

Deloitte.



Banking Trends 2023

Mai 2023

Sommaire

01

**Perspectives réglementaires
des marchés financiers 2023**



02

**Le pilotage des trajectoires
de décarbonation**



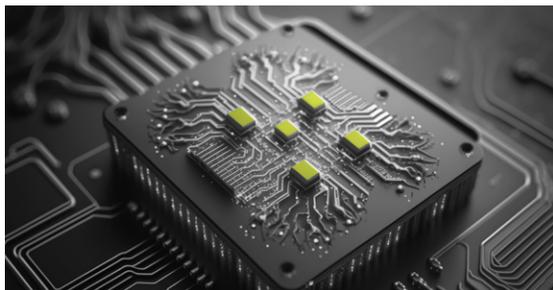
03

Les enjeux de la DeFi



04

**Envisager de nouvelles façons de
servir et d'engager les clients *via* l'IA
multimodale**



05

Transformation cloud



Introduction

Le début de l'année 2023 a été marqué par la faillite de Silicon Valley Bank (SVB), le rachat de Crédit Suisse, en grande difficulté, par UBS et plus récemment la reprise de First Republic Bank par JP Morgan Chase. Ces événements ont fait craindre une contagion à l'ensemble du secteur bancaire avec en filigrane le spectre de la crise de 2008-2009 ! Que nenni ! La situation a bien changé. Les exigences prudentielles que ce soit en capital et liquidité avec la finalisation du paquet bancaire et la mise en œuvre de CR2/CRDV fin 2021 et bientôt de CRR3/CRD6 garantissent, au moins pour les banques en Europe, une solidité financière et les marges de manœuvre en cas de crise. Cela a permis de vite rassurer les marchés, malgré quelques jours d'agitation, et la situation est désormais apaisée.

Dans ce contexte, les banques vont poursuivre la réinvention de leur modèle dans un monde post-Covid-19 :

- des facteurs sociaux et environnementaux devenant la pierre angulaire de la stratégie des banques dans un monde où l'économie se décarbone et où les clients attendent de leurs banques que leur argent soit utilisé pour la transition climatique ;
- une adaptation aux nouveaux usages des clients notamment autour des actifs numériques ou du Web 3 ;
- la nécessité de réduire encore les coûts – les sujets de rentabilité étant toujours d'actualité en misant notamment sur le digital.

L'heure est maintenant à l'opérationnalisation de ce nouveau modèle, opérationnalisation qui s'articule autour de trois axes :

1. Intégration des indicateurs ESG dans le dispositif de pilotage de la performance ;
2. Digitalisation des processus via l'intelligence artificielle ou le cloud ;
3. Adaptation des dispositifs de gestion des risques aux nouveaux types de risques (climatique, cyber, etc.).

Cette nouvelle édition des banking trends est l'occasion de revenir sur quelques illustrations des enjeux et des tendances liés à la mise en œuvre de ce nouveau modèle d'activité :

- **un pilotage des trajectoires de décarbonation à mettre en place.** Outre la mesure de l'empreinte carbone, il s'agit également de faire le lien avec les indicateurs traditionnels de risque et de rentabilité. C'est bien de décarboner, il faut cependant rester rentable et ne pas dépasser ses limites de risque !
- **saisir les opportunités de la finance décentralisée (DeFi) tout en gérant les risques induits par celle-ci.** La DeFi est porteuse de nouvelles opportunités en termes de développement de produits

ou de transformation des processus financiers notamment en matière de paiement ou d'exécution ou de conservation. Les banques devront néanmoins adapter leur gestion des risques à la DeFi : des risques technologiques et cyber significatifs, des modélisations différentes des risques financiers, un environnement encore trop peu régulé avec des risques de conformité ou fiscaux.

- **une relation client qui se réinvente grâce à l'intelligence artificielle multimodale.** L'IA multimodale popularisée par ChatGPT est considérée comme le facteur qui impactera le plus le modèle de la banque de détail dans les années à venir. Elle transformera radicalement les modalités d'interaction avec les clients et simplifiera un très grand nombre d'étapes du parcours client (réclamation, authentification, etc.). C'est aussi une opportunité pour attirer une clientèle jeune avec des produits et des applications spécialement développés pour elle. Son développement nécessite cependant de repenser le rôle du conseiller et sa façon d'interagir avec les clients.
- **le cloud : colonne vertébrale du nouveau modèle opérationnel bancaire !** La digitalisation des banques ou leur succès en matière d'innovation dépendent aujourd'hui du *cloud computing*. Le cloud, outre une performance accrue à un coût nettement moindre, est aussi un moyen pour les banques de conquérir de nouveaux marchés et de s'ouvrir à leur écosystème. Ces transitions au cloud doivent cependant s'accompagner d'une réflexion sur la souveraineté numérique au même titre que la compétitivité, la sécurité, la réversibilité, la responsabilité numérique (ESG).

Les attentes du régulateur évoluent aussi pour accompagner cette transformation tout en étant attentif au contexte économique actuel. Cela se traduit par des réglementations traitant spécifiquement des aspects liés à la digitalisation et aux cryptoactifs (DORA, MiCA, Digital Market Act) ou à la transition climatique. Compte tenu du contexte d'augmentation des taux et inflationniste, l'accent est également mis sur la mesure du risque de crédit et la transparence sur les pratiques tarifaires.

2023 est marquée pour les banques par des enjeux forts en matière d'opérationnalisation de leur nouveau modèle fondé sur le développement des produits répondant aux nouveaux usages, notamment DeFi ou produits à impact. Cette opérationnalisation s'appuie sur la digitalisation au travers de l'IA multimodale ou le cloud ainsi que le déploiement de nouveaux dispositifs de pilotage de la performance et des risques comme les trajectoires de décarbonation ou les plans de transition.



01

02

03

04

05



01

Perspectives réglementaires des marchés financiers 2023



01

02

03

04

05



Nouveau devoir du consommateur - mise en place de nouvelles protections

Les superviseurs et les régulateurs restent attentifs aux conséquences du contexte économique et de l'inflation sur les clients. Afin de garantir aux consommateurs une transparence totale sur les pratiques tarifaires, les institutions financières doivent s'assurer de la qualité de leurs différents processus qui vont être davantage contrôlés en 2023.



- La récente augmentation de l'inflation dans l'UE peut avoir un impact sur les clients de détail. L'ESMA prévoit que les entreprises sensibilisent les clients à ce risque en fournissant des informations, effectuant des évaluations d'adéquation et mettant en place des processus de gouvernance des produits.
- Suite à l'action de supervision commune de l'ESMA sur les coûts et charges MIFID II, nous attendons en 2023 un retour d'information *via* la publication d'un rapport dédié.
- L'Autorité a également demandé aux Autorités nationales d'examiner les processus de tarification des gestionnaires de fonds pour identifier les manquements (principes et formalisme). Les sociétés devraient s'attendre, dès le premier semestre, à une surveillance accrue en raison de l'importance accordée à la prévention des coûts non justifiés.



01

02

03

04

05



Risque de crédit

Des perspectives économiques et financières plus incertaines pèsent sur le risque de crédit.



Particuliers

Les hausses significatives des taux d'intérêt, combinées à d'autres pressions inflationnistes, pèsent sur les revenus des ménages qui s'attendent par ailleurs à ce que leur situation financière se détériore en 2023. Alors que, les données de la BCE confirment le principe empirique que les ménages disposant des revenus les plus bas ont le moins d'actifs liquides disponibles, les entreprises devront continuer à concilier leurs obligations de traiter les clients de manière équitable, tout en répondant aux attentes de leurs actionnaires de minimiser les pertes.

Entreprises

Un contexte économique moins dynamique et des préoccupations sur les coûts de production entraînent des pressions sur les chiffres d'affaires et la rentabilité des entreprises, avec, potentiellement, des capacités de remboursement plus réduites et des structures financières plus fragiles. Les superviseurs sont par ailleurs préoccupés par le volume croissant de l'exposition des banques à la dette à effet de levier. Les établissements devront donc être en mesure d'expliquer les modalités de gestion des risques associés.

Établissements financiers

Les banques doivent se préparer à une augmentation des dépréciations en 2023, tout en étant vraisemblablement invités par les autorités politiques, monétaires, voire les superviseurs, à continuer à prêter et à investir afin de soutenir l'économie. Concilier ces deux objectifs induira d'une part un besoin de documenter plus précisément les décisions stratégiques et orientations afin d'être en mesure de justifier des conditions d'octroi plus restrictives, et d'autre part à renforcer les dispositifs de financement et de pilotage des risques afin de prévenir ou faire face à la hausse du risque de solvabilité.



Capital réglementaire

Les banques sont confrontées à une refonte importante du cadre réglementaire pour les fonds propres, dont la forme définitive sera disponible en 2023. L'UE devrait ainsi mettre en œuvre Bâle 3.1 avant le 1^{er} janvier 2025, soit deux ans après l'échéance initiale.



- La publication des règles finales permettra aux banques d'analyser l'impact sur leur positionnement stratégique, leur consommation de capital et leur rentabilité. Par ailleurs, à mesure que les règles seront finalisées, les banques actives à l'international auront une vision plus précise des problématiques liées à la fragmentation réglementaire et aux divergences entre pays.
- L'UE a proposé des dérogations par rapport aux normes du Comité de Bâle, telles que : l'application du plancher minimum de capital au niveau du groupe, le traitement des entreprises non notées, les exemptions CVA pour les entreprises emprunteuses, la prolongation de la période de transition pour le plancher minimum de capital et, enfin, l'UE applique des règles uniformes à l'ensemble des établissements de crédit.
- En ce qui concerne la CRD6/CRR3, la position générale adoptée par le Conseil de l'Union européenne en novembre 2022 prévoit : la simplification des exigences pour les succursales de pays tiers, l'application du plancher minimum de capital à tous les niveaux de consolidation, l'affirmation du soutien aux modifications des dispositions relatives à l'aptitude et l'intégrité des dirigeants (*fit and proper*), la reconnaissance des garanties publiques résultant de l'ère Covid-19, et le soutien à l'amélioration du reporting ESG.
- De nouvelles dérogations au cadre de Bâle restent possibles. En termes de processus, les négociations de l'UE sur le « paquet bancaire CRD6/CRR3 devraient se conclure au cours du second semestre 2023.
- Les banques devront renforcer les capacités qui soutiendront la mise en œuvre de Bâle 3.1 en se concentrant principalement sur la précision des calculs des emplois pondérés et le développement de nouvelles capacités de gestion des données et de reporting.



Gestion des risques liés aux modèles

De plus en plus de modèles sont utilisés dans le secteur financier, historiquement pour faciliter la gestion des risques dans les domaines du crédit ou de la solvabilité. En même temps, d'autres défis de modélisation concernant les risques climatiques, la lutte contre la criminalité financière et l'utilisation de l'IA/ML apparaissent. Cependant, ils ne sont pas toujours compris, et les superviseurs tiennent à s'assurer que les établissements restent autonomes dans leur compréhension et leur prise de décision.



Compte tenu des conditions économiques (taux d'intérêt, inflation), des modèles tels que IFRS 9 et IRRBB suscitent des interrogations. Les autorités s'inquiètent notamment de leur fiabilité et de leur capacité à résister aux variations des taux d'intérêt.

En matière de gestion du risque climatique, les régulateurs et les superviseurs s'attendent en 2023 à ce que les établissements :

- intègrent les risques climatiques dans leur modélisation des risques et des tests de résistance conformément aux normes ;
- fournissent des modèles supplémentaires pour démontrer que la dépréciation des actifs établie conformément à IFRS 9 est appropriée dans le contexte des risques financiers liés au changement climatique ;
- diversifient les sources de données pour en garantir la disponibilité et la qualité afin d'obtenir des résultats pertinents.

D'autres risques découlent de l'intégration de l'IA/ML dans les modèles. Les banques devraient se doter d'équipes spécialisées pour garantir la validité de ces modèles d'IA/ML, et s'assurer que les informations tirées de ces modèles ne soient conçues que comme une aide à la prise de décision.

Plus généralement, la surveillance de la conformité et de la sécurité financière s'appuie sur des modèles statistiques qui devront faire l'objet d'une surveillance appropriée.

Dans l'année à venir les superviseurs devront trouver des moyens d'augmenter leur capacité à examiner les modèles sans compromettre leur capacité à couvrir les autres thèmes. Quant aux établissements, il est recommandé d'investir dès maintenant afin d'éviter de devoir subir la pression des autorités à l'avenir.



Marchés des capitaux

Les régulateurs s'inquiètent des risques liés à la forte volatilité des prix et aux perturbations brutales de la liquidité du marché depuis la *dash for cash* de mars 2020, à la suite de laquelle les banques centrales ont dû intervenir à grande échelle pour rétablir l'ordre sur le marché.



Certains superviseurs sont préoccupés par le fait que les origines de l'instabilité du marché résident dans le fait que les acteurs n'ont pas suffisamment appris des dernières crises financières mondiales. Ces préoccupations amènent les superviseurs à se concentrer sur trois questions distinctes, mais ayant des liens entre elles :

- **Les cadres de gestion des risques de crédit des contreparties des banques**

Les superviseurs s'attendent à ce que les banques renforcent l'analyse du risque de concentration non seulement pour chaque client, mais aussi pour l'ensemble des clients combinés et, surtout, de la sensibilité d'un portefeuille de clients donné à des activités ou actifs. Cela exigera des entreprises qu'elles collectent significativement plus de données qu'elles ne le font actuellement, tandis que leur capacité à le faire dépendra en partie de la volonté des contreparties de les fournir.

- **Appels de marge, y compris la gestion des garanties**

À court terme, nous nous attendons à ce que les autorités de surveillance examinent la capacité de tous les types d'établissements régulés à gérer leurs appels de marge, en modélisant les entrées et les sorties de garanties, dans une série de scénarios, et en testant leur capacité à mobiliser des liquidités pour répondre aux appels de marge dans des conditions normales et difficiles.

- **L'efficacité des organisations, des modèles de comptabilisation et de la gestion des risques associés**

Les superviseurs ayant renforcé leurs attentes avec des exigences prudentielles plus élevées, les établissements sont invités à investir de manière significative pour éliminer toute complexité inutile et améliorer leurs processus. Des progrès restent à faire pour certains établissements, par exemple en termes structures juridiques, de modèles de booking, portefeuilles d'activités, gouvernance, etc. Nous ne nous attendons donc pas à un relâchement de la vigilance des autorités de contrôle dans ce domaine.

Dans l'UE, l'accent mis par les autorités de surveillance sur les acteurs des marchés de capitaux a été complété par la révision de l'EMIR par la Commission européenne, qui a publié une série de propositions visant à développer l'Union des marchés de capitaux de l'UE. Ces propositions comprennent des modifications de la législation visant à rendre les services de compensation de l'UE plus attrayants et plus résistants, à harmoniser certaines règles d'insolvabilité des entreprises dans l'ensemble de l'UE et à alléger la charge administrative des sociétés cotées en Bourse.



01

02

03

04

05



Résilience opérationnelle et tiers critiques

Maintenant que DORA a été adopté, les entreprises doivent désormais se concentrer sur la mise en œuvre des exigences en matière de résilience opérationnelle, avec des autorités de surveillance qui suivront les progrès réalisés.



- Le déploiement du règlement sur la résilience opérationnelle (DORA) débutera cette année, la date limite de mise en conformité étant fixée à Janvier 2025. Si certaines des attentes sont similaires à celles formulées dans les lignes directrices en vigueur, d'autres sont beaucoup plus engageantes. Il sera important pour les acteurs de suivre les publications de normes techniques réglementaires prévues d'ici à fin 2024.
- Les superviseurs de l'UE étendent leurs compétences relatives au risque cyber et informatique, 2023 devrait donc être l'année des enquêtes ciblées cyberrésilience.
- Les régulateurs devraient accorder une attention particulière aux prestations et tiers critiques. Afin de répondre aux attentes des autorités de surveillance, les établissements doivent approfondir la connaissance de leurs fournisseurs critiques, et élaborer des stratégies de sortie et des plans de continuité des activités.
- La cyberrésilience est également une question essentielle car la proposition de loi sur la Cyberrésilience (CRA) pourrait se concrétiser avant la fin de 2023. L'adoption de cette nouvelle réglementation inclurait le secteur financier dans son champ d'application et créerait donc de nouvelles obligations pour les établissements.



Actifs et paiements numériques

Malgré un fort engouement pour les actifs numériques, les marchés ont connu d'importantes perturbations en 2022. En conséquence, les décideurs européens ont continué à façonner leurs futurs cadres réglementaires pour cette classe d'actifs notamment par le biais du règlement sur les marchés des crypto-actifs (MiCA).



- Le MiCA finalisé, prévu pour le T1 2023, couvrira la majorité des entreprises d'actifs numériques non réglementées et les aidera, ainsi que leurs homologues traditionnels, en harmonisant le cadre réglementaire de l'UE. Les principaux sujets sont les instruments financiers tokenisés (par exemple les obligations), les actifs numériques non garantis (par exemple le bitcoin) et surtout les stablecoins (par exemple Circle USDC).
- Le principal sujet relatif aux instruments financiers tokenisés est la collaboration entre banques et fournisseurs de blockchain afin de fournir des services d'émission/conservation. Les actifs numériques non adossés seront affectés par MiCA qui prévoit une réglementation complète des intermédiaires. Enfin, MiCA vise à réglementer les stablecoins adossés à une monnaie fiduciaire ou à un autre actif.
- Actions attendues des entreprises d'actifs numériques européennes : effectuer un *gap analysis* des exigences réglementaires et évaluer leur impact. Décider de devenir une société de services financiers réglementée ou de poursuivre d'autres options.
- Actions attendues des entreprises de services financiers déjà régulées en UE : revoir et renforcer la gestion des risques liés aux relations directes ou indirectes avec les acteurs de blockchain. Mettre à jour la déclaration d'appétence pour le risque afin de refléter les risques liés aux actifs numériques. Mettre en place des compétences de gouvernance dédiées aux actifs numériques et renforcer les capacités d'audit et de contrôle sur ce domaine.



01

02

03

04

05



Zoom sur les données

2023 marquera la date d'entrée en vigueur de la loi européenne sur les marchés numériques (Digital Market Act), qui introduira des mesures visant à limiter les comportements anticoncurrentiels des gardiens du numérique désignés par la Commission européenne.



- Les entreprises auront jusqu'au début de 2024 pour se mettre en conformité et de nombreux détails ne seront précisés que dans la législation de second niveau qui est à venir.
- Les plateformes numériques et technologiques mondiales, telles que celles qui fournissent des services cloud ou en ligne, sont susceptibles d'entrer dans le champ d'application.
- Certaines des mesures de la DMA sont susceptibles de soutenir la concurrence dans les services financiers numériques



01

02

03

04

05



Criminalité financière

Pour de nombreuses institutions financières, les attentes des autorités concernant leurs dispositifs de lutte contre la criminalité financière ne sont pas encore pleinement satisfaites. Cette situation s'explique par un contexte de renforcement des exigences, de l'émergence de nouveaux risques, de la sophistication des dispositifs mis en œuvre et des modalités de contrôle.



Les institutions financières doivent toujours faire face à de nombreuses contraintes telles que le volume considérable d'alertes générées (majorité de faux positifs), les limites inhérentes aux systèmes existants, des enquêtes continues et approfondies des autorités de contrôle et le renforcement et l'évolution constante des attentes réglementaires et de l'environnement externe.

Les mesures suivantes seront requises pour sécuriser les dispositifs :

- **Revue du modèle opérationnel**

Une évaluation des dispositifs et outils existants doit être réalisée en vue de déployer des solutions plus avancées. L'intelligence artificielle et l'apprentissage automatique doivent être intégrés dans les programmes des institutions financières. On peut s'attendre à des changements chez les fournisseurs historiques de solutions alors que de nouveaux acteurs émergent.

- **Révision des stratégies technologiques en matière de criminalité financière**

Les méthodes de travail doivent être revues, notamment concernant la définition des processus, de gouvernance et de traçabilité. Le changement d'organisation et la mise à disposition de nouvelles ressources sont au cœur des actions à mener.

- **Période de transition pour l'incorporation de l'AMLA**

2023 sera une période de transition pour incorporer l'AMLA dans le paysage financier européen, la nouvelle autorité devant être opérationnelle en 2024



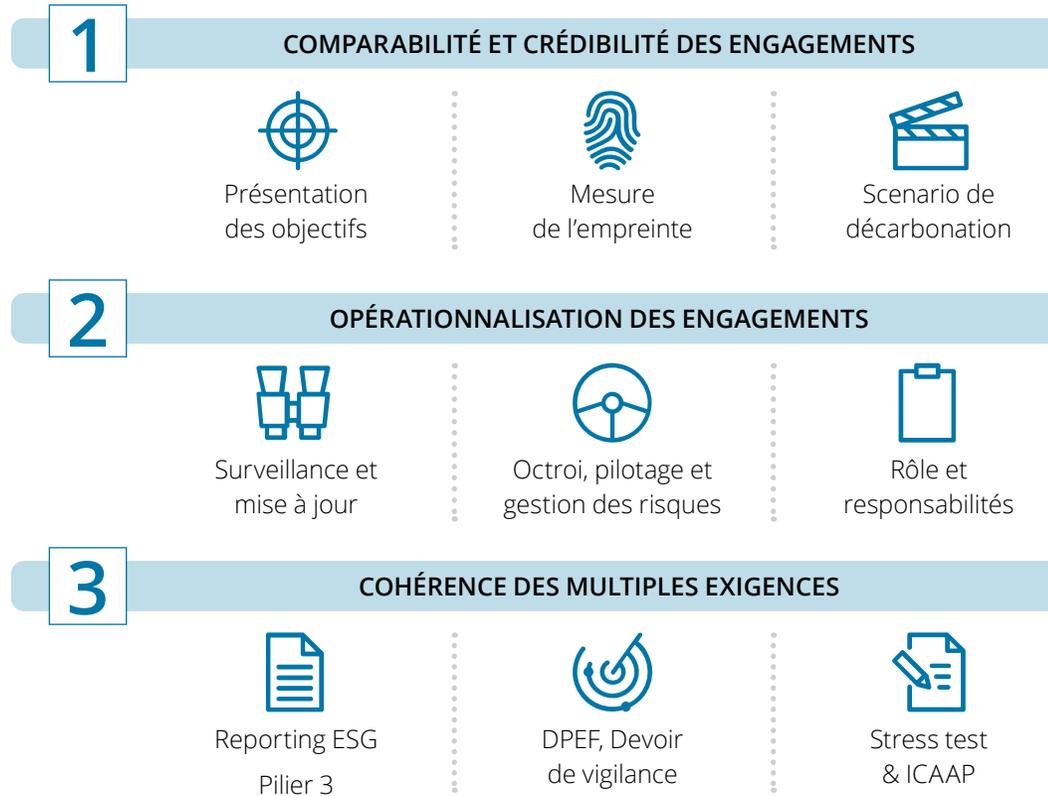
Le pilotage des trajectoires de décarbonation



2023 est une année cruciale pour le respect des engagements 2030

- Les banques sont de plus en plus nombreuses à publier leurs engagements de décarbonation sur les portefeuilles de prêts des secteurs carbo-intensifs.
- Il y a aujourd'hui le développement de bonnes pratiques sur la méthode de calcul des empreintes ou les scénarios de décarbonation à retenir.
- La mise en œuvre opérationnelle notamment le lien entre les trajectoires de décarbonation et les impacts financiers (évolution des encours, du coût du risque, des revenus, etc.) sont les jalons forts de l'année 2023.
- La formation des équipes est le levier à ne pas sous-estimer pour accélérer la transition et la maîtrise des risques.

Les challenges 2023



01

02

03

04

05



Les engagements exprimés seulement en intensité physique rendent complexes les liens avec l'activité de la banque et donc leur crédibilité.



Présentation des engagements

- L'approche généralement utilisée consiste à couvrir les secteurs les plus émissifs en CO₂. Toutefois, la présentation qui est aujourd'hui réalisée par les banques ne permet pas d'appréhender la part que représentent les engagements sur la totalité des émissions financées et des encours.
- Les engagements exprimés seulement en intensité physique rendent complexes les liens avec l'activité de la banque et donc leur crédibilité. **Notre conviction est que la traduction de ces engagements sous forme d'émissions en valeur absolue et d'encours financés est indispensable tant pour la communication externe que le pilotage interne.**



La mesure de l'empreinte

- Les travaux de standardisation des modalités de mesure d'empreinte par PCAF* ou la FBF* sont indispensables pour promouvoir une méthode homogène de mesure d'empreinte. Il demeure toutefois de nombreuses zones d'incertitudes.
- **Notre conviction est que les établissements bancaires doivent aujourd'hui communiquer précisément et en toute transparence sur les approches retenues pour les mesures d'empreinte et les limites associées. La prime à la transparence surtout lorsque les pratiques se structurent à une valeur importante pour les banques pionnières.**



Les scénarios de décarbonation

- Les scénarios de décarbonation, aussi reconnus soient-ils, s'appuient tous sur de nombreuses hypothèses.
- L'analyse fine de ces hypothèses et surtout ce qu'elles induisent sur les leviers de pilotage des acteurs bancaires sont aujourd'hui vitaux. Il peut par exemple s'agir d'une hypothèse forte sur l'évolution du mix énergétique d'un pays, sur l'évolution du comportement des clients (tout le monde devient vertueux) ou sur l'introduction de nouvelles technologies.
- Toutes ces hypothèses sont structurantes et absolument pas entre les mains des institutions financières. Toutefois, elles devront expliquer pourquoi elles ne sont pas en mesure de suivre la trajectoire cohérente avec le scénario à un moment ou un autre.
- **La pleine maîtrise des scénarios par l'ensemble des parties prenantes fera la différence sur la crédibilité des engagements pris.**



2

OPÉRATIONNALISATION DES ENGAGEMENTS

L'opérationnalisation des engagements nécessite de traduire les objectifs dans l'ensemble des processus de la banque avec parfois des challenges inédits.



Monitoring et mise à jour des trajectoires

- Calcul périodique des trajectoires
- Suivi du respect des engagements
- Évolution de périmètre
- Communication interne et externe
- Veille méthodologique
- Augmentation des données disponibles



Octroi, pilotage et gestion des risques

- Extension de l'horizon de gestion
- Pilotage des portefeuilles et arbitrage entre trajectoire CO₂ et rentabilité
- Identification des leviers de pilotage de la trajectoire :
 - les stratégies produits ;
 - les critères d'octroi ;
 - la gestion active des opérations.
- Détermination des politiques et limites sectorielles
- Adaptation des modèles de provisionnement



Rôle et responsabilités

- Équipe en charge du suivi de la trajectoire CO₂
- Équipe en charge de l'intégration dans les processus financiers
- Équipe en charge des données ESG

Nos cinq actions pour 2023

1. Mise en place de solution tactique et rapide pour calculer l'empreinte CO₂, la projection d'empreinte et l'écart à la trajectoire sur les périmètres concernés
2. Mise à disposition des solutions pour les équipes commerciales afin qu'elles intègrent ces éléments dans leur pilotage
3. Évolution des bases de données pour l'intégration des données climatiques des contreparties
4. Mise en place d'une équipe transverse en charge de la transformation des fonctions pour l'intégration des critères carbone
5. Intégration de l'empreinte CO₂ dans le budget 2023 et le plan moyen terme pour toutes les *business lines*



01

02

03

04

05



3

COHÉRENCE DES MULTIPLES EXIGENCES

Les engagements de décarbonation sont à la croisée de multiples exigences et parties prenantes, ce qui nécessite plus que jamais de former les collaborateurs à l'ensemble des enjeux des plans de transition.

- La communication d'éléments chiffrés autour des secteurs financés les plus émissifs est requise *via* de très nombreux canaux (green asset ratio, pilier 3 ESG, déclaration de performance extra-financière, etc.). À cela s'ajoute bien sûr la pression des associations, investisseurs, de la banque centrale européenne, etc.
- Le fonctionnement en silo de nombreux établissements bancaires tant pour les projets que les processus (reporting réglementaire, stratégie, communication financière, etc.) augmente fortement le risque d'incohérence et d'erreur.
- Au-delà des organigrammes et d'un énième département en charge, l'investissement dans la formation de l'ensemble des équipes (Direction des Risques, Direction Financière, Direction Métier, Conformité, etc.) à l'ensemble des sujets liés aux plans de transition est une action 2023 impérieuse pour tous les établissements

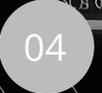
« Dans les bonnes pratiques observées, le plan de transition est utilisé comme un moyen de gérer les expositions des institutions au risque de transition. L'état d'esprit stratégique qui sous-tend ces efforts de planification permet aux institutions de mieux répondre aux risques sur des horizons temporels qui dépassent l'horizon usuel de gestion (généralement limité à trois à cinq ans). »

Source

BCE SSM, *Guide des bonnes pratiques sur la gestion des risques climatiques et environnementaux*, novembre 2022 – traduction libre



Les enjeux de la DeFi



Les réseaux Web 3 pourraient former une infrastructure financière plus résiliente et plus efficace

Certains professionnels de la finance considèrent la crise bancaire actuelle comme un signe d'affaiblissement du système, ce qui renforce la crédibilité de la décentralisation et des infrastructures qui l'accompagnent.

La récente vague de fermetures de banques aux États-Unis a mis en lumière la vulnérabilité du système bancaire traditionnel, incitant les experts du secteur de la cryptographie à plaider en faveur d'une infrastructure financière décentralisée comme alternative plus sûre et plus fiable.



Qu'est-ce que la « DeFi » ?

La DeFi est un terme générique pour les services financiers basés sur les réseaux-registres distribués (blockchains publiques sans permission), les réseaux Web 3, visant à fournir des services financiers sans intermédiaires financiers centraux ni institutions traditionnelles. Elle utilise des applications décentralisées (*dapps*) émettrices de jetons pour offrir ces services. La DeFi forme un système financier immuable et accessible avec une transparence sans précédent et des droits d'accès égaux entre tous les acteurs.

La finance traditionnelle (TradFi) a commencé à évoluer en raison des avancées numériques dans la jetonisation, donnant naissance à la finance centralisée (CeFi) qui utilise la blockchain (ou technologie assimilée de type DLT) tout en étant régie par des organismes centraux, et soumise à la réglementation (par exemple : portefeuilles hébergés PSAN en France). Les systèmes CeFi sont donc réglementés comme la TradFi, avec des organes de gouvernance centralisés responsables de la sécurité des transactions.

La DeFi, bien que pouvant chevaucher les services de TradFi et CeFi, fonctionne de manière largement décentralisée. Sa structure pair à pair limite la capacité d'une seule partie à modifier l'application et réduit le nombre d'intermédiaires dans les transactions. Comme la DeFi dessert désormais des clients dans des domaines traditionnellement dominés par la TradFi, tels que l'emprunt, le prêt et les échanges, son impact et son influence devraient continuer à croître, sous réserve des limites imposées par les autorités de régulation.



01

02

03

04

05



L'architecture Web 3 de la DeFi est nativement « ouverte » et « composable »



Couche d'agrégation

Plateforme centrée sur l'utilisateur qui se connecte à plusieurs applications et protocoles pour fournir des outils pour comparer et évaluer les services. Cela permet aux utilisateurs d'effectuer facilement des tâches complexes en se connectant à plusieurs protocoles simultanément.

Agrégateurs de rendement

Portefeuilles

Interfaces multiprotocoles



Couche d'applications

Interface orientée vers l'utilisateur proposant des produits et services financiers.

Emprunt/prêt

Produits dérivés

Assurance

Échanges décentralisés

Paiements

Gestion d'actifs



Couche de protocoles

Contrats intelligents, visibles publiquement, dont l'exécution permet de régir la façon dont les transactions ont lieu dans les applications DeFi. Ils fournissent les fonctionnalités sous-jacente des cas d'usage de la DeFi.

Contrats intelligents



Couche d'actifs

Actifs numériques émis pris en charge par les blockchains.

Jetons fongibles (interchangeables)

Jetons non fongibles



Couche de règlement

Les registres distribués des réseaux blockchain permettent le stockage sécurisé des informations relatives à la propriété et garantissent que tout changement respecte les règles de gouvernance et protocoles du réseau.

Bitcoin

Ethereum

BNB ...

Cardano

Solana

Tezos



01

02

03

04

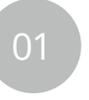
05



La DeFi se veut plus inclusive, plus pratique, plus transparente et plus automatisée

	TradFi	CeFi	DeFi
Accessibilité Facilité avec laquelle les gens peuvent accéder et utiliser le service financier	Opère par l'intermédiaire de succursales locales, régionales, nationales et dépend d'intermédiaires pour fournir des services	<ul style="list-style-type: none"> Favorise une portée mondiale Exigences minimales, voire inexistantes, en matière d'intermédiaires pour fournir des services 24 heures/24 et 7 jours/7 	<ul style="list-style-type: none"> Favorise une portée mondiale Exigences minimales, voire inexistantes, en matière d'intermédiaires pour fournir des services 24 heures/24 et 7 jours/7
Réglementation Niveau de cadre réglementaire dans lequel opère le service	Exigences élevées, notamment en matière d'agrément de la part des superviseurs (AMF et ACPR en France)	<ul style="list-style-type: none"> Nécessite un enregistrement PSAN en France Possible obligation d'agrément avec l'entrée en vigueur règlement européen MiCA 	Les entités de la DeFi sont peu réglementées, mais sont confrontées à l'incertitude réglementaire
Jetonisation Capacité des actifs corporels, tangibles ou non, à être convertis en jetons de blockchain	Jetonisation uniquement des titres financiers	Champs de jetonisation très vaste, sous forme de jetons d'utilité, de gouvernance, de stablecoins, de NFT...	Champs de jetonisation très vaste, sous forme de jetons d'utilité, de gouvernance, de stablecoins, de NFT...
Liquidité Capacité à démontrer une liquidité suffisante avec un mécanisme de tarification solide, des prévisions de liquidité et un plan de financement d'urgence	Forte liquidité de la plupart des marchés financiers (actions, obligations, devises)	Forte liquidité des échanges de cryptoactifs, même s'ils sont moins liquides que les marchés financiers traditionnels	Faible liquidité en raison de la nature émergente des applications DeFi et du nombre limité de mécanismes adoptés et testés par l'industrie
Gouvernance Solidité des structures de gouvernance et des protocoles définis pour les services et les opérations interentités	Structures de gouvernance traditionnelles bien définies avec un conseil d'administration, une direction, du personnel, des intermédiaires	La majorité des décisions est prise par les parties prenantes	<ul style="list-style-type: none"> Gouvernance décentralisée <i>via</i> des jetons de gouvernance qui permettent la prise de décision par droits de vote Risque de concentration asymétrique des jetons de gouvernance
Transparence Degré de disponibilité et de symétrie des informations disponibles dans le type de service financier	Transparence périodique, lorsque les informations financières périodiques sont rendues publiques	Moins d'informations rendues publiques que pour les institutions traditionnelles	Transparence en temps réel, toutes les données transactionnelles sont en permanence publiques
Contrat autoexécutés Utilisation de contrats autoexécutés dans la fourniture de services aux clients	Utilisation très faible ou nulle des contrats autoexécutés	Utilisation limitée des contrats autoexécutés dans certains domaines	Utilisation intensive de contrats intelligents, dont le codage contrôle le fonctionnement de l'application DeFi (<i>dapps</i>)

■ Alignement faible sur les facteurs définis
 ■ Alignement modéré sur les facteurs définis
 ■ Alignement élevé sur les facteurs définis



La DeFi offre des innovations de rupture à l'intégralité des services financiers (1/2)



Tenue de marché

Les applications de la DeFi peuvent être utilisées pour assurer des fonctions de tenue de marché. La transaction se fait par rapport à une réserve liquidité de cryptoactifs gérée par l'application plutôt que par rapport à des contreparties potentielles. Les contrats intelligents peuvent être utilisés pour surveiller la liquidité des cryptoactifs échangés et fournir des prix en conséquence.

Cas d'usage

Développement d'une réserve de liquidité pour un certain jeton, qui peut être négocié automatiquement par un algorithme plutôt que par le carnet d'ordres traditionnel.



Épargne/dépôts en cryptomonnaies

Les cryptoactifs détenus par des particuliers peuvent être ajoutés à des pools de liquidités gérés par les applications DeFi pour obtenir un rendement. Les contrats intelligents enregistrent l'ajout d'un actif à la réserve de liquidité, gèrent la durée de ces actifs et le remboursement correspondant du principal et du rendement en temps voulu.

Cas d'utilisation

Un particulier conserve des actifs cryptographiques dans le portefeuille de l'application DeFi, qui génèrent un rendement.



Conservation

Si certaines applications permettent aux utilisateurs de conserver eux-mêmes leurs cryptoactifs, d'autres fournissent des services de garde au sein de l'application, ce qui permet le contrôle de la gestion des actifs dans les contrats intelligents régissant l'application elle-même.

Cas d'utilisation

Les utilisateurs stockent des actifs numériques dans l'application DeFi, atténuant le risque de perte, de vol ou de données perdues, volées ou compromises.



Échanges

Les échanges en DeFi sont accessibles aux utilisateurs disposant de portefeuilles numériques non hébergés. La tarification est dynamique et basée sur l'offre et la demande des cryptoactifs échangés. Les contrats intelligents gèrent l'échange d'un cryptoactif contre un autre sans nécessiter de contrepartie.

Cas d'utilisation

Échanger des titres jetonisés sur une place de marché ouverte, facilitée par des contrats intelligents, sans qu'il soit nécessaire de compenser les transactions par l'intermédiaire d'une autorité centrale.



Gestion des actifs

Les protocoles de gestion d'actifs de DeFi sont mis en œuvre par des contrats intelligents qui regroupent les cryptoactifs déposés par des particuliers dans un portefeuille d'actifs numériques. Ils peuvent également inclure des jetons qui suivent les mouvements de prix d'actifs externes tels que les actions et l'immobilier qui dépendent d'oracles pour obtenir des informations sur les prix. Par rapport à la gestion d'actifs traditionnelle, cela promet une transparence et une efficacité accrues.

Cas d'utilisation

Un gestionnaire d'actifs facilite la tokenisation de l'immobilier commercial et négocie en tant que jeton fractionné afin d'obtenir l'accès à des liquidités supplémentaires qui lui étaient auparavant inaccessibles.



01

02

03

04

05



La DeFi offre des innovations de rupture à l'intégralité des services financiers (2/2)



Monnaies stables

Les applications DeFi peuvent être utilisées pour émettre des stablecoins, augmentant potentiellement la fiabilité en tirant parti de la blockchain ouverte pour permettre la transparence du collatéral sous-jacent. Bien que la nécessité de collatéraliser, ou d'ancrer, le stablecoin sous la forme d'un autre actif numérique (par opposition au fiat) puisse augmenter sa volatilité inhérente, des mécanismes tels que les algorithmes de contrats intelligents et la surcollatéralisation peuvent être utilisés pour atténuer ces risques.

Cas d'usage

Un stablecoin soutenu par un algorithme est développé et émis, rattaché au bitcoin ou à un autre actif de référence. Ce stablecoin peut alors permettre d'autres activités, telles que le commerce et le prêt en tant que bitcoin futur.



Produits dérivés

Les applications dérivées du DeFi mettent en relation directe les acheteurs et les vendeurs de produits dérivés. Les produits dérivés peuvent être créés à l'aide de contrats intelligents avec n'importe quel type d'actif tokenisé servant d'actif sous-jacent. Les exemples incluent les actions, les matières premières, les jetons non fongibles (NFT), et d'autres actifs numériques.

Cas d'utilisation

La volatilité des cryptomonnaies peut être couverte à l'aide de dérivés de cryptomonnaies tels que les contrats à terme sur le bitcoin.



Paiements

Les applications DeFi permettent d'utiliser des actifs numériques pour acheter des biens et des services, tant en B2C qu'en B2B. Par rapport au CeFi, il n'y a pas d'intermédiaires dans ce processus. Les applications de paiement permettent même la conversion automatique des actifs numériques de l'acheteur en une forme d'actifs numériques acceptée par le vendeur.

Cas d'utilisation

Les particuliers échangent des paiements en cryptomonnaies de pair à pair sans aucun intermédiaire.



Prêts

DeFi ouvre l'accès au crédit pour les institutionnels et les particuliers, avec moins de barrières à l'entrée. Les cryptomonnaies forment un pool de liquidités, qui peut ensuite être utilisé pour accorder des prêts aux emprunteurs qui peuvent accéder à ces liquidités en apportant divers actifs numériques en garantie. Les conditions sont régies par des contrats intelligents, qui enregistrent la garantie, distribuent les produits du prêt, dictent le rendement, acheminent les paiements du rendement de l'emprunteur au prêteur (sans marge intermédiaire) et conservent la garantie, y compris toute liquidation nécessaire découlant du dépassement d'un seuil ou d'une limite de ratio.

Cas d'utilisation

Une organisation établit un pool de cryptoprêts immobiliers, financé par des investisseurs particuliers et activé par des contrats intelligents qui déterminent le rendement et régissent les conditions de paiement, afin de financer un développement immobilier commercial.



Assurance

Les services d'assurance peuvent être fournis aux clients pour se couvrir contre les événements indésirables. Les clients paient des primes sous la forme d'actifs numériques, avec un montant de la demande d'indemnisation à verser si un événement prédéterminé, tel qu'enregistré dans le contrat intelligent, survient. Les personnes qui apportent le capital initial (généralement aussi sous la forme d'un actif numérique) obtiennent un retour sur investissement du capital excédentaire du pool d'assurance, sous réserve d'un risque de gain si les pertes dépassent les prévisions. Les contrats intelligents déterminent également la réalisation de l'événement assuré et régissent les primes ainsi que les paiements.

Cas d'utilisation

Les particuliers utilisent cryptomonnaie comme dépôt, dans une application DeFi, pour obtenir une assurance contre un événement particulier (par exemple, piratage d'un protocole DeFi ou contrat intelligent).



01

02

03

04

05



Les opportunités sont multiples...

Simplification du processus

La DeFi réduit la dépendance aux intermédiaires, qui sont actuellement nécessaires pour maintenir la confiance entre les participants à une transaction financière, et permet aux transactions d'être réglées directement entre les participants. En réduisant le nombre de parties impliquées et en rationalisant les opérations, l'efficacité des processus financiers peut être accrue.

Automatisation des processus

Les contrats intelligents permettent aux organisations d'automatiser les processus et les services par le biais d'une couche de protocole auto-exécutoire. Cette fonctionnalité offre aux organisations la possibilité de mettre à l'échelle certains services qui dépendaient auparavant de l'exécution humaine (par exemple, les approbations de prêts, les paiements de rendement, etc.), et de mieux adapter les services aux besoins des clients grâce à la flexibilité du code source.

Réduction des coûts de transaction

Le modèle d'interaction simplifié entre les participants de la transaction (par exemple, un emprunteur et un prêteur), géré par les protocoles sous-jacents intégrés dans les contrats intelligents, peut réduire les coûts de transaction pour les participants. Ce modèle peut aider les institutions financières à réduire les coûts opérationnels et le coût du service, offrant un avantage concurrentiel dans l'acquisition de clients. Les taux de rendement peuvent être plus attractifs qu'avec les banques traditionnelles, et la barrière à l'entrée (par exemple, la cote de crédit d'un emprunteur) pour emprunter est souvent plus faible par rapport à celle d'un système traditionnel. Bien que les participants doivent souvent payer une redevance pour effectuer des transactions sur un réseau,

cette « redevance » est souvent inférieure aux redevances courantes et aux autres conditions d'accès imposées par les institutions de TradFi aujourd'hui.

Contrôle accru

Les actifs sont stockés dans des comptes (c'est-à-dire des portefeuilles) non hébergés ou auto-hébergés, ce qui permet aux utilisateurs de bénéficier d'une plus grande autonomie, de contrôler leurs propres actifs et d'interagir directement avec un système de monnaie numérique au lieu de passer par un intermédiaire. Bien que la DeFi renforce les mécanismes de sécurité organisationnelle, les cybermenaces restent un risque important.

Transparence

La DeFi améliore la transparence en garantissant que la blockchain sous-jacente reste publique, tandis que les portefeuilles privés permettent aux utilisateurs de contrôler pleinement leur argent grâce à des « clés » non publiques, détenues à titre privé. Une transparence accrue peut permettre aux institutions financières d'améliorer leur expérience utilisateur et d'offrir à leurs clients une série d'informations et de produits mieux adaptés.

Règlements plus rapides

La technologie blockchain permet un règlement « instantané » en temps réel, offrant la possibilité d'éliminer les temps d'attente en matière de règlement. Dans de nombreuses formes traditionnelles, le règlement peut prendre jusqu'à trois jours alors que l'opération de compensation proprement dite ne prend que quelques secondes. Les applications DeFi peuvent réduire considérablement le temps de règlement, l'objectif étant de le faire passer de T+1 à T+0 (c'est-à-dire instantanément).

Liquidité

Le DeFi peut promouvoir l'inclusion financière, en atteignant les populations sous-bancarisées ou non bancarisées, grâce à un accès aux services sans permission et sans frontière. Cette connectivité mondiale accrue, associée à la possibilité d'adapter les services à toute personne disposant d'une connexion internet, pourrait également permettre aux institutions d'accéder à des réserves de liquidités qui n'étaient pas disponibles auparavant. Elle pourrait également servir à rationaliser la vérification du crédit et l'approbation des prêts. La tokenisation permettrait en outre aux organisations d'effectuer des transactions sur un large éventail d'actifs (par exemple, des actifs du monde réel), en introduisant la flexibilité nécessaire pour répondre aux besoins du marché et en permettant aux organisations de débloquer des capitaux et de générer des revenus supplémentaires.

Innovation facilitée

L'architecture ouverte, programmable et sans autorisation de la DeFi permet aux participants de visualiser et de vérifier les protocoles et de « forker le code » (c'est-à-dire de prendre le code source et de développer une utilisation indépendante par-dessus), ce qui permet de créer des services et des produits alternatifs et dérivés. L'accès au code source des protocoles DeFi permet aux utilisateurs de composer divers éléments pour créer des services et des instruments financiers qui répondent à leurs besoins spécifiques.



01

02

03

04

05



... et les risques se précisent à mesure que se dessine un nouveau système financier (1/2)

Risque technologique

La complexité technologique et la relative faible maturité de la DeFi augmentent ses vulnérabilités. Les réseaux blockchain et les protocoles à la base de la DeFi sont très hétérogènes, avec peu de normes et de standards et les attaques sur ces réseaux s'amplifient à mesure que ces infrastructures se développent. Les traitements en temps réel se heurtent parfois à la limite de capacité physique de la blockchain. En outre, la dépendance à l'égard des contrats autoexécutés expose les *dapps* DeFi à des dysfonctionnements logiciels et à des défauts générés par la complexité. Ce risque est aggravé par la dépendance aux oracles qui assurent l'alimentation du contrat autoexécuté en données externes, avec un risque d'inexactitude de ces données. La complexité requise pour permettre l'exécution efficace des applications DeFi présente un niveau de risque proportionnel, qui s'inscrit souvent dans un environnement non testé et non réglementé. L'absence de normalisation ou de mécanismes de contrôle de la qualité imposés par la réglementation ou adoptés par le secteur crée des incertitudes importantes dans le processus de conservation et de règlement.



Risque de sécurité (cybersécurité et fraude)

Les risques de sécurité liés aux accords DeFi comprennent la fraude, le détournement, les conflits d'intérêts, le blanchiment d'argent et le financement du terrorisme, ainsi que les risques d'intégrité du marché résultant d'une activité de négociation manipulatrice ou trompeuse. Les contrats intelligents, qui sont autoexécutés et développés manuellement, sont susceptibles de contenir des erreurs de codage qui peuvent être utilisées à mauvais escient par les utilisateurs d'un réseau *open source*. Les faiblesses du code source du contrat intelligent peuvent permettre à des acteurs malveillants d'exploiter l'application en siphonnant les actifs du réseau de manière unilatérale. En outre, les clés privées peuvent être mal gérées ou volées si les processus de récupération et les contrôles de sécurité appropriés ne sont pas mis en place. Bien que le risque de sécurité puisse être atténué par des audits préemptifs des modèles de contrats intelligents (y compris par des tiers indépendants) et par de multiples couches d'examen du codage, qui sont en train de devenir les meilleures pratiques de l'industrie, il y a toujours un manque général de surveillance réglementaire et de mécanismes de contrôle éprouvés pour fournir des garanties suffisantes.

Risque opérationnel et de gouvernance

Ces dispositifs présentent également des risques liés aux abus de marché et aux asymétries d'information résultant d'informations inexactes, limitées ou non standard (par exemple, les rapports sur les transactions et les prix) qui pourraient avoir un impact négatif sur les utilisateurs. Ces risques sont encore exacerbés par une possible dépendance à l'égard des fondateurs ou des propriétaires de protocole, dont le départ pourrait avoir un impact négatif sur l'application. Bien que le code informatique soit accessible de tous, ce qui offre une grande transparence, en réalité de nombreux utilisateurs n'ont pas les connaissances ou les ressources nécessaires pour interpréter efficacement le code et évaluer tout risque ou irrégularité associé, ce qui peut conduire à des abus. L'aspect décentralisé engendre des incertitudes sur le porteur des responsabilités et les recours en cas de défaillance. Les mécanismes de gouvernance, qui peuvent être programmés, introduisent souvent un degré d'imprécision et d'incertitude. Même si la programmation des règles de gouvernance les rend immuables (mécanismes de consensus et l'utilisation de jetons de gouvernance, jetons de gouvernance confèrent des droits de vote sur certaines décisions), des risques de fraude pourraient émerger si une petite quantité d'individus concentraient un grand nombre de jetons de gouvernance. Ils pourraient alors effectuer des fraudes, manipuler la blockchain ou du contrat intelligent à des fins de gain financier.



01

02

03

04

05



... et les risques se précisent à mesure que se dessine un nouveau système financier (2/2)

Conformité et risque juridique

L'incertitude réglementaire est l'un des défis de la DeFi car l'aspect décentralisé de ces organisations les rend difficile à réguler. Il est également complexe d'identifier le responsable en cas de défaillance. En tant que telle, la DeFi peut être utilisée pour contourner les obligations légales ou réglementaires et augmenter de facto la possibilité d'activités malveillantes. Cela est particulièrement vrai dans le cas des réglementations relatives à la fraude, à la manipulation du marché et à la criminalité financière (telles que BSA/AML, qui s'articule autour des exigences de connaissance du client et du contrôle des activités).

Risque financier

Alors que les risques financiers sont généralement gérés par divers mécanismes contenus dans TradFi et CeFi, sous l'impulsion des organismes de réglementation gouvernementaux, l'absence actuelle d'un régime réglementaire généralement applicable au DeFi (lois, réglementations, organismes de réglementation dotés d'un pouvoir d'interprétation, de supervision, d'examen et d'application) expose les applications DeFi à un degré plus élevé de risques financiers tels que le risque de crédit, le risque de liquidité, le risque de marché et le risque fiscal.

Risque de crédit

L'anonymat du réseau DeFi fait qu'il est difficile d'évaluer correctement le risque, de procéder à des vérifications préalables, de déterminer la solvabilité et de calibrer les taux d'intérêt appropriés des emprunteurs, ainsi que d'exercer un recours au-delà de la garantie fournie. La facilité de création des crédits et la volatilité des actifs numériques sous-jacents entraînent également un risque plus élevé de sous-collatéralisation tout en inhibant les processus d'appel de marge pour tenir compte de toute baisse de la garantie. Si ces risques peuvent être atténués par des exigences de surcollatéralisation, cette approche ne tient pas suffisamment compte de la cause première du problème (par exemple, l'absence de souscription de crédit concernant l'emprunteur ou de recours contre lui) et il est souvent difficile de l'étendre efficacement à l'ensemble d'un portefeuille.

Risque de liquidité

En l'absence d'échange centralisé ou de contrepartie, les services DeFi s'appuient souvent sur l'incitation des teneurs de marché à liquider les prêts sous-collatéralisés. Bien que ces mécanismes soient souvent intégrés dans la structure du programme DeFi, le fait de s'appuyer sur une logique de gouvernance et une conception programmatique prédéterminées limite la capacité des applications DeFi à répondre à des conditions de marché ou à des comportements de consommateurs imprévus. Les contreparties initiales et les fournisseurs de liquidités peuvent ainsi être confrontés à un risque de défaillance imprévu résultant de l'incapacité à remplir leurs propres obligations en matière de liquidité. La nature décentralisée de ces applications accroît également le risque d'inadéquation entre l'actif et le passif, qui serait généralement géré par des intermédiaires dans le cadre de TradFi.

Risque de marché

La structure inhérente à la DeFi augmente la possibilité de divers abus de marché, que ce soit par les créateurs de protocoles DeFi, les opérateurs d'échanges ou d'autres manipulateurs. La nature spéculative des cryptoactifs soumet la DeFi à une plus grande volatilité, car les chutes soudaines de la valeur des actifs numériques peuvent avoir un impact asymétrique sur les applications DeFi (par exemple, la vente rapide de jetons DeFi pourrait entraîner une baisse de la valeur de ces jetons). En outre, le pseudonymat des propriétaires d'échanges et des contrats intelligents rend difficile l'identification des sources de manipulation du marché ou de fixation incorrecte des prix.

Risque fiscal

Il existe encore peu d'indications sur l'imposition des actifs numériques et encore moins sur les implications des transactions utilisant les protocoles DeFi. Les utilisateurs doivent donc analyser chaque volet de la transaction pour déterminer lequel peut constituer un événement de reconnaissance (imposable) à des fins fiscales. En outre, en raison de son architecture variée et de l'absence d'accords juridiques, les utilisateurs de DeFi sont contraints d'analyser les règles énoncées dans le code pour déterminer le traitement fiscal. L'incertitude demeure également quant à la nature et à l'origine du rendement, ainsi qu'au moment où le rendement est comptabilisé dans les recettes. Le moment de la comptabilisation des revenus à des fins fiscales peut également dicter le montant des revenus à comptabiliser étant donné la nature volatile des évaluations des actifs numériques.



01

02

03

04

05



Envisager de nouvelles façons de servir et d'engager les clients *via* l'IA multimodale



01

02

03

04

05



Les impacts de l'IA multimodale sur le secteur bancaire

Popularisée en mars 2023 par Google PALM-E et OpenAI, ChatGPT-4, l'IA multimodale peut être qualifiée de révolution en raison de son potentiel à transformer radicalement la façon dont les machines interagissent avec les humains et traitent les données provenant de différentes sources.



Capacités de traitement de l'information

Contrairement aux systèmes d'IA traditionnels qui traitent une seule modalité de données (comme le texte ou les images), l'IA multimodale peut traiter et analyser plusieurs types de données simultanément (texte, audio, images, vidéo, etc.). Cela permet une compréhension plus profonde et holistique des informations, ce qui était auparavant difficile, voire impossible, pour les machines.



Imitation des capacités humaines

L'IA multimodale est capable d'imiter plus étroitement les capacités humaines de perception, de raisonnement et d'interaction. En combinant différentes modalités de données, l'IA multimodale peut appréhender et résoudre des problèmes complexes de manière similaire à celle des humains, offrant ainsi une expérience utilisateur plus naturelle et intuitive.



Amélioration de l'interaction homme-machine

L'IA multimodale permet des interactions plus fluides et naturelles entre les humains et les machines. Les systèmes multimodaux peuvent comprendre et répondre aux requêtes des utilisateurs en utilisant des méthodes de communication similaires à celles des humains, comme la parole, le texte et les gestes. Cela rend les interfaces utilisateur plus accessibles et conviviales pour un public plus large.



Innovation et disruption dans divers secteurs

L'IA multimodale a le potentiel de révolutionner une multitude de secteurs, tels que les services financiers, la santé, l'éducation, le commerce de détail, etc. En combinant les données et les compétences de différentes modalités, les systèmes d'IA multimodale peuvent améliorer l'efficacité, la personnalisation et la qualité des services dans ces domaines, créant ainsi de nouvelles opportunités commerciales et bouleversant les modèles économiques établis.



Accélération de la recherche et du développement en IA

L'IA multimodale représente une avancée majeure dans le domaine de l'intelligence artificielle, stimulant la recherche et le développement de nouvelles techniques et approches pour résoudre des problèmes complexes. Les progrès réalisés dans l'IA multimodale peuvent entraîner des avancées dans d'autres domaines de l'IA, tels que l'apprentissage automatique, la vision par ordinateur et le traitement du langage naturel.

Cependant, il convient de noter que l'IA multimodale présente également des défis et des risques, tels que la protection des données, la vie privée, les biais algorithmiques et l'éthique de l'IA. Pour que l'IA multimodale puisse être considérée comme une révolution véritablement bénéfique, il est essentiel de relever ces défis et de mettre en place des réglementations et des normes appropriées pour encadrer son utilisation.



01

02

03

04

05



Illustration

Lorsque nous posons à ChatGPT-4 la question des usages de l'IA multimodale dans la relation client bancaire, bien qu'en version « Bêta », sa réponse éclaire les bénéfices et les risques sous la forme du tableau suivant :

Service client automatisé *via* chatbots et assistants vocaux

Les clients interagissent avec un chatbot ou un assistant vocal basé sur l'IA, qui comprend et répond aux questions et résout les problèmes.

 Réduction du temps d'attente, disponibilité 24/7, coûts réduits

 Incompréhension, frustration utilisateur, protection des données

Analyse des sentiments des clients pour améliorer les interactions

L'IA analyse les communications écrites ou vocales des clients pour évaluer leur satisfaction et adapter les interactions en conséquence.

 Amélioration de l'expérience client, fidélisation

 Fausses interprétations, biais, atteinte à la vie privée

Gestion des réclamations *via* l'analyse d'images

L'IA utilise la vision par ordinateur et l'OCR pour extraire des informations à partir des images fournies par les clients et traiter les réclamations.

 Traitement plus rapide, précis et objectif des réclamations

 Erreurs d'analyse, protection des données, coûts de mise en place

Reconnaissance faciale pour authentification et sécurité

Les clients sont identifiés et authentifiés en utilisant la reconnaissance faciale, ce qui permet un accès rapide et sécurisé à leurs comptes.

 Accès rapide et sécurisé, réduction de la fraude

 Atteinte à la vie privée, erreurs de reconnaissance

Conseil en investissement personnalisé grâce à l'analyse des données

L'IA analyse les données financières et le profil des clients pour offrir des recommandations d'investissement personnalisées.

 Prise de décision éclairée, optimisation des investissements

 Biais algorithmiques, responsabilité en cas d'échec

Prévention de la fraude par l'analyse de données transactionnelles

L'IA examine les transactions en temps réel pour détecter les comportements suspects et prévenir la fraude.

 Réduction de la fraude, détection précoce, sécurité accrue

 Faux positifs, atteinte à la vie privée, coûts de mise en place

Amélioration de l'accessibilité grâce à la synthèse vocale et audio

Les informations textuelles sont converties en audio et vice versa pour faciliter l'accès aux services financiers pour les personnes malentendantes ou malvoyantes.

 Accessibilité renforcée, satisfaction client

 Coûts de mise en place, erreurs de synthèse



01

02

03

04

05



Le rôle du conseiller aux côtés de l'IA multimodale

Même si l'IA multimodale peut répondre en autonomie à de nombreuses attentes des clients, le rôle du conseiller reste important dans plusieurs aspects. Nous identifions plusieurs domaines où le conseiller bancaire continuera à jouer un rôle essentiel :



Gestion des situations complexes

Les conseillers peuvent gérer des situations qui nécessitent une compréhension approfondie des produits et services, et dispose de compétences en résolution de problèmes et en négociation. Les clients peuvent préférer discuter de questions sensibles, telles que les problèmes de crédit ou les investissements, avec un conseiller plutôt qu'avec une IA.



Relations personnalisées

Les conseillers peuvent établir des relations personnalisées et durables avec les clients, en comprenant leurs besoins, leurs préférences et leurs objectifs financiers à long terme. Ils peuvent offrir un soutien émotionnel et un service personnalisé que l'IA ne peut pas encore reproduire pleinement.



Conseil en matière de planification financière

Les conseillers peuvent aider les clients à planifier leur avenir financier, en tenant compte de leurs objectifs personnels, de leur situation familiale et de leur tolérance au risque. Ils peuvent fournir des conseils sur la planification de la retraite, l'épargne pour l'éducation, la gestion de patrimoine et la planification fiscale.



Éducation financière

Les conseillers peuvent aider les clients à comprendre les produits et services financiers, les risques associés et les meilleures pratiques en matière de gestion financière.



Identification des opportunités commerciales

Les conseillers peuvent utiliser leur empathie et leur expertise pour identifier de nouvelles opportunités commerciales, en proposant des produits et services adaptés aux besoins spécifiques des clients et en développant de nouvelles offres.



Gestion du changement et adoption des technologies

Les conseillers peuvent jouer un rôle important dans la gestion du changement et l'adoption des technologies d'IA multimodale, en aidant les clients à comprendre et à utiliser ces technologies de manière efficace et en fournissant des retours d'information pour améliorer les systèmes.



Supervision et contrôle des IA

Les conseillers peuvent assurer la supervision et le contrôle des systèmes d'IA multimodale, en vérifiant leur performance, en identifiant les erreurs et les problèmes, et en intervenant lorsque cela est nécessaire pour garantir la conformité et la satisfaction des clients.

Le rôle du conseiller évolue avec l'adoption de l'IA multimodale, mais leur sens de l'humain, leur compréhension des besoins et leur capacité à gérer des situations complexes, restent essentielles pour offrir un service bancaire de qualité. Les conseillers peuvent se concentrer sur les aspects les plus importants et les plus complexes de la relation, tout en tirant parti des technologies d'IA pour améliorer l'efficacité et la personnalisation du service.



01

02

03

04

05



Les opportunités pour les clientèles jeunes

Les jeunes générations sont plus à l'aise avec les technologies émergentes, telles que l'IA multimodale. Les banques peuvent utiliser l'IA multimodale pour mieux répondre aux attentes des jeunes, afin d'améliorer l'expérience client et proposer des services personnalisés et innovants.



Applications mobiles améliorées

Les banques peuvent intégrer des fonctionnalités d'IA multimodale dans leurs applications mobiles pour offrir une expérience utilisateur plus riche et interactive, en utilisant des assistants virtuels capables de comprendre et de traiter des requêtes en texte, audio, image ou vidéo.



Chatbots et assistants virtuels intelligents

L'IA multimodale peut être utilisée pour créer des chatbots et des assistants virtuels capables de comprendre et de répondre aux questions des jeunes clients en utilisant un langage naturel et des informations visuelles. Ces outils peuvent offrir un support instantané et personnalisé, en résolvant des problèmes courants et en fournissant les informations recherchées.



Outils d'éducation financière

Les banques peuvent utiliser l'IA multimodale pour créer des ressources éducatives interactives et engageantes, en combinant du texte, des images, de l'audio et de la vidéo pour expliquer des concepts financiers complexes de manière accessible et ludique.



Analyse des données clients

Les banques peuvent utiliser l'IA multimodale pour analyser les données clients provenant de différentes sources, telles que les transactions, les interactions sur les réseaux sociaux et les communications avec les conseillers. Cette analyse peut aider les banques à mieux comprendre les besoins, les préférences et les comportements des jeunes clients.



Marketing et communication ciblée

L'IA multimodale peut être utilisée pour créer des campagnes de marketing et de communication ciblées et personnalisées pour les jeunes clients, en combinant du texte, des images, de l'audio et de la vidéo pour créer des messages engageants et adaptés à leurs préférences.



Services personnalisés et recommandations

L'IA multimodale peut aider les banques à proposer des services personnalisés et des recommandations basées sur les données clients, en identifiant les produits et services les plus pertinents pour chaque individu et en anticipant leurs besoins futurs.



Détection de la fraude et de la cybercriminalité

L'IA multimodale peut améliorer la détection de la fraude et de la cybercriminalité en analysant les données provenant de différentes sources, telles que les transactions, les communications et les comportements en ligne. Cela peut aider les banques à protéger les jeunes clients contre les risques financiers et à renforcer la confiance.

En utilisant l'IA multimodale de manière créative et innovante, les banques peuvent améliorer l'expérience client, offrir des services personnalisés et répondre aux attentes spécifiques des jeunes clients, tout en renforçant leur compétitivité et leur attractivité sur le marché.



01

02

03

04

05



Transformation cloud



Synthèse

Les banques accélèrent leur adoption du cloud tout en veillant aux enjeux de compétitivité, de sécurité, de souveraineté, de réversibilité, de responsabilité (ESG) et d'opérationnalité du cloud computing.

- Les dépenses informatiques des banques sur les trois prochaines années dans le domaine du cloud public vont augmenter en moyenne de 174 % (benchmark Deloitte banques Tier I et Tier II).
- La digitalisation des banques ou leur succès en matière d'innovation dépendent aujourd'hui du cloud computing (agilité et vitesse).
- *Bank as a platform* : les banques profitent de l'opportunité du cloud pour s'ouvrir de manière sécurisée à d'autres écosystèmes afin de conquérir de nouveaux marchés.
- La souveraineté numérique s'invite au menu de la stratégie cloud des banques au même titre que la compétitivité, la sécurité, la réversibilité, la responsabilité numérique (ESG).



Les banques accélèrent leur adoption du Cloud

L'objectif de cette étude comparative sur le Cloud public dans le secteur bancaire réalisée par Deloitte est d'analyser le marché à travers plusieurs banques Tier I et Tier II autour de leur stratégie d'évolution vers le Cloud public.



L'adoption croissante du **Cloud public** par les banques **répondra à un environnement plus complexe**, en capitalisant sur la **scalabilité et en réduisant les délais de mise sur le marché**.

En 2025, toutes les banques tablent sur une augmentation moyenne de leurs dépenses en matière de Cloud public de près de 174 % (hors SaaS).



Stratégie de **double fournisseur de cloud** à l'échelle mondiale, avec **AWS** comme **fournisseur principal** le plus plébiscité, suivi par **Azure** et **GCP** comme principaux **fournisseurs complémentaires** pour des cas d'utilisation spécifiques.



Dans l'ensemble, un **modèle de gouvernance centralisé prévaut**, avec une **landing zone mondiale définie centralement** et des lignes directrices d'adoption, en quête de normalisation.



01

02

03

04

05



Tendances stratégiques en matière de Cloud public dans les banques Tier 1



En **2025**, toutes les banques **tablent** sur une **augmentation** moyenne de leurs **dépenses en matière de Cloud public de près de 174 %** (hors SaaS).

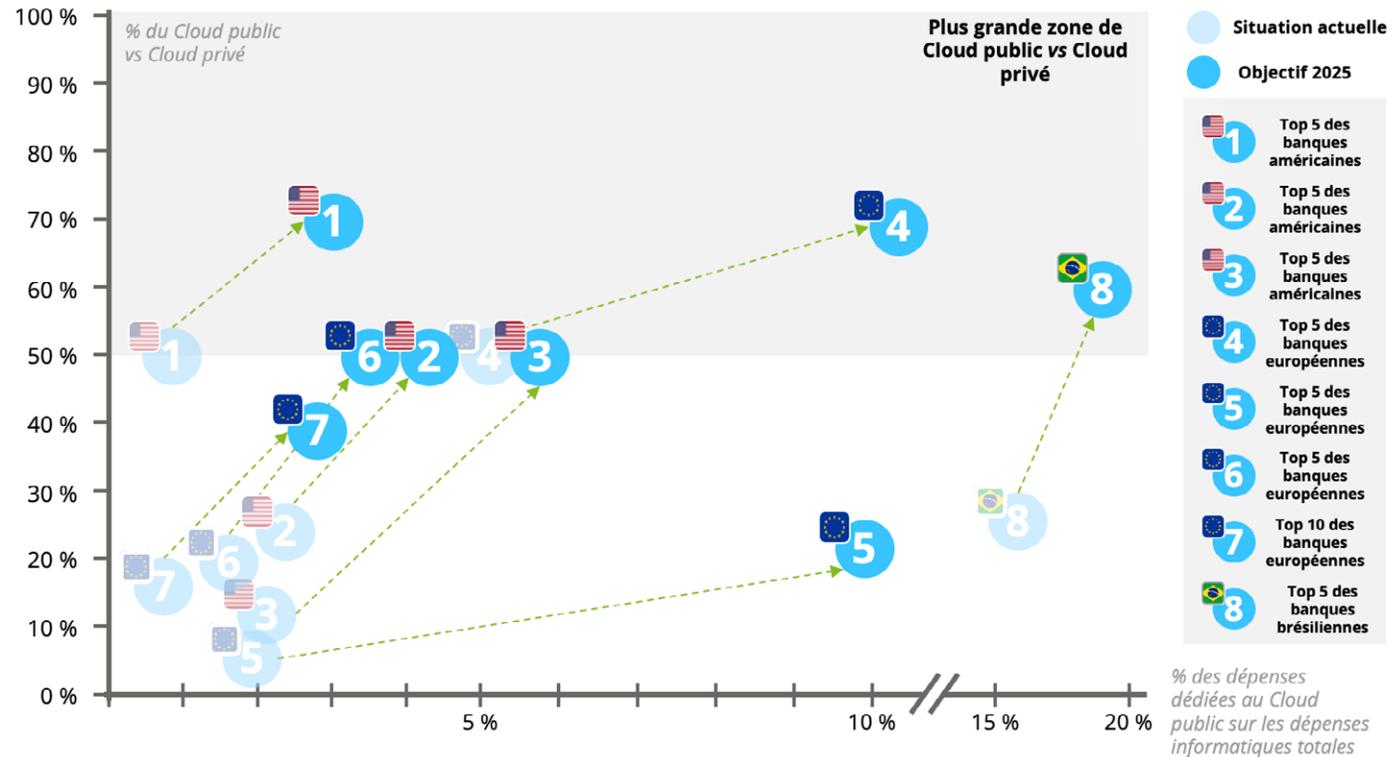
CAGR moyen sur trois ans de **38 %** (plus élevé que les prévisions à 18 % des analystes*).



Les banques envisagent d'**adopter le Cloud public à 50 % ou plus**, par rapport au Cloud privé.

38 % des banques adopteront le **Cloud public** au **détriment du recours au Cloud privé** d'ici 2025.

*IDC prévoit un CAGR de 18 % sur trois ans pour le Cloud public dans le secteur bancaire.



- Situation actuelle
- Objectif 2025
- 1 Top 5 des banques américaines
- 2 Top 5 des banques américaines
- 3 Top 5 des banques américaines
- 4 Top 5 des banques européennes
- 5 Top 5 des banques européennes
- 6 Top 5 des banques européennes
- 7 Top 10 des banques européennes
- 8 Top 5 des banques brésiliennes

L'adoption du Cloud public dans le secteur bancaire s'accélère en termes d'usage (par rapport au Cloud privé) et de dépenses (par rapport au budget informatique total).



01

02

03

04

05



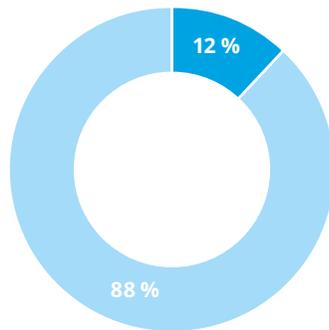
Tendances stratégiques en matière de Cloud public dans les banques Tier 1

Stratégies des fournisseurs de Cloud - Principaux résultats



En Europe et aux États-Unis,
88 % des banques disposent
d'une **stratégie claire** en matière
de fournisseurs de cloud.

Répartition de la stratégie
concernant les fournisseurs

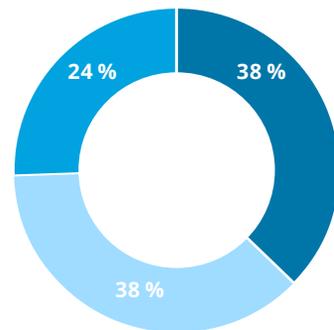


■ Fournisseur unique
■ Double fournisseur



AWS et Azure
sont les fournisseurs principaux
de la plupart des banques
Tier 1.

Principaux fournisseurs de Cloud
sollicités par les banques

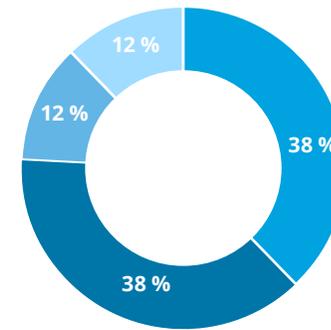


■ AWS ■ Google ■ Azure



GCP apparaît
comme un **fournisseur**
complémentaire pour des cas
d'utilisation spécifiques

Fournisseurs secondaires
de Cloud



■ AWS ■ Google ■ Azure
■ Pas de fournisseur secondaire



La stratégie du double fournisseur de cloud est privilégiée par les banques, principalement pour couvrir les besoins des plans de migrations, capitaliser sur les capacités natives propres au fournisseur, et optimiser les coûts.



01

02

03

04

05



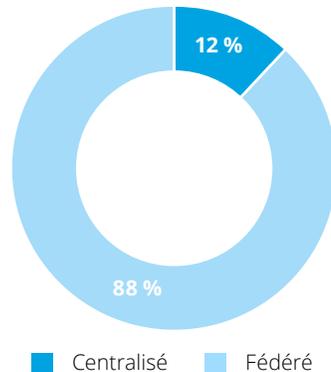
Tendances stratégiques en matière de Cloud public dans les banques Tier 1

Modèle de gouvernance du Cloud - Principaux résultats



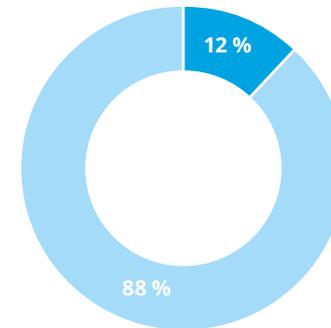
Un **modèle de gouvernance centralisé** du Cloud public est globalement **privilegié**

Modèle de gouvernance du Cloud à trois ans (à horizon 2025)



La plupart des **banques** ont défini de manière centralisée des **landing zone globales** qui doivent être adoptées localement et conformément à des principes d'adoption globaux et centralisés

Modèle de définition de la landing zone



- Zone d'atterrissage globale définie de manière centralisée
- Zone d'atterrissage définie de manière locale



Tendance claire vers un modèle de gouvernance centralisé et l'adoption d'une **landing zone** globale définie de manière centralisée.



01

02

03

04

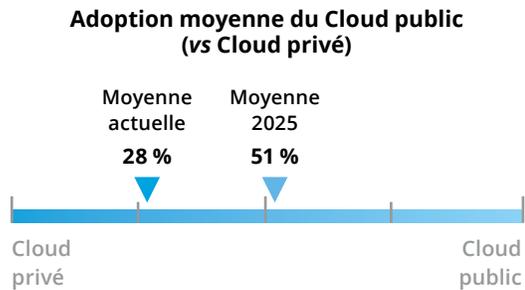
05



Tendances stratégiques en matière de Cloud - vision consolidée

Huit banques Tier I et sept banques Tier II

Taux d'adoption du Cloud public



145 %
Croissance moyenne des dépenses

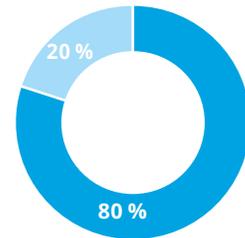
33 %
CAGR moyen sur trois ans



Les banques Tier II ayant adopté le Cloud public à un stade plus avancé affichent une croissance moyenne des dépenses légèrement plus faible.

Stratégie concernant les fournisseurs de Cloud

Répartition de la stratégie concernant les fournisseurs

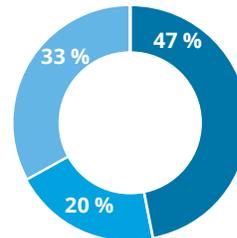


Fournisseur unique
Double fournisseur



Les banques Tier II conservent **AWS** comme fournisseur principal.

Fournisseur principal

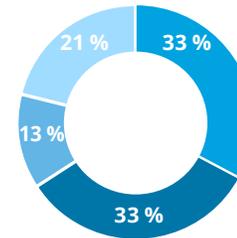


AWS
Google
Azure



La stratégie du double fournisseur cloud pour couvrir les besoins des plans de migration, capitaliser sur des capacités natives spécifiques et optimiser les coûts.

Fournisseur secondaire



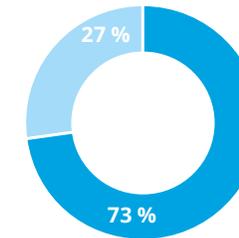
AWS
Google
Azure
Pas de fournisseur secondaire



AWS et **Azure** sont essentiellement considérés comme des fournisseurs supplémentaires. **GCP** apparaît comme le principal fournisseur complémentaire pour des cas d'utilisation spécifiques.

Taux d'adoption du Cloud public

Modèle de gouvernance du Cloud sur trois ans (horizon 2025)



Centralisé
Fédéré



Les banques Tier II ont tendance à conserver leur modèle de gouvernance, qui est principalement un modèle de gouvernance centralisé.



Toutes les banques Tier II analysées suivent les mêmes tendances que celles de Tier I.



01

02

03

04

05



Cas d'utilisation favorisant l'adoption du Cloud public

Principaux cas d'utilisation du Cloud public et leviers d'adoption

L'analyse de 53 sociétés de services financiers, dont des banques, a permis d'identifier les principaux cas d'utilisation et leviers d'adoption du Cloud public

Principaux cas d'utilisation		Entreprises adoptant le cas d'utilisation (%)	Nouveaux cas d'utilisation	Principaux leviers d'adoption du Cloud public identifiés	
	Banque en ligne et mobile → Envisage le passage vers la banque numérique ←	58 %			Échelle & Disponibilité → Utiliser les économies d'échelle pour s'adapter à la demande ←
	Traitement des données → Traitement et analyse de données ←	26 %	API de marketplace		Conteneurisation → Couches fonctionnelles pour tirer parti de l'évolutivité et de la portabilité ←
	Risques et Conformité → Y compris la sécurité ←	25 %	Open Banking		Modernisation → Applications et Processus pour améliorer l'efficacité et l'expérience client ←
	Paiements → Transferts, prélèvements automatiques et gestion centrale de trésorerie ←	17 %	Canaux numériques améliorés		DevOps/Agile → Faciliter l'évolution des processus et développements, réduire les délais de mise sur le marché ←
	Centre de contact → Centre d'appel, examens et analyse des clients ←	11 %			

 Les banques transforment leur modèle d'entreprise en s'appuyant sur les capacités du Cloud public.



01

02

03

04

05

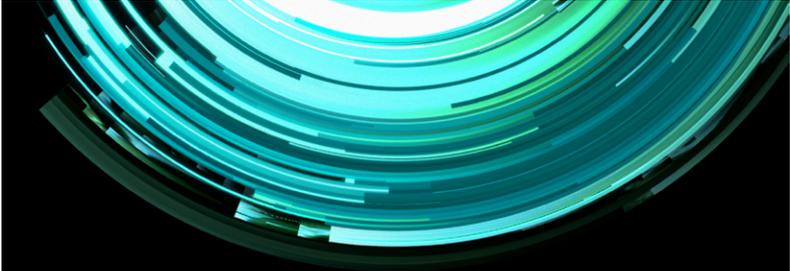


La souveraineté numérique s'invite au menu de la stratégie cloud des banques (1/2)

Libérer le potentiel du Cloud souverain : une passerelle vers la résilience et l'innovation

L'adoption du Cloud public est devenue une priorité pour les entreprises, car elle favorise l'agilité et l'innovation. Néanmoins, certaines stratégies Cloud compromettent l'autonomie et le contrôle nécessaires des clients concernant leurs données et applications. Par conséquent, la souveraineté du Cloud devient de plus en plus pertinente pour s'assurer d'un meilleur contrôle sur les actifs du Cloud et améliorer la conformité et l'autonomie opérationnelle, sans pour autant perdre le bénéfice des technologies émergentes.

Afin d'évaluer le degré de maturité d'une organisation en termes de souveraineté du Cloud, Deloitte a conçu un référentiel complet couvrant toute la chaîne du Cloud et basé sur cinq domaines. Ce référentiel s'applique aux entreprises de l'ensemble des secteurs des services financiers.



Cloud Sovereignty
Unleashing the potential of sovereign cloud:
A gateway to resilience and adaptability

Deloitte has developed a comprehensive framework to evaluate technical cloud sovereignty in organizations, that covers the entire cloud stack and includes five distinct domains:

-  Operational sovereignty
-  Data sovereignty
-  Software sovereignty
-  Infrastructure & Communications sovereignty
-  Security cross dimension

Faster together. Business transformation accelerated by Cloud.

Deloitte.



01

02

03

04

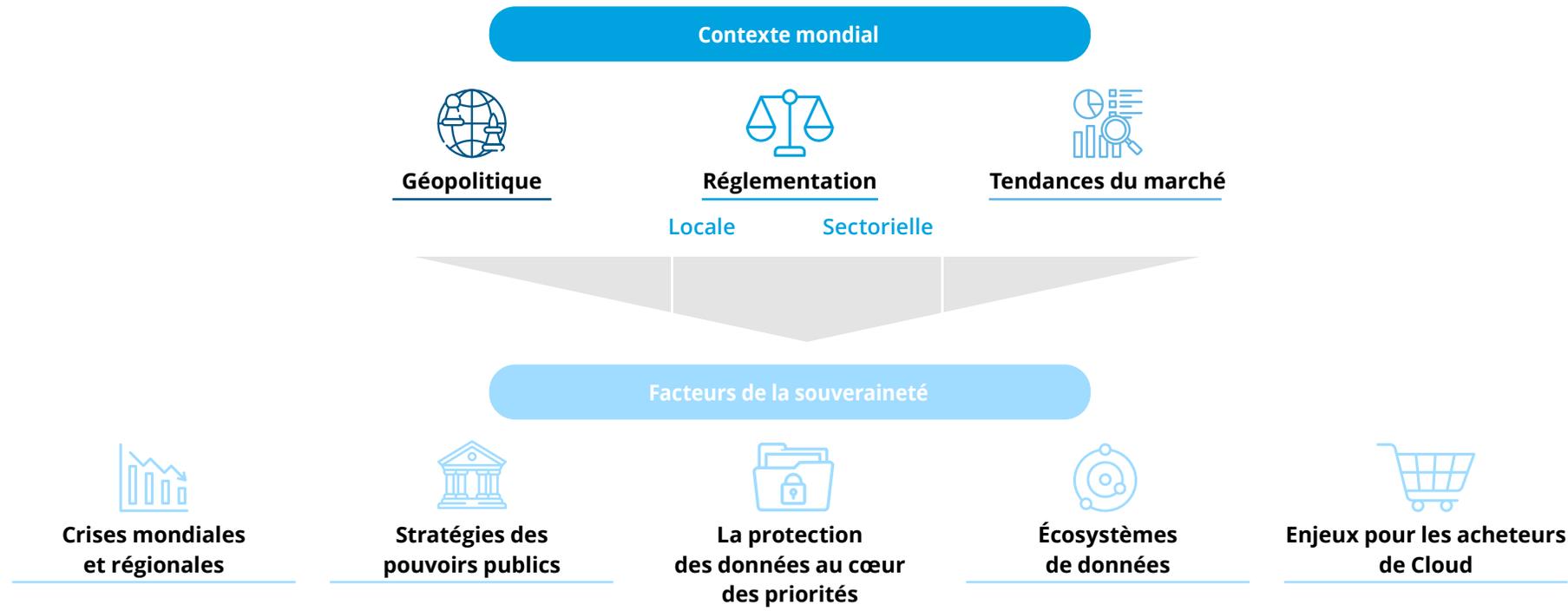
05



La souveraineté numérique s'invite au menu de la stratégie cloud des banques (2/2)

Principales caractéristiques de la souveraineté du Cloud

La souveraineté du Cloud aborde les dimensions politiques, commerciales et technologiques de la protection et de la sécurité des données, ainsi que le contrôle et l'indépendance des opérations, des données, des logiciels, de l'infrastructure et des prestataires de communications. Un Cloud souverain associe la stratégie, la gouvernance et les contrôles techniques pour garantir la **résilience, la flexibilité, l'autonomie et la conformité aux exigences réglementaires**.



01

02

03

04

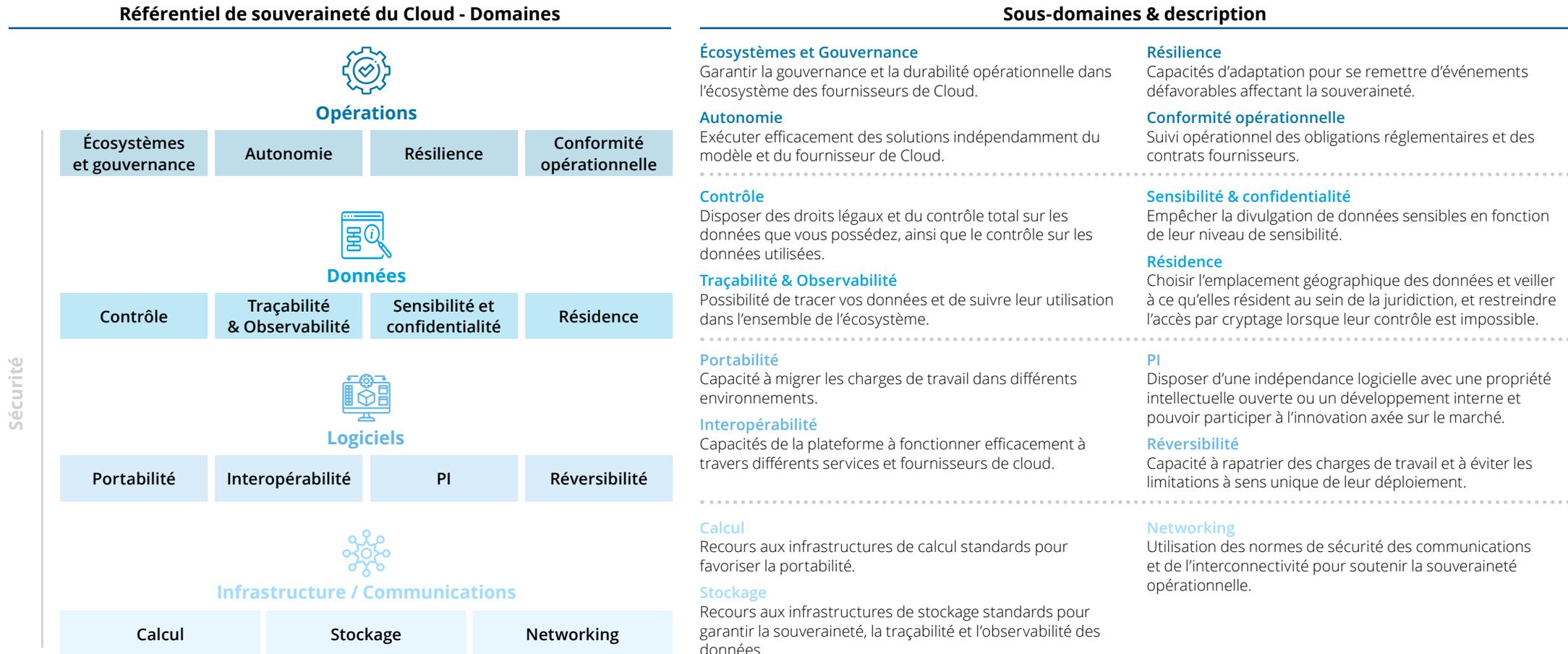
05



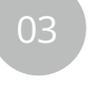
Référentiel de souveraineté du Cloud - Présentation

Deloitte propose un référentiel pour aborder le sujet de la souveraineté du Cloud en se fondant sur quatre domaines.

En décomposant les domaines en secteurs spécifiques, les organisations peuvent mieux appréhender les enjeux liés à l'adoption de la souveraineté du Cloud.



Sécurité

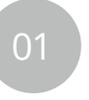


Référentiel de souveraineté du Cloud - Sécurité

La sécurité est une capacité majeure pour les cas d'utilisation de la souveraineté afin d'assurer le contrôle des charges de travail et des données.

Ce référentiel tient compte des facteurs pertinents de la sécurité pour chaque couche de souveraineté à un niveau élevé. Il ne prévoit pas d'analyser en profondeur les domaines de sécurité devant être mis en place pour déployer une solution souveraine.

Sécurité intégrée aux couches	Contrôles principaux	Faits marquants
 Opérations	Gouvernance & Surveillance	Gouvernance et surveillance permettant de définir les rôles et responsabilités dans le Cloud Politiques et Normes pour définir les attentes en matière de sécurité de l'information Gouvernance IAM pour permettre la gestion du cycle de vie des identités Planification de la reprise après sinistre.
 Données	Politiques & Normes	Politique de protection des données et de la vie privée, chiffrement des données, contrôle d'accès, confidentialité des données, prévention des pertes de données, gestion des clés, suivi de l'accès aux données, environnement d'exécution fiable, chiffrement à double clé (DKE), planification des sauvegardes.
 Logiciels	Gestion des identités et des accès	DevSecOps et CI/CD (intégration continue, livraison continue), cycle de vie du développement logiciel sécurisé, analyse de code SAST/DAST, surveillance de la chaîne d'approvisionnement en logiciels, analyse des vulnérabilités connues.
 Infrastructure / Communications	Gestion des accès privilégiés	Exécution sécurisée : support matériel pour les environnements informatiques sécurisés/de confiance (enclaves sécurisées), tunnels sécurisés, prévention des attaques par canal auxiliaire, surveillance du réseau (IDS/IPS, système de détection d'intrusion et système de prévention d'intrusion).



Scénarios de souveraineté du Cloud

Deloitte a identifié cinq scénarios types, basés sur les besoins de souveraineté d'une entreprise.

De la limite de localisation des données au Cloud totalement isolé pour une souveraineté opérationnelle maximale, chaque scénario présente différents niveaux de complexité et de coûts associés devant être pris en compte par les organisations.

Scénario

Limites de localisation des données

Définir un environnement de **données sécurisé** en prévoyant des exigences spécifiques permettant de garantir qu'elles demeurent au sein de **limites locales**.

Limites d'accès des données

Sécuriser les **données** stockées dans le Cloud contre la possibilité d'une **exposition** due à une **législation étrangère**.

Réglementations juridiques/sectorielles

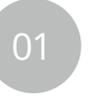
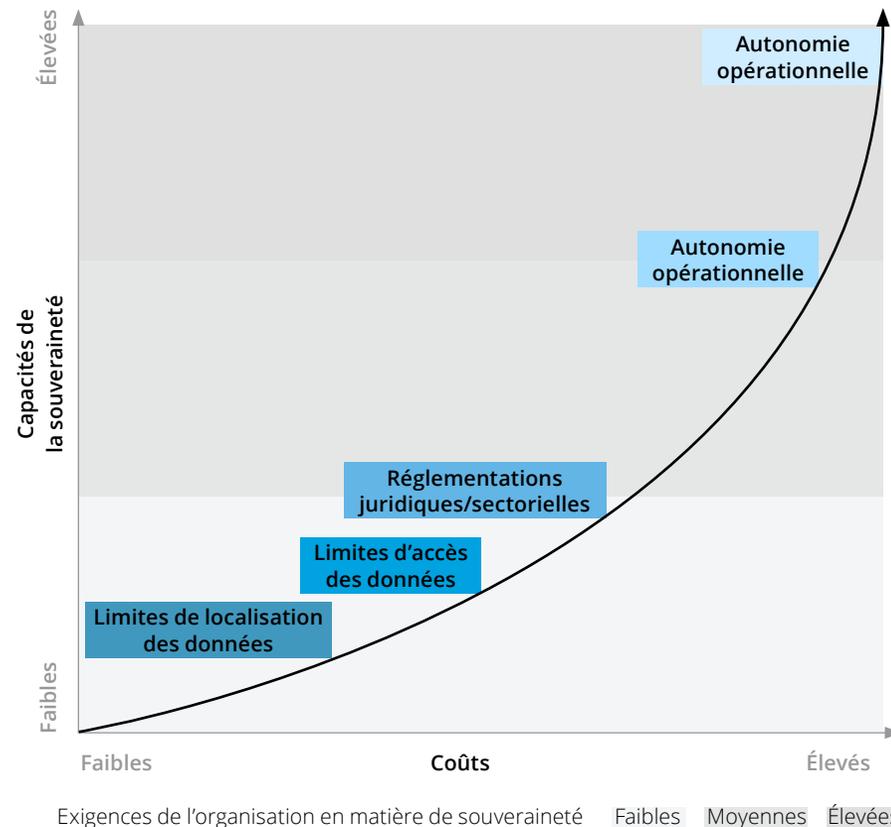
Conformité des services Cloud avec les **réglementations régionales/locales strictes** dans le secteur public ou des secteurs très réglementés.

Autonomie opérationnelle

Intégrer l'**autonomie opérationnelle** au niveau d'une **plateforme de données** européenne.

Cloud isolé

Opérer en **déconnexion absolue avec les hyperscalers**, afin d'atteindre le plus haut niveau de souveraineté numérique.



Experts



Frédéric Bujoc

Associé Risk Advisory
Banking & Capital Markets Leader

Frédéric a plus de 20 ans d'expérience dans l'accompagnement des banques dans leurs projets de transformation Finance et Risques. Frédéric dispose d'une expertise reconnue en matière de gestion actif/passif et pilotage des fonds propres et d'une excellente connaissance de banque de financement et d'investissement. Frédéric est responsable de nos offres de services relatives à la gestion de bilan et aux risques de marché et de contrepartie.



Nicolas Fleuret

Associé Risk Advisory
Responsable Risk & Regulatory

Avant de rejoindre Deloitte, Nicolas a passé près de 15 ans auprès des autorités bancaires françaises (Banque de France, Autorité de contrôle prudentiel) où il a occupé différents postes, notamment la supervision bancaire.

Il a intégré Deloitte en 2009 où il coordonne, depuis, les activités du pôle Regulatory à destination des institutions financières.

Nicolas représente également la firme française dans les centres d'expertise européens de Deloitte, à Londres et à Francfort.



Julien Maldonato

Associé Conseil
Innovation

Julien a plus de 22 années d'expérience dans l'accompagnement des institutions financières dans l'analyse et la mise en œuvre d'innovations technologiques.

Dans ce cadre, il a travaillé sur des innovations de rupture parmi lesquelles l'intelligence artificielle, la blockchain, les modèles en P2P, l'IoT et l'assurance connectée, les nouveaux modes de travail, la digitalisation du conseil financier...

Julien est responsable de l'offre de services Deloitte Innovation pour l'industrie financière.



Nicolas de Jenlis

Associé Risk Advisory
Sustainability

Nicolas a plus de 10 ans d'expérience dans l'accompagnement des entreprises sur leur stratégie, déploiement opérationnel et reporting en matière de développement durable et de responsabilité sociétale.

Il est spécialisé dans l'ESG (Environnement, social et gouvernance) appliqué au secteur financier : finance responsable, due diligences, impact investing, *green bonds*, ISR (investissement socialement responsable), etc.

Nicolas est responsable de l'offre de services en matière de finance durable (banque, assurance et gestion d'actifs).



01

02

03

04

05



Experts



Stéphane Kielbik

Directeur Conseil
Ops Tr Financial Services Industry
and Fintech

Stéphane accompagne les acteurs du secteur de la banque de détail depuis plus de 11 ans sur leurs problématiques métier. Son expertise et ses interventions s'articulent autour de la conquête de nouveaux clients, des modèles de relation client et commerciale, des approches distributives et du beyond banking. Stéphane accompagne nos clients de la définition de leur stratégie, à la déclinaison opérationnelle de cette dernière.



Mohamed Benlaribi

Associé Risk Advisory
Risques financiers et climatiques,
Financial Services

Mohamed a plus de 20 années d'expérience dans le secteur des services financiers. Ses domaines d'interventions sont : la gestion des risques d'entreprise et des risques financiers et matières premières, les risques climatiques, les trajectoires CO2, les projections financières, la gestion actif/passif et les Stress tests.



Didier Descombes

Associé Risk Advisory
Cloud Engineering

Associé au sein des activités Cloud Transformation, Didier a plus de 28 ans d'expérience dans la transformation digitale des entreprises et des institutions. Ses domaines d'interventions sont : le Conseil auprès des Directions Générales et des CXO, la transformation digitale des entreprises, les stratégies de Cloud and Business Transformation, les nouveaux business models et l'innovation technologique, les partenariats et investissements stratégiques, les enjeux de responsabilités numériques (ESG et souveraineté numérique), et l'efficacité opérationnelle.



Deloitte.

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited (« DTTL »), à son réseau mondial de cabinets membres et à leurs entités liées (collectivement dénommés « l'organisation Deloitte »), DTTL (également désigné « Deloitte Global ») et chacun de ses cabinets membres et entités liées sont constitués en entités indépendantes et juridiquement distinctes, qui ne peuvent pas s'engager ou se lier les uns aux autres à l'égard des tiers. DTTL et chacun de ses cabinets membres et entités liées sont uniquement responsables de leurs propres actes et manquements, et aucunement de ceux des autres. DTTL ne fournit aucun service aux clients. Pour en savoir plus, consulter www.deloitte.com/about. En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

Deloitte
6, place de la Pyramide – 92908 Paris-La Défense Cedex

© Mai 2023 - Deloitte Conseil - Une entité du réseau Deloitte
Designed by dot.