EGE Ecole de Guerre Economique

Pour une Europe financière plus résiliente et plus indépendante

Le règlement DORA.

Atténuer le risque lié à la transformation numérique.

Auteurs
Matthieu Bondy, Frederic Caubert, Abdelhalim Elmouadan, Pierre Hervé Gbingbehi, Patrick Tahiri

22 mai 2022

« Ce qui arrive en fin de compte, ce n'est pas l'inévitable mais l'imprévisible ».

John Maynard Keynes

Table des matières

Introduction **4**

CHAPITRE 1

Le panorama européen de la finance **6**

CHAPITRE 2

Les enjeux **23**

CHAPITRE 3

Le règlement DORA **28**

CHAPITRE 4

DORA et les tests de résilience opérationnelle numérique **42**

CHAPITRE 5

Gestion des fournisseurs tiers **56**

CHAPITRE 6

Approche pour la résilience numérique **79**

Conclusion **84**

Annexes 85

Glossaire 96

L'équipe 98

INTRODUCTION

La finance est par nature essentielle au bon fonctionnement de l'économie mondiale. Pour un Etat, elle est synonyme de stabilité, d'indépendance et de puissance. Ces notions s'avèrent plus cruciales que jamais dans la mesure où ses fondamentaux sont remis en question par une multitude de facteurs allant des taux bas, voire négatifs en Europe, à l'innovation technologique qui en bouscule l'ordre et la hiérarchie. Sa stabilité est en même temps menacée par des crises incessantes depuis quinze ans, qu'elles soient d'origines économiques et financières, sanitaires et désormais politiques et bien sûr « cyber ».

Forts de ce constat, nous avons décidé de réfléchir aux questions de résilience numérique et d'autonomie du secteur financier au sein de l'Union Européenne (UE).

Pour cela, nous l'appréhendons sous l'angle d'un futur règlement européen dont nous estimons qu'il doit positionner les vingt-sept Etats membres à l'avant-garde.

Le **Digital Operational and Resilience Act** (**DORA**) est un règlement de l'UE proposé en septembre 2020 et actuellement en discussion finale auprès du Conseil et du Parlement européen. Sa mise en œuvre est prévue entre fin 2022 et 2024, et le texte repose sur 5 piliers :

1. Gouvernance des risques informatiques.
2. Gestion, classification et notification des incidents liés à l'informatique.
3. Tests opérationnels.
4. Gestion des risques liés aux prestataires de services informatiques.
5. Dispositifs de partages d'informations.

L'apport de ce texte est décisif : il vient élargir, approfondir et harmoniser le corpus législatif existant, qu'il soit local ou européen, dans le domaine numérique et cyber-technologique qui jusqu'alors n'était pas spécifiquement couvert pour la finance. C'est un élément stratégique pour le secteur, par ailleurs grand consommateur de données et très exposé au risque cyber.

Depuis la crise financière de 2008, l'UE avait considérablement renforcé sa réglementation financière en particulier sur les aspects solvabilité et gestion des risques prudentiels. Il en a été de même pour les risques non financiers traitant de la conformité, la lutte anti-blanchiment et des risques opérationnels.

En revanche, les risques numériques n'avaient jusqu'alors pas fait l'objet d'un texte dédié. Cela sera donc rectifié avec DORA.

Ajoutons que la collaboration de la finance avec les géants du numérique, pour ne pas dire sa dépendance vis-à-vis des GAFAM[1] (Google - Amazon – Facebook - Apple - Microsoft), et la montée en puissance des risques cyber font de DORA une nécessité tout autant qu'une évidence pour l'UE.

Avec les néo-banques, les acteurs opérant sur les cryptoactifs ou bien encore la multiplication des « fournisseurs de services de paiements », le panorama du secteur financier se fait chaque jour plus large.

La finance numérique décentralisée accélère cette tendance : les nouveaux intervenants peuvent tout autant être des concurrents que des alliés des établissements traditionnels, qu'il s'agisse des banques ou des assurances. Ils ont tous en commun de modifier de façon irrévocable et profonde l'écosystème financier.

[1] Nous utiliserons l'acronyme GAFAM dans la suite de notre rapport pour désigner les géants américains du numérique.

Pour cette raison, et nous le détaillerons dans ce rapport, la définition de la finance au sens de DORA s'est voulue exhaustive, en y intégrant aussi bien les acteurs historiques que les nouveaux entrants, et ses fournisseurs stratégiques. Il est essentiel aux yeux du régulateur que tous soient assujettis aux mêmes obligations. C'est un principe d'équité et de cohérence. En même temps, et dicté par le pragmatisme, le régulateur européen appelle à une mise en œuvre proportionnée pour chacun des établissements concernés, en fonction de sa taille et de sa complexité.

Le secteur financier, par ailleurs totalement interconnecté à l'échelle mondiale, vit une profonde transformation. Il doit aussi et en même temps relever le défi du changement climatique tout en renforçant sa résilience et son indépendance.

Il lui est donc impératif de concilier innovation et croissance, comme de faire conjuguer profitabilité, sécurité, durabilité, et autonomie stratégique.

La question essentielle pour les acteurs du monde financier va désormais être celle de leur capacité à mener de front tous ces changements. La volonté est un prérequis, les réglementations donnent un cadre normatif, vertueux et incitatif. C'est ainsi qu'il faut l'envisager. A charge aux parties prenantes d'engager le changement de culture, la montée en compétences des équipes, et de concilier harmonieusement maîtrise des risques et attractivité économique.

Notre rapport abordera l'ensemble de ces thématiques, et les détaillera en cinq grands chapitres :

Panorama de la Finance : enjeux, mutations et déroulement historique réglementaire dans l'UE.	Les enjeux de la résilience numérique.
Présentation de DORA : le texte et ses points clés, les acteurs, et les implications concrètes attendues.	Les tests de résilience opérationnelle numérique.
La gestion des fournisseurs numériques.	

Nous conclurons en élargissant notre champ de réflexion aux questions de résilience et d'autonomie financière.

CHAPITRE 1

Le panorama européen de la finance

Historique, Réglementations et mise en perspective des enjeux

Cette première section décrit ce que l'on entend par secteur financier… quels en sont ses acteurs et que représente-t-il concrètement pour l'UE ?

L'objectif est ainsi d'illustrer le poids de cette industrie au sens large du terme dans le panorama Européen, que ce soit sous l'angle économique, financier, social mais aussi stratégique. Il apparaît en effet essentiel de rappeler ces éléments avant que d'aller plus loin dans les mesures concrètes prises par l'UE en matière digitale & cyber. Situer la criticité du monde financier est en somme un préalable à la gestion des risques et à leur encadrement de façon proportionnée.

En complément, un rappel sera effectué dans cette section sur les principales décisions et lois votées ces dernières années par l'UE pour renforcer la régulation du secteur financier. Cette chronologie vise à mettre en perspective le chemin parcouru en matière de gestion des risques sous toutes leurs formes. Et la nécessité de le continuer en y ajoutant de nouvelles dimensions liées à la globalisation, la question environnementale et la numérisation.

Sous cet angle, nous comprendrons mieux alors ce que DORA vient apporter dans ce dernier domaine. Nous illustrerons les risques cyber via des exemples concrets d'attaques ayant affecté des acteurs du monde financier, en soulignant leur impact.

En conclusion de cette première partie, nous ferons enfin un tour d'horizon des autres régions de par le globe en termes de réglementations ou dispositions existantes pouvant être comparées à DORA. L'idée via ce comparatif est de positionner l'UE et sa place financière sur la scène internationale de la « cyber résilience ».

Les acteurs européens de la Finance et contexte

Pour viser au plus juste avec notre thématique, prenons en compte le périmètre des entreprises concernées par DORA. A cette aune, on y recense plus de 21 200 entités en 2017, date à laquelle l'UE a établi un chiffrage des acteurs du monde financier, dans le détail[2] :

- 5 665 établissements de crédit.
- 5 934 entreprises d'investissement.
- 2 666 entreprises d'assurance.
- 2 500 établissements de paiement & de monnaie électronique agréés.
- 1 573 Institutions de retraite professionnelle.
- 2 500 entreprises de gestion d'investissements.
- 350 infrastructures de marché.
- 45 agences de notation de crédit.

[2] Rapport 2017 des autorités européennes de surveillance. Commission européenne [en ligne]. 20 septembre 2017. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2017%3A308%3AFIN

Il convient, de plus, d'y ajouter les entités de financement participatif, les contrôleurs légaux des comptes, les prestataires de services sur cryptoactifs, ou bien encore les administrateurs d'indices de référence. Un vaste ensemble donc. **En revanche, les cabinets d'audit qui figuraient dans la version initiale n'y figurent plus depuis l'accord provisoire du 11 mai 2022** (voir Annexes).

Ce point est d'autant plus critique que les sociétés gravitant dans le domaine des paiements ou des crypto-assets prennent une place croissante de mois en mois, tant par le nombre de leurs intervenants que par leur poids dans l'écosystème financier au sens le plus large du terme. Bien que ce rapport n'ait pas pour objet d'en détailler les modalités, il nous apparaît critique de souligner ici que jamais la mutation du secteur - pour ne pas dire sa disruption selon un terme désormais commun - n'a jamais été aussi forte, aussi rapide qu'au moment où nous écrivons ces lignes.

En effet, le panorama financier après une relative stabilité jusqu'au début des années 2000 a accéléré sa mutation. Celle-ci n'a eu dès lors de cesse que de s'accélérer sous l'effet des crises, comme celle financière de 2008, et d'un essor technologique sans précédent.

Cette évolution, devenue révolution, s'est effectuée d'abord par le biais de regroupements ou de fusions entre les mastodontes du secteur des banques et des assurances.

Elle s'est poursuivie par l'ouverture du jeu à de nouveaux acteurs, de type prestataires de paiements puis des néo-banques, lesquels sont venus progressivement s'attaquer au marché des acteurs dits traditionnels. Nous mentionnerons ici les néo-banques, telles N26[3] en Allemagne dont la valorisation boursière commence à approcher celles des géants allemands, français ou néerlandais, ou bien encore la Fintech Revolut[4] valorisée 33 milliards de dollars. Ces succès sur le plan boursier et de la valorisation financière demandent encore confirmation sur un plan économique, mais la position de leurs compétiteurs historiques est irrémédiablement bouleversée par ces derniers.

Le dernier phénomène, et non des moindres, concerne l'extension des frontières du monde financier avec l'émergence de la finance décentralisée, avec le Web 3 et la blockchain Elles apportent leur lot de synergies et d'améliorations aux acteurs traditionnels, tout en leur permettant de moderniser leurs services, par exemple, en matière de paiements.

Mais elles ont aussi ouvert la porte à de nouveaux modes de fonctionnement. Nous pensons bien sûr aux crypto-monnaies, dont la valorisation a excédé fin 2021 les 3 000 milliards USD, les stable coins, et désormais les Monnaies Digitales de Banque Centrale (MDBC). Autant d'éléments tantôt, et encore majoritairement, utilisés comme outils spéculatifs, tantôt comme moyens de paiements alternatifs… et bientôt complémentaires pour les MDBC sous l'égide des Banques Centrales[5].

Pour illustrer cette mutation, nous pouvons aussi relever l'envergure prise par les plateformes de Trading de cryptoactifs telles Kraken ou Coinbase. Tous ces éléments constituent des signes tangibles que la scène financière a connu une mue sans précédents ces toutes dernières années. Dans la même veine, le monde des paiements est en révolution. Selon une étude de Statista, le paiement en ligne mondial va passer de 1 500 milliards en 2019 à 2 000 milliards d'ici 2025. En Europe, la réglementation DSP2 a haussé les processus d'authentification et contribué à cette croissance.

[3] LAPALUS, Denis. N26 valorisée à 9 milliards de dollars après une nouvelle levée de fonds record de près de 900 millions. France Transactions [en ligne]. 18 octobre 2021. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.francetransactions.com/actus/news-banques/n26-valorisee-a-9-milliards-de-dollars-apres-une-nouvelle-levee-de-fonds-record.html

[4] AFP. La fintech britannique Revolut valorisée 33 milliards de dollars. Zonebourse [en ligne]. 15 juillet 2021. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.zonebourse.com/cours/action/SOFTBANK-GROUP-CORP-6492452/actualite/La-fintech-britannique-Revolut-valorisee-33-milliards-de-dollars-35864942/

[5] MAQUET, Clémence. MNBC : tout comprendre de la monnaie numérique de demain. SiècleDigital [en ligne]. 2 novembre 2020. (Mise à jour le 2 décembre 2021). [Consulté le 22 avril 2022]. Disponible à l'adresse : https://siecledigital.fr/2020/11/02/mnbc-tout-savoir-monnaie-numerique/

Le développement du paiement fractionné à grande échelle va se poursuivre. Toute la chaîne de valeurs se transforme et cela intègre les terminaux de paiements qui sont en train de muter vers les smartphones. « L'avenir des terminaux se trouve dans le Cloud et non dans le boîtier physique ». Cette phrase de Gilles Grapinet, PDG de Worldine, illustre encore le déplacement des enjeux vers de nouveaux acteurs. Avec une dimension clé, la donnée, car les paiements véhiculent de très grandes sources d'informations … et en cela c'est un élément stratégique pour tous ceux qui en ont la maîtrise. Ne l'oublions jamais.

Cette digitalisation des monnaies, la dématérialisation des paiements à l'heure de l'open Banking préludent l'open Finance de demain. Il est par conséquent vital de faire bouger les lignes et de prévoir des réglementations adaptées aux modes « banking as a service » et « banking as a platform ». Le régulateur, où qu'il soit, le sait et il a commencé à repenser le cadre de référence. Il est donc évident que toute nouvelle réglementation doit intégrer en premier un meilleur encadrement de la technologie numérique.

Le régulateur européen ne s'y est d'ailleurs pas trompé puisqu'il intègre tous ces aspects dans DORA, nous l'avons dit. Il rappelle par ailleurs à chaque occasion à ces nouveaux entrants le respect des règles et à la vigilance. C'est particulièrement vrai déjà sur la conformité[6]. Si nous restons sur l'exemple de N26, cet établissement a été condamné par la BAFIN - le régulateur financier allemand - en raison de pratiques déficientes en matière de lutte anti-blanchiment. Cela l'est aussi sur les questions d'accès aux marchés des paiements par exemple, confère l'exemple de la société Binance avec la Financial Conduct Authority (FCA) au Royaume-Uni[7]. Ce le sera demain sur l'application des règles du jeu numérique.

Quel est le poids de l'UE dans le monde financier ? L'exemple des Banques européennes

Estimer la puissance financière d'un pays ou d'une zone géographique est un exercice subjectif. Utilisons ici le secteur bancaire comme étalon. Sous cet angle, l'UE est très bien positionnée dans le classement mondial. Elle place en effet un tiers de ses représentants, 34 précisément, parmi les 100 premiers (selon la taille de leur bilan)[8]. A titre de comparaison, les USA, la Chine et le Japon en ont respectivement 18, 12 et 8. Si on regarde plus en profondeur ce même classement toutefois, elle n'en place cependant plus que deux dans le top 15, i.e. BNPP et Crédit Agricole … là où les USA, la Chine, et le Japon, en comptent chacun 4.

Ces chiffres sont utiles à souligner pour montrer le poids relatif des acteurs européens face aux mastodontes américains et asiatiques. Cette situation pourrait d'ailleurs continuer à s'accentuer en cas de concentration accrue du marché, hypothèse probable et plus forte encore dans l'ère post-Covid dans laquelle nous sommes rentrés, et à un recentrage des géants bancaires sur leurs marchés domestiques et régionaux.

Sans faire de *finance fiction*, il est aussi opportun de souligner que les entités européennes en cas de crise financière et/ou demain… de crise voire de conflit cyber, pourraient voir leur position s'affaiblir et donc devenir de potentielles cibles pour des concurrents étrangers.

Cette vulnérabilité cyber est aussi indirecte. Les acteurs bancaires et plus largement financiers sont fortement dépendants pour leur bon fonctionnement des industries et infrastructures vitales comme l'électricité pour citer un exemple simple. Toute cyber-attaque ou défaillance accidentelle touchant ces acteurs essentiels ou d'importance vitale serait une source de déstabilisation assurée pour l'économie européenne.

---

[6] ALRIC, Jean-Yves. Après N26 et le scandale Wirecard, l'Allemagne craint une nouvelle fintech. Presse-Citron [en ligne]. 15 février 2022. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.presse-citron.net/apres-n26-scandale-wirecard-allemagne-craint-une-autre-fintech/

[7] SELBY, Jenn. Binance access to UK payments network worries City watchdog. The Guardian [en ligne]. 16 février 2022. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.theguardian.com/technology/2022/feb/16/binance-access-to-uk-payments-network-worries-city-watchdog-fca-playsafe-cryptocurrency

[8] PROTSKA, Olga. Top 20 des plus grandes banques 2022 par le total des actifs. FXSSI [en ligne]. 27 janvier 2022. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://fr.fxssi.com/top-20-des-plus-grandes-banques

C'est la raison pour laquelle l'UE a mis en place la directive sur la sécurité des « Network and Information Security » (NIS) depuis 2016, et la France instauré la dimension cyber dans les lois de programmation militaire depuis 2013, avec d'une part des Opérateurs de Services Essentiels (OSE), et des Opérateurs d'Importance Vitale (OIV) d'autre part.

L'histoire récente a enfin montré que le secteur bancaire pouvait évoluer par des chemins inattendus du fait d'événements qui ont eu un impact majeur. Nous pouvons en citer deux :

Le premier est d'ordre juridique en raison des pratiques juridiques extraterritoriales. Les amendes infligées par le département de la justice (DOJ) américain à de grands acteurs européens tels BNPP ou HSBC dans les années 2010 en sont des exemples emblématiques. Rappelons que ces établissements se sont vu infliger des amendes respectives de neuf milliards et plus d'un milliard USD. L'effet a été profond et il a singulièrement infléchi le positionnement de ces géants bancaires dans leur rayonnement global ou leur positionnement métier. Ceux-ci ont en effet dû changer leur organisation, revoir leur politique commerciale, modifier leurs implantations et leurs activités, sans que cela n'ait été anticipé. Hier et aujourd'hui l'extra-territorialité du droit américain avec des sous-jacents Conformité et Sanctions Internationales… Demain ce seront peut-être des cyberattaques diligentées par des groupes « Advanced Persistent Threat » (APT), ou de trop fortes dépendances vis-à-vis de géants numériques qui seront à même de faire vaciller les géants financiers. Il est dans tous les cas certains que ces changements de référentiels sont à prendre en compte. Il n'est plus possible de continuer à mener ses affaires comme avant. Les risques juridiques, financiers, opérationnels et réputationnels sont devenus trop grands.

Le second est d'ordre sanitaire avec la crise Covid. Quand bien même le risque de pandémie était intégré, sa probabilité d'occurrence et son impact ont été au mieux sous-estimé, et plus certainement non considérés à leur juste valeur. Il est donc stratégique de faire preuve de davantage d'anticipation, de préparation, et de stratégie de plan de repli pour faire face à la menace. S'agissant du risque cyber, la question n'est plus de savoir « s'il touchera » mais « quand et comment ».

Comme le dit ce proverbe anglais « ***Qui me trompe une fois, honte à lui. Qui me trompe deux fois, honte à moi*** » … à méditer donc.

Cloud et dépendance. La place accrue prise par les fournisseurs numériques a un effet similaire. Parmi eux, le point crucial est celui du cloud, domaine concentré sur une poignée d'acteurs principalement américains. Cet état de fait crée à leur égard une très forte dépendance technologique, économique, de tout un secteur et induit de facto un risque juridique et de perte d'autonomie. Le bon sens populaire appelle à ne pas mettre tous ses œufs dans le même panier… son application serait en ce domaine une excellente chose à appliquer. Pour le secteur bancaire, le cabinet McKinsey a publié en 2020 une étude consacrée au cloud banking. En substance, il ressort que sur la décennie allant jusque 2030, les banques transféreraient de 40 à 90% de leur activité sur le Cloud. Ce basculement a commencé et les données transférées concernent non plus seulement des éléments de management des risques, mais aussi, et de plus en plus, des données commerciales et personnelles sensibles. Nous touchons ici un point stratégique incluant des dépendances en termes de souveraineté, de protection des données, et de résilience opérationnelle. Sous cet angle, notons cependant que les stratégies multicloud sont de plus en plus communes et apportent une plus grande résilience et flexibilité au secteur. **Nous développerons plus longuement ces points dans les prochains chapitres de ce mémoire.**

Poids de la Finance dans l'économie Européenne - L'exemple des Banques.

Regardons désormais ce que représente le secteur bancaire en Europe. Pour cela, nous allons prendre les critères suivants :

1. Poids versus le PIB.
2. Nombre d'employés.
3. Liste des plus grandes banques sur le territoire.

Sur le premier point relatif au PIB : un poids très conséquent. L'UE étant très diverse économiquement, retenons que globalement l'activité des banques représente entre 3 et 4 fois le PIB Européen. Pour un pays comme le Luxembourg, ce chiffre est supérieur à 20, alors que pour des Etats comme la Slovénie ou l'Estonie l'ordre de grandeur est très faible[9]. Si l'on prend uniquement les 19 pays de la zone Euro, ce chiffre est précisément de 4.9 fois le PIB. A titre de comparaison … c'est près de cinq fois plus qu'aux Etats-Unis ! Ce chiffre reflète l'engagement massif des banques européennes dans le financement de l'économie.

Si le secteur financier d'un pays est trop élevé par rapport à son PIB, une crise bancaire peut mettre en danger toute l'économie de ce pays. Cela est encore plus vrai si certaines banques présentent des risques systémiques.

La définition commune d'une banque systémique est la suivante : c'est une banque dont la taille et les activités sont tellement importantes que si elle venait à faire faillite, cela aurait un impact énorme sur le système financier mondial. Il en est recensé une trentaine dans le monde. Cette liste est régulièrement mise à jour par le Conseil de Stabilité Financière (CSF). Cette organisation est une organisation internationale rattachée au G20. La France compte dans cette liste BNP Paribas, le groupe BPCE, le Crédit Agricole ou encore la Société Générale.

Sur le deuxième point, à savoir celui de l'emploi[10]. Historiquement, la banque a été un très gros employeur mais un déclin inexorable a été enclenché depuis 15 ans, pour résumer. La digitalisation des activités financières, les taux bas et la crise Covid en ont accéléré les tendances.

En 2021 en France, le secteur employait ainsi 354 000 salariés selon les chiffres de la FBF. Ce chiffre décline cependant d'année en année depuis le début des années 2010.

Il en est de même dans les principaux pays européens, Ainsi à cette date l'Allemagne, qui est le plus gros employeur du secteur sur l'UE, comptait 657 000 salariés selon les données de la Fédération bancaire européenne (EBF), contre 579 000 à fin 2019. La chute est très forte aussi aux Pays-Bas, avec plus de 60 000 emplois en moins sur la période couvrant 2010 - 2019, soit près d'un sur deux.

Le contexte est aussi très perturbé dans le sud de l'Europe : en Espagne où se multiplient les fusions entre banques, et qui a été touchée de plein fouet par les deux crises de 2007 et 2011, la baisse a fait tomber l'effectif total à moins de 175 000 personnes à fin 2019. Selon ces mêmes données, l'Italie a perdu près de 40 000 emplois sur la période.

A la lueur des éléments précités, et en prenant évidemment en compte leur activité, on comprend donc aisément pourquoi les banques sont essentielles au bon équilibre financier, économique et social dans l'UE. Tout élément qui pourrait les fragiliser, crise cyber par exemple, aurait donc un impact « énorme » et explique que le secteur soit naturellement classé comme vital / essentiel par les autorités françaises et européennes.

[9] Bank assets (As % of GDP). HelgiLibrary [en ligne]. 2022. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://www.helgilibrary.com/indicators/bank-assets-as-of-gdp/

[10] LEDERER, Edouard ; GUEUGNAU, Romain. L'emploi dans la banque à son plus bas niveau depuis trente ans en France. Les Echos [en ligne]. 22 juin 2021. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/banque-assurances/lemploi-dans-la-banque-a-son-plus-bas-niveau-depuis-trente-ans-en-france-1325845#:~:text=Gestion%20d'actifs-,L'emploi%20dans%20la%20banque%20%C3%A0%20son%20plus%20bas%20niveau,ont%20jamais%20%C3%A9t%C3%A9%20aussi%20bas.

Pour le **troisième point**, zoomons enfin sur le Top 10 Européen, Royaume-Uni inclus[11] :

Rang	Nom de l'établissement	Nationalité
1	HSBC Holdings plc	Royaume-Uni
2	BNP Paribas SA	France
3	Crédit Agricole Group	France
4	Deutsche Bank AG	Allemagne
5	Banco Santander SA	Espagne
6	Barclays plc	Royaume-Uni
7	Société Générale SA	France
8	Groupe BPCE	France
9	Lloyds Banking Group plc	Royaume-Uni
10	UniCredit SpA	Italie

La France et le Royaume-Uni y prennent la part du lion avec 4 et 3 représentants respectivement. Le poids de l'Allemagne dans ce classement y est en revanche faible, en tout cas il ne reflète ni son poids économique dans l'UE, ni sa force en matière de commerce extérieur. Ceci découle aussi de la structure capitalistique de ses principales banques (à la fois régionales et mutualistes). Il faut aussi relever que l'UE a vu son profil bancaire, et plus globalement financier, se recomposer depuis le Brexit. Il est certain que la City possède une force de frappe très importante, mais elle s'inscrit désormais hors du jeu. Cet élément est à la fois un risque et une opportunité, nous y reviendrons, en offrant à Paris, Francfort ou Amsterdam, l'occasion d'y renforcer leurs positions et d'y relocaliser des activités stratégiques. C'est un point qu'il faut de même intégrer dans une logique souveraine.

Par-delà leur nombre d'employés, la taille de leur bilan, soulignons enfin le caractère stratégique des banques en matière de financement de l'économie. Un exemple suffira à l'illustrer : est-il possible d'imaginer un dispositif de soutien tel que le Prêt Garanti par l'Etat (PGE) en France, sans la participation active des banques commerciales[12] ? Pour mémoire ce sont près de 145 milliards EUR qui ont été débloqués aussi bien pour des TPE/PME que des fleurons de l'économie française (par exemple Air France ou Renault). Que ce soit en temps de crise, comme aujourd'hui, et demain pour son verdissement et sa digitalisation, il n'est point de salut pour une économie sans un système bancaire et financier, sain et résilient.

Une réglementation financière européenne en renforcement constant depuis 2008

La crise financière de 2008 a agi comme un révélateur pour les régulateurs du secteur financier partout dans le monde. Elle a en effet mis à jour une fragilité plus importante du secteur qu'on ne pouvait - devait - le supposer. Par conséquent, des nouvelles normes ont été graduellement mises en œuvre depuis lors, touchant ses domaines clés afin d'en garantir un niveau de résilience supérieur. C'est le cas par exemple des réformes Bâle III qui ont vu le jour à cette période sous l'impulsion du Conseil de Stabilité Financière et du G20 afin de garantir un niveau minimum de capitaux propres et renforcer la solidité financière bancaire.

[11] PROTSKA, Olga. Top 20 des plus grandes banques 2022 par le total des actifs. FXSSI [en ligne]. 27 janvier 2022. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://fr.fxssi.com/top-20-des-plus-grandes-banques

[12] MINISTERE DE L'ECONOMIE DES FINANCES ET DE LA RELANCE. Prêt Garantie par l'Etat – Situation au 31 décembre 2021. Ministère de l'Economie des Finances et de la Relance [en ligne]. 31 décembre 2021. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.economie.gouv.fr/files/files/directions_services/covid19-soutien-entreprises/PGE_20211231.pdf

En complément de ces dispositions prises au niveau mondial, l'UE s'est aussi positionnée à la pointe dans le domaine régulatoire par rapport aux autres zones économiques de référence. Ces dispositions sont venues souvent s'ajouter ou se compléter à d'autres dispositions prises à l'échelon national. Ces éléments illustrent la réglementation « robuste » de l'UE, entendre ce terme sous l'angle à la fois de sa densité et sa complexité.

De plus, ces dispositions propres au monde financier (« verticales ») sont complétées par des dispositions « horizontales », c'est à dire intersectorielles, lesquelles viennent donc enrichir l'encadrement du secteur. Dans ce domaine, la directive NIS aujourd'hui en vigueur est un élément essentiel dans le domaine de la cybersécurité en Europe. Nous en citerons quelques-unes plus bas dans cette section, afin d'illustrer les avancées en matières numériques tant sur la protection des données que des infrastructures.

Vue récapitulative des principales mesures pour la Finance dans l'UE[13]. Nous avons listé ci-après les réglementations majeures adoptées ces 10 dernières années. La liste est conséquente et démontre les frontières sans cesse évolutives des normes et lois auxquelles doivent se conformer les acteurs.

- Règlement (EU) No 648/2012 sur la transparence des marchés dérives (« EMIR »), en vigueur depuis Août 2012.
- Règlement (EU) No 236/2012 sur la vente à découvert, en vigueur depuis novembre 2012.
- Directive 2011/89/EU sur la surveillance complémentaire des entités financières en vigueur depuis juin 2013.
- Règles uniques sur les exigences prudentielles pour le capital, la liquidité et l'effet de levier des banques et règles plus strictes en matière de rémunération et amélioration de la transparence (« CRD IV / CRR »), en vigueur depuis Décembre 2013 et Janvier 2014.
- Nouveau cadre européen de surveillance des assureurs (« Omnibus II ») en vigueur depuis Mars 2015.
- Directive 2014/49/EU sur les Systèmes de garantie des dépôts, en vigueur depuis juillet 2015.
- Directive 2014/17/EU sur les crédits hypothécaires, en vigueur depuis Mars 2016.
- Renforcement du régime de lutte anti-blanchiment, en vigueur depuis mai 2017.
- Cadre renforcé pour les marchés d'instruments financiers (« MIFID II/MIFIR »), en vigueur depuis Janvier 2018.
- Directive (EU) 2015/2366 sur les services de paiements (PSD 2), en vigueur depuis janvier 2018.
- Règlement (EU) 2016/1011 sur les indices utilisés comme références dans les instruments financiers et les contrats financiers ou pour mesurer la performance des fonds d'investissement, appliquée depuis janvier 2018.
- Règlement (EU) 2017/1129 sur le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé, appliqué depuis juillet 2019.

A ces éléments propres au monde financier, ajoutons aussi des mesures numériques non sectorielles prises par l'UE, et impactant la Finance sous les angles cybersécurité, protection des données, ou encore fonctionnement de l'espace numérique.

RGPD et NIS. Ainsi depuis 2016, l'Europe a adopté puis mis en œuvre un pack numérique avec le Règlement Général sur la Protection des Données (RGPD) et la directive NIS. Le RGPD, entré en vigueur en mai 2018, est venue renforcer les obligations des entreprises en matière de protection des données personnelles, dont la Finance est une grosse consommatrice (confère plus bas).

[13] Rapport 2017 des autorités européennes de surveillance – 6.2 Problem definition. Commission européenne [en ligne]. 20 septembre 2017. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0308&from=GA

Dans la même veine, la directive NIS va être amendée avec NIS 2. Cette nouvelle mouture a pour principal objectif d'harmoniser les exigences de cybersécurité entre les Etats membres et de définir des mécanismes de coopération pour mieux gérer les risques cyber. Ainsi un réseau européen pour la préparation et la gestion des crises cyber (UE-CyCLONe) va voir le jour. Il sera chargé de coordonner la gestion des incidents majeurs et d'éviter une éventuelle crise cyber passée par un maillon faible de l'Union. La directive étend aussi et surtout le périmètre des secteurs concernés par des obligations de cybersécurité. Jusqu'alors la liste des opérateurs de services essentiels (OSE) était laissée à la discrétion des Etats membres.

Désormais, la directive en fixe directement les critères. Aux domaines d'ores et déjà concernés (banques, marchés financiers, énergie, transport, santé, eau potable et réseaux télécoms), il va s'ajouter de nouveaux secteurs comme la gestion des déchets, les services postaux, les grands distributeurs alimentaires, ou encore les fournisseurs d'accès à internet et les datacenters. Les obligations seront cependant modulées par secteur avec un « plafond » pour n'impacter que les grandes et moyennes structures. Un principe important, il faut le souligner comme pour DORA et attestant du caractère pragmatique du régulateur.

DMA, **DSA**, **MiCA**, **EPI**. Les éléments évoqués illustrent de façon plus large, le renforcement de l'agenda européen 2022 sur le numérique. La prochaine étape ouverte est celle du **Digital Market Act** (**DMA**) tout juste adopté, et qui qui vient poser une pierre supplémentaire dans le jardin des GAFAM.

Le règlement DMA entrera en vigueur en 2023. Pour résumer, l'objectif est d'empêcher les Google Amazon Facebook Apple Microsoft (GAFAM) de tirer avantage de leur place centrale dans l'écosystème pour affermir encore plus leur domination, mettre la concurrence hors-jeu, et rendre leurs utilisateurs plus dépendants. Le DMA met aussi l'accent, comprendre un frein, sur l'exploitation des données personnelles. Le texte comportera des « obligations applicables immédiatement, des délais courts et stricts et des sanctions dissuasives » dixit Thierry Breton, commissaire européen au Marché Intérieur. Sur ce dernier point, leur montant pourra aller de 6 à 20% du chiffre d'affaires mondial.

En plus du DMA, l'UE travaille au **Digital Service Act** (**DSA**). Ce règlement sur les services numériques vise, lui, à moderniser une partie de la directive e-commerce de 2000 jusque-là inchangée. Il s'attaque aux contenus (haineux, terroristes…) et aux produits illicites (contrefaits ou dangereux) proposés en ligne. Il vise en particulier à harmoniser les législations nationales déjà en place dans les Etats membres. Toutes les entreprises proposant des « services intermédiaires » aux utilisateurs européens sont concernées : fournisseurs d'accès à internet, services en nuage, messageries, places de marché, réseaux sociaux… Des obligations supplémentaires sont prévues pour les hébergeurs, dont les plateformes, et plus encore pour les très grandes plateformes (plus de 45 millions d'utilisateurs actifs chaque mois, soit 10 % de la population européenne).

Citons pour conclure le texte pour les **Markets in Crypto-Assets** (**MiCA**) actuellement discuté et qui va venir réguler les crypto assets[14]. Enfin pour les paiements, il y a la **European Payments Initiative** (**EPI**). En juillet 2020, seize grandes banques européennes de cinq pays (Allemagne, Belgique, Espagne, France et Pays-Bas) ont annoncé le futur lancement de l'EPI. Elle a pour ambition de créer une solution de paiement unifiée pour les consommateurs et les commerçants en Europe, comprenant une carte de paiement et un porte-monnaie numérique, et couvrant les paiements en magasin, les paiements en ligne, les paiements de particulier à particulier, ainsi que les retraits d'espèces.

La proactivité européenne sur ces questions fondamentales touchant à l'espace numérique et financier n'est donc plus à démontrer. Il est tout aussi fondamental par conséquent d'en assurer sa résilience, il en va de l'intérêt de toutes les parties prenantes.

[14] TZIALLI, Andrew. EU crypto regulation update (April 2022) : EU Bitcoin ban shelved – and MiCA moves forward. PhilipLee [en ligne]. 19 avril 2022. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.philiplee.ie/eu-crypto-regulation-update-april-2022-eu-bitcoin-ban-shelved-and-mica-moves-forward/

Soulignons au passage le rôle moteur de la France dans le cadre de sa présidence actuelle du Conseil de l'Union.

Et en conclusion, relevons un constat … Là aussi l'histoire s'accélère.

Eclairage de la Banque de France (BDF) sur les risques cyber et la transformation numérique

Dans son rapport annuel d'évaluation des risques financiers 2021[15], la Banque de France (BDF) a dressé, comme elle le fait à chaque occasion, une matrice des risques pour le secteur financier. En résumé, la BDF a recensé cinq risques majeurs :

1. Valorisation élevée des marchés.
2. Conséquences macro-financières de l'endettement élevé.
3. Pressions sur la rentabilité des banques et le rendement des placements des assurances.
4. Transformation numérique et menaces cyber.
5. Exposition au changement climatique.

Dans ce top 5, le premier risque cité est jugé « très élevé » avec une tendance jugée à la « hausse » dans les six prochains mois.

Les quatre autres dont le **cyber** sont évalués en « **risque élevé** » avec une tendance « stable » dans la même période.

Rappelons que cette évaluation est faite à dires d'experts et motivée ainsi :

Vulnérabilités

- Transformation numérique des acteurs financiers qui oblige à un changement de modèle d'affaire.
- Accroissement de la surface numérique augmentant l'exposition aux attaques cyber.

Résilience

- Initiatives pour renforcer le système financier face aux attaques cyber (exercices de crise, travaux règlementaires).

[15] BANQUE DE FRANCE. Rapport annuel 2021. Banque de France [en ligne]. Mars 2022. [Consulté le 15 février 2022]. Disponible à l'adresse : https://www.banque-france.fr/sites/default/files/medias/documents/rabdf-2021_web2.pdf

Ce constat est tout sauf une surprise. Il s'agit davantage d'une confirmation. Il rejoint directement les analyses européennes et internationales. Il est intéressant de noter que la BDF précise dans ce même rapport que le **projet de règlement DORA vise à « garantir une plus grande harmonisation des règles de gestion du risque cyber en Europe** ».

Cela découle du fait d'imposer aux entités du secteur de la finance une cartographie formalisée de leurs actifs informatiques et de leurs risques associés, avec une gouvernance adaptée à la gestion du risque cyber. Le document souligne les bienfaits de DORA en termes de mesures de protection des systèmes et des données, et d'un processus de détection des anomalies. Il souligne enfin le bien-fondé de mener des tests de sécurité et des exigences sur la gestion des risques liés aux prestataires informatiques.

En somme, DORA est attendu avec impatience et porte de nombreux espoirs en son sein pour la BDF. Réjouissons-nous de cette position, tout en demeurant conscients de la réalité des risques. Puisqu'ils sont élevés, les attentes sont élevées. Et soyons enfin conscients que le secteur est fortement exposé et ne présente pas, au moment où nous écrivons ces lignes, une homogénéité dans sa préparation, sa résilience, et sa capacité de traitement.

La finance ne se cantonne pas aux grandes banques et assurances, elle se ramifie et s' *« Uberise »* de plus en plus. Les acteurs émergents ont une longueur d'avance technologique mais ils ne disposent ni du vécu, ni des équipes en nombre et en compétences, et encore moins de l'organisation des géants en matière de résilience. Il est donc nécessaire que la réglementation les invite à faire plus et mieux en ce domaine. Il ne peut d'ailleurs pas en être autrement car il en va de la crédibilité et de la résilience du secteur dans son ensemble.

Tour d'horizon international comparatif

Comme évoqué précédemment, le monde financier est sans frontières et interconnecté. Ce faisant, il convient de porter un regard sur ce que les autres places fortes financières hors UE font en matière de régulation sur les aspects cyber et numériques.

A cette fin, notre regard va se porter dans cette section sur trois zones d'importance : les Etats-Unis, le Royaume-Uni (pour l'Europe hors UE) et enfin Hong Kong en tant que principale place financière asiatique avec Singapour.

Focus Etats-Unis[16]

Les Etats-Unis ont historiquement mis très en avant la nécessité d'agir pour la cybersécurité des acteurs financiers… et au-delà. Cette volonté est politique et elle s'est traduite dans les discours comme dans les actes.

Computer Fraud and Abuse Act (CFAA). Dès 1986, le gouvernement fédéral a adopté le CFAA, loi qui porte sur la sécurité des systèmes d'information. Il s'agit d'un amendement à une loi sur les fraudes informatiques, qui fait maintenant partie du « Comprehensive Crime Control Act of 1984 ». Pour justifier cette loi, la chambre des Représentants s'est basée sur le film « War Games » réalisé un an plus tôt et qui a alors marqué les esprits sur le risque d'intrusion informatique. Quand la fiction anticipe la réalité, cela peut aussi se traduire bénéfiquement.

Cette loi interdit tout accès à un ordinateur sans autorisation préalable ou tout accès qui excède les autorisations.

Notons qu'en théorie les seuls ordinateurs couverts par le CFAA sont définis comme des « ordinateurs protégés » selon cette définition: « *Ordinateur exclusivement à l'usage d'une institution financière ou du gouvernement des États-Unis, ou de tout ordinateur, lorsque le comportement constitutif de l'infraction affecte l'utilisation de l'ordinateur par ou pour l'institution financière ou le gouvernement ; ou qui est utilisé dans le cadre du commerce ou de la communication entre États ou à l'étranger ou qui a une incidence sur ceux-ci, y compris un ordinateur situé en dehors des États-Unis qui est utilisé d'une manière qui a une incidence sur le commerce ou la communication entre États ou à l'étranger*. »[17]

---

[16] DESAI, Shardul. The impact of cybersecurity regulations on the financial services industry in 2022. Holland&Knight [en ligne]. 12 janvier 2022. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://www.hklaw.com/en/insights/publications/2022/01/the-impact-of-cybersecurity-regulations

[17] Computer fraud and abuse act. Wikipedia [en ligne]. 2021. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Loi Gramm-Leach-Bliley Act (GLBA). Cette loi adoptée en 1999 est venue renforcer les obligations à destination des institutions financières. Pour mémoire, la GBLA[18] a réformé le secteur des services financiers, permettant aux banques commerciales et d'investissement, aux sociétés de titres et aux compagnies d'assurance de consolider et de résoudre les problèmes concernant la protection de la confidentialité des consommateurs.

Les différentes administrations ont depuis maintenu le cap initié dans les années 1980 et 1990. L'actuelle administration Biden a accentué le mouvement, plus que jamais consciente des enjeux et des risques associés à cette thématique cyber. Les dossiers Colonial Pipeline ou encore Solar Winds ont de ce point de vue été des accélérateurs sur la nécessité d'agir plus et mieux encore.

Le cyber, un enjeu majeur autour de la finance. En 2019, les Etats-Unis ont mis en place l'initiative dite « Safe Harbor », dont nous livrons les détails en annexe. Pour résumer, celle-ci est axée sur 3 piliers : un stockage sécurisé des données et comptes clients, la résilience des acteurs et une certification des entités participant via un processus de contrôle strict.

Il convient de noter que le « Safe harbor » a été soutenu par l'ensemble de l'écosystème de la finance, ce qui atteste de la volonté collective d'agir de ses membres.

De nouvelles mesures fin 2021 et en 2022. Les autorités financières américaines viennent de prendre de nouvelles mesures autour de 3 axes (i) Gouvernance cyber (ii) Contrôles internes et notification d'incidents et (iii) Culture des équipes.

Ces nouvelles dispositions se traduisent ainsi pour les acteurs du monde financier :

- L'obligation pour les intéressés de se conformer à des règles précises en matière de cybersécurité et de renforcer leurs procédures écrites de cybersécurité
- Les institutions financières doivent développer en interne un reporting visant à assurer une notification rapide aux régulateurs de tout incident cyber, et ce dès sa survenance ou le plus rapidement (voir détails plus bas)
- Les entreprises financières visées doivent enfin fortement encourager une culture de la conformité autour des enjeux de la cybersécurité et se préparer à toute visite de contrôle diligentée par les régulateurs.

En pratique, il est désormais requis :

1. **Aux institutions bancaires de** reporter sous 36 heures tout « incident de sécurité informatique ».
2. **Aux fournisseurs des établissements bancaires** de notifier tout « incident de sécurité informatique » dans les meilleurs délais.

[18] ROBMAZZ ; OLPROD. La loi Gramm-Leach-Bliley Act (GLBA). Microsoft [en ligne]. 23 septembre 2021. [Consulté le 23 avril 2022]. Disponible à l'adresse : https://docs.microsoft.com/fr-fr/compliance/regulatory/offering-glba

Tableau récapitulatif des obligations déclaratives - Source Holland and Knight (2022)

Obligations de Notifications pour le Secteur Financier		
Incidents à notifier	**Délais**	**Auprès de qui**
Notification d'incident	Dans les 36 heures	OCC, FRB, FDIC
Accès non autorisé ou utilisation d'informations sensibles sur les clients	Dès que possible	OCC, FRB, FDIC
Incident de sécurité informatique perturbant ou dégradant matériellement	Dès que possible	Clients des organismes bancaires
Risques ou incidents matériels en matière de cybersécurité	En temps opportun	Dépôt auprès de la SEC
Événement sur la conformité et l'intégrité des systèmes	Dans les 24 heures	SEC

Quatre entités font autorité en ce domaine réglementaire : la Federal Trade Commission (FTC), l'Office of the Controller of the Currency (OCC), le Board of Governors of the Federal Reserve System (FRB) et la Federal Deposit Insurance Corporation (FDIC). Leur volonté commune est de renforcer les mesures qui existaient jusqu'alors et d'assurer davantage de cohérence collective.

La SEC est aussi à la manœuvre. De plus, notons que la Securities and Exchange Commission (SEC)[19] a annoncé pour la première fois des mesures concrètes visant les institutions financières qui ne lui notifieraient pas ses contrôles déficients en matière de cybersécurité. En mars de cette année, elle a insisté sur quatre points visant à mieux protéger les investisseurs de marché (1) incidents cybers significatifs, (2) stratégie et risk management (3) gouvernance, and (4) expertise cyber du comité de direction. La SEC a aussi proposé d'établir des obligations en matière de reporting déclaratif, dont les modalités sont actuellement en cours de négociations.

Observe-Act-Report. Par-delà le monde de la finance, la Cybsersecurity and Infrastructure Agency (CISA) édicte bien sûr des mesures et normes intersectorielles. Relevons ces dernières semaines le Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Cet acte encourage aussi la collaboration et le partage d'informations entre les acteurs opérant dans les industries critiques. Il s'articule autour du triptyque « Observe – Act – Report ». Là encore, l'objectif est de promouvoir de bonnes pratiques en matière de remontée d'incident.

Les notions de transparence, de partage et de collaboration sont des facteurs clés de succès en matière de lutte cyber. « Success is a sports team » … une devise plus que jamais en vigueur dans le domaine cyber pour les autorités américaines.

[19] COIE, Perkins. SEC proposes new cybersecurity disclosure rules on incident reporting risk, risk management, strategy, and governance. JDSupra [en ligne]. 15 avril 2022. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.jdsupra.com/legalnews/sec-proposes-new-cybersecurity-7271669/

Focus Royaume-Uni

Chacun connaît le poids de l'industrie financière au Royaume-Uni, dont la ville de Londres est l'emblème. La sortie de l'Angleterre de l'UE a bien sûr eu une multitude d'impacts pour la City, nous en avons évoqué certains plus tôt dans notre rapport. Le Brexit a en même temps révélé la nécessité d'agir proactivement sur la résilience de monde de la finance. Cet enjeu a été pris en mains par les autorités, en premier lieu la Bank of England (BoE). **En 2019**, **la BoE**[20] a ainsi diligenté un rapport relatif aux enjeux à relever par le secteur financier. Ce document préparé par Huw van Steenis met alors clairement en avant neuf défis majeurs pour l'industrie, dont l'un est intitulé « Enhance protection against cyber-risks[21] ».

L'auteur relève que la finance est naturellement soumise chaque jour davantage au danger cyber et fraude, évalué à 450 milliards USD par an au niveau mondial. La Finance est une cible importante et pour cette raison les décideurs anglais le reconnaissent alors comme un des principaux risques systémiques. Le ministère leur recommande d'ailleurs, nous le citons, de « considérer la cybersécurité comme s'il s'agissait de la concurrence d'un rival digital plutôt que comme un sujet de gouvernance sur les risques et contrôles ».

En conclusion, le rapport préconisait déjà aux acteurs du secteur de se focaliser sur cinq piliers :

1. **Préparation**. Avoir un plan et une stratégie élaborés de réponse face au risque cyber.
2. **Evaluation** et **amélioration continue**. Tester ce plan via différents moyens dont des tests d'intrusion, et en tirer des enseignements en matière d'amélioration continue.
3. **Reprise et continuité d'activité**. Avoir un plan effectif, rapide à mettre en œuvre et offrant une vue d'ensemble.
4. **Leçons retenues**. Promouvoir des réponses coordonnées, en retenir les leçons via des
5. **Remontées** et des partages d'information de façon sécurisée.

[20] BANK OF ENGLAND. Future of the finance – Renew on the outlook for the UK Financial system : what it means for the Bank of England. Bank of England [en ligne]. Juin 2019. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.bankofengland.co.uk/-/media/boe/files/report/2019/future-of-finance-report

[21] En Français, Renforcer la protection contre les cyber-risques

Sous l'égide de la BoE, les autorités compétentes[22] ont depuis lors décidé de mesures concrètes visant à renforcer deux axes. Il s'agit de la cyber résilience et de la résilience opérationnelle pour le secteur financier dans son ensemble, incluant en cela les fournisseurs d'infrastructures numériques.

Résilience opérationnelle. Sous ce terme, la BoE entend la capacité des acteurs du secteur financier dans leur ensemble à absorber et à faire face à tout choc ou événement disruptif. Cette notion va au-delà des plans de continuité. Les entités financières et les fournisseurs doivent se doter de plans robustes pour délivrer leurs services essentiels en toutes circonstances.

Il leur faut pour cela englober les menaces de types humaines, comme celles d'origines physiques mais aussi les cyber-attaques, les pannes informatiques et les défaillances de fournisseurs. Cela inclut aussi les catastrophes naturelles et les pandémies.

Une action collective. Les autorités ont aussi mis sur pied un groupe appelé « Cross Market Operational Resilience Group » (CMORG). Il mène des actions de coordination pour l'ensemble du secteur financier sur les questions de résilience. Il est composé de 25 membres, représentatifs des banques, des assureurs et des fournisseurs, des autorités financières du pays et du National Cyber Security Centre (NCSC). Il est co-présidé par des membres dirigeants de la Prudential Regulation Authority (PRA) et du ministère des Finances.

Le CMORG a trois objectifs fondamentaux qui sont :

- Identifier les risques de continuité du secteur financier.
- Développer des solutions d'amélioration pour sa résilience opérationnelle.
- Partager connaissances et expertise.

Résilience Cyber. Afin de garantir la résilience du secteur et sa plus juste supervision, les autorités britanniques ont développé deux outils le CBEST et le CQUEST.

CBEST. C'est un dispositif mis en place par le régulateur. Il lui permet de travailler avec les acteurs financiers en vue de simuler des cyber attaques. Ce cadre permet à ces entités d'explorer comment une attaque peut 'disrupter' leur organisation et leurs contrôles sous les angles humains, technologiques et processus. L'objectif du CBEST est de :

- Tester les défenses de l'entité.
- Mesurer ses capacités en termes de Threat Intelligence[23].
- Évaluer sa capacité de détection et de réponse à une série d'attaques venues de l'externe ou de l'interne.

Le CBEST se base sur des simulations d'attaques. Les opérations sont menées par un prestataire agréé qui va donc tenter de s'infiltrer chez la cible via la « cyber kill chain ». Ils évaluent dans le même temps si la confidentialité, l'intégrité et la disponibilité des systèmes et process critiques à l'entreprise peuvent être compromis.

CQUEST. Si les autorités souhaitent estimer plus généralement la cyber résilience d'une entité, elles leur demandent d'utiliser le CQUEST. C'est un questionnaire qui aborde des points tels :

- Est -ce que votre entité a une stratégie cyber approuvée par la direction générale ?
- Est-ce que votre entité a identifié et protégé ses actifs clés ?
- Comment votre entité détecte et répond à un incident, restaure son activité et en tire les leçons ?

Les réponses fournissent un aperçu de la capacité de résilience d'un établissement et mettent en lumière des axes d'amélioration. S'agissant de la protection des données, le RGPD s'applique encore, mais une consultation a été lancée pour réformer ce cadre [24].

[22] Operational resilience of the financial sector. Bank of England [en ligne]. 20 octobre 2021. [Consulté le 24 avril 2022]. Disponible à l'adresse : https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector

[23] En français, «renseignement sur les menaces »

[24] HEYWOOD, Debbie.UK announces plans to depart from GDPR. TaylorWessing [en ligne]. 15 septembre 2021. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.taylorwessing.com/en/insights-and-events/insights/2021/09/uk-announces-plans-to-depart-from-gdpr

Focus Hong Kong

Terminons notre tour d'horizon comparatif par l'Asie en nous concentrant sur Hong Kong, la principale place financière de la zone avec Singapour.

Dès 2016, les autorités de la Région Administrative Spéciale de Hong Kong ont pris pleinement conscience de la menace cyber et décidé d'œuvrer à l'amélioration de la protection de leur écosystème financier.

Cette action a faite suite à l'incident ayant affecté le réseau SWIFT, à savoir une cyber-attaque attribuée au groupe APT 38 Lazarus, qui causa des dommages conséquents à différentes institutions financières dont la Banque du Bangladesh (i.e. circa 100 millions de dollars de pertes via son compte à la Réserve Fédérale US).

Des travaux ont alors été menés sous l'égide de la Hong Kong Monetary Authority (HKMA), l'autorité de tutelle du secteur financier local afin de renforcer la résilience de l'écosystème.

Cybersecurity Fortification initiative (**CFI**). La concrétisation s'est faite via le lancement de l'initiative dite CFI. Il s'agit d'une approche pluriannuelle visant à renforcer la cybersécurité des établissements bancaires.

L'initiative repose sur 3 piliers :

1. **Dispositif d'évaluation de Cyber Resilience** (**CRAF**). Ce cadre vise à évaluer (i) le risque inhérent de chaque établissement, avec un rating Low-Medium-High, (ii) son niveau de maturité et (iii) mener une « Intelligence-led Cyber Attack Simulation Testing » (iCAST) pour les établissements ayant été notés Low ou Medium. Le but est de simuler une cyberattaque sous les angles techniques, humains et processus.
2. **Programme de Développement Professionnel** (**PDP**). Cet aspect met en avant la dimension humaine via la formation et la sensibilisation des personnes. Notons que ce dispositif bénéficie du soutien du CREST entité du Royaume-Uni qui a contribué aux initiatives CBEST et CQUEST évoquées plus tôt.
3. **Cyber Intelligence Sharing Platform** (**CISP**). L'objectif est de mutualiser les efforts de chaque établissement en matière de Threat Intelligence et de favoriser la collaboration, facteur clef de succès en ce domaine.

Depuis le 1er janvier 2021, la HKMA a renforcé le dispositif CFI, devenu CFI 2.0[25]. Les nouveautés sont reprises ci-dessous (source site officiel HKMA). L'accent est mis sur la nécessité de hausser encore la qualité de la formation, et d'insister sur la coopération.

Évaluation des risques - Introduction de nouveaux principes de contrôle améliorés reflétant les récentes bonnes pratiques internationales en matière de réponse et de récupération en cas de cyber incident, ainsi que les dernières tendances technologiques (par exemple, le cloud) ;

Introduction des exigences de la « Blue Team » pour iCAST afin de mesurer l'efficacité des fonctions de détection, de réponse et de récupération des institutions visées ;

Permettre plus de flexibilité aux institutions pour exploiter les résultats d'évaluations similaires de la cyber-résilience réalisées par leurs groupes bancaires ou leur siège social ;

PDP

- Développement des talents.
- Mettre à jour et élargir la liste des cyber qualifications professionnelles minimum pour effectuer des évaluations C-RAF, y compris les nouvelles qualifications iCAST en matière de renseignements sur les menaces ;

CISP

- Partage d'informations
- Recommander le développement d'un modèle opérationnel cible pour améliorer la convivialité du CISP en décrivant la gouvernance, les rôles et les responsabilités des utilisateurs ;
- Élargir l'adhésion au CISP aux membres à bord de l'association des Deposit Taking Companies (DTC) et d'autres secteurs financiers.

Notons que la HKMA a complété ce dispositif de cyber résilience par deux autres mesures ayant trait à la :

1. Protection des données des clients des institutions financières (depuis 2014[26]) en instaurant règles et contrôles préventifs sur la perte / fuite de données personnelles et
2. Gestion du risque informatique des institutions financières[27], texte non réglementaire mais donnant des guidelines et recommandations pratiques

L'ensemble de ces mesures attestent du sérieux avec lequel les autorités hongkongaises s'attellent au sujet, et de leur pragmatisme en vue d'assurer une amélioration continue du dispositif en place.

[25] Cybersecurity fortification initiative 2.0. Hong Kong Monetary Authority [en ligne]. 3 novembre 2020. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201103e1a1.pdf

[26] Customer Data Protection. Hong Kong Monetary Authority [en ligne]. 14 octobre 2014. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf

[27] Supervisory Policy Manual – General principles for technology risk management. Hong Kong Monetary Authority [en ligne]. 24 juin 2003. [Consulté le 22 avril 2022]. Disponible à l'adresse : https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf

CHAPITRE 2

Les enjeux de la résilience opérationnelle numérique

Vers une nouvelle ère de la résilience

La résilience opérationnelle est sans doute désormais aussi importante pour le secteur des services financiers que la résilience financière elle-même. Cela a été évoqué à plusieurs reprises précédemment, le secteur financier est fortement exposé aux risques numériques avec le développement de la dématérialisation, l'augmentation et la concentration du nombre de fournisseurs tiers, la forte interconnexion entre les systèmes d'information et les vulnérabilités liées aux innovations technologiques.

Qu'est-ce qu'est la résilience opérationnelle aujourd'hui ?

La capacité à maintenir en continu les opérations face aux événements cyber : Prévenir, réagir, rétablir et apprendre des perturbations opérationnelles.

Exposition aux risques Un secteur financier très exposé au développement de la dématérialisation, de l'interopérabilité, des vulnérabilités dues aux innovations technologiques, et à l'accroissement des fournisseurs de TIC et prestataires de services.	**Nature des risques** La nature des risques évolue constamment et rapidement : des nouvelles cibles/surfaces d'attaques, des attaques plus sophistiquées et mieux préparées.
Pression régulatoire L'évolution des exigences des régulateurs : selon la BCE, Il y'a nécessité de veiller régulièrement à la performance des moyens/capabilités de résilience, ainsi qu'à l'évolution des innovations.	**Marchés** L'émergence de nouveaux canaux et marchés engendrent de nouveaux risques, de nouvelles surfaces d'exposition et d'attaques.
Volume de données Un volume de données qui explose.	

La résilience opérationnelle numérique c'est la résilience financière.

Avec l'augmentation des incidents opérationnels, réduire les risques d'interruptions des systèmes d'information dans les services financiers devient de plus en plus critique.

Ce ne sont pas seulement les entreprises de services financiers et les fournisseurs de services numériques tiers qui se focalisent sur la résilience opérationnelle. Les régulateurs du monde entier s'intéressent également de plus en plus à la capacité des entreprises à s'adapter et à se remettre des perturbations opérationnelles. Ceci montre le rôle central du secteur des services financiers dans le contexte sociétal et les impacts significatifs qui pourraient survenir lorsque certaines entreprises ne fonctionnent pas de manière résiliente.

La résilience opérationnelle est devenue une priorité pour les plus hautes instances politiques européennes, les acteurs du secteur financier et les régulateurs.

Pourquoi une entreprise de services financiers doit-elle être résiliente ?

A cette question, il faut apporter au moins 3 éléments de réponses :

Répondre aux exigences réglementaires en constante évolution

La résilience opérationnelle des entreprises du secteur financier est devenue une priorité pour les autorités de contrôle et la Commission Européenne, et est considérée comme non moins importante que la résilience financière.

Les banques centrales et les organes de surveillance évoluent pour faire face aux risques systémiques du système financier en s'appuyant et renforçant la résilience opérationnelle des entreprises du secteur financier.

La résilience opérationnelle est définie comme « la capacité des entreprises à prévenir, s'adapter et réagir, restaurer et tirer des leçons des interruptions/perturbations opérationnelles. »

Il s'agit notamment d'une responsabilité que les entreprises financières ont déjà envers leurs clients, actionnaires et l'économie dans son ensemble dans le cadre de la législation en vigueur et dans des domaines spécifiques tels que la cybersécurité, la gestion des risques et l'externalisation de leurs services.

La résilience opérationnelle des entreprises du secteur financier évolue en fonction des changements du secteur et des innovations technologiques. Ces changements incluent :

Une **interconnexion accrue** entre les entreprises et services du secteur financier et les fournisseurs tiers (tels que les fournisseurs de services cloud) qui augmente le risque d'incidents de service ;

Une **sophistication et surface accrue des cyberattaques** pouvant entrainer un plus grand potentiel de perturbation des services financiers et ainsi impacter des marchés entiers ;

Une **dépendance plus grande vis-à-vis d'un groupe restreint de prestataires**, ce qui a le potentiel d'augmenter le risque de concentration.

Pour ces raisons, la résilience opérationnelle des entreprises est désormais aussi importante que leur résilience financière, car un manque de résilience opérationnelle pourrait entraîner une instabilité financière.

Les régulateurs sont donc censés demander aux entreprises de définir leurs services métiers critiques et de prouver leur résilience par des tests.

Réduire les risques et minimiser les impacts d'interruptions

La complexité des risques liés aux TIC augmente la fréquence des incidents.

La résilience opérationnelle des entreprises est un objectif multidimensionnel qui s'est complexifié ces dernières années.

Nombre d'entreprises du secteur financier développent des services pour répondre plus rapidement que jamais aux attentes ou exigences croissantes des clients ou du marché. La nécessité de s'adapter rapidement et d'accélérer le rythme des changements et innovations augmente le risque d'interruptions.

La résilience opérationnelle de l'entreprise va désormais au-delà des quatre murs d'une organisation, et englobe tout un ensemble d'un écosystème complexe, comprenant des partenaires et des fournisseurs tiers nécessaires pour fournir ses services.

Grâce aux médias sociaux, le public est désormais informé des pannes majeures ou mineures plus rapidement que jamais. Les interruptions de service peuvent ainsi ternir la réputation des entreprises auprès des clients, des parties prenantes ou des régulateurs, et avoir un impact sur leurs résultats.

De plus, l'impact d'une interruption opérationnelle est désormais bien plus qu'une simple question de pannes de système. De nombreuses entreprises du secteur financier détiennent des quantités toujours croissantes de données. Et cela peut entraîner une plus grande exposition au risque lorsque la fiabilité et l'intégrité de ces données sont menacées par une faille de sécurité. Les entreprises du secteur financier doivent mettre en place des processus pour que les données sensibles restent protégées et ne soient pas compromises.

La reprise d'activité est donc un élément essentiel dans son ensemble.

Se préparer aux menaces de sécurité

Une numérisation, une interconnexion et une dépendance en augmentation constantes à l'égard de tiers ont accru la vulnérabilité du secteur des services financiers aux attaques de sécurité externes.

Un environnement cyber plus hostile a intensifié la nécessité pour les ISF de planifier et d'atténuer les menaces de sécurité. Contrairement à de nombreuses autres sources de risque, les cyberattaques malveillantes sont souvent difficiles à identifier ou à éradiquer complètement.

L'ampleur des dommages peut être difficile à évaluer : les violations de données peuvent passer inaperçues pendant plusieurs mois et peuvent nécessiter plusieurs semaines, voire des mois pour être totalement confinées. Pour rendre les choses plus complexes, alors que la menace d'une cyberattaque externe se développe, les attaques internes deviennent également une préoccupation majeure à prendre en compte.

Que signifie la résilience opérationnelle ?

La résilience opérationnelle fait référence à la capacité des entreprises à prévenir, réagir, restaurer et apprendre des interruptions opérationnelles.

Une entreprise résiliente est en mesure de récupérer ses services commerciaux clés après une interruption imprévue importante, protégeant ainsi ses clients, ses actionnaires et, en définitive, l'intégrité du système financier. La résilience opérationnelle de l'entreprise ne se limite pas à protéger la résilience des systèmes ; il couvre également la gouvernance, la stratégie, les services commerciaux, la sécurité de l'information, la gestion du changement, l'exécution des processus et la reprise après sinistre. Éviter l'interruption d'un système particulier qui prend en charge un service métier contribue à la résilience opérationnelle. Mais en fin de compte, c'est le service métier lui-même qui doit être résilient.

Un élément clé d'une entreprise résiliente est son personnel. Un changement culturel est donc nécessaire pour faire de la résilience opérationnelle une priorité dans l'ensemble de l'organisation, et que tout le monde soit engagé et travaille à cette fin.

Cela comprend la formation du personnel pour comprendre ce qu'implique le risque opérationnel, ainsi que la communication de la haute direction. La propriété des risques clés et les contrôles qui les atténuent doivent être attribués pour maintenir les pratiques de résilience. Des actions correctives doivent être identifiées et, surtout, menées à bien pour créer un cadre de résilience plus solide.

En cas de perturbation, les institutions visées devraient également pouvoir se recapitaliser et se restructurer en utilisant leurs propres ressources financières. En cas de défaillance catastrophique, il est impératif que les institutions du secteur financier puissent continuer à fonctionner pendant que des décisions sont prises sur une éventuelle restructuration ou la fermeture d'opérations pour réduire les dommages et éviter la propagation à d'autres actifs. Un cadre de résilience opérationnelle complet est essentiel pour limiter l'impact des défaillances et assurer une résilience continue du marché, et pas simplement une résilience au sein de l'organisation.

Les défis

Difficultés à améliorer, adapter et maintenir l'efficacité des contrôles…	**... tout en réduisant les coûts**
▪ Les impacts des risques cyber sont assez méconnus, spécialement concernant les environnements critiques, souvent étendus et complexes, tandis que le panorama des menaces est plus large ▪ Un focus cyber quasi-exclusivement orienté vers les technologies, sans tenir compte des priorités « business » de l'entreprise, qui aboutissent à des stratégies cyber décorrélées des intérêts économiques de l'entreprise. ▪ Le développement des contrôles/mesures cyber est une approche principalement « bottom-up » est n'est pas adaptée optimalement aux besoins des métiers. ▪ Un effort cyber mal équilibré avec une attention plus soutenue sur la prévention ou défense (amont) que la détection et la remédiation (aval).	▪ Les nouvelles mesures (contrôles) se chevauchent sans approches de rationalisation stratégique. ▪ Les investissements et le temps sont orientés sur les politiques de conformité de façon déséquilibrée aux dépens de la protection des environnements numériques les plus critiques, et le management des risques et menaces cyber. ▪ Les budgets sont souvent inadéquats, pas efficacement attribués, et l'impact financier des attaques cyber est difficile à évaluer. ▪ Difficultés de gérer un nombre croissant de mesures (ou contrôles) cyber sans changer les structures et la taille des organisations.

Les obstacles les plus courants

Priorité et culture

Un service financier unique peut souvent s'étendre sur de nombreuses technologies et fournisseurs tiers. Prenons l'exemple des paiements, où une entreprise financière peut disposer d'une application mobile hébergée dans le cloud, des moteurs de paiement sur un site local, des systèmes de détection de fraude s'appuyant sur une solution tierce et d'un certain nombre de middleware et de composants d'intégration. Lorsque les risques liés à la cybercriminalité et aux personnes sont ajoutés à cette équation, il peut être difficile d'avoir la supervision et le contrôle nécessaire pour avoir une résilience opérationnelle efficace.

Une responsabilité clairement définie est nécessaire pour mesurer, gérer et stimuler la résilience des services métiers et l'orchestration des équipes critiques.

L'approche peut être nouvelle pour certaines organisations, elle nécessite une hiérarchisation et des changements culturels pour être efficace. Chaque équipe concernée doit apporter sa contribution aux évaluations, en améliorant et en testant « leur » composante du service métier. Les équipes doivent être formées, entrainées et intégrées dans le cadre de résilience opérationnelle afin qu'elles disposent des outils et de la motivation nécessaire.

Dans ce cadre, la direction doit se préparer et s'engager dans un programme de résilience et le communiquer aux équipes et aux tiers concernés.

Investissement

Selon la maturité de la résilience de l'entreprise, le coût de la résilience opérationnelle peut être élevé.

Cependant, avec l'attention accrue des organismes de réglementation, l'augmentation des incidents très médiatisés et des cybermenaces, cet investissement dans la résilience est essentiel au maintien et à l'amélioration des services aux entreprises.

À ce titre, les entreprises de la finance doivent également :

Evaluer régulièrement les **risques** opérationnels auxquels elles sont confrontées en fonction des évolutions réglementaires et des risques émergents ;

Analyser les **vulnérabilités** potentielles ;

Mettre en place des **mécanismes** de **défense** appropriés.

Un programme de gestion des risques opérationnels bien aligné et résilient peut non seulement contrôler la volatilité et réduire les coûts engendrés par les défaillances des processus, des personnes et des systèmes, mais aussi libérer et augmenter la valeur intrinsèque des opérations de l'entreprise.

Complexité des systèmes « hérités »

Les systèmes hérités (« *legacy systems* ») des institutions financières peuvent être complexes, et leur maintien à niveau difficile et coûteux.

Pour améliorer la résilience opérationnelle, les applications, ainsi que l'infrastructure et la plateforme complète de ces systèmes hérités, doivent être évalués, mise à niveau, corrigés pour améliorer leurs capacités de résilience.

CHAPITRE 3

Le règlement DORA

Après avoir dressé un panorama général du secteur financier en Europe et rappelé la nécessité de mieux encadrer les questions du numérique, nous allons désormais nous pencher plus en détails sur le texte du règlement DORA.

Rappels et objectifs. La Commission Européenne a publié le 24 septembre 2020 son projet de loi sur la résilience opérationnelle numérique intitulé « *Digital Operational and Resilience Act* », ou DORA.

Le texte, actuellement en cours d'approbation finale, s'appuie sur les exigences existantes en matière de gestion des risques liés aux technologies de l'information et des communications (TIC) déjà élaborées par d'autres institutions de l'UE et regroupe plusieurs initiatives récentes européennes en un seul règlement.

L'objectif est d'établir une base beaucoup plus cohérente et claire afin que les régulateurs et superviseurs financiers de l'UE puissent élargir leur champ d'action en veillant à ce que les entreprises maintiennent des opérations résilientes en cas de perturbations opérationnelles graves. Et restent donc financièrement stables.

Ce règlement constitue un développement réglementaire majeur pour les entreprises du système financier. Il s'appuie sur les exigences existantes en matière de gestion des risques liés aux TIC déjà élaborées par d'autres institutions de l'UE. Il regroupe plusieurs initiatives récentes de l'UE en un seul règlement.

DORA vise à :

Etablir un cadre unifié d'exigences pour un éventail large d'entreprises de services financiers dans l'UE dans les domaines de la gestion des risques cyber et TIC, des rapports d'incidents, des tests de résilience et de l'externalisation par des tiers.	Introduire également un cadre qui permet aux superviseurs Européens financiers de superviser les fournisseurs tiers critiques de TIC directement, y compris les fournisseurs de services cloud.
Fournir un cadre complet afin d'harmoniser les processus et les normes de résilience numérique dans l'ensemble du secteur financier.	Renforcer les pouvoirs des superviseurs et permettre une surveillance directe.

Les exigences s'appliqueront aux entités du secteur financier traditionnel, mais aussi aux fintechs et aux prestataires de services tiers des entités financières.

Calendrier. La proposition qui est actuellement en cours d'examen par le Parlement Européen (PE) et le Conseil de l'Europe (CE), devrait entrer en vigueur dans le courant de l'année 2022.

Une fois que DORA entrera en vigueur, les exigences s'appliqueront dans les 27 États membres de l'UE. Elle s'appliquera tel-quelle sous la forme d'une réglementation. Elle renforcera de façon légale avec d'éventuelles sanctions, la gestion des technologies de l'information et de la communication (TIC), des fournisseurs de services tiers, et des risques qui en découlent.

Le règlement aura probablement une période de mise en œuvre de 24 mois. Toutefois, d'importantes normes techniques prendront plus de temps à se déployer, laissant le temps aux entreprises de se conformer aux nouvelles exigences auxquelles elles seront dorénavant confrontées.

La proposition initiale de la CE prévoyait une période de mise en œuvre de 12 mois pour la plupart des exigences du règlement et une période de 36 mois pour les exigences de test de résilience.

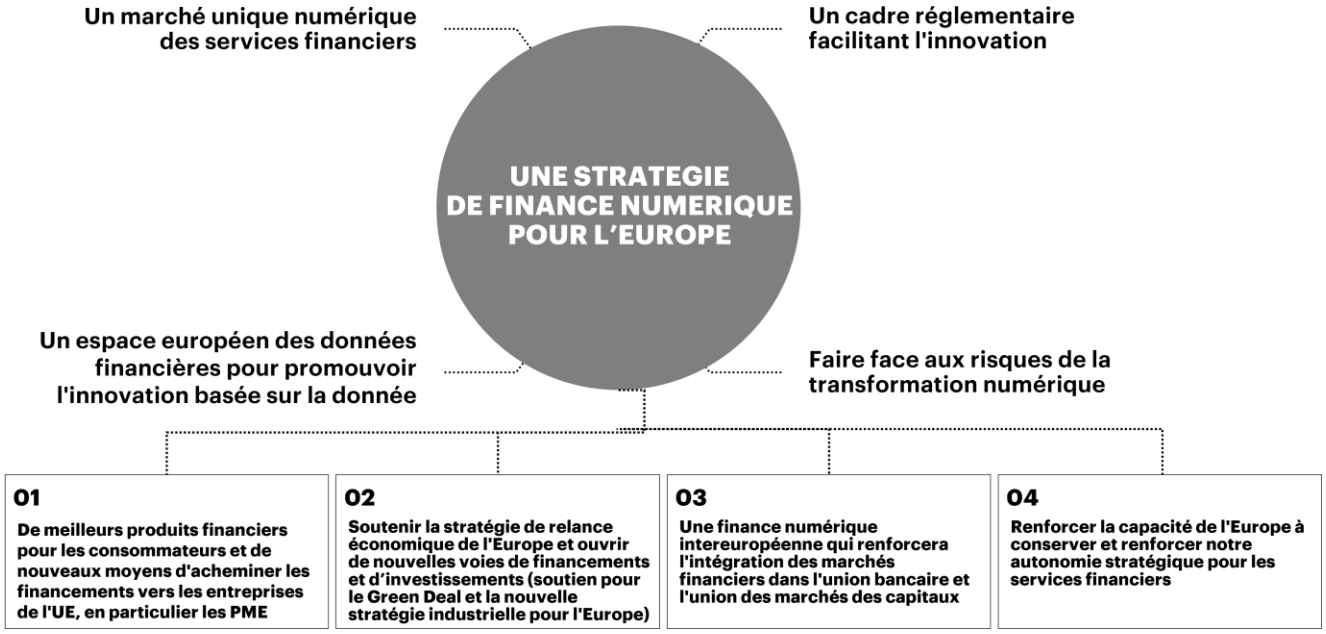
Le PE et le CE souhaitent étendre la période de mise en œuvre générale à 24 mois. Cependant, ils ne sont pas d'accord sur le calendrier de mise en œuvre des exigences en matière de tests de résilience. Le PE souhaite conserver la période de 36 mois, tandis que le CE souhaite qu'elle soit réduite à 24 mois. Un délai plus court pourrait être difficile à réaliser pour les entreprises de taille moyenne qui n'ont pas effectué de tests auparavant. Bien que les délais puissent encore changer, le texte du règlement actuel du CE est susceptible d'influencer fortement le résultat.

En conséquence, nous pensons que les entreprises devraient utiliser l'hypothèse de travail d'une période de mise en œuvre de 24 mois pour toutes les exigences du règlement, allant de mi 2022 à mi 2024.

Pourquoi la conformité est cruciale ? Bien que le recours à des fournisseurs tiers soit précieux ou nécessaire pour de nombreuses entités financières, une dépendance en hausse entraîne une croissance correspondante des risques opérationnels, et une gestion de ces risques potentiels moins performante et plus complexe.

Le renforcement de la résilience opérationnelle du secteur financier au sens large est essentiel et de notre intérêt commun.

Les avantages de la finance numérique pour l'Europe



Pourquoi un règlement sur la résilience opérationnelle numérique ?

01

Atténuer le risque posé par les vulnérabilités croissantes résultant de l'interconnectivité croissante du secteur.

02

Faire face à l'augmentation de la numérisation qui modifie le profil de risque des organisations financières.

03

Reconnaître et traiter la dépendance à des fournisseurs tiers qui peut menacer la stabilité du secteur financier.

04

Remédier et améliorer l'approche de supervision fragmentée dans l'ensemble de l'UE.

Les 5 piliers du règlement

Contexte et rappels

DORA fait partie intégrante de la stratégie de finance numérique européenne. Sur un plan juridique, il s'agit d'un règlement, rappelons-le, et non d'une directive. Cela permettra une adoption sans nécessité de transposition au niveau national. Elle sera donc appliquée uniformément par chaque État membre de l'UE.

D'autres normes techniques seront élaborées par les Autorités Européennes de Supervision (AES) et leur bonne mise en application sera assurée par les autorités nationales compétentes.

1

Gouvernance des TIC et gestion des risques

Cadre de gouvernance qui s'appuie sur les directives de l'Autorité Bancaire Européenne (ABE et EBA en anglais) en matière de TIC.

Mettre à jour les politiques et règles existantes sur la gouvernance des TIC pour aligner les stratégies commerciales et métiers.

Cadre de gestion des risques qui s'appuie largement sur les directives de l'Autorité Bancaire Européenne (ABE) en matière de TIC et de risque de sécurité, mettant l'accent sur le rôle de la haute direction et élargissant les exigences pour inclure une stratégie de résilience numérique.

Il existe également des exigences supplémentaires concernant la reprise après interruptions d'activités, les communications et la gestion des crises.

2

Tests de résilience opérationnelle numérique

Exige que les entreprises mettent en place des programmes de tests proportionnel à leur taille, à leurs profils d'activités et de risques. Les tests doivent tenir compte du principe de l'application de « scénarios extrêmes » et impliquer, le cas échéant, la participation de tiers sous contrat.

3

Gestion du risque des fournisseurs tiers

Supervision indirecte : règles d'externalisation renforcées et outils de surveillance pour les superviseurs.

Supervision directe des fournisseurs de services tiers critiques en matière de TIC.

Le règlement exige également des entreprises qu'elles aient une stratégie sur le risque des fournisseurs tiers, lié aux TIC, avec des orientations plus détaillées concernant les plans de sortie et des évaluations de la substituabilité ainsi que les exigences pour les tester. Il semblerait aussi que le règlement cherche aussi à contrôler ou limiter l'utilisation de fournisseurs tiers en dehors de l'UE.

4

Rapport d'incidents

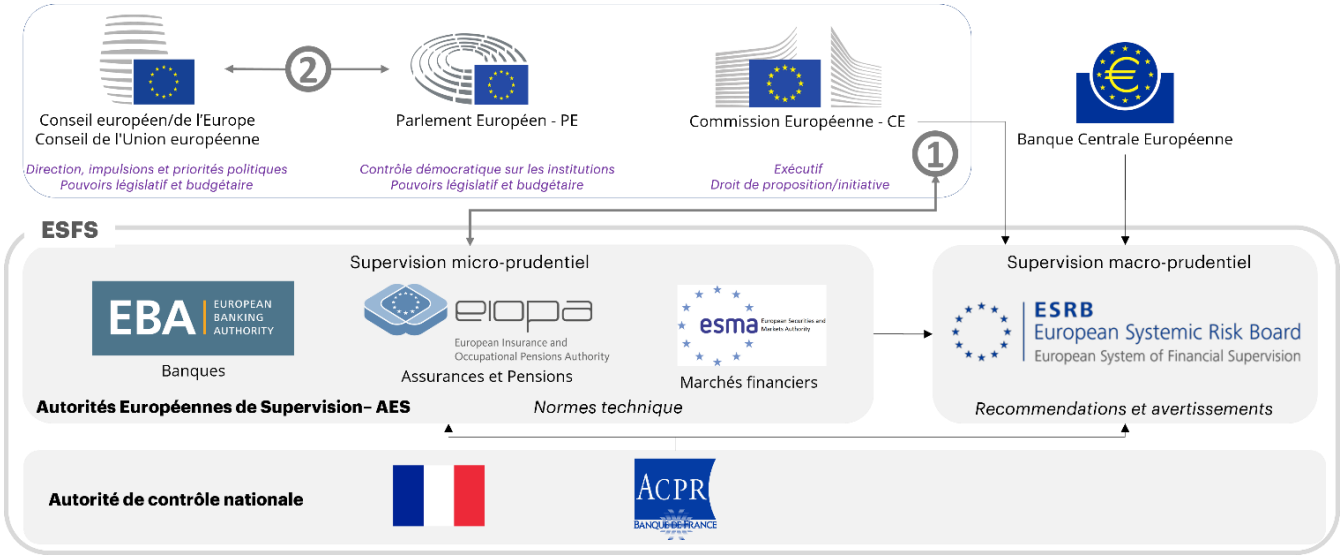
Rapports simplifiés de notifications et d'incidents avec des modèles de rapport communs, des délais, une autorité compétente à laquelle il faudra soumettre le rapport, etc.

5

Partage d'informations

Promouvoir et soutenir les programmes de partage de renseignements sur les menaces entre les institutions financières.

Les acteurs du Règlement



Le système européen de supervision financière

Le système européen de supervision financière (SESF) est une architecture ou un système institutionnel de l'UE proposé par la CE en 2009 en réponse à la crise économique et financière de 2008. Ce système est opérationnel depuis 2011 avec la création des Autorités européennes de surveillance, les AES. Le principal objectif du SESF est de veiller à ce que les règles applicables au secteur financier soient correctement mises en œuvre dans les États membres afin de préserver la stabilité financière, de promouvoir la confiance et de protéger les consommateurs. Les objectifs du SESF incluent également le développement d'une culture prudentielle commune et la facilitation d'un marché financier européen unique.

Le système SESF se compose comme suit :

Les 3 **Autorités Européennes de Supervision – AES**

EBA EUROPEAN BANKING AUTHORITY

L'**Autorité bancaire européenne**, **ABE** - 2011
(European Banking Authority, EBA)

eiopa
European Insurance and Occupational Pensions Authority

L'**Autorité européenne des assurances et des pensions professionnelles** - 2011 (European Insurance and Occupational Pensions Authority, EIOPA)

esma European Securities and Markets Authority

L'**Autorité européenne des marchés financiers** - 2011
(European Securities and Markets Authority, ESMA)

Le **comité mixte** (Joint Commitee) – 2011
Un forum dont l'objectif est de renforcer la coopération entre les trois AES.

Autorité de contrôle nationale des États membres de l'UE

ESRB
European Systemic Risk Board
European System of Financial Supervision

Conseil européen du risque systémique
CERS
(European Systemic Risk Board, ESRB)

Les trois AES renforcent le fonctionnement du marché intérieur en développant une réglementation paneuropéenne uniforme et en harmonisant les pratiques de supervision dans l'UE.

Création et développement de la DORA

Les réforme de l'UE qui a suivi la crise financière de 2008 a principalement renforcé la résilience financière du secteur financier de l'UE, ne s'attaquant qu'indirectement aux risques informatiques dans certains domaines. Les risques informatiques continuent de menacer la résilience opérationnelle, les performances et la stabilité du système financier de l'UE.

Les mesures prises par l'UE n'ont jusqu'alors pas traité pleinement la question de la résilience opérationnelle numérique. Cette situation ou chaque pays membres a ses propres règles et contrôles de la résilience opérationnelle numérique, à différents niveaux, fragmente le marché, compromet la stabilité et l'intégrité du secteur financier de l'UE et porte atteinte à la protection des consommateurs et des investisseurs.

Extrait de la DORA[28] :

> Jusqu'à présent, l'intervention de l'Union a contribué à répondre aux besoins et aux problèmes qui sont apparus au lendemain de la crise financière de 2008 : les établissements de crédit n'étaient pas suffisamment capitalisés, les marchés financiers n'étaient pas suffisamment intégrés, et l'harmonisation était jusqu'alors demeurée minimale. Le risque informatique n'était pas considéré comme une priorité à l'époque et, par conséquent, les cadres juridiques applicables aux différents sous-secteurs financiers ont évolué de manière non coordonnée.
>
> Néanmoins, l'action de l'Union a atteint ses objectifs, à savoir garantir la stabilité financière et instaurer un ensemble unique de règles prudentielles et de conduite, harmonisées et applicables aux entités financières dans toute l'UE.

Il est par conséquent nécessaire de mettre en place un cadre plus détaillé et exhaustif sur la résilience opérationnelle numérique pour les entités financières de l'UE. Ce cadre :

① La Commission a consulté les parties intéressées et les AES tout au long du processus d'élaboration de la proposition de la DORA entre 2019 et 2020. Chaque pilier du présent règlement repose sur un exercice d'évaluation implicite et sur les modifications législatives correspondantes.

L'objectif de la consultation était d'éclairer la Commission sur l'élaboration d'un éventuel cadre de résilience opérationnelle numérique trans-sectoriel de l'Union européenne dans le domaine des services financiers.

Sur le plan institutionnel, les principales contributions ont été apportées par le comité européen du risque systémique (CERS), les AES, l'Agence de l'UE pour la cybersécurité (ENISA) et la Banque centrale européenne (BCE), ainsi que par les autorités compétentes des États membres.

Pour élaborer cette proposition de règlement DORA, la Commission s'est appuyée sur les avis techniques conjoints des AES.

② Le Parlement européen et le Conseil européen ont arrêté leurs positions respectives sur la proposition du règlement DORA et ont entamé des négociations interinstitutionnelles, qui sont les dernières étapes nécessaires avant que le règlement ne devienne loi. Cela vise à aligner les positions du Parlement Européen et du Conseil là où elles diffèrent actuellement. Nous nous attendons à ce que ces pourparlers se concluent d'ici à la mi-2022.

[28] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA). Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 19 décembre 2021]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

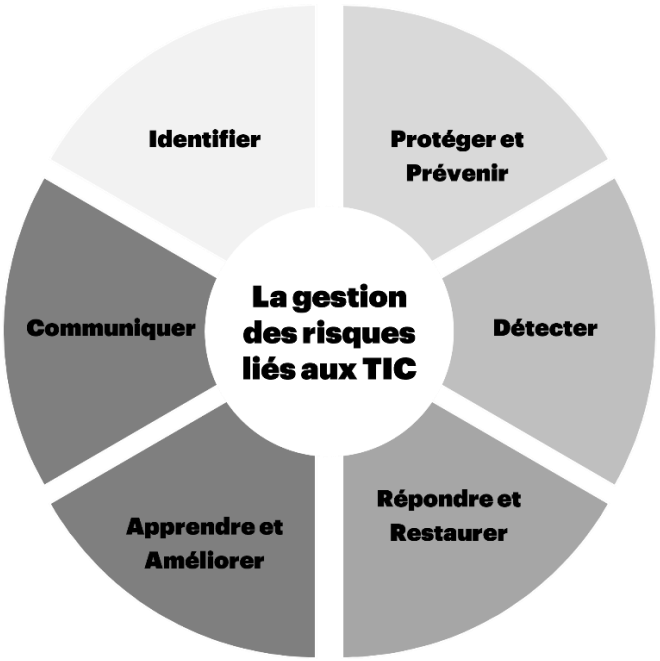
Les composants principaux du règlement

Nous allons mener dans cette section une revue des composantes majeurs du texte.

Paquet législatif sur la finance numérique	**Un règlement** Harmonisation et rationalisation des règles existantes en matière de gestion des risques liés aux TIC et de notification des incidents liés aux TIC. De nouvelles règles sur les tests numériques, le partage d'informations et la gestion des risques tiers liés aux TIC, y compris un cadre de supervision pour le risque numérique des fournisseurs de services tiers critiques en matière de TIC. Le lien ici[29].
Portée (Article 2)	▪ 20 types d'entités financières réglementées par l'UE. ▪ Hors champ d'application : systèmes de paiement, systèmes de paiement par carte, certains opérateurs de système et participants au SFD, le registre de l'Union pour les quotas d'émission.
Principe de Proportionnalité	▪ Exonérations : régime allégé pour les micro-entreprises. ▪ Règles adaptées en fonction de la criticité de l'organisation financière (tests numériques avancés uniquement pour les entités financières importantes). ▪ Règles adaptées pour les mesures liés aux rapports et notifications (rapports d'incidents liés aux TIC uniquement pour les incidents majeurs liés aux TIC).
Gouvernance (Article 4)	▪ Responsabilité et imputabilité de la direction. ▪ Définition, approbation, contrôle et responsabilisation pour mettre en œuvre des mesures de mitigations dans un cadre de gestion des risques liés aux TIC. ▪ Rôles et responsabilités clairs pour toutes les fonctions liées aux TIC. ▪ Définition des seuils de tolérance aux risques liés aux TIC. ▪ Processus d'approbation, de contrôle, de révision et tests pour la mise en œuvre des plans de continuité des activités et de reprise après sinistre des TIC, des plans d'audit des TIC et des risques de fournisseurs tiers des TIC. ▪ Répartition appropriée des investissements dans les TIC. ▪ Formation régulière pour le comité de direction.

[29] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA). Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 19 décembre 2021]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

La gestion des risques
(Article 5 à 14)



Identifier
(Article 7)

- Fonctions commerciales ou métiers.
- Patrimoine d'information pour le support.
- Configurations du système TIC.
- Interconnexions avec les systèmes internes et externes.
- Sources de risque TIC.
- Les comptes de systèmes TIC.
- Ressources en termes de réseau et équipement matériel.
- Équipement physique critique.
- Tous les processus dépendants et interconnectés avec des fournisseurs de services tiers TIC.

Principe de **proportionnalité** pour les **microentreprises** : pas d'évaluation des risques lors de modifications majeures de l'infrastructure du réseau et du système d'information, pas d'évaluation spécifique des risques sur les systèmes TIC (*legacy*).

Protéger et Prévenir
(Article 8)

- Résilience, continuité et disponibilité des systèmes TIC.
- Sécurité, confidentialité et intégrité des données
- Surveillance et contrôle continus des systèmes et outils TIC
- Minimiser les risques.
- Approche basée sur le risque.
- Politique de sécurité des informations : limiter les accès physique et virtuel aux systèmes TIC, protocoles d'authentification forts, gestion du changement, mises à jour et patch.

Détecter
(Article 9)

- Détection rapide des activités anormales ou suspicieuses.
- Identification des points individuels de défaillance (*Single Point of Failure - SPOF*).
- Allouer des ressources et des capacités.

Répondre et restaurer (Articles 10 et 11)	▪ Politique de continuité des activités TIC. ▪ Plans de reprise après sinistre TIC. ▪ Politiques de backup. ▪ Méthodes de restauration. ▪ Objectifs de Temps de Récupération flexibles. Principe de **proportionnalité** pour les **microentreprises** : pas d'audit Plans de reprise après sinistre TIC, pas de scénarios de test de cyberattaques et de basculements entre l'infrastructure TIC principale et la capacité redondante, les sauvegardes et les installations redondantes, pas de fonction de gestion de crise, aucun signalement aux autorités compétentes de tous les coûts et pertes causés par les perturbations des TIC et les incidents liés aux TIC.
Apprendre et améliorer (Article 12)	▪ Collecte d'informations sur les vulnérabilités et les cybermenaces. ▪ Examens post-incident après d'importantes perturbations des TIC. ▪ Analyse des causes des perturbations. ▪ Reporting à l'organe de gestion. ▪ Programmes et formations de sensibilisation à la sécurité des TIC.
Communiquer (Article 13)	▪ Plans de communication avec les clients, les homologues du secteur et le public. ▪ Avoir au moins une personne responsable pour mettre en œuvre la stratégie de communication pour les incidents liés aux TIC.
Rapports d'incidents liés aux TIC (Articles 15 à 20)	**Exigences générales** ▪ Établir et mettre en œuvre un processus de gestion pour surveiller et attribuer les incidents. ▪ Classifier les incidents sur la base de critères détaillés par le Règlement et développés par les AES. **Notification des incidents majeurs aux autorités compétentes** ▪ Modèles et procédures harmonisés élaborés par les AES ▪ Rapports initiaux, intermédiaires et finaux. ▪ Obligation d'informer les utilisateurs et les clients en cas d'impact sur leurs intérêts financiers. ▪ Les autorités compétentes sont encouragées à fournir des détails sur les incidents à d'autres institutions ou autorités : AES, BCE et points de contact uniques désignés par la directive NIS 2.

Test de résilience opérationnelle numérique (Articles 21 à 24)	**Tests de base** Valide pour toutes les entités financières. **Tests avancés** ▪ Seules les entités financières identifiées comme importantes par les autorités compétentes (sur la base des critères du règlement et développés plus spécifiquement par les AES). ▪ Tests avancés basés sur les *Threat-Led Penetration Testing* (TLPT) ▪ Reconnaissance mutuelle des résultats TLPT.
Risque des fournisseurs tiers de TIC (Articles 25 à 39)	**Harmonisation des éléments clés des relations avec les fournisseurs de services tiers TIC** Aspects cruciaux minimaux pour un suivi complet du risque des fournisseurs tiers TIC dans l'exécution, la résiliation et les étapes post-contractuelles des accords contractuels. **Cadre de supervision direct de l'Union pour les fournisseurs de services tiers critiques dans le domaine des TIC** ▪ Désignation des tiers fournisseurs de services TIC critiques par les AES. ▪ Les AES désignés en tant que superviseurs principaux avec des pouvoirs de supervision ▪ Le forum de supervision assure la coordination intersectorielle sur toutes les questions relatives aux risques liés aux TIC et effectue des travaux préparatoires aux décisions individuelles et aux recommandations collectives.
Dispositions contractuelles (Articles 25 à 27)	**Principes généraux** ▪ Pleine responsabilité des entités financières. ▪ Principes de proportionnalité. ▪ Stratégie de risque de fournisseurs tiers de TIC. ▪ Documentation et preuves. ▪ Registre d'informations. ▪ Principes pré, pendant et post contractuels. **Évaluation préliminaire du risque de concentration de services TIC** **Principales dispositions contractuelles** ▪ Description de toutes les fonctions et services et niveau de service (SLAs). ▪ Indication de l'emplacement et du stockage des données. ▪ Accessibilité, disponibilité, intégrité, sécurité et protection des données personnelles. ▪ Descriptions complètes des services ▪ Délais de préavis et obligations de reporting du fournisseur tiers. ▪ Assistance par le fournisseur tiers. ▪ Droit de supervision ▪ Stratégies de résiliation et de sortie de contrat.

Cadre de supervision
(Article 28)

Désignation des fournisseurs tiers critiques de TIC par les AES

1. La défaillance du fournisseur tiers de TIC entraînerait un impact systémique (stabilité, continuité ou qualité de la fourniture de services financiers).

   Prendre en compte le nombre d'entités financières auxquelles le fournisseur de services TIC en question fournit ses services.

2. Le caractère systémique (ou importance) des entités financières elles-mêmes.

   Prendre en compte le nombre de OIVs / OSEs dépendant du fournisseur de services tiers TIC en question, ainsi que les interdépendances entre les OIVs ou OSEs.

3. Les services soutenant des fonctions critiques ou importantes impliquent en fin de compte le même fournisseur de services tiers TIC (directement ou indirectement).

4. Degré de remplacement du fournisseur de services tiers TIC.
   - Prendre en compte l'absence d'alternatives réelles (même partielles) : nombre limité de fournisseurs, parts de marché, complexité technique
   - Prendre en compte les difficultés à migrer partiellement ou totalement les données et les charges de travail vers un autre fournisseur de services tiers TIC en raison des coûts ou des risques

5. Nombre d'États membres pour lesquels le fournisseur tiers de services TIC concerné fournit des services.

6. Nombre d'États membres dans lesquels opèrent des entités financières utilisant le fournisseur de services TIC tiers concerné.

Dérogation

La désignation ne s'applique pas aux tiers fournisseurs de services TIC soumis à des cadres de surveillance établis aux fins de soutenir les objectifs du traité visés à l'article 127, paragraphe 2, du TFUE.

Participation volontaire

Les fournisseurs de services tiers TIC non inclus ou désignés peuvent demander à être soumis au cadre de supervision.

Superviseur principal

Un AES est nommé superviseur principal pour chaque fournisseur tiers critique de TIC (sur la base de la valeur des actifs des entités financières relevant des attributions de l'AES respective).

Rôle du forum de contrôle

Cadre de supervision (Articles 29 et 35)

Forum de contrôle

- Coordination intersectorielle sur le risque tiers TIC.

  Le Forum de contrôle prépare des projets de positions communes et d'actes communs du Comité mixte.
- Recommandations : analyse de faits effectuées ou parvenus avant qu'ils se soient produits, résultant à des mesures d'anticipations ou compensatoires (ex ante : variable prévisionnelle évaluée avant la réalisation de l'évènement *modélisé*).

  Le superviseur principal consulte le forum de supervision avant d'exercer ses pouvoirs et avant d'adresser des recommandations aux fournisseurs critiques
- Recommandations : analyse de faits ou d'évènements effectuées ou parvenus après qu'ils se sont produits (ex post : basé sur des faits ou événements *empiriques*).

  Favorise les meilleures pratiques sur le risque de concentration des TIC et explore les facteurs d'atténuation pour les transferts de risques intersectoriels.

  Soumet des références complètes des fournisseurs de services tiers critiques en matière de TIC qui seront adoptées par le comité mixte (*Joint Committee*).

Structure du forum de contrôle

Cadre de supervision (Article 29)

Comité mixte

Il se compose :

- De présidents des AES
- D'un représentant de haut niveau de chaque autorité nationale compétente concernée.
- D'observateurs : directeur exécutif de chaque AES, un représentant de la Commission, du ESRB, de la BCE et de l'ENISA.

Tâches, pouvoirs, conduite

Cadre de supervision (Articles 30 à 39)

Tâches

- Exigences en matière de TIC et sécurité physique, processus de gestion des risques et dispositifs de gouvernance, gestion des incidents liés aux TIC.
- La portabilité des données pour faciliter une résiliation contractuelle effective.
- Processus de test de résilience des TIC.
- Utilisation des normes ou cadres nationaux et internationaux.

Pouvoirs de supervision

- Demander toutes les informations et documentations pertinentes.
- Mener des enquêtes générales et des inspections.
- Demander des rapports.
- Recommandations.

Sanctions et pénalités périodiques

Non soumission de documents, refus d'accorder des accès et de se soumettre à des inspections, etc.

Conduite

- Des superviseurs principaux assistés d'experts nationaux dans les équipes d'examen.

Coopération internationale

Partage d'information

(Article 40)

Échange volontaire entre les entreprises financières d'informations et de renseignements sur les cybermenaces dans le cadre de communautés ou forums de confiance

- Indicateurs de compromissions.
- Tactiques, Techniques et Processus
- Alertes de cybersécurité.
- Outils de configuration et meilleurs pratiques.

Autorités compétentes

(Articles 41 à 49)

- Coopération avec les structures et autorités impliqués dans la Directive NIS.
- Exercices trans-sectorielles, communication et coopération.
- Sanctions administratives et mesures correctives.

Modifications
(Articles 52à 55 et Directives)

Synchronisation ou mises à jour nécessaires des exigences actuelles en matière de risque opérationnel ou de gestion des risques dans la législation financière pour assurer une cohérence totale avec la proposition du Règlement.

- Règlement (EC) No 1060/2009 (CRAR)
- Règlement (EU) No 648/2012 (EMIR)
- Règlement (EU) No 600/2014 (MiFIR)
- Règlement (EU) No 909/2014 (CSDR)
- Directive 2006/43/EC (Audit)
- Directive 2009/65/EC (UCITS)
- Directive 2009/138/EU (Solvency II)
- Directive 2011/61/EU (AIFMD)
- Directive EU/2013/36 (CRD IV)
- Directive 2014/65/EU (MiFID II)
- Directive (EU) 2015/2366 (PSD II)
- Directive EU/2016/2341 (IORPs)

CHAPITRE 4

DORA et les tests de résilience opérationnelle numérique

« Les attaques informatiques pourraient cibler des institutions financières d'importance systémique. En cas de succès, ces attaques pourraient entraîner une perte de confiance dans le système financier plus large, avec un impact potentiellement négatif sur la stabilité financière mondiale ».

Extrait - Rapport FMI 2022

Nous allons aborder ce chapitre en expliquant pourquoi faire des tests de résilience opérationnelle numérique, puis nous nous focaliserons sur une partie bien spécifique que sont les tests de résilience face aux cyberattaques. Dans cette seconde partie de chapitre, nous nous pencherons sur la méthodologie TIBER-EU que nous estimons la plus adaptée.

Le test de résilience opérationnelle numérique

Au-delà de la continuité des activités et de la reprise après sinistre, l'un des piliers du règlement, articles 21 à 24[30], invite les organismes financiers à mettre en œuvre des plans solides pour continuer à fournir les services essentiels, quelle que soit la cause de la perturbation. Mais élaborer un plan ne suffit pas, encore faut-il le mettre à l'épreuve. C'est là qu'intervient le test de résilience opérationnel numérique.

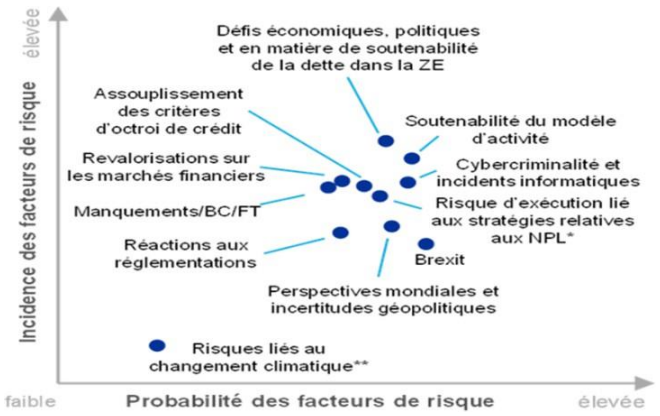
L'objectif est d'évaluer la préparation des organismes financiers face à un événement majeur impactant leurs systèmes d'information. De cette évaluation ressortiront les faiblesses, les défaillances et/ou les lacunes de leur système d'information leur permettant d'identifier et de mettre en œuvre les actions correctives nécessaires.

La résilience du système d'information est un sujet vaste, allant de la redondance des systèmes physiques face aux pannes (data center, serveurs, stockage de données, réseaux, télécoms …), à celle des systèmes logiques (applications, donnés), en incluant la continuité d'activité en cas de sinistre (événement naturel ou non).

Pour ce faire, la DORA préconise aux établissements financiers d'élaborer des programmes périodiques de test de la résilience sur la base de risques. Ces risques prennent en compte les spécificités (par exemple domaine d'activité, profil, degré d'exposition etc..) de l'organisme financier. Ils incluent aussi les menaces d'origine humaines telles que les attaques physiques ou cybernétiques, les pannes physiques des systèmes informatiques et les défaillances de fournisseurs tiers, les risques naturels tels que les incendies, les inondations, les intempéries et les pandémies.

Ce graphique [31] édité par la BCE nous démontre que le sujet est à appréhender avec sérieux au vu du niveau de probabilité et d'impact.

Nous comprenons d'autant mieux la nécessité de développer une réglementation ciblée pour obliger le secteur financier dans son ensemble à adopter une démarche d'amélioration continue.



En comparaison des autres risques du SI, les cyberattaques ont pris une part prépondérante. Notre étude de la DORA se focalisera sur la cyber-résilience, c'est-à-dire la capacité de l'établissement financier à se protéger des attaques informatiques communément appelées cyberattaques.

[30] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA). Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 19 décembre 2021]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

[31] Cartographie des risques réalisés par le MSU pour 2020 [graphique]. In : Banque Centrale Européenne [en ligne]. 2019. [Consulté le 7 mai 2022]. Disponible à l'adresse : https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2020~a9164196cc.fr.html#toc2

La résilience opérationnelle numérique face aux cyberattaques

Dans cette section, nous allons aborder de façon plus spécifique les cyberattaques. Ce sont des actions volontaires et malveillantes menées au moyen d'un réseau informatique visant à causer un dommage aux informations et/ou aux personnes qui les traitent. Les cibles sont diverses, les particuliers, les entreprises, les institutions gouvernementales, les services administratifs et de santé.

Elles peuvent être le fait d'une personne seule, d'un groupe, d'une organisation criminelle ou même d'un État. Leurs motivations sont multiples (politique, militaire, concurrentiel, éthique ou tout simplement pécuniaire).

Le monde de la finance est bien entendu une cible de choix en raison de sa nature mais aussi de sa digitalisation et du développement de la FinTech (entreprises, généralement des start-ups, qui évoluent dans le secteur de l'innovation technologique appliqué aux services financiers et bancaires) et la quantité croissante d'informations mises en ligne facilite ces cyberattaques.

Sur les 12 derniers mois, on ne dénombre pas moins de 8 institutions financières ayant rapporté avoir subi une cyberattaque de grande ampleur avec des conséquences fâcheuses pour l'entreprise elle-même mais pas seulement[32].

A titre d'exemple, AXA a subi une attaque par rançongiciel et vol de 3 Terabits de données, BDO Unibank, une banque aux Philippines, a été victime de transferts de fonds frauduleux à partir de comptes bancaires de 700 clients, d'autres exemples en annexe.

DORA et Cyber résilience

Revenons maintenant au règlement et voyons comment elle aborde ce sujet de test de résilience cyber.

Le règlement met en avant deux types de test :

Tests basiques, relatifs aux exigences de base. On peut faire référence à ce que l'ANSSI appelle « l'hygiène informatique », comme par exemple l'évaluation et l'analyse en source ouverte des vulnérabilités, des évaluations de la sécurité des réseaux, ou des analyses du code source des applications.

Tests avancés, dont le principe est un test de pénétration / d'attaque informatique fondé sur la menace.

Nous allons développer dans ce chapitre les tests avancés.

La DORA précise que ces tests sont spécifiques à certains établissements financiers selon un critère défini par les autorités compétentes et devront être effectués à minima tous les trois ans.

Le test de pénétration fondé sur la menace - ou « Threat Led Penetration Testing » (TLPT) en anglais - est un cadre simulant les tactiques, les techniques et les procédures d'acteurs mal intentionnés ou d'un logiciel malveillant sur les systèmes d'information critiques et en production, de manière contrôlée et sur mesure.

Les scénarios de tests sont élaborés en fonction des renseignements de menaces et risques collectés auparavant, aussi bien en sources ouvertes que fermées.

Le règlement DORA ne fait pas mention d'une méthodologie particulière à appliquer pour les tests de résilience opérationnelle. Néanmoins, relevons l'existence depuis mai 2018 de la directive « Threat Intelligence based Ethical Redteam » (TIBER-EU). Celle-ci développe en effet une méthodologie pour ce genre de tests avancés. Elle a aussi été élaborée par l'UE et elle couvre le même champ d'application que la DORA.

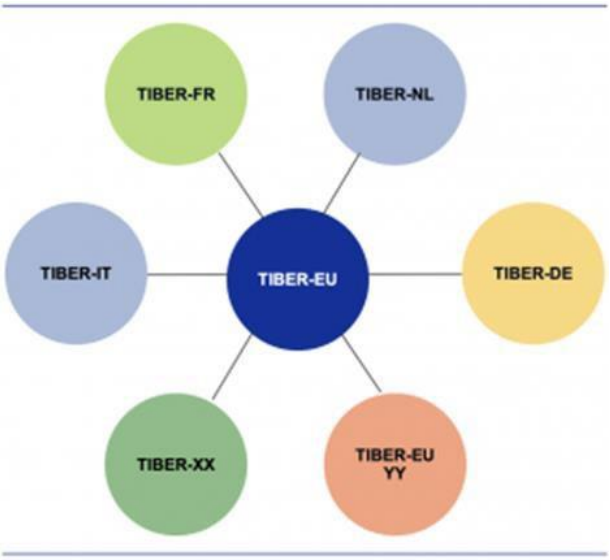
[32] Cyber attacks database. Jam Cyber [en ligne]. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://jamcyber.com/resources/cyber-attacks/

Tous deux s'adressent spécifiquement au même domaine d'activité, à savoir le monde de la finance au sens large. Notons que DORA est toutefois plus exhaustive en termes de couverture (voir tableau ci-dessous).

Type d'établissement	**DORA**	**TIBER**
Les établissements de crédit	✓	✓
Les établissements de paiement	✓	✓
Les établissements de monnaie électronique	✓	
Les entreprises d'investissement	✓	✓
Les prestataires de services sur cryptoactifs, les émetteurs de cryptoactifs, les émetteurs de jetons se référant à un ou des actifs et les émetteurs de jetons se référant à un ou des actifs et revêtant une importance significative	✓	
Les dépositaires centraux de titres	✓	✓
Les contreparties centrales	✓	✓
Les plates-formes de négociation	✓	✓
Les référentiels centraux	✓	✓
Les gestionnaires de fonds d'investissement alternatifs	✓	✓
Les sociétés de gestion	✓	
Les prestataires de services de communication de données	✓	
Les entreprises d'assurance et de réassurance	✓	✓
Les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire	✓	
Les institutions de retraite professionnelle	✓	
Les agences de notation de crédit	✓	✓
Les administrateurs d'indices de référence d'importance critique	✓	✓
Les prestataires de services de financement participatif,	✓	
Les référentiels des titrisations	✓	✓
Les tiers prestataires de services informatiques	✓	

Une approche collaborative

Il est utile de relever que dans la phase d'élaboration de la DORA, les états membres de l'UE ont été consultés. Plus précisément, ce sont les banques centrales des pays membres qui ont été consultées. Il en ressort que la préconisation de la BCE a été de désigner la méthodologie TIBER-EU pour les tests de résilience cyber avancés.



Certaines banques centrales d'états membres ont déjà mis en pratique cette méthodologie avec quelques adaptations du fait de spécificités propres.

Gardons à l'esprit que l'un des objectifs de la DORA est l'homogénéisation du cadre réglementaire et donc une mutuelle reconnaissance des tests de résilience opérationnelle entre états membres.

Cet objectif permettra aux institutions financières de ne pas multiplier les tests en fonction du pays où elles sont implantées. Le bénéfice est multiple : simplification et optimisation des efforts et des ressources humaines.

Notons que la méthodologie TIBER-EU est de plus en plus utilisée comme référence pour ce qui est des tests de pénétration bien au-delàs de la finance.

Ces éléments nous ont amené à développer et expliquer TIBER-EU dans l'objectif de répondre au règlement DORA.

TIBER-EU pour la DORA

Qu'est-ce que TIBER-EU ?

Comme évoqué plus avant, TIBER-EU est un acronyme qui signifie « **Threat Intelligence based Ethical RedTeam** » que l'on pourrait traduire par « Test de pénétration basé sur les renseignements de la menace ». C'est une méthodologie de travail développée par la BCE afin d'aider les institutions financières des États membres à tester leurs capacités de protection face aux cyberattaques, que ces dernières soient ciblées sur le système d'information lui-même, sur l'employé ou bien encore sur le processus fonctionnel.

Cela consiste en des tests contrôlés et sur mesure de cyber-piratages éthiques, fondés sur les renseignements connectés à des menaces réelles, des tactiques et techniques utilisées par les acteurs malveillants.

TIBER-EU a donc pour but d'aider les institutions financières à évaluer leur capacité de protection, la détection et la réponse face à des scénarios réels de cyber-attaque.

Sur cette base, un retour d'expérience soulignant les points faibles relevés par les tests sera produit en fin de processus. Il sera suivi un plan d'action et d'un planning associés définissant les solutions à mettre en œuvre pour résoudre ou diminuer les faiblesses mises en lumière.

Il ne faut donc absolument pas classer TIBER-EU comme un test que l'on réussit ou non, du type certification, mais comme un processus d'amélioration continue de la protection contre les cyber-attaques.

Pourquoi TIBER-EU ?

Dans une optique d'harmonisation et pour éviter que chaque pays membre de l'UE ne développe ses propres méthodologies, qui pourraient de plus entrer en concurrence, la BCE a décidé de construire un cadre paneuropéen unique.

TIBER-EU a été conçu pour fournir des approches communes, mais aussi de la flexibilité permettant une éventuelle adaptation aux spécificités locales.

Un peu d'historique

TIBER trouve sa source au Pays-Bas au travers de la Banque Nationale Néerlandaise (DNB) qui a développé le programme TIBER-NL en 2016.

TIBER-EU poursuit les améliorations entamées par TIBER-NL et s'appuie davantage sur les principes fondamentaux de l'approche de test de pénétration basée sur le renseignement de la menace. Il existe un alignement significatif entre les cadres TIBER-NL et TIBER-EU, les principales différences équivalant aux exigences nationales et européennes en matière de portée et de surveillance.

L'adoption par les autorités nationales et européennes s'accélère, la Belgique, le Danemark, l'Allemagne, l'Irlande, la Suède, la France et l'Italie utilisant TIBER-EU pour développer et mettre en œuvre leurs propres régimes TIBER nationaux.

Hors de l'UE, c'est au Royaume-Uni que l'on trouve les références les plus anciennes avec le « Simulated Targeted Attack and Response » (START) devenue ensuite le CBEST développé par le BoE et la FCA avec l'aide du CREST qui est l'organisation à but non lucratif représentant l'industrie cyber. Nous en avons développé les détails plus tôt dans ce rapport.

Ailleurs dans le monde, d'autres références ont vu le jour. Ainsi à Hong Kong, l'« Intelligence-led Cyber Attack Simulation Testing » (iCAST) a vu le jour et l' « Adversarial Attack Simulation Exercises » (AAES) existe pour les banques à Singapour.

Il est utile d'en dresser un tableau comparatif. A la lueur du tableau suivant, il apparaît bien entendu des similitudes mais aussi des différences entre ces méthodologies :

	CBEST	iCAST	AASE	TIBER-EU
Renseignement de la menace	✓			✓
Evaluation du système de surveillance (détection et de la réaction)	✓			✓
Evaluation des risques liés à l'organisation		✓		
Evaluation de la maturité au regard des standard du secteur		✓		
Exercice supervisé par le régulateur	✓			✓
Mesure de la capacité de détection et de réponse	✓			✓
Interopérabilité de la méthodologie entre les pays				✓
Utilisation de compétence interne pour l'équipe RT			✓	
Utilisation d'entreprise externe qualifié	✓			
Qualification pour les personnes intervenant	CREST	CREST		Plusieurs
Résultat des tests partager avec l'agence gouvernemental	✓			✓
Format du rapport de test définit	✓		✓	✓
Format du rapport d'identification de la menace défini				✓
Possibilité pour la « Red team » d'ajouter des scénarii de test				✓

Il ressort de cette comparaison synthétique que TIBER-EU est à date le plus avancé des modèles. C'est assurément un point à mettre au crédit de l'UE, confirmant son positionnement à la pointe en ce domaine.

Les objectifs de TIBER-EU

On peut les résumer en six points :

Améliorer la cyber résiliences de l'entité financière et du secteur financier en général.	Harmoniser et standardiser les tests entre Etats membres.
Fournir aux Etats membres une méthodologie commune.	Fournir une méthodologie aux entités financières transfrontalières.
Réduire la charge réglementaire pesant sur les entités et favoriser la reconnaissance mutuelle dans l'ensemble de l'UE.	Favoriser une collaboration inter-autorités/transfrontalière de partage et l'analyse des résultats.

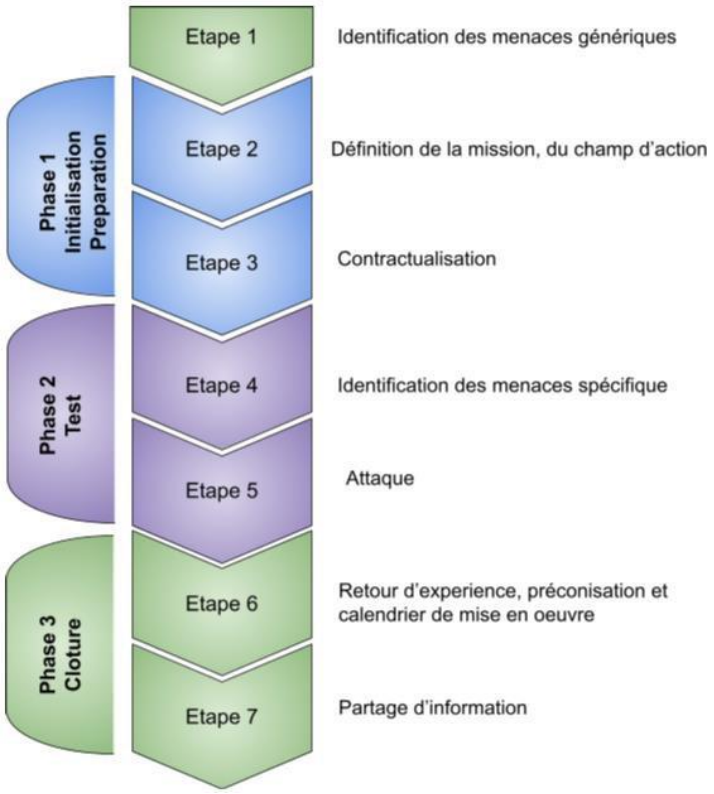
En complément et pour continuer à faire le lien avec DORA, notons que ce règlement stipule que les conclusions seront à partager avec les autorités compétentes. Ces dernières ne sont pas clairement désignées dans la DORA.

Les experts prédisent que les agences nationales de cybersécurité seront sollicitées dans ce but précis comme l'ANSSI pour la France, le BSI pour l'Allemagne, la NSM pour la Norvège, etc...

Nous pourrions imaginer que l'« European Network and Information Security Agency » (ENISA), qui est l'agence de l'UE pour la cybersécurité émane directement du Parlement européen créée en 2004, pourrait participer à ce processus de partage d'informations.

Explorons TIBER-EU

TIBER-EU se définit en **3 phases** linéaires et totalise **7 étapes** représentées par le schéma ci-dessous. Cependant à chaque phase, on trouve des interactions de processus.



	Phase 1 Initialisation et préparation		Phase 2 Test		Phase 3 Clôture	
Etape 1	Etape 2	Etape 3	Etape 4	Etape 5	Etape 6	Etape 7

Etape 1 - Identification des menaces générales

Cette phase identifie la menace relative au secteur financier de manière générale, sans prendre en compte les spécificités du donneur d'ordre.

Certaines menaces sont communes à l'ensemble du secteur financier, mais d'autres sont propres à un sous-secteur en particulier.

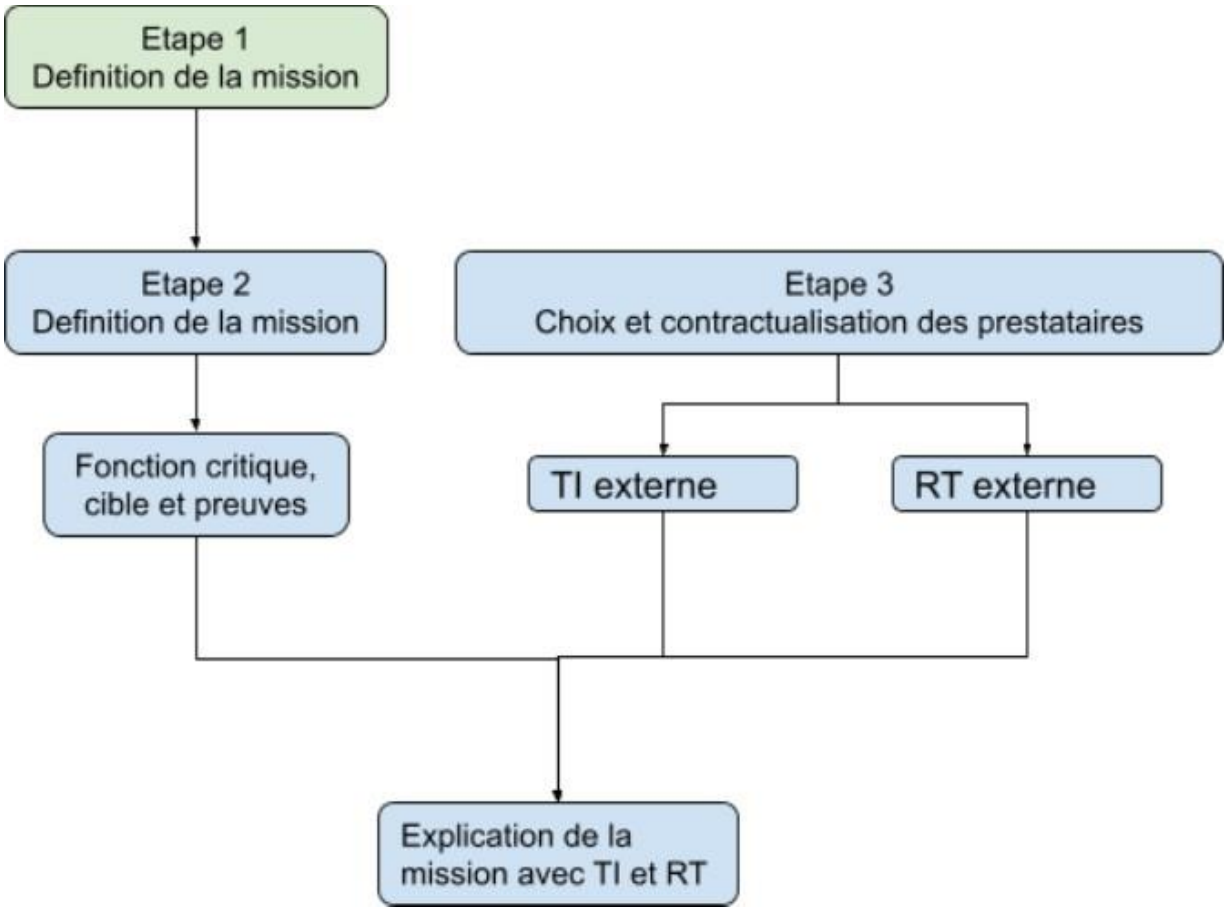
Prenons l'exemple d'une menace spécifique aux banques, le Bank Drops. Pour dissimuler leur localisation aux autorités, les cybercriminels stockent souvent les fonds volés dans de faux comptes bancaires ouverts avec des identifiants de clients volés.

S'agissant du secteur de l'assurance, il existe ce qu'on appelle « le fichier compromis ». En substance, les assureurs acceptent un grand nombre de fichiers provenant d'un large éventail d'expéditeurs, soit directement, soit via des places de marché et des portails destinés aux clients. Il peut s'agir d'un formulaire de police, d'un document de réclamation ou d'un certificat de couverture. Ces compagnies s'exposent donc aux menaces transmises à partir de tout appareil ou système impliqué dans l'échange de fichiers. Par exemple, si l'ordinateur personnel d'un client a été infecté par un logiciel malveillant, cette infection peut facilement se propager à un fichier envoyé par le client qui est ensuite traité par la compagnie d'assurance.

	Phase 1 **Initialisation et préparation**		Phase 2 Test		Phase 3 Clôture	
Etape 1	Etape 2	Etape 3	Etape 4	Etape 5	Etape 6	Etape 7

Phase 1 - Initialisation et préparation

Cette phase de préparation comprend l'identification et la contractualisation des fournisseurs de recherche de menace « Threat Intelligence » (TI) et de test de pénétration « Red Team » (RT), le processus de cadrage et l'élaboration du calendrier.



	Phase 1 Initialisation et préparation		Phase 2 Test		Phase 3 Clôture	
Etape 1	**Etape 2**	Etape 3	Etape 4	Etape 5	Etape 6	Etape 7

Etape 2 - Définition de la mission et du champ d'action

Le processus de cadrage définit la portée et le contenu du test et détermine ainsi de manière significative l'expressivité du rapport. Elle consiste à identifier les systèmes et services clés qui assurent les fonctions essentielles.

Les fonctions critiques sont définies comme suit : les personnes, les processus et les technologies dont le donneur d'ordre (ici l'institution financière) a besoin pour fournir un service de base. Leur interruption pourrait nuire à la stabilité financière, à la sécurité et à l'intégrité de l'entité, à sa clientèle ou au comportement de l'organisation sur le marché.

Vient ensuite la description d'actions ou de cibles qui confirment que l'attaque a réussi, ce que l'on appelle communément « Capture the flag » dans le monde cyber.

Un exemple est de réussir à compromettre un distributeur de billets de banque et à en extraire de l'argent, ou encore l'exfiltration des données bancaires de clients.

	Phase 1 Initialisation et préparation		Phase 2 Test		Phase 3 Clôture	
Etape 1	Etape 2	**Etape 3**	Etape 4	Etape 5	Etape 6	Etape 7

Etape 3 - Contractualisation

Une attention particulière est portée à la sélection des prestataires TI et RT externes et indépendants. Leurs compétences et leurs qualités sont déterminantes pour estimer la valeur du test et pour une exécution fluide et sécurisée. Des exigences élevées doivent être fixées pour garantir la qualité et le soin nécessaires pour le test sensible.

TIBER-EU décrit que la responsabilité de la sélection des fournisseurs TI et RT incombe à l'organisation cible.

	Phase 1 Initialisation et préparation		**Phase 2 Test**		Phase 3 Clôture	
Etape 1	Etape 2	Etape 3	Etape 4	Etape 5	Etape 6	Etape 7

Phase 2 - Test

TIBER-EU définit des scénarios d'attaques. Ils doivent être développés comme point de départ pour la RT sur la base du rapport des menaces fournies par l'équipe TI.

	Phase 1 Initialisation et préparation		**Phase 2 Test**		Phase 3 Clôture	
Etape 1	Etape 2	Etape 3	**Etape 4**	Etape 5	Etape 6	Etape 7

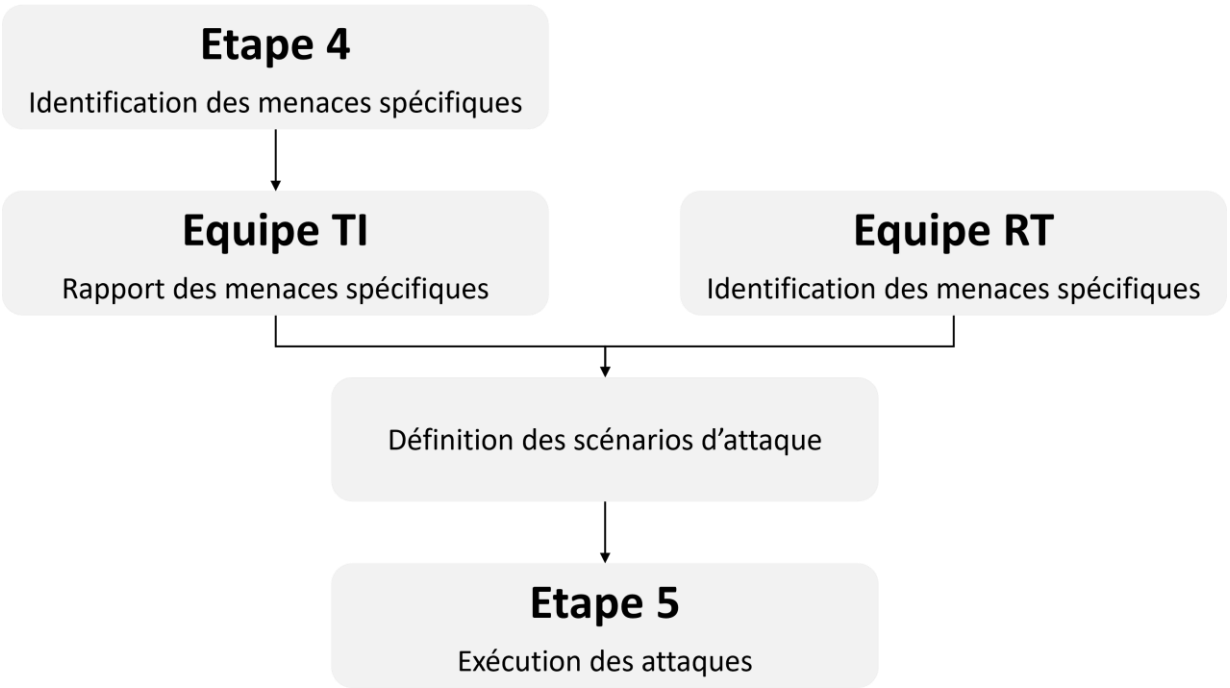
Etape 4 - Identification des menaces spécifique

L'équipe TI intervient ici. Elle cartographie les menaces spécifiques à l'entreprise donneur d'ordre. Cette équipe simule la phase de reconnaissance d'un attaquant en collectant un maximum d'informations - que ce soit en source ouverte ou non - sur l'écosystème du donneur d'ordre, en évaluant la surface d'attaque et en cartographiant les menaces qui pèsent sur lui dans le but de proposer des scénarios d'attaques adaptés à la cible définie lors de l'étape 2.

Le résultat devrait être un rapport de renseignements sur les menaces ciblées qui identifie des zones d'attaque des personnes, des processus et des technologies. Des scénarios d'attaque efficaces doivent être définis en fonction des connaissances acquises.

Notons que TIBER-EU prévoit que l'équipe RT puisse influencer le scénario d'attaque.

A ce titre, il serait intéressant d'étudier comment la méthodologie d'« Expression des Besoins et Identification des Objectifs de Sécurité » (EBIOS Risk Manager) développée par l'ANSSI pourrait intervenir dans les étapes 1 et 3.



	Phase 1 Initialisation et préparation		**Phase 2 Test**		Phase 3 Clôture	
Etape 1	Etape 2	Etape 3	Etape 4	**Etape 5**	Etape 6	Etape 7

Etape 5 - Attaque

Lors de cette cinquième étape, l'équipe spécialisée ET prend la main.

C'est elle qui est chargée d'exécuter les tests sur les environnements de production cible définis lors de la phase 2 en s'appuyant sur la cartographie des menaces et les scénarios définis par l'équipe TI lors de la phase 4.

Pour ce faire, la RT utilisera les tactiques, techniques et les procédures d'attaque que les vrais acteurs malveillants utilisent. Elle mettra à l'épreuve les infrastructures techniques du système d'information (application, serveur, réseau…), les infrastructures physiques (bureaux, locaux, centre de données…), les réflexes des collaborateurs (employés, prestataires, sous-traitant), ainsi que la mise à l'épreuve des processus métiers si nécessaire.

TIBER-EU admet explicitement que la portée, les drapeaux et les Tactiques, Techniques et Procédures (TTP) peuvent être modifiés au cours du test et que le RT doit bénéficier de la plus grande flexibilité et créativité possible.

Notons que l'ENISA fait référence à cette méthodologie dans son chapitre consacré à la gestion des menaces et des risques. Ceci ajoute de la légitimité à introduire EBIOS - RM dans TIBER et par ricochet dans le règlement DORA.

	Phase 1 Initialisation et préparation		Phase 2 Test		**Phase 3 Clôture**	
Etape 1	Etape 2	Etape 3	Etape 4	Etape 5	**Etape 6**	Etape 7

Phase 3 - Clôture

Etape 6 - Retour d'expérience, préconisation et calendrier de mise en œuvre

Cette phase consiste en une restitution des résultats au travers du rapport de l'équipe RT. Elle mettra en évidence les lacunes, les vulnérabilités, les faiblesses de la protection du système d'information du donneur d'ordre. De même, elle détaillera les failles ayant permis à l'équipe RT d'atteindre les objectifs visés ou une partie d'entre eux.

L'équipe responsable de la protection du système d'information souvent appelée la « Blue Team » (BT) du donneur d'ordre est maintenant informée du test et doit créer un rapport avec les contre-mesures correspondantes sur la base du rapport de l'équipe RT. Et enfin le donneur d'ordre doit maintenant planifier et exécuter la mise en œuvre de toutes les contre-mesures appropriées.

	Phase 1 Initialisation et préparation		Phase 2 Test		**Phase 3 Clôture**	
Etape 1	Etape 2	Etape 3	Etape 4	Etape 5	Etape 6	**Etape 7**

Phase 3 - Clôture

Etape 7 - Partage d'informations

Étant donné que l'un des principaux objectifs du cadre TIBER-EU est de renforcer la résilience du secteur, il est prévu que chaque juridiction analyse les reports BT afin d'identifier de nouvelles menaces et vulnérabilités communes et de les diffuser sous la forme appropriée aux parties prenantes concernées. Ici encore, nous pourrions très bien imaginer que l'ANSSI joue ce rôle fédérateur pour la France.

L'ANSSI pourrait partager de manière anonymisé ces rapports, ou les enseignements d'un centre de connaissance au niveau européen afin que toutes les leçons apprises puissent être bénéfiques à l'ensemble du secteur financier de la zone euro.

Il s'agit d'un élément clé du principe « apprendre et évoluer » qui sous-tend le TIBER-EU.

CHAPITRE 5

Gestion des fournisseurs tiers

Dans ce chapitre, nous allons analyser plus en détails le « pilier » de DORA dédié à la gestion des fournisseurs tiers, avec une attention plus particulière sur le cloud dans un second temps.

La digitalisation croissante des affaires nécessite des expertises et des moyens techniques chaque jour plus grands. Ce phénomène concerne toutes les entreprises du secteur financier, qu'elles disposent de ressources internes ou qu'elles fassent appel à des tiers prestataires informatiques.

Nous distinguons principalement deux types de prestations informatiques dans la finance : l'outsourcing des compétences techniques et l'informatique dans le nuage - que nous appelons aussi cloud dans notre rapport.

Le développement de la FinTech a entrainé un besoin accru d'expertise technique dans de nouveaux domaines de l'informatique, de l'intelligence artificielle (IA) et des blockchains. Ces avancées permettent aux organisations financières d'améliorer leur activité en proposant des services innovants et radicalement différents de leur activité traditionnelle.

Selon le cabinet de conseils Price Waterhouse Coopers (PwC)[33], « La clé de la réussite de la FinTech est soit de proposer quelque chose de radicalement différent de ce que fait une banque, soit de réussir à modifier en profondeur un mode de distribution qui permet d'atteindre une masse critique très rapidement et d'être pérenne. » D'après cette même étude de 2017, 82% des établissements financiers traditionnels prévoyaient de renforcer leur partenariat avec les FinTech d'ici cinq ans. Ceci sous-entend un développement des activités financières via des ressources et des expertises externes.

La stratégie des organismes financiers a historiquement été de confier des activités de faible valeur ajoutée à des sous-traitants. Les choses évoluent. Les entreprises ne disposant pas de ressources internes sur certains profils de techniciens informatiques ou logiciels, ont en effet de plus en plus recours à des experts externes. Un tiers prestataire informatique peut alors être défini comme une entreprise qui fournit une prestation informatique et met à disposition des experts techniques, des logiciels, ou des composants d'infrastructure. **Cet état de fait soulève donc le problème de la maitrise des compétences techniques externes pour une résilience accrue et une autonomie des activités du secteur financier.**

Dans le cas du cloud, le prestataire fournit des services de type serveur, stockage de données, ou bien encore de logiciels au travers d'internet.

Le bénéficiaire peut également utiliser la puissance de calcul du fournisseur pour développer son activité. Il n'est pas propriétaire des ressources et il est facturé à la consommation. D'abord utilisé pour compléter ou renforcer ses infrastructures, le service s'est accru pour progressivement se substituer aux capacités du bénéficiaire.

Les organismes financiers investissent massivement dans des programmes de transformation, sans pour autant réduire leur marge et leur rentabilité. Ils se trouvent donc contraints de trouver d'autres leviers comme l'externalisation de leurs infrastructures.

L'informatique en nuage, comme nous le verrons, s'est fortement développée pour leur permettre de se focaliser sur leur cœur de métier.

[33] BITTON, Edouard. Les Fintech, nouveau souffle pour le secteur bancaire. PWC [en ligne]. 2017. [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.pwc.fr/fr/decryptages/transformation/les-fintech-nouveau-souffle-pour-le-secteur-bancaire.html

De même, l'externalisation et le recours de plus en plus important à des infrastructures déléguées a produit deux conséquences principales que nous développerons :

- La dépendance à l'égard des prestataires d'informatique dans le nuage. En effet, une partie de la connaissance technique et des éléments structurant de l'architecture sont détenus par le prestataire. Les organismes financiers ne sont ainsi pas autonomes dans les modifications d'architecture.
- Le déséquilibre du rapport de force. Au début de la contractualisation, les banques et les assurances sont en position de force. Ce rapport de force est modifié lorsque l'activité des organismes financiers devient totalement dépendante de l'informatique dans le nuage.

Avant tout cela, il est important de voir comment le règlement DORA définit et qualifie les prestataires TIC, ainsi que leur degré de criticité.

Description d'un tiers Prestataire - vision DORA [34]

L'ACPR, l'autorité de régulation française, exerce un contrôle sur tous les projets d'externalisation des activités et fonctions importantes. Ce contrôle concerne en priorité les activités et fonctions critiques de l'organisme financier.

Dans le rapport 2019 de l'autorité EBA[35], deux types de prestaires étaient déjà identifiés :

- PSE : Prestataire de service externalisé.
- PSEE : Prestaire de service externalisé essentiel (PSEE).

Les autorités de régulation ont donc fait une distinction entre les prestataires, ainsi que des recommandations concernant les prestataires essentiels[36].

Le règlement DORA vient renforcer ces règles. Un tiers prestataire informatique sera qualifié de « critique » sur la base de critères liés à sa stabilité et à sa performance, à son degré d'implication dans l'activité des entités financières, et à son implantation sur le territoire européen.

En synthèse les principaux critères d'éligibilité sont :

- L'activité et l'organisation du tiers prestataire.
- Le nombre d'entités financières ayant contractualisé avec le tiers prestataire.
- La taille et la criticité de l'activité des entités financières.
- La dépendance des entités financières au tiers prestataire.
- Le nombre de pays d'implantation du tiers prestataire.

La classification des tiers prestaires informatiques est faite, quant à elle, par les AES. Elle permet d'avoir une meilleure surveillance et un niveau adéquat de contrôle des prestataires.

Les exigences contractuelles et opérationnelles sont définies à la fois pour les organisations financières, et pour les tiers prestataires informatiques identifiés comme critiques.

Les tiers prestaires identifiés comme critiques doivent respecter des normes élevées de sécurité afin de permettre aux organisations d'avoir une résilience numérique.

Une défaillance du prestataire ne doit pas impacter la continuité et la qualité du service de l'organisation financière.

L'incident d'OVH[37] du 13 octobre 2021, lié à un problème de configuration de son réseau, a rendu inaccessible pendant plusieurs heures les sites internet d'un grand nombre de ses clients. Cela illustre parfaitement l'impact que peut avoir ce type de prestataire sur toutes les entreprises utilisant leurs services, y compris les entités financières.

Mentionnons aussi un autre incident cloud, cette fois-ci sur l'infrastructure Microsoft Azure, intervenu en mai 2019. Il a eu un impact sur un nombre important d'entreprises. Pendant près d'une heure, les services de travail collaboratif Microsoft Office 365 et Microsoft Teams n'étaient pas disponibles.

Une heure, cela peut sembler court, mais multipliée par le nombre de salariés n'ayant pas pu travailler pendant ce laps de temps, cela représente des milliers de journées de travail perdues.

---

[34] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA) - Article 28. Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 5 mai 2022]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

[35] EUROPEAN BANKING AUTHORITY. Final report on EBA guidelines on outsourcing arrangements. EBA [en ligne]. 25 février 2019. [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1

[36] Les nouveaux enjeux de l'externalisation : un dispositif ad hoc au 30 septembre 2019. Revue Banque [en ligne]. 3 juin 2019. [Consulté le 5 mai 2022]. Disponible à l'adresse : http://www.revue-banque.fr/management-fonctions-supports/breve/les-nouveaux-enjeux-externalisation-un-dispositif

[37] CROCHET-DAMAIS, Antoine. Panne mondiale d'OVH : l'incident est clos, le groupe s'explique. JDN [en ligne]. 13 octobre 2019. [Consulté le 5 mai 2022]. Disponible à l'adresse suivante : https://www.journaldunet.com/web-tech/cloud/1505999-panne-mondiale-d-ovh-l-incident-est-clos-le-groupe-s-explique/

Ce type d'incident a des impacts majeurs dans tous les secteurs, y compris celui financier.

Des éléments conjoncturels sont également venus amplifier le recours à des prestataires : la pénurie des compétences techniques en local. Ce manque d'expertise a entrainé une extension des recherches à toute l'Europe. C'est le cas notamment dans le secteur de la cybersécurité et dans le développement des logiciels.

Les experts mis à disposition peuvent être dans le pays d'implantation de l'entité financière ou dans un autre pays de l'UE, qui, dans ce dernier cas n'est pas soumis aux mêmes lois et réglementations que le pays d'implantation du commanditaire. Cette diversité réglementaire complexifie la contractualisation des prestations.

DORA se base sur l'implantation territoriale et définit des règles applicables à tous. Le niveau de criticité du tiers prestaire est fortement dépendant du nombre de pays de l'UE où il exerce son activité.

C'est en partie pour cela que les leaders du cloud peuvent être considérés comme prestataires critiques. Leurs datacenters sont implantés dans plusieurs pays membres de l'UE.

Les principaux datacenters d'AWS sont en France, en Italie, en Allemagne[38], ceux de Microsoft sont principalement en France, et en Allemagne[39].

Il en est de même pour les entreprises du secteur de la cybersécurité qui accompagnent les entités financières dans la mise en œuvre de leur programme de sécurité informatique.

Certaines organisations financières ont un cœur de métier qui s'appuie - partiellement ou totalement - sur des services fournis par des prestaires informatiques. Cela entraine une dépendance forte entre l'entité financière et le prestataire. Une défaillance de ces prestataires entrainerait une cessation partielle ou totale des activités des entités financières.

En définitive, l'organisation financière ne dispose plus de la maitrise de son application ou de son système d'information.

L'identification des prestaires critiques permet d'évaluer les activités ou les services transférés et de définir un cadre contractuel afin d'assurer la résilience de l'activité de l'entité financière.

[38] Carte des régions et réseaux périphériques. [carte]. AWS [en ligne]. [Consulté le 5 mai 2022]. Disponible à l'adresse suivante : https://aws.amazon.com/fr/about-aws/global-infrastructure/regions_az/

[39] VICE, Kelley. Emplacement de données pour l'Union Européenne. Microsoft [en ligne]. [Consulté le 5 mai 2022]. Disponible à l'adresse suivante : https://docs.microsoft.com/fr-fr/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide

Focus sur les prestataires cloud

> ***« You are not late, you are out! »***.
>
> Jeff Bezos, s'adressant à Bruno Le Maire. Propos rapporté par le Ministre de l'Economie, en réponse au constat que l'Europe accuse du retard sur l'intéressé et sur les dirigeants des GAFAM.
>
> Un éternel soleil. Le Maire, Bruno. Paris : Editions Albin Michel. 2021, page 21.

Parmi tous les prestataires TIC du secteur financier, nous avons vu qu'une catégorie est à l'heure actuelle plus critique que les autres : les fournisseurs de solutions d'informatique dans le nuage.

Afin de plus asseoir les enjeux de ce type de fournisseurs, il convient de commencer par un tour d'horizon de ce qu'est le cloud avant de se focaliser sur l'utilisation qui en est faite par les institutions financières, et plus particulièrement au sein du secteur bancaire. Ces éléments permettront de mettre en exergue les apports du règlement DORA afin de réduire les risques inhérents à l'usage des solutions cloud.

Notions entourant le cloud

Le « cloud computing », ou informatique dans le nuage, correspond au fait de pouvoir accéder à distance, et de n'importe où dans le monde, aux logiciels et bases de données hébergés sur des serveurs. Ces serveurs sont entreposés dans des centres de données, ou datacenter, qui peuvent également être eux-mêmes dispersés dans le monde entier.

« L'utilisation du cloud computing permet aux utilisateurs et aux entreprises de s'affranchir de la nécessité de gérer des serveurs physiques eux-mêmes ou d'exécuter des applications logicielles sur leurs propres équipements.[40] *»*

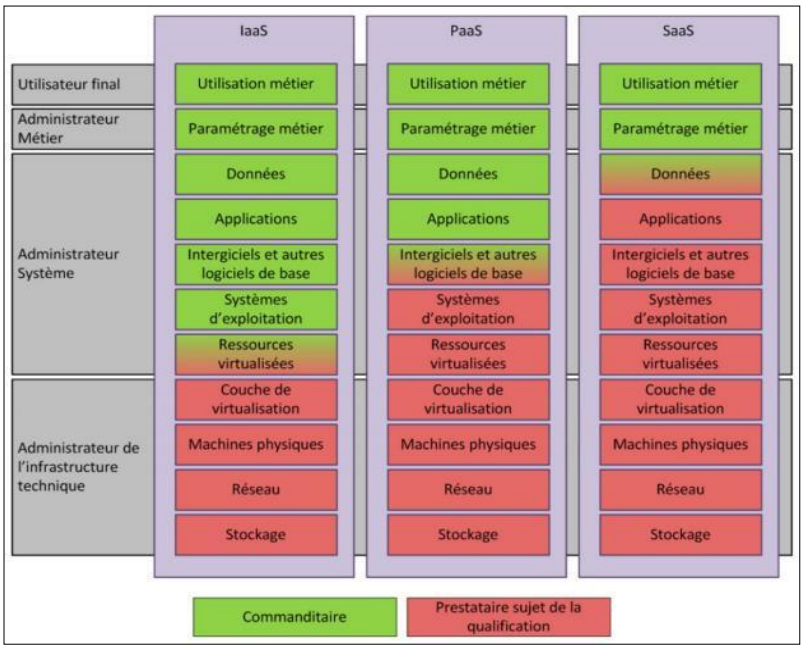
Le cloud permet de mettre à disposition du plus grand nombre d'utilisateurs, ou à un groupe d'utilisateurs identifiés, une panoplie assez large de services tout en permettant aux directions et services informatiques des entreprises une optimisation de leurs ressources.

En effet, les fournisseurs de solutions cloud vont mettre à leur disposition une palette très large de services.

Cela va de la location de locaux aménagés au sein de leurs Datacenter, où les entreprises vont pouvoir installer leurs propres serveurs qui accueilleront leurs applications et leurs données, à la fourniture complète des serveurs et applications qui seront nécessaires au fonctionnement de l'entreprise.

C'est ainsi qu'ont émergé différents types d'offres où graduellement la gouvernance des organisations informatiques peut aller d'une simple mise à disposition d'une infrastructure informatique, dit modèle « IaaS », pour « Infrastructure as a Service », à la mise à disposition d'une solution applicative complète donnant accès à une ou plusieurs applications hébergées et accessibles via une connexion et un navigateur internet. Cette dernière solution, une des plus connues à ce jour, est appelée modèle « SaaS », c'est-à-dire « Software as a Service ». Entre les modèles IaaS et SaaS, nous rencontrerons très souvent le modèle PaaS, pour « Platform as a Service », qui est un modèle intermédiaire où l'entreprise apporte applications et données, les autres constituantes de l'organisation informatique étant déléguées au prestataire (cf. figure ci-après).

[40] Cloudflare. Qu'est-ce que le cloud ?. Cloudflare [en ligne]. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.cloudflare.com/fr-fr/learning/cloud/what-is-the-cloud/



41

Ces solutions peuvent être déployées de différentes façons auprès des clients de ces fournisseurs. Nous rencontrons alors les appellations de cloud privé, de cloud public, ainsi qu'une solution intermédiaire qui est le cloud hybride.

Le **cloud privé** va désigner un serveur, ou un Datacenter, entièrement dédié à une entreprise ou une organisation.

Le **cloud public** va, quant à lui, désigner le fait de passer par un fournisseur qui va partager ses infrastructures (Datacenter et serveurs) entre de nombreuses entreprises et organisations. Il faut alors voir le cloud public comme un immeuble détenu par un même propriétaire qui loue un ou plusieurs de ses logements disponibles. Charge au locataire de sécuriser et de faire bon usage du logement pour lequel il vient de signer un contrat.

Enfin, le **cloud hybride** est une solution qui consiste, pour une même entreprise, à détenir à la fois une solution de cloud privé et une solution de cloud public qui interagissent entre elles. Le cloud hybride est généralement utilisé de la façon suivante : les données et applications sensibles, d'un point de vue réglementaires et/ou sécurité, sont hébergées sur le cloud privé de l'entreprise, tandis que les applications bureautiques et messageries internes, mais également des applications métier jugées non-sensibles, sont hébergées sur la partie cloud public. Les utilisateurs de l'entreprise, dans le cadre de leurs missions quotidiennes, ont accès de manière complètement transparente tant à leurs applications bureautiques et de messageries, qu'à leurs applications métiers, sensibles comme non-sensibles, et leurs données associées, à partir de leur poste de travail.

[41] HAUT COMITÉ JURIDIQUE DE LA PLACE FINANCIÈRE DE PARIS. Rapport sur le cloud bancaire : état des lieux et propositions du Haut Comité Juridique de la Place Financière de Paris. Banque de France [en ligne]. Mai 2021. 14 p. [consulté le 13 mai 2022]. Disponible à l'adresse : https://www.banque-france.fr/sites/default/files/rapport_42_f.pdf

Avantages

Ces différents modèles de prestations de services cloud, IaaS/PaaS/SaaS, alliés à des modes de déploiement très souples et interconnectables, permettent d'envisager de nombreuses combinaisons tout en mutualisant une quantité de ressources toujours plus importantes.

Les avantages du recours à des solutions cloud sont multiples, liés essentiellement à la mutualisation des ressources disponibles, et surtout à leur bonne gestion et optimisation :

- Un accès à de grandes puissances de calcul, ce qui permet le recours à l'intelligence artificielle (IA), ou bien encore aux moteurs d'apprentissage automatique (*machine learning*).
- Une infrastructure et une capacité de stockage déléguées qui peuvent s'adapter aux besoins des clients, tant à la hausse qu'à la baisse. Il sera alors question de scalabilité.
- Une multitude d'applications tierces disponibles et intégrables aisément dans les processus métiers de nombreux secteurs d'activité.
- Une résilience accrue grâce aux services de sauvegardes et de redondance proposées par les fournisseurs de prestations cloud.
- Un niveau de sécurité et de conformité correspondant aux standards attendus dans nombre de domaines dont la banque et l'assurance en répondant aux exigences de multiples certifications et normes à travers le monde.

Les économies d'échelle aidant, les prestataires cloud peuvent proposer des solutions adaptées aux entreprises, quelle que soit leur taille, et, cerise sur le gâteau, le tout en maîtrisant les coûts. Les prix affichés par les divers prestataires cloud sont très attractifs : le prix de la machine Google est de l'ordre de moins 1 dollar de l'heure, il en est de même pour les instances AWS[42] .

[42] WAYNER, Peter ; CERTES, Nicolas. 7 noirs secrets derrière les tarifs du cloud. Le Monde Informatique [en ligne]. 21 juin 2020. [Consulté le 7 mai 2022]. Disponible à l'adresse suivante : https://www.lemondeinformatique.fr/actualites/lire-7-noirs-secrets-derriere-les-tarifs-du-cloud-79497.html

Le rapport du secteur bancaire avec les services dans le cloud

L'Open Banking, un premier pas vers un recours au cloud quasi obligatoire

L'ouverture du système bancaire, ou Open Banking, est un mouvement qui a démarré dans le secteur bancaire il y a environ une dizaine d'années à la suite des évolutions des modes de consommation des produits bancaires. Face à la demande croissante de produits toujours plus innovants, et un besoin pressant de simplifier les transactions pour les rendre aussi rapides et efficaces dans l'exécution qu'une commande sur Amazon, notamment depuis un téléphone mobile, le secteur bancaire n'a eu d'autres choix que de s'adapter.

Ce domaine d'activité étant très régulé, les normes et réglementations ont été revues pour accompagner et sécuriser ces évolutions. C'est dans ce contexte que la seconde « Directive des Services de Paiement » (DSP2), a été mise en œuvre en France en 2018. A partir de là, et grâce à l'ouverture des systèmes de paiement à de nouveaux acteurs et au partage sécurisé de données rendu possible par cette directive, sont apparues des initiatives innovantes autour des moyens de paiement et d'opérations bancaires de base, telles que la consultation de ses comptes bancaires et de procéder à des virements à partir de l'application pour téléphone mobile fournie par sa banque.

Depuis, de nouveaux modes de paiement ont été développés et mis en place tels que le virement depuis votre application bancaire vers l'un de vos contacts grâce à son numéro de téléphone mobile, sans qu'il soit nécessaire de connaître au préalable ses coordonnées bancaires, ou bien encore le paiement sans contact, et, dernièrement, l'apparition du virement instantané.

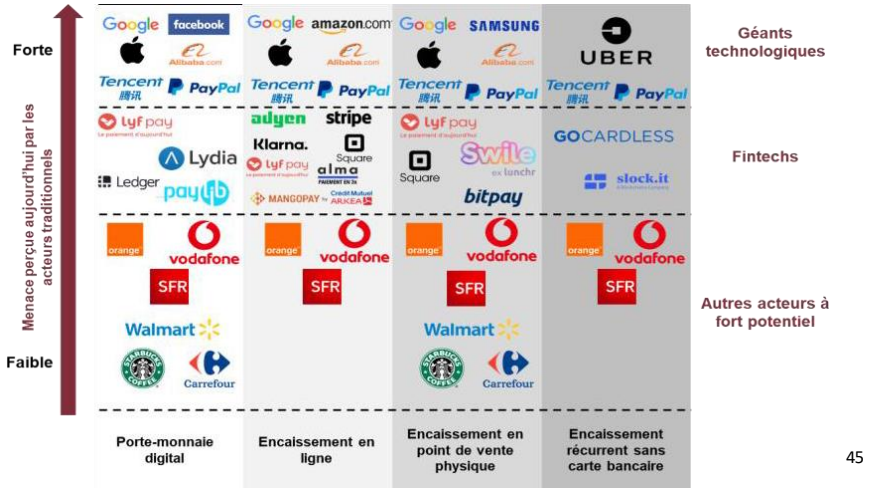
La plupart de ces innovations sont issues de startup qui se sont spécialisées dès leur création dans ces nouveaux modes de consommation, et constituent aujourd'hui ce qui est appelé « la FinTech », évoqué en première partie de ce rapport. *« La FinTech, contraction de Financial Technology (technologie financière), désigne des petites entreprises (start-up et PME) qui fournissent des services financiers grâce à des solutions innovantes. Les domaines d'application sont variés : paiement mobile, financement participatif (crowdfunding), gestion de l'épargne, assurance et crédit, conseil financier en ligne, aide à la décision grâce aux algorithmes[43]. »*

Les FinTechs ont recours, de manière systématique, à toutes les ressources que peuvent leur mettre à disposition les technologies hébergées dans le cloud : puissance de calcul, rapidité de développement des applications et de leur mise à disposition aux clients et partenaires, tout en assurant le niveau de sécurité attendu par les différentes réglementations en vigueur comme la DSP2.

En 2020, il était estimé que le marché des paiements générerait près de 2 000 milliards de dollars à horizon 2025. La plupart de ces revenus, selon une étude du cabinet Accenture, relayée par le journal *Les Echos*[44], échapperaient aux banques traditionnelles si celles-ci n'adaptaient pas rapidement leur modèle pour contrer les initiatives de FinTechs telles que la startup américaine Stripe, ou bien encore la néerlandaise Adyen, qui se sont développées en ayant le paiement comme seule et unique activité. Sans compter que les GAFAM, qui cherchent également à capter une partie de ces revenus, peuvent investir des sommes colossales dans ce domaine. La pression concurrentielle sur les acteurs traditionnels du secteur, que sont les banques, est parfaitement résumée dans le tableau ci-dessous :

[43] MINISTERE DE L'ECONOMIE DES FINANCES ET DE LA RELANCE. La Fintech, le numérique au service du secteur financier. [en ligne]. 19 janvier 2018. [Consulté le 7 mai 2022]. Disponible à l'adresse : https://www.economie.gouv.fr/entreprises/fintech-innovation-finance

[44] BLOCH, Raphaël. Paiement : ces 280 milliards qui pourraient échapper aux banques d'ici à 2025. Les Echos [en ligne]. 23 janvier 2020. [Consulté le 8 mai 2022]. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/banque-assurances/paiement-ces-280-milliards-qui-pourraient-echapper-aux-banques-dici-a-2025-1165392



45

Un développement soutenu des API

La réponse à ces nouveaux besoins des consommateurs, de même que la mise en place efficiente d'interactions entre les acteurs déjà en présence sur le marché bancaire, n'a été possible que grâce au développement de nombreuses interfaces de programmation d'application (API). Même si plusieurs stratégies ont été déployées par les forces en présence, allant d'acquisitions pures et simples de FinTech par les banques, jusqu'à la mise en place de partenariats entre acteurs[46], il n'en demeure pas moins que le point commun de leurs multiples réussites fut la bonne utilisation des API.

Il était nécessaire de pouvoir mettre à disposition, d'une manière simple, les données que leurs clients souhaitaient voir utilisées par un fournisseur tiers, comme un agrégateur de compte bancaire. En cas d'absence de mise à disposition de ce nouveau service à un tiers, la banque s'exposait à voir partir son client pour l'un de ses concurrents qui, lui, satisferait ses besoins.

Les **API** sont apparues comme des solutions relativement peu coûteuses, rapides à développer, et compatibles avec les nouvelles technologies issues du cloud. Ce qui n'était pas le cas des systèmes d'informations des banques, âgés de plusieurs dizaines d'années et qui ont été développés dans une logique d'utilisation et d'accès sécurisés uniquement en interne. Faire évoluer ou changer ces infrastructures et ces applications fait peser un coût trop élevé à la banque, et ces travaux prendraient plusieurs années avant de pouvoir être finalisés[47].

Les API solutionnent toutes ces problématiques[48], et permettent à des tiers de se connecter, via des authentifications fortes répondant aux exigences DSP2 ou d'autres réglementations, tout en mettant à disposition uniquement les données nécessaires au traitement souhaité.

Tout naturellement, les acteurs du secteur bancaire et financier ont développé leurs solutions hébergées sur une structure de cloud hybride pour à la fois sécuriser leurs données et applications stratégiques sur leurs espaces privés. Ils ont également mis à disposition sur leurs espaces publics les interfaces donnant accès aux solutions et produits développés pour les tiers et les clients.

---

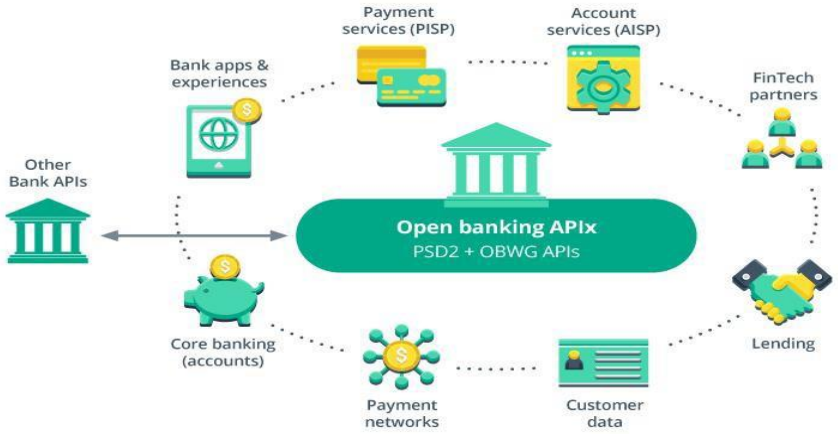
[45] GALOPIN, David ; RASOARAHONA Thomas. Les banques face à la menace des nouveaux acteurs du monde des paiements. [graphique]. In : Blog CGI [en ligne]. 8 octobre 2020. [Consulté le 8 mai 2022]. Disponible à l'adresse : https://www.cgi.com/france/fr-fr/blog/banques-face-menace-nouveaux-acteurs-monde-des-paiements

[46] CUNY, Delphine. Pas d'avenir sans les banques pour les startups de la FinTech. La Tribune [en ligne]. 5 avril 2017. [Consulté le 8 mai 2022]. Disponible à l'adresse : https://www.latribune.fr/entreprises-finance/banques-finance/pas-d-avenir-sans-les-banques-pour-les-startups-de-la-fintech-679157.html

[47] RENAUD, Ninon. Banques et FinTech construisent la banque de demain. Les Echos [en ligne]. 12 septembre 2017. [Consulté le 9 mai 2022]. Disponible à l'adresse : https://www.lesechos.fr/2017/09/banques-et-fintech-construisent-la-banque-de-demain-176548

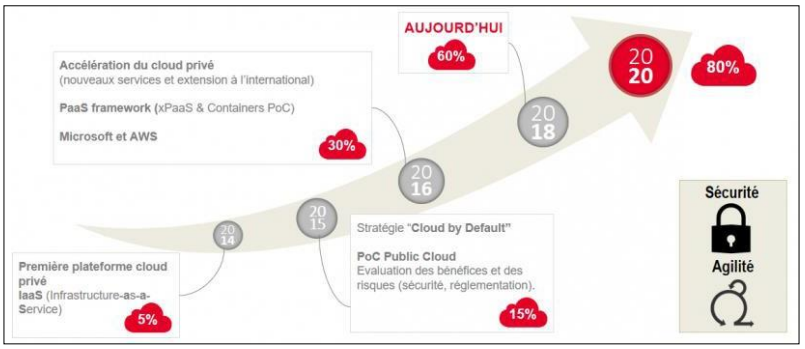
[48] DELATTRE, Laurent. Priorité aux API : une nécessité d'ouverture et Business. IT for Business [en ligne]. 28 mars 2022. [Consulté le 9 mai 2022]. Disponible à l'adresse : https://www.itforbusiness.fr/priorite-aux-api-une-necessite-douverture-et-business-47590

Une illustration de l'universalité des API DSP2 ci-après :



49

Il en va de même pour les FinTechs qui, au début de leur activité, construisent une architecture de base en utilisant quelques composants cloud. Puis, au fur et à mesure de leur croissance, elles vont adapter leur infrastructure et leur offre. De quelques API ou instances, ils vont progressivement augmenter leur nombre à une dizaine voire des centaines, afin de faire face aux exigences et aux contraintes du secteur financier, comme de leurs clients. Dans ce contexte, la mise en œuvre d'infrastructures résilientes et sécurisées augmente fortement les coûts intrinsèques, sans possibilité de renégocier les tarifs.



Selon Carlos GONCALVES, Directeur des Infrastructures Informatiques pour le Groupe Société Générale, « *on peut considérer que le cloud public est aujourd'hui plus sécurisé que notre ancien réseau !*[50] ». Cette déclaration prend une certaine dimension quand, en parallèle, la Société Générale indique en octobre 2020 que 78% de ses infrastructures étaient d'ores et déjà sur le cloud, sachant que l'objectif, fixé par le Groupe en 2016, était d'atteindre 80% avant la fin de l'année 2020[51].

[49] RYFIAK, Solomiia. This is what Open Banking APIs look like. [graphique]. In : How will PSD2 beca [en ligne]. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://intellias.com/how-will-psd2-become-a-game-changer-for-merchants/

[50] BEST, Ivan. Les banques optent pour le cloud mais avec des garanties. Option Finance [en ligne]. 3 septembre 2021. [Consulté le 10 mai 2022]. Disponible à l'adresse : https://www.optionfinance.fr/innovation/les-banques-optent-pour-le-cloud-mais-avec-des-garanties.html

[51] SOCIETE GENERALE. Société Générale accélère sa stratégie cloud. [en ligne]. 18 octobre 2018. [Consulté le 9 mai 2022]. Disponible à l'adresse : https://www.societegenerale.com/fr/actualites/newsroom/societe-generale-accelere-sa-strategie-cloud

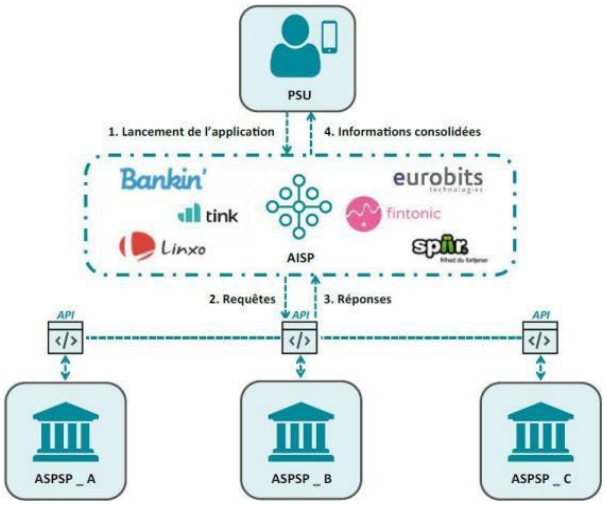
Cas d'usage de solution cloud : les agrégateurs bancaires

Depuis la mise en œuvre de la réglementation DSP2, les banques ont l'obligation de mettre à disposition des applications tierces les données relatives aux transactions bancaires de leurs clients communs l'ayant demandé.

C'est ainsi que le statut de prestataire de services d'informations de compte, ou « Account Information Service Provider » (AISP), est apparu.

Comme le montre le circuit à droite[52], le client, une fois son consentement donné, peut voir s'afficher les informations consolidées de l'ensemble de ses comptes bancaires détenus dans plusieurs établissements bancaires, via l'application mobile de son prestataire AISP.

Dans les coulisses, l'application de l'AISP va se connecter à chaque API dédiée à ce type de requêtes dans les banques sélectionnées par l'utilisateur. Via l'identification renseignée par l'utilisateur dans l'application de l'AISP, et les vérifications d'usage effectuées par les API des différentes banques, ces dernières vont communiquer les informations souhaitées à l'application de l'AISP.



Ainsi, notre utilisateur a pu, grâce à une seule application, avoir accès à l'ensemble de ses informations bancaires.

Cas d'usage de solution cloud : la lutte contre la fraude

La lutte contre la fraude est l'une des priorités dans le secteur bancaire, tant du côté du financement que du côté des paiements.

C'est ainsi que le Groupe Société Générale a investi de manière importante, et cela pendant plusieurs années, sur une solution de cloud hybride alliant cloud public, pour la puissance de calcul et les solutions d'analyses massives de données, afin de faire progresser les algorithmes dédiés à la lutte contre la fraude.

Cet engagement a permis de mettre en place la solution MOSAIC, « *More Security with Artificial Intelligence*[53] », qui est aujourd'hui déployée dans tout le Groupe et permet de détecter des tentatives de fraudes sur tout type de moyens de paiement[54], y compris les paiements instantanés. Sur ceux-ci la détection s'effectue en moins d'une demi-seconde et génère la mise en attente de la délivrance des fonds, le temps que l'alerte générée soit traitée[55].

---

[52] GALITT. Livre blanc - DSP 2 et open API : Menaces et opportunités pour le secteur bancaire ... en route vers l'Open-Banking ?. [graphique]. Galitt [en ligne]. 31 mars 2018. [Consulté le 8 mai 2022]. Disponible à l'adresse : https://www.galitt.com/wp-content/uploads/2020/11/Livre-Blanc-Galitt-DSP2-OPEN-API-En-route-vers-Open-Banking.pdf

[53] CALMEJANE, Claire. Innovation Insider avec Anne BRIEC sur la lutte contre la fraude et la protection de nos clients. LinkedIn [en ligne]. 27 novembre 2020. [Consulté le 9 mai 2022]. Disponible à l'adresse : https://www.linkedin.com/pulse/innovation-insider-avec-anne-briec-sur-la-lutte-contre-calmejane/?originalSubdomain=fr

[54] CROCHET-DAMAIS, Antoine. Comment l'IA se met au service de la lutte contre la fraude financière ?. JDN [en ligne]. (Mise à jour le 2 mai 2022). [Consulté le 5 mai 2022]. Disponible à l'adresse : https://www.journaldunet.com/solutions/dsi/1510875-comment-l-ia-se-met-au-service-de-la-lutte-contre-la-fraude-financiere/

[55] SOCIETE GENERALE. Co-construire la banque du futur avec nos clients. [en ligne]. 20 octobre 2020. [Consulté le 9 mai 2022]. Disponible à l'adresse : https://www.societegenerale.com/sites/default/files/documents/2020-10/societe-generale-dossier-presse-strategie-digitale-et-innovation-2020-10-20_0.pdf

Cette solution, après avoir suffisamment mûri en interne, s'est ouverte sur l'extérieur grâce à un partenariat avec Trustpair pour proposer aux entreprises, via une application, une solution d'automatisation des contrôles de flux de virements émis par la société utilisatrice. L'objectif est de sécuriser ces flux en luttant à la fois contre la fraude, mais également en bloquant les virements comportant des erreurs de saisie[56].

Nous avons cité ici uniquement quelques cas d'usages qui ont pu se développer uniquement grâce aux bénéfices apportés par le recours aux technologies cloud. Nous aurions pu en mentionner bien d'autres tels que l'apport de la signature électronique et le recours aux technologies de reconnaissance et de lecture documentaire qui ont grandement allégé le poids des traitements entourant l'ouverture d'un compte bancaire, ou bien encore les agents conversationnels, appelés « *chatbot* », qui permettent dorénavant une assistance personnalisée aux clients, et cela à toute heure du jour et de la nuit.

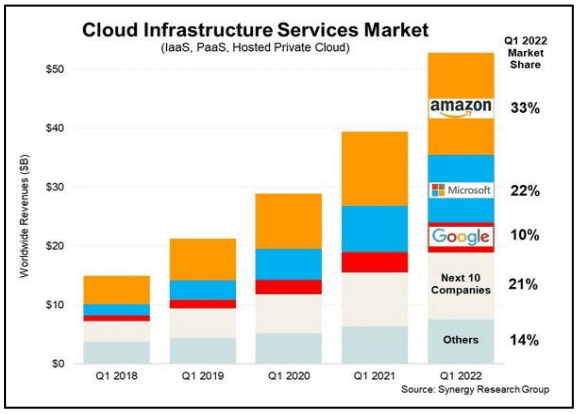
Il n'en demeure pas moins que ces recours croissants aux prestataires de solutions cloud peuvent également être sources de risques par ailleurs.

Les risques inhérents aux services dans le cloud

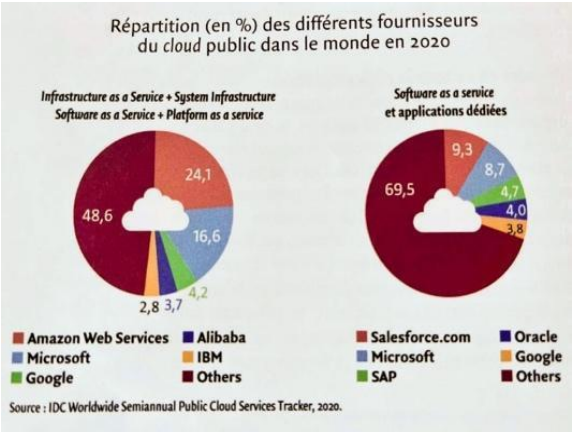
Une dépendance forte à quelques acteurs

Quel que soit le besoin recherché en matière de prestation cloud, à savoir une solution IaaS, une solution PaaS, ou bien encore une solution SaaS, les plus grands fournisseurs sont des entreprises non européennes. Et la plupart d'entre elles ont leur maison mère aux Etats-Unis d'Amérique.

En cumulant tous les types de solutions, Amazon Web Services, Microsoft et Google détenaient près de 65%[57] des parts de marché mondial au premier trimestre 2022, en forte progression ces dernières années.



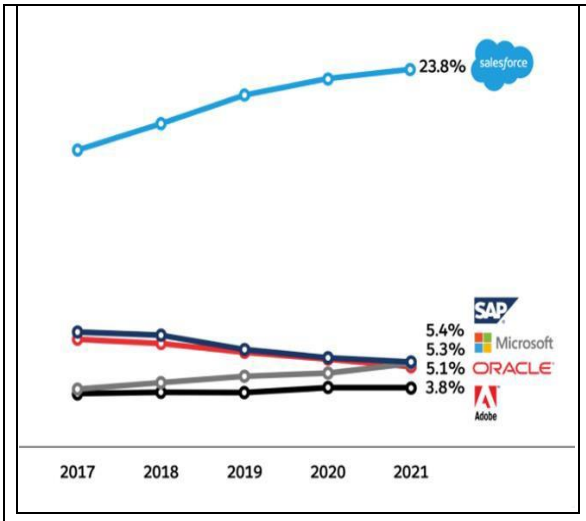
Le plus connu des fournisseurs de solutions SaaS est Salesforces.com. Cette entreprise américaine représentait, à elle seule, près de 70%[58] des prestations SaaS fournies dans le monde en 2020.



[56] LEFEBVRE, Arnaud. Société Générale et Trustpair s'associent dans la lutte contre la fraude. Option Finance [en ligne]. 10 juillet 2020. [Consulté le 12 mai 2022]. Disponible à l'adresse : https://www.optionfinance.fr/innovation/societe-generale-et-trustpair-sassocient-dans-la-lutte-contre-la-fraude.html

[57] BEKY, Ariane. Cloud infrastructure Services Market. (2022) [graphique]. In : Silicon.fr [en ligne]. 4 mai 2022. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.silicon.fr/infrastructure-cloud-aws-azure-google-437850.html

[58] CHAPTAL, Stéphanie. Répartition (en %) des différents fournisseurs du cloud public dans le monde en 2020. (2020) [graphique]. In : Revue Banque [en ligne]. 22 avril 2022 [Consulté le 11 mai 2022]. Disponible à l'adresse : http://www.revue-banque.fr/inline_content/node/466539

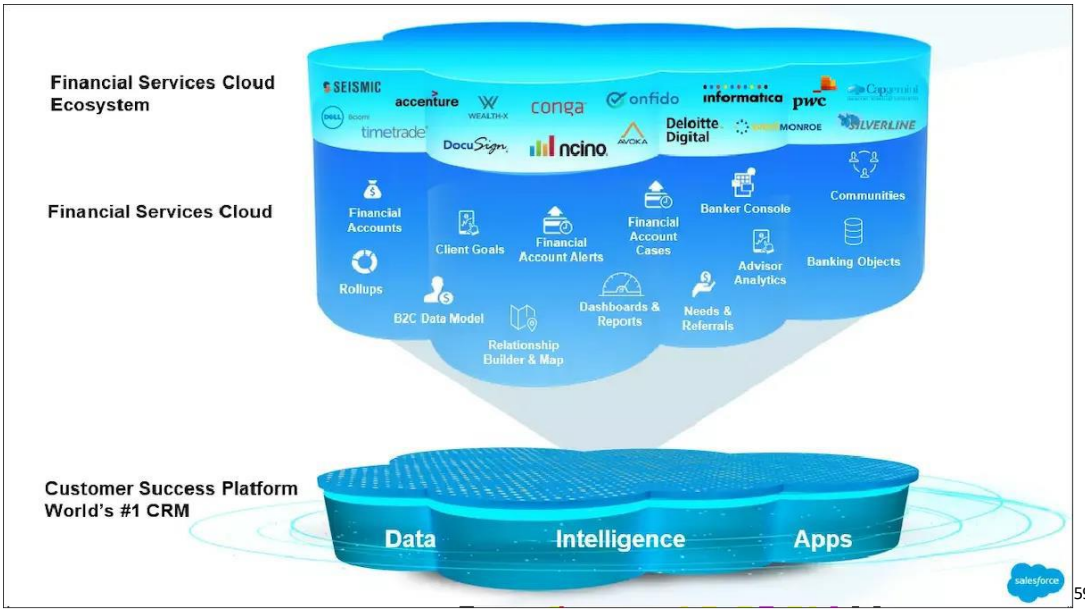


Pour ceux découvrant le nom de Salesforce.com, ce fournisseur de solutions SaaS est un incontournable pour ce qui est des applications de gestion de la relation client (Consumer Relation Management, ou CRM). Pour la huitième année consécutive, Salesforce.com est le numéro un mondial des applications CRM, selon une étude de IDC Worldwide Semiannual Software Tracker sur l'année 2021.

Source: Salesforce.com. Ranked #1 for CRM Applications based on IDC 2021 Revenue Market Share Worldwide. (2022) [graphique]. In : Salesforce.com [en ligne]. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.salesforce.com/campaign/worlds-number-one-CRM/

En prenant l'exemple de la solution *Financial Services Cloud* de Salesforce.com, il est aisé de comprendre quelle a été la stratégie gagnante de cet éditeur. Ce plan de bataille est parfaitement huilé après 23 ans d'existence, et il conquiert de plus en plus de directions commerciales au sein des institutions financières, grâce à l'étendue de l'offre (confère présentation ci-après), son efficacité et l'ergonomie des applications. Certaines directions des services informatiques apprécient également ces solutions, qui peuvent être intégrées rapidement au sein du système d'information qui, rappelons-le, communique et travaille de manière optimale avec les technologies issues du cloud.

Mais il n'en demeure pas moins que Salesforce.com gère de plus en plus de données sensibles et stratégiques, pour un nombre croissant d'institutions financières en France comme en Europe.

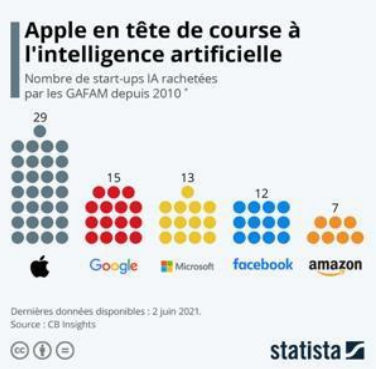


[59]

[59] TRAILHEAD. Illustration de la solution Financial Services Cloud de Salesforce.com. [image]. In : Trailhead [en ligne]. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://trailhead.salesforce.com/fr/content/learn/modules/fsc_basics/fsc_basics_unit_1

Il en va de même si la recherche de prestation se tourne vers une solution d'intelligence artificielle. En dehors de ce que propose l'écosystème

Salesforce.com, vous croiserez nécessairement sur ce marché les GAFAM. Ces derniers ont fait l'acquisition de dizaines de startups spécialisées dans l'intelligence artificielle, comme le montre le graphique ci-contre[60], démultipliant leur surface de contact avec les entreprises du monde entier.



Les institutions financières n'en demeurent pas moins des entreprises commerciales qui ont besoin d'innover en ayant, par exemple, de plus en plus recours aux technologies d'intelligence artificielle afin de conserver leur clientèle, de la développer en proposant des produits innovants, et accroître ainsi ses parts de marchés.

De plus, grâce à leur taille critique, les prix proposés par les divers prestataires cloud sont très attractifs : le prix de la machine google est de l'ordre de moins 1 dollar de l'heure. Il en est de même pour les instances AWS[61] .

Ces contrats, négociés en début de projet, sont difficilement modifiables par la suite. Surtout lorsque toutes vos données sont hébergées chez votre prestataire. Après quelques années d'utilisation du service, les négociations sont d'autant plus complexes que la quantité de données hébergées a cru proportionnellement à l'augmentation de votre activité. Les entités financières disposent donc d'assez peu de marge de manœuvre pour réévaluer leurs contrats une fois la migration dans le cloud effectuée. Ces difficultés se voient amplifiées par la taille de l'acteur financier qui souhaite contractualiser avec un fournisseur cloud. Bien souvent, les petits acteurs ne disposeront pas de moyens leur permettant d'avoir des contrats qui évolueront et s'adapteront à leurs besoins tout au long de leur croissance.

Face à de tels poids lourds dans ces différents domaines, il n'est donc pas simple de négocier l'intégration de clauses contractuelles spécifiques tant pour se prémunir de risques juridiques, que d'autres catégories de risques inhérents aux prestataires de services informatiques dans le cloud. Souvent, ces contrats ne prévoient pas des garanties en lien avec la criticité de l'activité des entités financières et les règlementations en vigueur en union européen. Ils ne tiennent pas compte également du pays où exerce l'entité financière.

Seuls les acteurs financiers d'une taille significative auront les moyens et les compétences nécessaires pour négocier l'intégration de clauses qui seront propres à leurs besoins et suffisamment ouvertes pour permettre de répondre aux besoins présents, mais également à venir. Pour ce qui des clauses permettant d'effectuer des audits et des tests de pénétrations, dont les résultats seront nécessairement partagés afin de confirmer le degré de sécurité et de résilience opérationnelle du fournisseur.

En parallèle, une coalition de banques s'est constituée pour mettre en place une solution dite de « cloud communautaire[62] » afin de mieux répondre aux besoins spécifiques des institutions financières. L'objectif de cette initiative est assez simple. Au-delà de faire front face aux fournisseurs de stockage américains pour résister à leur domination, c'est également pour s'assurer du bon respect des différentes réglementations en vigueur sur le sol européen. De plus en plus de données des institutions bancaires transitent par les solutions hébergées par les fournisseurs de cloud. Elles sont alors exposées au risque juridique que constitue le « Cloud Act ».

---

[60] JENIK, Claire. Apple en tête de course à l'intelligence artificielle. (2 juin 2021) [graphique]. In : Statista [en ligne]. 20 juillet 2021. [Consulté le 13 mai 2022]. Disponible à l'adresse : .https://fr.statista.com/infographie/9418/gafam-rachats-et-acquisitions-de-startups-ia/#:~:text=D'apr%C3%A8s%20les%20donn%C3%A9es%20de,de%20pr%C3%A9curseurs%20dans%20le%20domaine.

[61] WAYNER, Peter ; CERTES, Nicolas. 7 noirs secrets derrière les tarifs du cloud. Le Monde Informatique [en ligne]. 21 juin 2020. [Consulté le 7 mai 2022]. Disponible à l'adresse suivante : https://www.lemondeinformatique.fr/actualites/lire-7-noirs-secrets-derriere-les-tarifs-du-cloud-79497.html

[62] Auteur inconnu, Frankfurter Allgemeine Zeitung. Nuage - Des banques européennes s'allient contre la puissance du cloud américain. Courrier International [en ligne]. 28 janvier 2021. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.courrierinternational.com/article/nuage-des-banques-europeennes-sallient-contre-la-puissance-du-cloud-americain

Une exposition aux lois extraterritoriales

Avec l'adoption, en 2018, du « Cloud Act » par l'administration du Président Américain de l'époque, Donald Trump, les données des entreprises françaises, et plus particulièrement des institutions financières se retrouvaient de facto accessibles par voie judiciaire.

En effet, par le truchement de cette réglementation à portée extraterritoriale, les autorités américaines peuvent exiger, de n'importe quelle entreprise américaine, y compris et surtout des fournisseurs de cloud américains, le transfert de données stockées n'importe où dans le monde vers les Etats-Unis. En conséquence, si ce transfert de données comporte des données personnelles protégées par le Règlement Général sur la Protection des Données (RGPD), l'entreprise française enfreint ce dernier, et encourt des sanctions financières qui, rappelons-le, peuvent aller, selon la catégorie de l'infraction, de 10 à 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé entre les deux calculs étant retenu.

La Commission Nationale de l'Informatique et des Libertés (CNIL) a par ailleurs émis des recommandations à destination des entreprises françaises qui souhaitent souscrire des prestations avec les fournisseurs de solutions cloud, visant plus particulièrement les solutions dites SaaS[63].

Face à cela, et pour ne pas perdre de parts de marchés, notamment auprès des institutions financières, les fournisseurs de prestations cloud, ont redoublé d'efforts et d'imagination en proposant des solutions techniques en réponse à ces menaces juridiques, notamment via un double chiffrement des données stockées sur leurs serveurs[64]. Ainsi, même en cas de saisie des données par les autorités américaines, les données personnelles pouvant se trouver parmi toutes les données transférées, restent indéchiffrables, ce qui évite aux entreprises européennes d'enfreindre le règlement RGPD.

Ces solutions, certes plus sécuritaires, s'avèrent coûteuses et contraignantes pour les clients : il faut prévoir sauvegardes et solutions alternatives en cas d'immobilisation des serveurs par les autorités américaines afin de continuer l'activité, le temps que la justice fasse son œuvre.

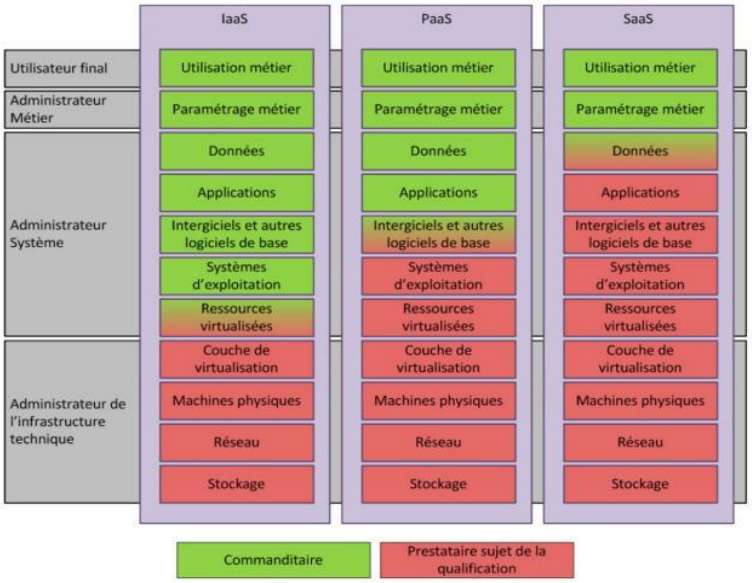
Une méconnaissance des rôles et responsabilités de chacun

Lorsque l'institution financière souscrit une prestation avec le fournisseur cloud, un contrat est établi pour régir la relation entre les parties. Toutefois, ce n'est que depuis les récents incidents que les commanditaires prennent véritablement conscience de l'importance de la bonne compréhension de toutes les clauses des contrats signés, et des responsabilités sous-jacentes.

En effet, en reprenant le schéma présenté précédemment et remis ci-dessous, force est de constater que la relation de dépendance s'intensifie au fur et à mesure de la délégation donnée par le commanditaire au prestataire (zone colorée en rouge). Ce qui expose d'autant la société aux aléas que peut subir le fournisseur.

[63] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Recommandations pour les entreprises qui envisagent de souscrire à des services de cloud. [en ligne]. [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

[64] BOHIC, Clément. Cloud Act : pour AWS, la parade est dans le chiffrement des données. Silicon [en ligne]. 16 septembre 2019. (Mise à jour le 31 décembre 2021). [Consulté le 13 mai 2022]. Disponible à l'adresse : https://www.silicon.fr/cloud-act-aws-chiffrement-des-donnees-260865.html



65

L'exemple de l'incendie de l'entreprise OVH, en mars 2021 fut instructif sur ces aspects-là. Au-delà des éléments physiques liés à l'origine et à la propagation de l'incendie, il est intéressant de regarder de plus près les enseignements tirés des aspects contractuels. Au cours de cette crise, nombre de clients d'OVH ont été surpris par les réponses à leurs interrogations sur les plans de continuité et de reprise d'activité qui entouraient les solutions qu'ils avaient souscrits : à défaut d'avoir souscrit l'option payante de sauvegarde, « *OVHcloud n'effectue aucune sauvegarde spécifique du Contenu stocké dans le cadre des Services. Il appartient en conséquence au Client de prendre toutes mesures nécessaires à la sauvegarde de ses Contenus afin de se prémunir contre les risques de perte ou de détérioration, quelle qu'en soit la cause*[66] ».

En d'autres termes, soit l'entreprise avait souscrit l'option de sauvegarde et pouvait faire appel à ce service pour continuer son activité, soit l'option n'était pas souscrite, auquel cas l'entreprise devait avoir été prévoyante en ayant mis en place une solution de sauvegarde par ailleurs. Rappelons que la perte ou la destruction de données protégées dans le cadre du règlement RGPD doit être notifiée à la CNIL, cet évènement étant considéré comme une faille de sécurité au sens de cette réglementation.

Malheureusement même en ayant souscrit l'option de sauvegarde, des clients ont eu la désagréable surprise d'apprendre que leurs sauvegardes étaient bien effectuées sur un autre serveur, mais que celui-ci se situait sur le même site géographique, dans le bâtiment adjacent, lui aussi détruit par l'incendie. Un recours collectif en justice à l'encontre d'OVH a été déposé début 2022 par plus de 80 entreprises touchées par cet évènement[67].

Une autre répercussion, plus directe cette fois de l'incendie d'OVH, fut du côté de l'assureur Axa France qui a été victime d'une fuite de données[68].

L'un des prestataires de l'assureur hébergeait les données d'Axa pour délivrer un service interne. À la suite de l'incendie, la sécurité de son infrastructure s'est retrouvée fragilisée, et exposée à une cyberattaque, qui a eu pour conséquence une extraction non autorisée de données concernant des employés d'Axa.

---

[65] HAUT COMITÉ JURIDIQUE DE LA PLACE FINANCIÈRE DE PARIS. Rapport sur le cloud bancaire : état des lieux et propositions du Haut Comité Juridique de la Place Financière de Paris. Banque de France [en ligne]. Mai 2021. 14 p. [consulté le 13 mai 2022]. Disponible à l'adresse : https://www.banque-france.fr/sites/default/files/rapport_42_f.pdf

[66] OVH. Conditions générales de services - Version en date du 1er septembre 2020. OVH [en ligne]. 1 septembre 2020. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://www.ovh.com/fr/support/documents_legaux/conditions%20generales%20de%20service.pdf

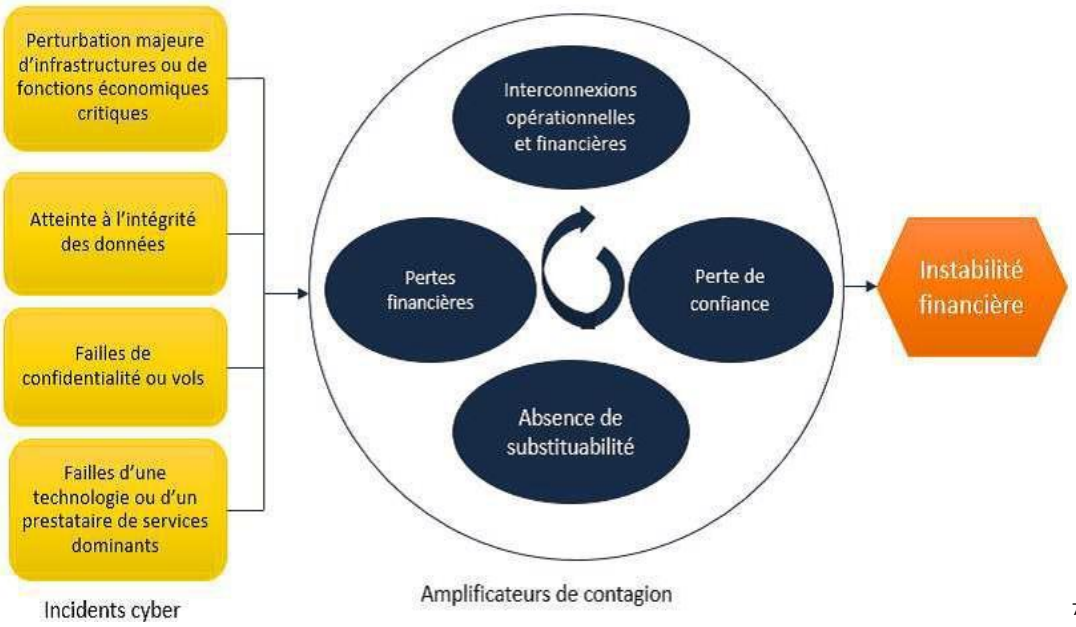
[67] BRASSAC, Leslie. Recours collectif contre OVH : "la piste du RGPD est privilégiée", A. DAKOS. Editions Législatives Lefebvre Dalloz [en ligne]. 19 janvier 2022. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://www.editions-legislatives.fr/actualite/recours-collectif-contre-ovh-la-piste-du-rgpd-est-privilegiee-a-dakos

[68] DE MEYER, Bertrand. 7.500 salariés d'Axa ont été victimes d'une fuite de données. L'AGEFI [en ligne]. 3 mai 2022. [Consulté le 5 mai 2022]. Disponible à l'adresse suivante : https://www.agefi.fr/banque-assurance/actualites/quotidien/20210504/7500-salaries-d-axa-ont-ete-victimes-d-fuite-320647

Ces éléments de résilience opérationnelle, à savoir effectuer plusieurs sauvegardes stockées sur des sites distincts, sont intégrés dans le règlement DORA[69], de même que l'obligation pour le tiers prestataire de services informatiques tel que le fournisseur de cloud, de préciser, clairement et sans ambiguïté, dans le contrat le liant à l'institution financière, les lieux de stockage des données confiées[70].

Une sécurité des prestataires TIC à positionner au bon niveau

Le recours important aux technologies apportées par les FinTechs ainsi que les fournisseurs de solutions cloud, étend d'autant la surface d'attaque et augmente le risque cyber auquel sont exposés les acteurs du secteur financier. L'exploitation de potentielles failles de sécurité au sein de l'écosystème des acteurs du système financier entraînerait, en plus du gain financier, une perte de confiance et pourrait déclencher une crise systémique[71], déstabilisant la finance mondiale (cf. schéma ci-après).



72

[69] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA) - Article 10-5. Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

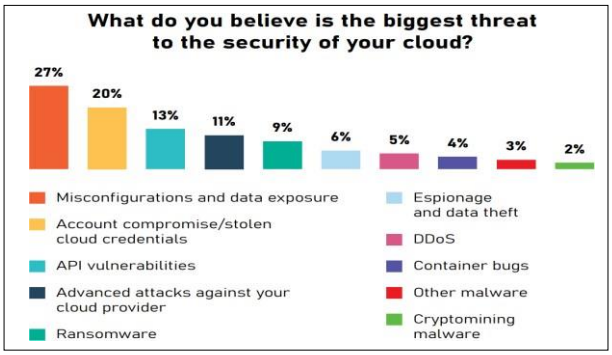
[70] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA) - Article 27-2. Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

[71] DUBOIS, Marion. Une attaque informatique géante, ce cauchemar redouté par les banques du monde entier. Ouest-France [en ligne]. 17 février 2022. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://www.ouest-france.fr/leditiondusoir/2022-02-17/une-attaque-informatique-geante-ce-cauchemar-redoute-par-les-banques-du-monde-entier-537001b6-e09d-419e-97a6-8677eac58a74

[72] BANQUE DE FRANCE. Incidents cyber et risques pour la stabilité financière. (juin 2021) [graphique]. In : BANQUE DE FRANCE. Evaluation des risques du système financier français [en ligne]. Juin 2021. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://publications.banque-france.fr/sites/default/files/medias/documents/2021_s1_ers_0.pdf

Une étude du site threatpost.com menée en 2021, révèle que les menaces les plus importantes pesant sur l'utilisation des technologies cloud sont les suivantes :

1. Le défaut de paramétrage et l'exposition des données en découlant – 27%
2. La compromission de compte, l'usurpation d'identité – 20%
3. Les vulnérabilités des API – 13%
4. Les attaques sophistiquées à l'encontre des fournisseurs de prestation cloud – 11%



[73]

Ces différentes menaces et scénarios d'attaques, sont connus de longue date et pris en considération par les grands acteurs du secteur financier que sont les banques et les assurances. Il est à noter que les médias se font plus facilement l'écho de problématiques de sécurité informatique rencontrées par les acteurs bancaires, ou les systèmes de paiement, tel que le système SWIFT[74], alors que les sociétés d'assurances et de courtages sont tout autant prises pour cibles[75].

Relevons quelques exemples choisis parmi, malheureusement, d'autres :

- L'assureur Chubb Ltd, spécialisé dans les risques informatiques, victime en 2020, d'une attaque par rançongiciel de grande ampleur. Le moyen employé fut l'obtention d'un accès non autorisé à des données clients. Les attaquants se sont concentrés, non pas sur le réseau de l'assureur, mais sur ceux de leurs fournisseurs de services indépendants76 pour y déceler et exploiter une vulnérabilité.
- L'assureur mutualiste MMA, victime d'une attaque par logiciel malveillant à l'été 2020, a vu ses activités fortement perturbées pendant plusieurs semaines77. Pour contenir la menace, des mesures radicales ont dû être prises, comme la mise à l'arrêt du système d'information de l'assureur.

Ces différentes attaques ont des conséquences difficiles à appréhender, et pour lesquelles un retour à la situation nominale « *peut varier selon l'ampleur de l'attaque. De quelques jours pour le groupe April à quelques semaines pour Assurone* [78]».

---

[73] VAAS, Lisa. What do you believe is the biggest threat to the security of your cloud ? (29 avril 2022). [graphique]. In : Threatpost.com [en ligne]. 29 avril 2022. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://threatpost.com/security-turbulence-in-the-cloud-survey-says/179437/

[74] CHEMINAT, Jacques. Après les attaques, SWIFT révise un peu sa sécurité. Silicon [en ligne]. 30 mai 2016. (Mise à jour le 28 décembre 2021). [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.silicon.fr/apres-les-attaques-swift-revise-un-peu-sa-securite-148775.html

[75] CARRERE, Marie-Caroline. Cyberattaques : l'assurance et le secteur financier premières cibles des ransomwares. L'Argus de l'assurance [en ligne]. 31 janvier 2022. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/cyber-attaques-les-services-financiers-et-l-assurance.194312?preview=11

[76] CARRERE, Marie-Caroline ; ACEDO, Sébastien. Risques d'entreprises : un assureur victime d'une cyberattaque. L'Argus de l'assurance [en ligne]. 1 avril 2020. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.argusdelassurance.com/assurance-dommages/risques-d-entreprise/risques-d-entreprises-un-assureur-victime-d-une-cyberattaque.162886

[77] POULLENNEC, Solenn. MMA : cinq questions sur une cyberattaque qui pénalise l'assureur. Les Echos [en ligne]. 27 juillet 2020. Disponible à l'adresse : https://www.lesechos.fr/finance-marches/banque-assurances/lassureur-mma-toujours-perturbe-dix-jours-apres-une-cyberattaque-1226584

[78] ACEDO, Sébastien. Cyberattaque en cours dans un grand groupe de courtage. L'Argus de l'assurance [en ligne]. 30 novembre 2021. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.argusdelassurance.com/les-distributeurs/cyberattaque-en-cours-chez-un-courtier.191747?preview=11

Forts de ces observations, pour les plus chanceux, ou à la suite d'une attaque réussie, les acteurs du monde bancaire et des assurances prennent conseil et suivent les recommandations de l'ANSSI, en faisant régulièrement des tests de résilience et d'intrusion dans le but de déceler et colmater toute vulnérabilité révélée.

Ce n'est malheureusement pas le cas d'autres acteurs de ce secteur, plus petits, qui ignorent ces bonnes pratiques. Souvent par méconnaissance, mais aussi par manque de compétences des équipes de direction de ces acteurs.

Des mesures d'accompagnement des acteurs de petite taille du secteur financier, plus particulièrement les FinTechs, ont été prises récemment :

- L'ACPR a publié en janvier 2022 une charte pour l'instruction des dossiers d'autorisation FinTech[79]
- L'ANSSI est partenaire du « Forum FinTech », qui a lieu une fois par an, pour sensibiliser ce public aux risques cyber et partager les bonnes pratiques en matière de sécurité des systèmes d'information.

[79] AUTORITE DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION. Charte pour l'introduction des dossiers d'autorisation "Fintech". Autorité de Contrôle Prudentiel et de Résolution [en ligne]. 6 janvier 2022. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://acpr.banque-france.fr/sites/default/files/media/2022/01/06/20220106_charte_fintech_fr.pdf

Quels seront les leviers à disposition du règlement Dora pour réduire les risques liés à l'informatique dans le nuage ?

Nous comprenons mieux, à présent, pourquoi la solution à ces problématiques liées aux prestataires TIC passe par le législateur.

Une fois le règlement DORA publié, des éléments de sécurité et de résilience opérationnelle seront à mettre en œuvre par tous les acteurs des services financiers en déployant, de manière proportionnée à leur structure, une gouvernance ainsi qu'un dispositif de contrôle interne spécifique, sans oublier d'y intégrer la supervision de leurs fournisseurs de prestations de services informatiques.

De plus, il imposera aux prestataires informatiques qualifiés de « critique » de mettre en place tous les moyens techniques, humains, et organisationnels afin de délivrer un service de qualité.

La DORA va permettre d'harmoniser les clauses contractuelles et d'appliquer les mêmes exigences pour tous :

- Une description claire et exhaustive des services contractualisés avec un niveau d'exigence élevé pour les fonctions critiques sous-traités.
- Le contrat doit préciser les lieux où les services et les différentes fonctions sont fournis.
- Il doit également préciser les lieux de traitements des données.
- Il préconise de préciser, dans les contrats, les règles permettant de couvrir les droits d'accès et d'audit afin de s'assurer de disposer d'accès aux sites de fourniture de la prestation et de pouvoir diligenter des audits en lien avec la prestation.
- Il préconise également de définir des garanties minimales applicables à tous les prestaires identifiés comme critiques et intervenant sur un profil d'une entité financière.

L'objectif visé précédemment est clair : mettre en œuvre de clauses contractuelles types lors des négociations entre un tiers prestataire informatiques et les entités financières concernant des services identifiés comme critiques.

Rappelons-le, la DORA introduit le fait que les tiers prestaires informatiques ont l'obligation de coopérer avec les autorités compétentes et les autorités de résolution de toutes les entités financières.

Une publication, chaque année, de la liste des tiers prestataires critiques de services informatiques au niveau de l'Union est même au programme.

Mais tout cela ne peut se réaliser sans un organe de supervision transnational…

Cadre de supervision des tiers prestataires critiques de services informatiques [80]

La DORA préconise la mise en œuvre d'un organisme de supervision qui aura pour mission principale l'identification, l'évaluation, et la supervision des tiers prestataires informatiques critiques. Ces tiers informatiques seront évalués au regard des risques pesant sur les activités et missions critiques des entités financières.

Cette surveillance prendra la forme d'un « **forum de supervision** » qui sera composé des présidents des AES et d'un représentant à haut niveau du personnel en poste de l'autorité compétente concernée de chaque État membre, ainsi que de quelques observateurs que sont les directeurs exécutifs de chaque AES et un représentant de la Commission européenne, du CERS, de la BCE et de l'ENISA.

Une fonction de « superviseur principal » viendra compléter le dispositif. Pour chaque tiers prestataire informatique, l'ABE, l'AEMF ou l'AEAPP sera désignée comme superviseur principal en fonction de la valeur des actifs et des bilans consolidés des entités financières qui utilisent les services de ce tiers.

[80] Proposition de règlement du Parlement Européen et du Conseil sur la résilience opérationnelle numérique du secteur financier (DORA) – Articles 30 à 35. Commission Européenne [en ligne]. 24 septembre 2020. [Consulté le 14 mai 2022]. Disponible à l'adresse : https://data.consilium.europa.eu/doc/document/ST-11051-2020-INIT/fr/pdf

Le superviseur principal travaillera en étroite collaboration avec le forum de supervision sous-comité de l'AES.

Pour s'assurer du bon niveau de résilience des activités critiques des entités financières, et que tous les moyens sont mis en œuvre par les prestataires informatiques critiques, le forum de supervision effectuera des **évaluations des prestataires** sur son périmètre d'intervention. Ces évaluations s'effectueront tant sur le terrain physique, que virtuel, mais également exploreront les aspects juridiques et de gouvernance entre le prestataire et son commanditaire, comme souhaité dans le cadre du règlement DORA.

La partie physique s'intéressera à la sécurité des locaux, des installations, et des centres de données afin de garantir la sûreté des systèmes que le prestataire héberge. Ce dernier devra d'ailleurs démontrer sa bonne maturité en matière de gestion des risques par l'intermédiaire de la tenue de **plans de continuité** de ses activités, mais également ceux qui ont trait au **rétablissement de l'activité**.

Des **tests et des audits** devront être effectués régulièrement, et leurs rapports conservés afin de pouvoir les produire à la demande du superviseur principal.

La gestion des incidents informatiques devra aussi être satisfaisante, tant dans la **notification rapide** de l'incident à l'entité financière, que dans la **transparence et la qualité des informations transmises**, en particulier pour les cyberattaques.

Comme indiqué plus haut, les aspects juridiques ne sont pas laissés de côté et les **clauses contractuelles** utilisées par le prestataire donnent lieu à vérifications afin de lutter contre tout abus de la part des prestataires vis-à-vis d'entités financières moins compétentes sur le terrain juridique. Il en va de même pour ce qui est des aspects techniques rendant difficile, voire impossible, tout changement de prestataires. C'est ainsi que même les **mécanismes de portabilité** des données et des applications seront vérifiés.

Ces évaluations seront effectuées chaque année, et communiquées au superviseur central.

Ce dernier pourra contraindre les prestataires à lui transmettre tout document complémentaire, y compris des documents stratégiques, afin de protéger au mieux les intérêts des institutions financières et de garantir par là-même un haut degré de résilience.

Ainsi, à l'instar des grosses entités financières, les petites Fintech disposeront par ce biais d'un moyen de protection contre de potentiels abus ou manquements de la part de ses prestataires critiques.

Fort de tout cela, le superviseur principal pourra émettre des **sanctions** pouvant aller de simples recommandations afin que les prestataires visés reviennent à un niveau de prestation conforme à l'attendu par le règlement DORA, jusqu'à des sanctions financières qui pourront être rendues publiques.

Ces sanctions prendront la forme d'astreintes dont le montant est dissuasif : 1 % du chiffre d'affaires quotidien moyen réalisé au niveau mondial par le tiers prestataire critique.

Le superviseur principal aura également des pouvoirs d'inspection. Ces inspections peuvent être effectuées par ses propres services, ou déléguées à des équipes d'auditeurs dûment mandatés. **Un refus d'inspection peut entrainer une résiliation de contrat.**

Les activités de supervision seront financées par une redevance auprès des tiers prestataires critiques de services informatiques. Le montant sera proportionnel au chiffre d'affaires du tiers prestataire critique.

Cette supervision pourrait paraître rédhibitoire pour la bonne mise en place du règlement DORA, et son acceptation par les parties prenantes. D'autant plus quand il est indiqué que ces activités de supervision seront financées par une redevance, redevance perçue auprès des prestataires critiques de services informatiques, dont le montant sera proportionnel à leur chiffre d'affaires. Il est bon de rappeler également que le texte du règlement est le fruit de nombreuses consultations et travaux, tant avec les acteurs et les autorités présentes sur la place européenne qu'avec des autorités étrangères, telles que la FED américaine, ou supranationales comme la Banque des Règlements Internationaux [81].

[81] VETRIAK, Nicolas ; CHAPPOTTEAU, Georges. DORA, la nécessité d'une gouvernance encore plus efficace pour la résilience opérationnelle. Décideurs magazine [en ligne]. 14 septembre 2021. [Consulté le 15 mai 2022]. Disponible à l'adresse : https://www.magazine-decideurs.com/news/dora-la-necessite-d-une-gouvernance-encore-plus-efficace-pour-la-resilience-operationnelle

Le règlement DORA est aussi l'opportunité de faire monter en compétence les FinTechs, tout comme les équipes d'institutions financières de plus grande envergure, sur ces sujets de résilience numérique et de la nécessaire formalisation de la cartographie de leurs actifs informatiques et numériques. En effet, de plus en plus d'incidents de fuite de données, ou de succès de cyberattaques, apparaissent ces deux dernières années et démontrent un manque de compétence des commanditaires de prestations cloud au sujet du paramétrage des solutions qu'ils sollicitent, et cela quelle que soit leur degré de complexité.

Selon une étude de McAfee[82]parue en 2019, « *90 % des personnes interrogées ont déclaré avoir rencontré des problèmes de sécurité avec le IaaS, mais seulement 26 % ont déclaré qu'elles étaient équipées pour faire face à des audits de mauvaise configuration ».*

Autre exemple plus récent, la CNIL[83], en février 2022, relève comme causes potentielles d'incident facilitant l'accès à des données, qu'elles soient sensibles ou non :

- Mauvaise configuration d'un conteneur qui, même si celui-ci est en « accès privé », peut contenir des objets qui, eux, répondront à une politique d'accès public.
- Des droits non différenciés selon le type d'utilisateur.

Le point important de la supervision des prestataires informatiques critiques est l'application des sanctions.

La menace des sanctions les oblige à mettre les moyens nécessaires à la fourniture de prestations respectant un haut niveau de sécurité.

Comment sanctionner un tiers prestataire qui ne dispose d'aucun bureau sur le territoire européen ?

Les grosses entreprises de l'informatique dans les nuages ont tendance à penser être au-dessus des lois et directives de l'UE. Elles appliquent souvent des règles qui protègent leurs intérêts et désavantage les entreprises européennes de tous secteurs d'activés. Elles mettent en place des mécanismes et des systèmes de protection qui enfreignent ou permettent de contourner l'arsenal législatif de l'UE.

Plusieurs acteurs de l'hébergement ont dénoncé les pratiques anticoncurrentielles des entreprises américaines[84]. Microsoft vend les logiciels de sa Suite Office à un prix plus élevé aux prestataires cloud européens qu'aux autres prestataires qui vendent ces mêmes services.

Dans un souci d'économies, l'entité financière sera obligée choisir Microsoft plutôt qu'un prestaire d'informatique dans les nuages européen.

A l'évidence, il apparait nécessaire de dénoncer ces pratiques qui représentent un risque pour la résilience du secteur financier notamment dans le choix des solutions cloud et des prestataires de service informatique dans les nuages. Il apparait plus important de disposer d'outils juridiques qui les obligent ou à défaut les sanctionnent.

Mais comment faire appliquer ces sanctions sur des tiers prestataires qui ne disposent pas de bureau ou de locaux sur le territoire de l'UE. Comme évoqué dans les chapitres précédents, les prestations de services dans les nuages peuvent être fournis depuis un pays tiers. Les règles de sécurité de ces pays peuvent être en contradiction avec celles préconisées par le règlement DORA. Les composants informatiques utilisés pour la prestation critique peuvent aussi être configurés, voir même fabriqués et commercialisés, avec des vulnérabilités qui exposent le système des entreprises financières ou les postes de travail de leurs collaborateurs[85].

---

[82] OSBORNE, Charlie. 99% des erreurs de configuration dans le cloud public ne sont pas signalées. ZDNet [en ligne]. 25 septembre 2019. [Consulté le 15 mai 2022]. Disponible à l'adresse : https://www.zdnet.fr/actualites/99-des-erreurs-de-configuration-dans-le-cloud-public-ne-sont-pas-signalees-39891083.htm

[83] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES. Violation du trimestre : les défauts de configuration des espaces de stockage dans le cloud public. CNIL [en ligne]. 7 février 2022. [Consulté le 16 mai 2022]. Disponible à l'adresse : https://www.cnil.fr/en/node/122148

[84] PIQUARD, Alexandre. Les géants américains du cloud accusés de fausser la concurrence. Le Monde [en ligne]. 17 mai 2022. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.lemonde.fr/economie/article/2022/05/17/les-geants-americains-du-cloud-accuses-de-fausser-la-concurrence_6126468_3234.html

[85] KALLENBORN, Gilles. Lenovo a laissé traîner des backdoor dans des millions de PC portables. 21 avril 2022. 01net [en ligne]. [Consulté le 17 mai 2022]. Disponible à l'adresse : https://www.01net.com/actualites/lenovo-a-laisse-trainer-des-backdoors-dans-des-millions-de-pc-portables-2055955.html

Et sous le couvert de la protection du secret industriel, aucune possibilité n'est donnée aux entités financières de se rendre dans les locaux nationaux des prestataires et de faire des contrôles ou des audits de sécurité.

Lorsqu'on se penche sur le cas du Royaume-Uni, depuis le Brexit, quelles sont les possibilités de sanctions si des prestataires britanniques ne respectent pas le règlement DORA ? Londres « ancienne capitale de la finance européenne » abrite plusieurs Fintechs qui fournissent des services aux entités financières européennes. Il nous faut donc nous assurer que ces solutions ne représentent pas de menaces cyber pour l'UE.

C'est en ayant tout cela en tête que, le 11 mai 2022, un accord provisoire[86] a été trouvé entre la présidence du Conseil et le Parlement européen en ce qui concerne le règlement DORA. L'accord Provisoire prévoit des moyens d'appliquer les sanctions aux prestataires critiques fournissant leurs services depuis un état tiers : ils ont l'obligation de disposer d'une filiale sur le territoire de l'UE.

[86] Communiqué de presse. Finance numérique : accord provisoire concernant le règlement sur la résilience opérationnelle numérique. Conseil de l'Union Européenne [en ligne]. 11 mai 2022. [Consulté le 16 mai 2022]. Disponible à l'adresse : https://www.consilium.europa.eu/fr/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

CHAPITRE 6

Approche pour la résilience numérique

Dans cet ultime chapitre avant de conclure, nous nous proposons de livrer quelques pistes de réflexions et conseils sur une mise en œuvre optimisée de la résilience numérique.

Définir la résilience numérique

Une entreprise résiliente est en mesure de restaurer ses services clés après une interruption imprévue importante, protégeant ainsi ses clients, ses actionnaires et l'intégrité du système financier.

La résilience opérationnelle de l'entreprise ne se limite pas à protéger uniquement la résilience des systèmes d'information, elle couvre également la gouvernance, la stratégie, les services métiers, la sécurité de l'information, la gestion du changement, l'exécution des processus et la reprise après sinistre ou d'interruption. Éviter l'interruption d'un système particulier qui supporte un service commercial contribue à la résilience opérationnelle. Mais en fin de compte, c'est le service commercial lui-même et à part entière qui doit être résilient.

La résilience opérationnelle est une approche holistique qui combine la résilience cyber, technologique et humaine, y compris la restauration après sinistre.		
Résilience humaine	Résilience cyber	Résilience technologique
La gestion des incidents	La continuité d'activité	Restauration après sinistre

Un élément clé d'une entreprise résiliente est son personnel. Un changement culturel et une sensibilisation est donc nécessaire pour faire de la résilience opérationnelle une priorité dans l'ensemble de l'organisation, et que tout le monde soit engagé et travaille à cette fin.

Cela comprend la formation du personnel pour comprendre ce qu'implique le risque opérationnel, ainsi que la communication de la direction.

Les responsabilités des risques clés et les mesures qui les atténuent doivent être attribués pour maintenir les bonnes pratiques de résilience. Les actions correctives doivent être identifiées et, surtout, menées à bien pour créer un cadre de résilience robuste.

En cas d'interruption, les entreprises du secteur financier devraient également pouvoir se recapitaliser et se restructurer en utilisant leurs propres ressources financières. En cas de défaillance catastrophique, il est impératif que les institutions de services financiers puissent continuer à fonctionner et à se rétablir pendant que des décisions sont prises sur une éventuelle restructuration ou l'arrêt d'opérations pour arrêter d'autres dommages. Un cadre de résilience opérationnelle complet est essentiel pour limiter l'impact des défaillances et assurer une résilience continue du marché financier (pas simplement une résilience au sein de l'organisation).

Quels sont les moteurs de la résilience numérique ?

Les critères de valeurs et motivation de résilience opérationnelle pour une entreprise vont au-delà des exigences réglementaires. Ils apportent la sécurité, la robustesse et confiance des systèmes financier, l'innovation, la croissance, la fidélisation et l'expérience positive des clients et consommateurs.

Améliorer la sécurité et la confiance	Prévenir, adapter, gérer, répondre, restaurer, et apprendre des incidents pour réduire l'impact des services financiers et sur leurs écosystèmes.
Minimiser les impacts sur les services	Continuer à fournir des services et des fonctions en cas d'incident et reprendre rapidement les opérations normales.
Améliorer la réputation et la fidélité des clients et consommateurs	Renforcer la réputation et la fidélité tout au long de la gestion des incidents, en maintenant la disponibilité des services et en exécutant des plans de communication solides et proactifs démontrant la réactivité.
Améliorer la rétention des employés	Les capacités de résilience opérationnelle à la pointe renforcent l'attraction pour les meilleurs talents et promouvoir la confiance et une expérience positive des employés.
Renforcer la conformité réglementaire	Répondre de manière proactive aux exigences émergentes des réglementations qui évoluent rapidement.

Les trois lignes de défense

Lors de notre entretien avec l'autorité nationale de contrôle Norvégienne, « Finanstilsynet », nous avons compris que les Autorités Européennes de Supervision (AES) auront une attention particulière sur la manière dont les entreprises de la finance opérationnaliseront leur résilience opérationnelle numérique.

Les trois lignes de défense un modèle ou processus de gestion des risques standardisé et complet.

Les trois lignes de défense est un modèle qui fournit une approche opérationnelle et de gestion des risques de cybersécurité efficace. Avoir ce modèle en place au sein de son entreprise sera clairement un avantage aux yeux des AES et des autorités nationales de contrôle.

Les principes de fonctionnement des trois lignes de défense :

- Responsabilités et pouvoirs bien définis et attribués.
- Processus de gestion des risques, rôles et responsabilités définis.
- Séparer les fonctions de conseil, d'exécution et d'assurance.

Première ligne de défense

Surveillance des contrôles ou mesures, tests, gérer les incidents et améliorer la sécurité technique et opérationnelle.

Opérationnaliser les contrôles de sécurité au travers des polices, processus et procédures.

Management opérationnel	Contrôles internes

➔ Direction opérationnelle

- Responsabilité des processus de gestion des risques au niveau opérationnel.
- Élaborer et maintenir des procédures en phase avec les risques et suivant les politiques.
- Identifie, gère, atténue et rend compte des risques et contrôle l'efficacité.
- Surveille les critères de performance ou d'efficacité liés à l'appétit et aux tolérances aux risques de l'entreprise.
- Possède et exécute les plans de continuité et de gestion des incidents.
- Suivi concernant les pertes de données.
- Gère les incidents et les problèmes.

Deuxième ligne de défense

Définir, conseiller, faciliter, surveiller et rapporter.

Risk, compliance et programme de sécurité : développer des polices et des contrôles, surveiller er faire des rapports sur l'efficacité des mesures de sécurité, promulguer des recommandations et informer sur les incidents, problèmes, risques, et des opportunités d'amélioration.

Compliance	Gestion du risque
Polices de sécurité	Qualité

➔ Direction

- Développe le cadre global de gestion des risques (politiques, normes, outils).
- Surveille l'adhésion de 1ère ligne au cadre et à la stratégie posés.
- Fournit des conseils d'expert et un soutien aux processus de contrôle de 1ère ligne (tests, surveillance).
- Analyse les résultats de l'évaluation des risques de 1ère ligne.
- Analyse les risques au travers des lignes de défense et informe la direction des menaces, problèmes et des risques.
- Calcule la tolérance au risque au niveau de l'entreprise.

Troisième ligne de défense

Tester, valider, décision, assurance, recommander des améliorations.

Supervision de la posture sécurité de l'entreprise, et décisions pour les menaces, risques et mesures à engager.

Audits internes et externes

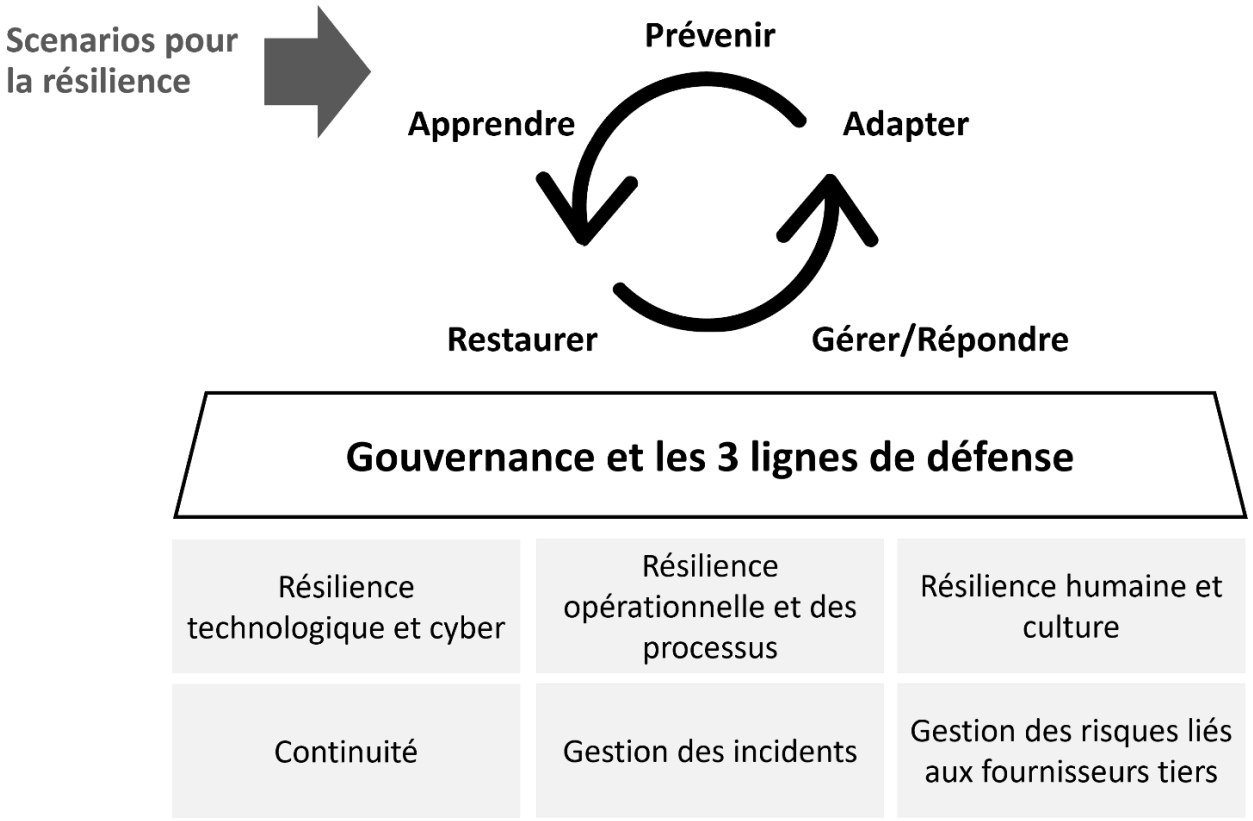
➔ Gouvernance d'entreprise, comité de direction, comité d'audit.

- Vérification indépendante de l'efficacité des normes d'entreprise et de la conformité.
- Valide le cadre global de gestion des risques.
- Performe des tests.
- Fournit l'assurance que les processus de gestion des risques en 1ère et 2ème lignes fonctionnent comme prévu.
- Identifie les opportunités d'amélioration.

Modèle de cadre de résilience opérationnelle

Il n'y a pas d'approche à « taille unique » pour une solution de résilience opérationnelle adéquate, basé sur le principe de proportionnalité et alignée sur les besoins uniques d'une entreprise.

Pour évaluer l'état actuel d'une entreprise en matière de résilience opérationnelle ou établir la stratégie/le modèle opérationnel, le cadre et ses composants ci-dessous décrivent une approche suggérée pour les bonnes pratiques liées à la résilience opérationnelle :



CONCLUSION

Tel qu'évoqué dans ce rapport, il est impératif que tous les acteurs financiers européens s'emparent de DORA pour rendre l'écosystème plus résilient et plus indépendant.

La sécurité, la collaboration et l'efficacité du secteur tout entier seront améliorées. Il faut aussi souligner le pragmatisme du régulateur dans l'approche proportionnée qui est proposée. Ce règlement établit des standards minimums, assure une équité de traitement à chacun, tout en conciliant harmonisation et flexibilité.

Pour mener à bien ces objectifs, il faut toutefois voir DORA comme un moyen et non une fin en soi.

Etayons ici notre propos : en matière financière, être souverain c'est être indépendant sur ses sources de financements et c'est avoir la faculté à édicter ses propres règles du jeu.

Dupliquer ce raisonnement au numérique pour la finance revient à être autonome technologiquement - au sens traiter avec des fournisseurs TIC de sa zone géographique - et en capacité à établir ses propres réglementations. DORA répond clairement au second point, c'est « la lettre » de ce règlement européen.

« L'esprit » en est le premier point selon nous. Sur ce plan, une volonté politique et un engagement financier de l'UE à la hauteur des enjeux seront nécessaires pour se doter de solutions susceptibles de proposer une alternative crédible aux GAFAM.

Chacun a en effet compris qu'aujourd'hui, l'Europe dépend très – trop – fortement d'une poignée d'acteurs dont la force technologique et financière est tout autant source de compétitivité que de risques.

Il faudra du temps car rien ne pourra se faire en un jour. Pour y parvenir ultimement, il reste donc encore des étapes à franchir. Le challenge sera de maintenir dans ce même temps la compétitivité de notre industrie financière.

C'est une nécessité pour assurer la stabilité à long-terme de l'Europe financière.

ANNEXES

Annexe : Communiqué de presse de l'UE sur DORA |Mai 2022

Source : https://www.consilium.europa.eu/fr/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

Conseil de l'UE / Communiqué de presse / 11 mai 2022 - 12:10

Finance numérique : accord provisoire concernant le règlement sur la résilience opérationnelle numérique

Compte tenu des risques toujours plus importants de cyberattaques, l'UE renforce la sécurité informatique des entités financières telles que les banques, les compagnies d'assurance et les entreprises d'investissement. Hier soir, la présidence du Conseil et le Parlement européen sont parvenus à un accord provisoire en ce qui concerne le **règlement sur la résilience opérationnelle numérique** (règlement DORA), qui doit permettre au secteur financier européen de maintenir des opérations résilientes en cas de perturbation opérationnelle grave.

Le règlement DORA fixe des exigences uniformes pour la sécurité des réseaux et des systèmes d'information des entreprises et des organisations actives dans le secteur financier ainsi que des tiers critiques qui leur fournissent des services liés aux technologies de l'information et de la communication (TIC), tels que des plateformes d'informatique en nuage ou des services d'analyse de données. Le règlement DORA crée un cadre réglementaire sur la résilience opérationnelle numérique en vertu duquel **toutes les entreprises doivent veiller à pouvoir résister à tous les types de perturbations et de menaces liées aux TIC, y répondre et s'en remettre**. Ces exigences sont homogènes dans tous les États membres de l'UE. L'objectif principal est de prévenir et d'atténuer les cybermenaces.

En vertu de l'accord provisoire, la nouvelle réglementation constituera **un cadre très solide qui favorisera la sécurité informatique du secteur financier**. Les efforts demandés aux entités financières seront proportionnels aux risques potentiels.

Presque toutes les entités financières seront soumises à la nouvelle réglementation. Au titre de l'accord provisoire, les **auditeurs** ne seront pas soumis au règlement DORA, mais feront partie d'un futur réexamen du règlement, dans le cadre duquel une éventuelle révision des règles pourrait être envisagée.

Les prestataires critiques établis dans un pays tiers qui fournissent des services informatiques aux entités financières dans l'UE seront tenus d'établir une filiale dans l'UE, afin que la supervision puisse être correctement mise en œuvre.

En ce qui concerne le cadre de **supervision**, les colégislateurs sont convenus d'opter pour un réseau de supervision commun supplémentaire, qui renforcera la coordination entre les autorités européennes de surveillance sur ce sujet transsectoriel.

En vertu de l'accord provisoire, des **tests de pénétration** seront effectués en mode fonctionnel et il sera possible d'inclure les autorités de plusieurs États membres dans les procédures de test. Le recours à des auditeurs internes ne sera possible que dans un certain nombre de circonstances strictement limitées, sous réserve de conditions de sauvegarde.

En ce qui concerne l'interaction du règlement DORA avec la **directive sur la sécurité des réseaux et des systèmes d'information (directive SRI)**, en vertu de l'accord provisoire, les entités financières sauront très clairement les différentes règles qu'elles doivent respecter en matière de résilience opérationnelle numérique, en particulier pour les entités financières détenant plusieurs agréments et opérant sur différents marchés au sein de l'UE.

La directive SRI continue de s'appliquer. Le règlement DORA s'appuie sur la directive SRI et supprime d'éventuels chevauchements au travers d'une exemption dite de lex specialis.

L'accord provisoire conclu hier soir doit être approuvé par le Conseil et le Parlement européen avant de faire l'objet de la procédure d'adoption formelle.

Une fois que la proposition de règlement aura été formellement adoptée, elle sera intégrée à la législation de chaque État membre de l'UE. Les autorités européennes de surveillance (AES) concernées, telles que l'Autorité bancaire européenne (ABE), l'Autorité européenne des marchés financiers (AEMF) et l'Autorité européenne des assurances et des pensions professionnelles (AEAPP), élaboreront ensuite des normes techniques que tous les établissements de services financiers devront respecter, qu'ils soient chargés d'opérations bancaires, de produits d'assurance ou de la gestion d'actifs. Les autorités nationales compétentes seront chargées de la surveillance de la conformité et feront respecter le règlement en tant que de besoin.

Contexte

La Commission a présenté la proposition de règlement DORA le 24 septembre 2020. Celle-ci s'inscrit dans le cadre plus large du train de mesures sur la finance numérique, qui vise à mettre au point une approche européenne favorisant le développement technologique et assurant la stabilité financière et la protection des consommateurs. Outre la proposition de règlement DORA, ce train de mesures contient une stratégie en matière de finance numérique, une proposition sur les marchés de crypto-actifs (MiCA) et une proposition sur la technologie des registres distribués (DLT).

Il comble une lacune dans la législation existante de l'UE en permettant de s'assurer que le cadre juridique actuel ne fasse pas obstacle à l'utilisation de nouveaux instruments financiers numériques. Dans le même temps, il s'agit de veiller à ce que ces nouvelles technologies et nouveaux produits entrent dans le champ d'application de la réglementation financière et des dispositifs de gestion des risques opérationnels des entreprises actives au sein de l'UE. Le paquet vise donc à soutenir l'innovation et l'adoption de nouvelles technologies financières tout en assurant un niveau approprié de protection des consommateurs et des investisseurs.

Le Conseil a adopté son mandat de négociation sur le règlement DORA le 24 novembre 2021. Les trilogues entre les colégislateurs ont débuté le 25 janvier 2022 et se sont terminés par l'accord provisoire intervenu hier.

- Ensemble de mesures sur la finance numérique: le Conseil parvient à un accord sur le MiCA (règlement sur les marchés de crypto-actifs) et le DORA (règlement sur la résilience opérationnelle numérique du secteur financier) (communiqué de presse, 24 novembre 2021)
- Proposition de règlement de la Commission sur la résilience opérationnelle numérique
- Finance numérique (informations générales)

Annexe Juridique : éclairage législatif en Europe

Extrait d'une correspondance avec Olivier de Maison Rouge, sur les différents textes législatifs européens - mars 2022 :

L'UE est en mesure d'adopter 2 types de règlementation :

1**/ le règlement**, qui est un texte qui n'est pas soumis à transposition, d'application directe (sans passer par la case « transposition »), et qui touche un secteur économique concerné (et non pas tous les citoyens).

2/ **la directive**, qui est un texte qui affecte tous les citoyens de l'UE, dans les domaines de compétence d'attribution de l'UE, et qui oblige, une fois adoptée, les états membres à les intégrer à leur législation. Sans être d'application directe, l'UE laisse un délai (la plupart du temps 24 mois) pour transposer. Certains pays ont cependant fait le choix d'appliquer directement les règlements dans leur législation, sans processus de transposition, contrairement à la France dont les directives font l'objet d'une loi de transposition.

Annexe : focus cyber risque et finance … un secteur très touché par les ransomwares

Source : Rapport 2021 Trellix cité par la revue en ligne Silicon

Site https://www.silicon.fr, consulté le 15 avril 2022

L'entreprise de cybersécurité Trellix a livré son rapport sur les menaces avancées de sécurité au troisième trimestre 2021. REvil/Sodinokibi, BlackMatter, LockBit 2.0…

« Au troisième trimestre de 2021, les groupes de ransomwares (rançongiciels) de haut niveau ont disparu, sont réapparus, se sont réinventés et ont même tenté de changer de nom, tout en restant pertinents et répandus en tant que menace diffuse et potentiellement dévastatrice contre un spectre croissant de secteurs », soulignent les auteurs du rapport Trellix.

Selon l'entreprise de cybersécurité, les services bancaires et financiers ont été la cible la plus courante, à l'échelle mondiale, des attaques de ransomwares au cours de la période de référence, représentant 22% des attaques détectées.

Les services publics et le commerce de détail (retail) arrivent ensuite, agrégeant respectivement 20% et 16% des attaques. Les assauts contre ces trois secteurs combinés ont ainsi représenté 58% de toutes les attaques de ransomwares détectées entre juillet et septembre 2021. Les autres secteurs d'activité qui ont été particulièrement visés sur la période sont l'éducation (9% des attaques), les gouvernements centraux (8%) et l'industrie (4,3%).

Annexe : trois exemples de cyberattaques dans le monde financier début 2021

Janvier 2021 : la **banque centrale de Nouvelle-Zélande** a été victime d'un piratage via le système de partage de fichiers tiers Accellion, la même plate-forme qui a causé la violation de Flagstar Bank.

Dave Parry, professeur d'informatique à l'université d'Auckland, a déclaré à Radio New Zealand en janvier que cette violation était probablement l'œuvre d'un État-nation plutôt que d'un réseau criminel.

Mars 2021 : la Flagstar **Bank, basée dans le Michigan**, a été victime d'une violation de données causée par une vulnérabilité de son service de partage de fichiers Accellion service de Cloud californien.

Selon Vice, les criminels ont publié les données personnelles des employés de la banque en ligne via le dark web après la violation.

Mars 2021 : une cyberattaque a contraint **l'Autorité bancaire européenne (ABE)** à fermer l'ensemble de son système de messagerie. L'attaque faisait partie d'un assaut généralisé contre les serveurs Microsoft Exchange des organisations.

Annexe : Cyberattaque de la Banque de la Valette

Illustration des conséquences d'une cyber attaque pour une banque majeure à Malte (2019)

Bank of Valletta downgraded by S&P over cyberattack and international litigation

Source disponible sur Bank of Valletta downgraded by S&P over cyberattack and international litigation (maltatoday.com.mt) – Article du 31 Juillet 2019 | Auteur: Matthew Vella

Standard & Poor's a abaissé la note de crédit de Banque de la Valette de BBB-/A-3 à BBB/A-2, en raison d'observations réglementaires et d'une cyberattaque qui ont accru les doutes quant à la robustesse de la gestion du risque opérationnel de BOV. Ces événements se sont ajoutés aux risques de litiges importants auxquels la banque est exposée dans les affaires Deiulemar, l'agence suédoise des pensions et le fonds immobilier La Valette.

« Tous ces événements entraînent une incertitude quant à l'efficacité de la surveillance des risques de BOV et à la capacité de la direction à contrôler les complexités du modèle économique de la banque, que nous considérons comme relativement plus élevé que les banques de taille similaire », a déclaré S&P.

S&P a déclaré que la Banque centrale européenne et l'Autorité maltaise des services financiers (MFSA) avaient encouragé la banque à prendre certaines mesures pour renforcer ses contrôles internes et sa surveillance des risques, notamment en ce qui concerne la diligence raisonnable et les processus d'intégration de nouveaux clients.

En février, BOV a été victime d'une cyberattaque qui l'a contraint à fermer son accès Internet, ainsi que ses agences et distributeurs automatiques, pendant plusieurs heures.

"La cyber-attaque remet en question la conformité de l'efficacité des outils informatiques et de surveillance de la conformité de la banque avec les meilleures pratiques", a déclaré S&P.

Suite aux recommandations des régulateurs, BOV a déclaré qu'il s'efforçait de renforcer ses procédures de contrôle interne et d'adapter son modèle commercial pour se concentrer davantage sur ses opérations nationales et ses activités commerciales traditionnelles.

« Cependant, comme c'est généralement le cas dans de telles situations, nous pensons qu'il faudra du temps et un engagement fort de la part de la haute direction de BOV pour mettre en œuvre ces changements et véritablement transformer sa gouvernance des risques avant de produire des résultats significatifs.

"En outre, les événements négatifs susmentionnés spécifiques à BOV, ainsi qu'aux institutions financières maltaises en général, peuvent avoir accru le risque de réputation pour la banque. Par exemple, la banque correspondante en dollars américains de BOV a annoncé en juin qu'elle mettrait fin à sa relation de correspondance avec BOV en décembre. « Nous prévoyons que le plan de transformation que la banque met en œuvre pour relever les défis opérationnels entraînera probablement une augmentation significative de ses charges d'exploitation.

Cela exercera une pression sur sa rentabilité et, par conséquent, sur sa génération de capital interne. En outre, nous prévoyons que certains litiges encore en cours contre la banque pourraient nécessiter des provisions supplémentaires.

Cependant, il reste un risque de baisse important pour la projection de S&P en raison de l'exposition aux litiges en cours. Plus précisément, BOV a affecté 75 millions d'euros aux provisions pour litiges de précaution au premier semestre 2018. Le principal litige a débuté en avril 2015. Il s'agissait d'actions détenues dans une fiducie à BOV par les propriétaires de la compagnie maritime effondrée Deiulemar, qui a fait faillite en 2012. En 2018, la justice italienne a demandé à BOV de saisir un mandat conservatoire de 363 millions d'euros. C'est important par rapport aux capitaux propres totaux de BOV qui s'élèvent à 994 millions d'euros.

BOV prévoit désormais d'émettre un instrument de catégorie 1 supplémentaire de 150 millions d'euros au cours du second semestre 2019, ciblant les investisseurs institutionnels. Cela pourrait amortir le fardeau potentiel sur la capitalisation de la banque que les litiges et autres défis pourraient générer. Cependant, la banque a déjà retardé son émission.

S&P a cependant déclaré ne voir aucune détérioration immédiate de la franchise de la banque suite au mandat de précaution du tribunal, à la cyber-attaque et aux rapports réglementaires.

« La position dominante de BOV sur le marché, avec une part de marché de 46 % dans les prêts et les dépôts, et une solide franchise de vente au détail continuent de soutenir les notations de la banque, à notre avis. En outre, la participation de 25,23 % du gouvernement maltais devrait renforcer la confiance des déposants dans BOV et contribuer à sa stabilité. »

S&P a déclaré que la possibilité d'une mise à niveau était peu probable à ce stade car il faudra du temps pour que les mesures correctives de la banque sur ses contrôles internes et sa gestion des risques opérationnels prouvent leur efficacité. Les procès sur les affaires contentieuses pendantes pourraient également durer plusieurs années avant de se conclure.

Annexe : Illustration du risque cyber sous l'angle américain

Source : Bank of America CTO: Cyberattacks on banks "surged" during pandemic Site: https://www.fintechfutures.com/us/fintechfutures.com)

Auteur Ruby Hinchliffe – article du 05 Mai 2021

Cathy Bessant, directrice des opérations et de la technologie de Bank of America, a déclaré que la banque avait augmenté ses dépenses en cyberdéfense ces dernières années pour atteindre environ 1 milliard de dollars par an.

L'unité mondiale de sécurité de l'information de la banque consacre la majorité de ce budget au personnel et à la technologie. Cathy Bessant, directrice des opérations et de la technologie de Bank of America. Bessant a ajouté lundi dans un briefing, comme le rapporte Bloomberg, que les cyberattaques ont considérablement augmenté pendant la pandémie. « Les criminels sont par définition très rusés, très entreprenants - et les périodes de stress créent des opportunités », explique Bessant. « Il ne fait aucun doute que le taux et le rythme des attaques, ainsi que la nature des attaques, ont considérablement augmenté. »

La banque est ainsi constamment en garde contre un « scénario Armageddon », selon son responsable technologique.

Les dépenses liées au cyber ont bondi de 15 % en 2020, selon une enquête Deloitte & Touche.

Ce pourcentage équivaut à environ 1 milliard de dollars pour chacune des plus grandes banques américaines. Ce qui souligne que Bank of America n'est qu'une des nombreuses banques américaines qui renforcent leurs cyberdéfenses.

Deloitte estime également que 64 % des responsables financiers s'attendent à ce que les budgets de cybersécurité continuent d'augmenter.

Le cyber-risque bat la crise financière

En avril 2021, le président de la Réserve fédérale, Jerome Powell, a déclaré à CBS News qu'il était plus préoccupé par le cyber-risque que par un autre crash financier. Powell a déclaré qu'« un cyber-événement » pourrait avoir « un rôle important » à jouer dans le système financier « en train de s'arrêter ». Mais que le risque d'un effondrement financier de type 2008 est « très, très faible ». "Je dirais que le risque sur lequel nous gardons le plus l'œil est le cyber-risque", a déclaré Powell à CBS News.

Il a déclaré que la banque centrale américaine la surveillait donc très attentivement et investissait massivement dans la prévention des violations majeures.

« C'est vraiment là que se situe le risque, je dirais maintenant, plutôt que quelque chose qui ressemblait à la crise financière mondiale. »

Annexe : ” The Sheltered Harbor initiative (2019)”

Source : Sheltered Harbor - Home | Disponible à l’adresse https://shelteredharbor.org/index.php/about

Consulté le 14 mars 2022

Contexte. Les cybermenaces émergentes sont imprévisibles. Elles évoluent d'une motivation principalement financière (accès aux données des clients) à des motivations politiques (déstabilisation du système financier), parfois par des acteurs étatiques très sophistiqués. La cybersécurité empêche les dirigeants et les administrateurs des banques de dormir la nuit, 84 % d'entre eux la classant dans le top 3 des risques auxquels leur banque est confrontée, selon la dernière enquête de Bank Director.

McAfee estime que la cybercriminalité coûte actuellement à l'économie mondiale 600 milliards de dollars par an, en hausse de 34 % au cours des trois dernières années. Le secteur financier est la première cible. Les institutions individuelles ne peuvent empêcher toutes les attaques. Pourtant, dans le monde connecté d'aujourd'hui, une attaque paralysante contre ne serait-ce qu'une seule institution qui empêche les clients d'accéder à leurs comptes pourrait provoquer une panique qui infecte l'ensemble du système financier.

Le secteur américain des services financiers a mis au point une solution pour protéger les clients, les institutions et la confiance du public dans le système financier lui-même en cas de perturbation aussi dévastatrice.

Sheltered Harbor est la norme à but non lucratif dirigée par l'industrie pour la protection et la récupération des données des comptes clients dans le cas où un événement catastrophique comme une cyberattaque causerait des systèmes critiques, y compris des sauvegardes. Sheltered Harbor est actuellement ouvert aux banques américaines, aux coopératives de crédit, aux courtiers, aux gestionnaires d'actifs et aux fournisseurs de services de toutes tailles, et a déjà une masse critique d'adoption par l'industrie.

Depuis janvier 2019, les participants détiennent 70 % des comptes de dépôt américains et 55 % des actifs des clients de courtage de détail aux États-Unis.

Comment ça fonctionne. **Il y a trois piliers :**

1. **Stockage des données**. Les institutions sauvegardent chaque nuit les données critiques des comptes clients dans le format standard Sheltered Harbor, soit en gérant leur propre coffre-fort, soit en utilisant leur fournisseur de services. Le coffre-fort de données est crypté, immuable et complètement séparé de l'infrastructure de l'institution, y compris toutes les sauvegardes.

2. **Planification de la résilience**. Les institutions préparent les processus commerciaux et techniques et les principales dispositions décisionnelles à activer en cas d'événement Sheltered Harbour ; où toutes les autres options de restauration des systèmes critiques - y compris les sauvegardes - ont échoué. Ils désignent également un partenaire de restauration afin que si le plan de résilience Sheltered Harbor est activé, le partenaire puisse récupérer les données du coffre-fort pour restaurer l'accès aux fonds des clients le plus rapidement possible pendant que l'institution s'efforce de se remettre en ligne.

3. **Attestation**. Il s'agit d'un élément essentiel de l'initiative Sheltered Harbour. Les participants adoptent un ensemble solide de contrôles internes prescrits et effectuent des audits professionnels pour assurer la conformité.

Après avoir satisfait aux exigences de Data Vaulting, l'institution se verra attribuer un sceau de certification, informant le public que les données des comptes clients sont protégées.

Cette initiative est née d'une série de simulations de cybersécurité public-privé menées par le Département du Trésor américain, connues sous le nom de Hamilton Series. La conclusion des exercices était que le secteur des services financiers - et l'économie américaine - pourraient être vulnérables si une attaque désactivant une institution individuelle entraînait une panique à grande échelle chez les clients. Ainsi, les principales institutions financières, les groupes commerciaux de l'industrie et les grands fournisseurs de services ont mis en place l'initiative Sheltered Harbor pour créer une norme de résilience à l'échelle du système pour le scénario dans lequel une institution financière perd ses capacités opérationnelles. Structure Sheltered Harbour est une LLC à but non lucratif, structurée comme une filiale de FS-ISAC (Financial Services Information Sharing and Analysis Center) avec un conseil d'administration indépendant. Il dispose d'une équipe de base dont les principales fonctions sont d'établir la norme, de promouvoir l'adoption dans l'industrie, de soutenir la mise en œuvre et d'assurer le respect.

Écosystème Depuis le début, Sheltered Harbour a bénéficié du soutien critique de l'industrie de la part d'institutions financières, de chambres de compensation, de processeurs principaux et d'associations professionnelles de l'industrie.

Plus d'une centaine d'experts en la matière ont conçu la solution en collaboration. L'initiative continue de soutenir plusieurs flux de travail, mobilisant jusqu'à deux cents experts en la matière et professionnels de l'industrie à tout moment, qui travaillent ensemble pour garantir que le modèle Sheltered Harbor est la référence en matière de résilience du secteur. www.ShelteredHarbor.org 4 Sheltered Harbor s'associe à des sociétés de conseil et d'assurance mondiales et nationales de premier plan pour aider à la mise en œuvre des participants. Le nombre et la portée de ces partenariats continuent d'augmenter au fur et à mesure que l'initiative mûrit. Leadership Sheltered Harbor est régi par son conseil d'administration, composé d'institutions financières de toutes tailles, de chambres de compensation, de processeurs principaux et d'associations professionnelles de l'industrie.

Renseignements sur la participation et questions : Joan Meltzer 347-797-1297 info@shelteredharbor.org

Annexe : Echange avec Stig Ulstein, Conseiller paiements et TI à « Finanstilsynet » (« ACPR » Norvégien)

Dans le cadre des travaux sur DORA, nous avions été amenés à interroger différents acteurs européens connectés à la DORA, entre autres ici, Stig dont voici la synthèse :

Dans notre méthodologie, nous avons aussi consulte des publications belge et néerlandaise consacrées à DORA. Citons ici celle de et celles de DIGITALEUROPE www.digitaleurope.org représentant une centaine d'industries numériques en européenne et la « Dutch Payments Association » www.betaalvereniging.nl/en .

En France nous avions également consulté l'agence numérique AFNUM, laquelle nous avait informé n'avoir pas travaillé sur le sujet.

GLOSSAIRE

ABE
Autorité Bancaire Européenne

ACPR
Autorité de Contrôle Prudentiel et de Résolution
Adossée à la Banque de France, l'Autorité de contrôle prudentiel et de résolution (ACPR) est en charge de l'agrément et de la surveillance des établissements bancaires, d'assurance et de leurs intermédiaires, dans l'intérêt de leurs clientèles et de la préservation de la stabilité du système financier.

AEMF
Autorité Européenne des Marchés Financiers

AES
Autorités Européennes de Surveillance

AISP
Account Information Service Provider
En français : prestataire de services d'informations de compte.

ANSSI
Agence Nationale de la Sécurité des Systèmes d'Information

API
Application Programming Interface
En français : interface de programmation d'application. Il s'agit d'une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités.

BAFIN
Autorité Fédérale des Services Financiers en Allemagne

BCE
Banque Centrale Européenne

BDF
Banque de France

BoE
Bank of England

BSI
Bundesamt für Sicherheit in der Informationstechnik
Équivalent de l'ANSSI allemande.

CERS
Comité Européen de Risques Stratégiques

CISA
Cybersecurity and Infrastructure Security Agency
Équivalent de l'ANSSI américaine.

CNIL
Commission Nationale de l'Informatique et des Libertés

DSP2
Seconde Directive sur les Services de Paiement
Entrée en vigueur le 13 janvier 2018, cette directive vise à encadrer la prestation de service de paiements et renforcer la sécurité des paiements à l'échelle européenne.

DMA
Digital Market Act

DORA
Digital Operational Resilience Act

EBA
European Banking Authority

ENISA
Agence de l'Union Européenne pour la Cybersécurité

EIOPA
European Insurance and Occupational Pensions Authority

FCA
Financial Conduct Authority (Royaume-Uni)

GAFAM
Google, Amazon, Facebook, Apple, Microsoft

HKMA
Hong Kong Monetary Authority

IaaS
Infrastructure as a Service

MiCA
Markets in Crypto-assets Regulation

MDBC
Monnaie Digitale de Banque Centrale

MOSAIC
More Security with Artificial Intelligence
Solution interne au Groupe Société Générale permettant de lutter contre la fraude au sein des systèmes de paiements.

NCSC
National Cyber Security Centre
Équivalent ANSSI au Royaume-Uni

NIS
Network and Information System Security

OSE
Opérateurs Services Essentiels

OIV
Opérateurs Importance Vitale

PaaS
Platform as a Service

PRA
Prudential Regulation Authority, part of the BoE

RGPD
Règlement Général sur la Protection des Données

SaaS
Software as a Service

SEAE
Service Européen pour l'Action Extérieure

SEC
Securities and Exchange Commission

SRI
Directive sur la Sécurité des réseaux et des Systèmes d'Information
Entrée en vigueur en 2016 et renforcée en 2020 SRI 2 pour tenir compte de la crise Covid

TIC
Technologies de l'Information et de la Communication

TIBER
Threat Intelligence-Based Ethical Red Teaming

Web 3
Web 3 est une génération du web exploitant la technologie des chaînes de blocs (blockchain), alors que le Web 2.0 est le web « social ».
Bien qu'impliquant une critique du Web 2.0 pour sa centralisation des données des utilisateurs et de l'oligopole des plateformes, le Web 3 embryonnaire tel qu'il existe en 2022 n'est pas à l'abri de la centralisation et consolidation de ces quelques acteurs en oligopole (source Wikipedia).

L’équipe

Matthieu Bondy
Analyste risques opérationnels
Société Générale

Frederic Caubert
Expert Bancaire et Financier

Abdelhalim Elmouadan
Directeur Sécurité IT
Groupe EssilorLuxottica

Pierre Hervé Gbingbehi
Responsable Sécurité Informatique
Mutex

Patrick Tahiri
Consultant en Cybersécurité
Accenture

Rendu le 22 mai 2022