmes critiques ;

Revoir régulièrement les droits et révoquer ceux qui ne sont plus justifiés.

DORA impose par ailleurs des politiques formalisées de gestion des accès et des droits d'audit sur les prestataires liés aux technologies de l'information et de la communication.