CLUBBANQUE

REVUE BANQUE

« CLUB BANQUE » DU 17 NOVEMBRE 2022

Cyber-résilience opérationnelle

Introduction

Niamkey ACKABLE, Deputy Core Practice Leader Security & Resiliency, Kyndryl

Règlement sur la résilience opérationnelle numérique du secteur financier

Ruxandra-Gabriela ADAM, Legal and Policy-Officer, DG FISMA, Commission européenne

Mise en œuvre de DORA : principaux enjeux pour les banques et les superviseurs

Emmanuel ROCHER, Directeur des Affaires internationales au sein de l'ACPR

Table ronde

Ruxandra-Gabriela ADAM, Legal and policy-Supervisor, DG FISMA, Commission européenne

Emmanuel ROCHER, Directeur des Affaires internationales au sein de l'ACPR

Romain ELIOT, CISO Groupe adjoint, Responsable des Relations Institutionnelles et Analyses Stratégiques, Groupe Crédit Agricole

Christophe LEBLANC, Head of the group operational Resilience Mission, Société Générale

Table ronde

Questions / réponses

INTRODUCTION

Niamkey ACKABLE, Deputy Core Practice Leader Security & Resiliency, Kyndryl

Bonsoir à tous. J'ai aujourd'hui la chance et l'honneur de présider cette table ronde consacrée à la cyber-résilience opérationnelle.

En quelques mots, Kyndryl est née de la séparation des activités de l'IBM et existe désormais depuis un an. En tant que start-up de grande échelle, nous employons plus de 90 personnes et notre rayonnement est international. Historiquement, nous traitons les sujets liés à l'infogérance, mais nous développons également des services de conseil et d'implémentation autour de différents volets technologiques tels que le cloud network, la sécurité et la résilience.

Je laisse à présent les panélistes qui m'accompagnent se présenter.

Ruxandra-Gabriela ADAM

Bonsoir. Je travaille à la Commission européenne à la direction FISMA, laquelle s'occupe de la stabilité financière. Au sein de l'unité Finance Digitale, je m'occupe notamment du règlement DORA (Digital Operational Resilience Act).

Emmanuel ROCHER

Bonsoir à tous. Je suis directeur des affaires internationales de l'ACPR. Cette direction est chargée de participer aux négociations des textes internationaux et européens sur les sujets qui couvrent à la fois la banque et l'assurance, mais également la cyber-résilience. Nous travaillons notamment à la transposition de Bâle 3 et à la finalisation du texte de la Solvabilité 2 pour l'assurance.

Christophe LEBLANC

Bonsoir. Je suis membre du Comité de direction du groupe Société Générale. Je suis actuellement responsable de plusieurs missions stratégiques, parmi lesquelles figure notamment la mission Résilience Opérationnelle du Groupe. Auparavant, j'ai exercé au sein du groupe la fonction de directeur des Ressources et de la Transformation numérique. Je suis donc familier des sujets informatiques.

Romain ELIOT

Bonsoir. Au sein du groupe Crédit Agricole, j'occupe le poste d'adjoint Responsable de la Sécurité des Systèmes d'information du Groupe. Je m'occupe notamment des relations institutionnelles (superviseurs, régulateurs, etc.) dans le domaine des risques informatiques. Je gère les *reportings* adressés aux superviseurs, mais je travaille également sur la politique de sécurité en interne et sur d'autres éléments stratégiques pour le groupe.

Niamkey ACKABLE

Dans un premier temps, nous aborderons la cyber-résilience opérationnelle sous un angle réglementaire en compagnie de Ruxandra-Gabriela ADAM. Elle nous présentera notamment le périmètre et les conditions d'application de la réglementation DORA.

Dans un second temps, Emmanuel ROCHER, en tant que superviseur français, nous exposera son point de vue sur DORA.

Dans un troisième temps, nous discuterons de la résilience sous un aspect plus pratique. Nous nous interrogerons sur les moyens et les outils dont les banques et les institutions financières disposent pour être conformes à DORA et lutter contre les événements disruptifs.

RÈGLEMENT SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DU SECTEUR FINANCIER

Ruxandra-Gabriela ADAM, Legal and Policy Officer, DG FISMA, Commission européenne

La procédure d'adoption du règlement DORA est en cours. La semaine précédente, le texte a été adopté par le Parlement européen. Les votes au COREPER et au Conseil sont attendus les 23 et 28 novembre, respectivement. Le texte devrait ensuite être signé par les présidents du Parlement et du Conseil en décembre. Enfin, nous estimons que le texte pourra être publié en décembre entrera en vigueur l'année prochaine et s'appliquera en 2025.

Je résumerai d'abord les quelques éléments de contexte inhérents à ce projet de résilience numérique. C'est conjointement à l'avis technique rendu en 2019 que nous avons dans un premier temps pris conscience de la dépendance de l'ensemble du système financier aux outils numériques. Les institutions européennes n'avaient jusqu'alors pas accordé d'attention ciblée sur ces aspects de résilience numérique. De plus, sous un rapport réglementaire, il existait nombre de disparités entre les acteurs du système financier. Au niveau international, des discussions se sont tenues, notamment avec le comité de Bâle. Nous avons également pris en considération le risque posé par les tiers fournisseurs.

Ces divers éléments ont entraîné des réflexions sur la résilience. Dans le cadre de nos travaux, nous avons adopté une approche transversale et avons souhaité élaborer un règlement qui regarde la plage d'opérateurs financiers réglementés au niveau européen. En conséquence, le champ d'application de DORA s'avère large, car les acteurs financiers sont interconnectés. Il n'est donc pas possible de concentrer des exigences en matière de risque sur seulement une partie du système financier. La majorité des acteurs concernés est toutefois composée d'entités financières soumises à la réglementation européenne. DORA vise ainsi à harmoniser ces règles communes.

Certains acteurs font cependant l'objet d'exemption. C'est notamment le cas de certains acteurs du domaine des fonds d'investissement ou de l'assurance, lesquels se situent sous le seuil des Directives AIFMD et Solvency. D'autres encore sont soumis à des règles allégées dans le régime de base prudentiel. DORA reflète ainsi ces différentes spécificités.

La gestion des risques informatiques constitue le cœur de DORA. Certains établissements de crédit très importants ont déjà mis en place de telles règles. DORA a toutefois pour objet de consolider et d'harmoniser le système de gestion des risques. Par ailleurs, DORA ne constitue pas en soi un règlement particulièrement prescriptif.

En effet, les sociétés ont des tailles différentes et ne disposent pas des mêmes ressources.

De plus, le risque informatique ne concerne pas uniquement les équipes IT, mais également la gouvernance de la société. Il est donc nécessaire que les organes de direction s'y investissent.

Il s'ensuit que DORA oblige les entités financières à notifier aux autorités compétentes seulement les incidents majeurs. Chacun doit mettre en place un système de gestion des incidents (système d'alerte, notifications, etc.). Désormais, les autorités NIS recevront les notifications par l'intermédiaire des autorités compétentes, et parfois directement des entités financières.

En ce qui concerne les tests de résilience opérationnelle numérique, des tests de base seront effectués par chacun. Pour certaines petites entreprises, nous avons essayé d'aménager les conditions en étudiant leurs possibilités de ressources. En revanche, des tests avancés, intitulés tests de pénétration fondés sur la menace (TPFM) seront seulement réalisés par les entités financières d'une taille importante dont les critères de désignation sont définis dans DORA. Ces tests sont essentiels, car ils permettent de simuler une situation proche du réel. Enfin, les entités financières auront également la possibilité de participer à des tests groupés.

Enfin, DORA sensibilise également aux risques posés par les tiers. Pour la première fois, des accords contractuels permettront aux entités financières d'engager les prestataires tiers à respecter les exigences de DORA. Par ailleurs, le règlement introduit un cadre de supervision pour les prestataires critiques de services informatiques.

MISE EN ŒUVRE DORA : PRINCIPAUX ENJEUX POUR LES BANQUES ET LES SUPERVISEURS

Emmanuel ROCHER, Directeur des Affaires internationales au sein de l'ACPR

J'insisterai davantage sur les enjeux que nous percevons à l'ACPR pour la place et pour le superviseur.

D'un point de vue thématique, DORA s'inscrit dans le prisme du renforcement de la résilience opérationnelle des entités financières. Ce prisme se concentre véritablement sur la sécurité des systèmes d'information. En revanche, le spectre des entités assujetties à ce cadre est très large. Près d'une vingtaine de catégories d'établissements et d'entités seront concernées.

L'ACPR a d'emblée jugé le cadre de DORA comme bienvenu et l'a soutenu dès son lancement. En effet, il nous semple que DORA constitue un texte législatif majeur en matière de résilience opérationnelle des établissements, et ce, pour plusieurs raisons.

Premièrement, DORA permettra d'harmoniser par le haut un certain nombre de règles et de pratiques préexistantes à certains pays et entités et s'appliquera à un vaste panorama d'établissements financiers au sein de l'Union européenne.

Deuxièmement, DORA correspond à une réforme de simplification appropriée. Les grands établissements internationaux étaient déjà soumis à des exigences, mais devaient se confronter à une grande variété de cadres. DORA instaurera un cadre unique. Il s'agit également d'une réforme de simplification pour les plus petits établissements qui disposeront d'un texte unique de référence, lequel permettra de construire leurs relations contractuelles avec les prestataires.

Troisièmement, ce texte aura pour la place financière française un impact dans sa mise en œuvre qui sera mesuré. Nombre d'établissements appliquaient déjà certaines exigences fixées aux niveaux national et européen. Ainsi, DORA s'inscrit dans la continuité de ces exigences.

En ce qui concerne la supervision du risque cyber, DORA ne constitue pas une nouveauté. En effet, nous avons dès 2015 inscrit le risque cyber parmi les priorités du contrôle que nous exerçons à l'égard d'un certain nombre d'établissements en France.

DORA vise la résilience opérationnelle et ne se cantonne donc pas à examiner le risque opérationnel. Son approche est davantage qualitative, et ce, en lien avec la gouvernance.

De plus, DORA reflète pleinement la priorité donnée à la prévention et à l'encadrement du risque cyber, aussi bien pour le superviseur que pour le législateur. Mais elle reflète également cette priorité vécue par les établissements eux-mêmes dans leur analyse des risques. C'est pourquoi DORA a prévu de fixer un certain nombre d'outils de gouvernance dédiés. Le *reporting* des incidents constitue également un élément essentiel.

Les colégislateurs européens ont par l'intermédiaire de ce nouveau cadre essayé de développer une relation de confiance avec les autorités et les établissements. DORA inclut ainsi des éléments relatifs à la participation volontaire aux dispositifs de prévention des risques, comme le *reporting* volontaire des menaces. Enfin, DORA met en place le cadre de surveillance des prestataires critiques. Ce dernier est utile aux superviseurs, à la stabilité financière globale et pour les établissements de manière générale.

DORA consacre une attention particulière au cadre de gestion du risque de tiers. L'objectif consiste à intégrer la gestion du risque de tiers dans la gouvernance dans les dispositifs de gestion des risques des établissements. Les principes de ce domaine ne sont pas nouveaux et sont définis comme il s'ensuit :

- l'entité financière reste la responsable du risque ;
- le risque doit être géré de manière proportionnelle ;
- les entités financières doivent établir une stratégie de gestion du risque de tiers ;
- les entités financières doivent tenir un registre d'informations (relations passées avec des tiers) disponibles pour le superviseur. Ces éléments doivent être signalés au superviseur lorsque le contrat porte sur des fonctions critiques ou importantes ;
- les entités financières doivent étudier les risques et les stratégies de sortie préalablement à la signature du contrat.

Certaines bonnes pratiques sont également réaffirmées parmi lesquelles figurent :

- la clarté des obligations contractuelles ;
- les accords de niveau de service : mesures de remédiation à mettre en œuvre en cas de défaillance.

DORA fixe des exigences précises dans le texte de niveau 1, mais certaines d'entre elles devront être détaillées au travers de 13 mandats de développement de normes de niveau 2 (RTS et ITS) confiées aux Autorités européennes de surveillance. Dans ce contexte, la relation avec les prestataires tiers, le cadre de supervision des prestataires critiques ou encore le dispositif de *reporting* des incidents seront amenés à être précisés. L'ACPR fournira des moyens importants pour contribuer à la rédaction de ces différents textes. Nous sommes également appelés à renforcer nos recrutements dans le domaine du cyber et dans notre pôle d'expertise. Ces enjeux sont d'autant plus essentiels que nous aurons des compétences renforcées en matière de supervision nationale des risques IT et que nous devrons contribuer nous-mêmes à la mise en place du dispositif de surveillance des prestataires critiques, bien que le dispositif soit piloté au niveau européen.

Niamkey ACKABLE

Ainsi, nous avons abordé la thématique de résilience opérationnelle sous le prisme réglementaire. Selon moi, DORA souligne plusieurs points :

- la validation du besoin de protéger et la capacité à se remettre d'une situation défavorable (attaque cyber) ;
- la croissance des cybermenaces : DORA permet de cadrer des pratiques hétérogènes pour lutter contre cette menace grandissante et de plus en plus protéiforme.

TABLE RONDE

Niamkey ACKABLE

Romain ELIOT, comment définiriez-vous la résilience opérationnelle ?

Romain ELIOT

La résilience opérationnelle doit être appréhendée au niveau métier et de l'entreprise. Pour préserver l'intégrité et la fiabilité des processus inhérents à l'entreprise, il est nécessaire d'investir dans des moyens et des capacités informatiques qui seront au service de la protection des processus métier, tout en cherchant à assurer la continuité et la qualité des services fournis. L'objectif consiste à faire face à des événements averses, d'être capable de les gérer et de les surmonter.

Niamkey ACKABLE

Si nous nous basons sur le référentiel du NIS, la cyber-résilience opérationnelle s'intègre aussi à la cybersécurité. Romain ELIOT, en tant qu'entité assujettie à cette nouvelle réglementation, avez-vous été consulté lors de la phase de rédaction du projet de loi ?

Romain ELIOT

Tout à fait. Dès le départ, nous avons été consultés par la Commission afin de rendre un avis et de réaliser un état des lieux. Dans le cadre du processus réglementaire, nous avons également pu intervenir par le biais d'activités de lobbying auprès des parlementaires européens dans l'optique d'améliorer le texte. Nous avons considéré favorablement l'approche, car elle permet à des groupes comme les nôtres de disposer enfin d'un texte commun. En effet, DORA compile des mesures incluses dans de précédents textes et couvre l'ensemble de nos métiers, banque, services financiers et assurance.

Je me suis notamment impliqué dans la gestion des incidents et des notifications. Aujourd'hui, à l'échelle européenne, lorsque nous subissons un incident, nous devons réaliser plusieurs notifications. Les délais, les objectifs, les formulaires et parfois même les langues diffèrent d'une notification à une autre. Nous pouvons espérer simplifier ce système grâce à DORA.

Des standards d'application doivent être décrits au cours des deux prochaines années. Nous espérons que ces standards définiront davantage des orientations dans la lignée de ce que nous mettons déjà en œuvre dans les établissements. Il est également souhaitable que la rédaction des standards ne soit pas retardée, auquel cas nous ne disposerions que de très peu de temps pour les mettre en œuvre. En effet, des standards sur les clauses contractuelles ou sur la politique de sécurité ne peuvent être mis en œuvre à courte échéance.

Niamkey ACKABLE

Merci pour ces précisions. Christophe LEBLANC, pouvez-vous nous partager votre point de vue sur ce texte réglementaire ? Comment appréhendez-vous l'entrée en vigueur de cette réglementation ?

Christophe LEBLANC

Beaucoup s'accordent à dire que nous sommes passés d'un monde de la performance à un monde de la résilience. Mais ce n'est pas sans raison. Premièrement, des tensions internationales ont obligé les établissements financiers à prendre des mesures de protection forte. Ces tensions internationales nous montrent ainsi la nécessité d'investir dans la résilience opérationnelle.

Deuxièmement, les cyberattaques se multiplient, se professionnalisent et s'industrialisent. De nos jours, lorsque des vulnérabilités sont exposées, vous ne disposez que d'un ou deux jours pour réagir et éviter une exploitation de cette vulnérabilité par des cybercriminels. Les cyberpirates font ainsi peser une importante pression sur les établissements.

Troisièmement, la part du digital a fortement augmenté, tandis que la tolérance de nos clients aux interruptions a nettement diminué. L'interruption momentanée des services digitaux peut en effet être source de grande frustration pour les clients. Nous devons donc en tenir compte.

C'est pourquoi la résilience opérationnelle constitue un sujet stratégique au sein des établissements financiers. Plus précisément, la résilience opérationnelle doit être prise en charge par le CEO ou le Chief Risk Officer de la banque.

En ce qui concerne DORA et son implémentation au sein du groupe Société Générale, certains éléments étaient déjà compris dans notre réglementation. J'estime que DORA nous obligera toutefois à être plus clairs sur l'IT Risk Management, lequel n'a pas nécessairement été correctement formalisé. Ainsi, DORA permettra de standardiser et de formaliser la manière dont les incidents sont reportés.

En revanche, l'effort sur la partie *testing* sera plus compliqué à réaliser. Effectuer davantage de tests requerrait d'investir une quantité non négligeable de ressources. Nos relations avec les prestataires IT constitueront un autre enjeu. Nous devrons en effet *screener* l'ensemble de nos fournisseurs IT dont nous devrons tester ensuite la résilience grâce à des clauses contractuelles. Pour ce faire, nous allons devoir multiplier les audits.

Niamkey ACKABLE

Emmanuel ROCHER, dans le cadre de vos activités de régulateur français, vous ne vous occupez pas seulement du contrôle, mais vous disposez également d'autres moyens pour accompagner les différentes institutions à ces enjeux et exigences.

Emmanuel ROCHER

Je confirme. L'ACPR assume pleinement son rôle de consultation pour les nouveaux textes avec les établissements. Par ailleurs, nous organisons régulièrement des exercices de simulation de crise. Il en existe deux types : d'une part, les exercices de place à opérer dans le cadre de simulation d'attaque cyber. D'autre part, au niveau national, il existe des exercices de simulation de crise au sein du groupe de place robustesse (GPR). Ces tests sont organisés annuellement. Ces exercices visent à s'assurer que nous sommes pleinement mobilisés lors du développement des scénarios, lesquels sont à chaque fois renouvelés. Plus précisément, le but est de vérifier la capacité interne transversale et collective à rapidement identifier le bon diagnostic et à mettre en œuvre les solutions les plus efficaces.

Niamkey ACKABLE

Romain ELIOT, comment pratiquez-vous la résilience opérationnelle ? Cette fonction est propre à toute entité qui souhaite pérenniser son activité. De quels moyens disposez-vous pour répondre à ces enjeux ?

Romain ELIOT

Il existe plusieurs niveaux de réponse :

- la modélisation : savoir à quel risque nous faisons face, forme et impact du risque sur nos systèmes ;
- le développement de solutions : être capable de faire face à la crise ;
- les tests.

En ce qui concerne la modélisation, nous mettons en place depuis quelques années une approche par scénario au niveau du groupe Crédit Agricole. Dans ce contexte, nous avons collecté tous les scénarios imaginables. Nous avons ensuite identifié la *kill chain*, soit la succession d'événements qui mènent à l'impact final. Enfin, nous avons déterminé les mesures qui pouvaient bloquer cette *kill chain*.

Nous travaillons également depuis plusieurs années sur des solutions spécifiquement adaptées à la réponse aux incidents. Nous avons travaillé sur les capacités de restauration de données et de reconstruction de poste de travail pour de gros volumes. Lors du dernier exercice de place, nous nous sommes interrogés sur nos capacités de reconstruction.

Il existe une dernière catégorie de test : les tests d'intrusion que DORA incitera à étendre. En effet, nous en réalisons déjà, mais nous devrons aller encore plus loin. Ces tests s'effectueront en coopération avec le superviseur. Si le résultat du test n'est pas concluant, nous devrons être efficaces sur la correction et l'exécution du plan d'action, et le superviseur suivra notre remédiation.

Niamkey ACKABLE

Aujourd'hui, l'évolution de la menace cyber, constante et changeante, impose une redistribution des rôles et des responsabilités. À ce sujet, Christophe LEBLANC, pouvez-vous nous dire, d'un point de vue organisationnel, qui a la charge de la résilience opérationnelle au sein de la banque ?

Christophe LEBLANC

A la Société Générale, la filière *business continuity management* (BCM), dans laquelle s'insère la résilience opérationnelle et le cyber, dépend de la direction de la sécurité. En coopération avec la filière BCM, nous avons mené des études de *market intelligence*. En général, il existe un *split* entre la filière sécurité informatique et la filière BCM. Le BCM est en général beaucoup plus souvent rattaché au risque opérationnel dans d'autres établissements.

Quoi qu'il en soit, la filière BCM doit se renforcer qualitativement et quantitativement. Une révolution est nécessaire pour prendre désormais en compte le niveau de disruption à envisager (cyber menaces, tensions géopolitiques, etc.). Il est donc impératif que la filière BCM soit désormais considérée comme un enjeu stratégique.

Niamkey ACKABLE

En matière de résilience, existe-t-il d'autres réglementations internationales auxquelles vous êtes assujettis ?

Christophe LEBLANC

Tout à fait. Parmi elles figure notamment la réglementation UK. Cette réglementation incite à définir les *importants Business Services*, soit vos activités cœur. Ce sont les activités dont la survie de la banque dépend. C'est sur ce cœur de business que vous appliquerez les scénarios. Ils doivent être extrêmes, mais plausibles. L'esprit de la réglementation DORA est relativement similaire.

Niamkey ACKABLE

Ruxandra-Gabriela ADAM, pourriez-vous nous dire comment DORA tient compte du cadre réglementaire préexistant ?

Ruxandra-Gabriela ADAM

DORA intervient dans un exercice de consolidation et d'agrégation de toutes les règles préexistantes. D'une part, la société financière et son management devront appliquer les règles DORA. Pour certains établissements, ces règles ne seront pas nouvelles, mais d'autres sociétés rencontreront davantage de difficultés.

D'autre part, les autorités nationales devront intégrer dans leur supervision le risque opérationnel d'une manière beaucoup plus approfondie. En outre, durant les deux prochaines années, les sociétés devront réviser leur contrat pour que les exigences portant sur les risques opérationnels soient présentes dans ces contrats.

Niamkey ACKABLE

La réglementation DORA met en avant la notion de tiers critique. Qui sont-ils ? Quels sont leurs critères de qualification ?

Ruxandra-Gabriela ADAM

Le cadre de surveillance s'intéresse aux rôles des tiers critiques. En effet, nous avons remarqué la dépendance forte des marchés financiers aux services qu'ils fournissent. Notre problématique concerne ainsi la stabilité financière. À travers leur impact, leurs contrats, leur pénétration dans le système financier et leurs services, les tiers critiques présentent un risque systémique. D'un point de vue juridique, nous avons dû créer les mécanismes pour permettre leur identification par les autorités de surveillance financières européennes.

Certains de ces critères interrogent les éléments de niche, soit des services IT très difficiles à trouver sur le marché, et donc difficiles à substituer. Ces critères sont déjà établis dans DORA.

Nous devons désormais identifier dans un acte délégué les indicateurs qui en détaillant les critères DORA, permettront de cibler la population de fournisseur critique de services digitaux.

Niamkey ACKABLE

Emmanuel ROCHER, en ce qui concerne la supervision des tiers critiques, pensez-vous qu'il s'agit d'un moyen mis à disposition du régulateur pour renforcer son pouvoir de contrôle ainsi que la souveraineté européenne et nationale ?

Emmanuel ROCHER

Ce sera clairement un instrument de surveillance. Nous regarderons, tout comme les autorités européennes, les moyens et les outils à disposition des prestataires critiques pour assurer la continuité de leurs services. En tant que superviseur, ce qui nous importe, c'est la sécurité des établissements en France, la sécurité informatique, ainsi que la stabilité financière pour les établissements et leurs clients.

Ruxandra-Gabriela ADAM

Jusqu'alors, avec la crise, nous nous étions occupés des causes purement économiques. Avec DORA, nous nous posons la question des répercussions sur le système financier en cas de cyber attaques. Il est ainsi nécessaire de gérer cette dépendance des tiers et de prévenir le risque de crise systémique.

Par ailleurs, DORA n'impose pas des exigences de localisation de données. Dans les contrats, nous demandons seulement que les règles précisent où les données sont traitées.

Je tiens à préciser que d'autres discussions, débats et instruments adressent mieux le sujet de la souveraineté numérique dans le respect des règles internationales et des engagements de l'Union européenne.

Niamkey ACKABLE

Cette supervision des tiers critiques permet d'apporter davantage de confiance au sein d'un écosystème financier. Christophe LEBLANC, en qualité de banque et d'assureur, membre de cet écosystème financier, comment œuvrez-vous pour maintenir votre confiance vis-à-vis des parties prenantes de cet écosystème ?

Christophe LEBLANC

Je pense qu'il est bienvenu que le superviseur européen s'intéresse à la solidité des fournisseurs informatiques les plus importants. Nous devons maintenir avec nos partenaires les plus importants, une relation équilibrée. Il est judicieux de regarder la manière dont ils sont sécurisés et de leur demander leurs solutions de secours en cas de problème. Mais nous-mêmes, nous essayons de nous appliquer ces mêmes règles.

De plus, certains partenaires sont essentiels dans le fonctionnement de nos *core activities*. C'est pourquoi il est important de discuter avec eux. Nous sommes interconnectés, ils dépendent de nous et nous dépendons d'eux. C'est donc en anticipation que nous devons dialoguer sur les éléments de sécurité qui nous permettraient de continuer à travailler sur des activités sensibles en cas de cyber-attaques.

QUESTIONS/RÉPONSES

De la salle,

DORA a-t-il une portée extraterritoriale ? Une banque française doit-elle appliquer DORA dans les établissements situés hors de l'espace européen ? À l'inverse, qu'en sera-t-il pour un établissement hors Union européenne qui possède par exemple une filiale en France ?

Ruxandra-Gabriela ADAM

En tant que règlement européen, le champ d'application de DORA est très clair : il s'adresse aux entités financières qui sont réglementées et supervisées. DORA s'applique donc sur le territoire de l'Union européenne. Un élément d'extraterritorialité vise les tiers critiques dans certaines conditions. Par exemple, dans le cas où le superviseur principal a besoin de davantage d'éléments sur la base de ses

inspections, il peut alors effectivement exercer des pouvoirs en dehors de l'Union européenne. Il est cependant nécessaire que le tiers critique ait donné son accord et que l'autorité du pays tiers lui notifie son accord. S'il existe des succursales établies hors du territoire de l'Union européenne, il est nécessaire de veiller à développer une cohérence au niveau du groupe en matière des règles applicables. Mais en principe, l'application du règlement demeure territoriale.

Niamkey ACKABLE

Des internautes demandent comment DORA impactera les contrats en cours. Sera-t-il demandé de procéder à une mise à jour des contrats en cours ? Si oui, selon quel délai ?

Ruxandra-Gabriela ADAM

Absolument. Il existe de nouvelles exigences en matière de contrats. Concrètement, dès lors que DORA sera applicable en 2025, un contrat entre une banque et un prestataire tiers devra répondre à ces exigences. Ces dernières ne dictent pas la manière de formaliser les clauses du contrat, mais déterminent certains objectifs, afin que la société financière puisse comprendre le risque provenant du tiers et de disposer des outils pour gérer ce risque. Un contrat qui ne répond pas aux exigences imposées par DORA devra donc être renégocié et revisité. Les autorités doivent en conséquence expliquer aux sociétés financières la nécessité d'assurer la révision des contrats au cours des deux prochaines années.

De la salle,

Les prestataires – qu'ils soient jugés critiques ou non – devront-ils donner la possibilité aux banques de réaliser des tests de pénétration ?

Romain ELIOT

Je pense que nous procéderons comme pour le PCA : nous laissons le fournisseur réaliser certains tests, lesquels font partie de sa démarche de sécurité et son niveau de maturité. Toutefois, nous possédons des connexions informatiques avec des fournisseurs qui méritent également d'être auditées et testées. Nous devrons donc anticiper que certains de nos tests débordent chez le fournisseur et inversement. Nous avons d'ores et déjà des clauses d'audit dans les contrats qui peuvent inclure des tests d'intrusion chez le fournisseur. Cependant, nous avons des milliers de fournisseurs et cette démarche de test d'intrusion est lourde à mettre en place. En conséquence, je pense qu'il sera assez rare d'aller mener nous-mêmes un test d'intrusion chez le fournisseur.

De la salle,

La transmission d'une preuve de tests par le fournisseur pourra-t-elle vous être utile ?

Romain ELIOT

Le mot clé est la maturité. Si un fournisseur dispose d'une vraie gestion des risques, d'un plan de contrôle, d'une politique de sécurité consolidée et s'il procède à des tests, nous aurons évidemment tendance à lui faire confiance. Cependant, pour des fournisseurs de grande échelle tels que les géants du cloud, il est plus judicieux de dialoguer avec leurs responsables de sécurité, plutôt que de les auditer.

De la salle,

Ruxandra-Gabriela ADAM, est-ce une démarche acceptable au niveau réglementaire ? Ou bien l'audit constituera-t-il une obligation ?

Ruxandra-Gabriela ADAM

Les tests de pénétration constituent une obligation qui s'applique aux entités financières dans le champ d'application de DORA. En conséquence, les grandes entités financières seront soumises à ces tests de manière régulière avec des testeurs externes ou internes. Comme ces tests approfondis sont lourds à mettre en place, il est possible d'inclure les fournisseurs tiers.

Les pouvoirs accordés pour une société financière soumise à DORA et pour une autorité nationale, en ce qui concerne les droits d'accès et les droits d'audit pour ces tiers, ne se situent pas au même plan que les tests.

Ainsi, le *testing* des tiers définis dans DORA et le droit d'audit d'une entité soumise à DORA constituent deux éléments différents.

Niamkey ACKABLE

L'audience à distance demande quels sont les moyens d'action prévus lorsqu'un prestataire critique refuserait par exemple de remédier à l'apparition d'une faille grave. Quel serait le partage entre les régulateurs et les établissements bancaires en termes de plan d'action ?

Ruxandra-Gabriela ADAM

C'est une question très complexe. Le cadre de supervision ne correspond pas à proprement parler à une surveillance. Après des entretiens et des inspections, le superviseur principal peut conclure dans certaines situations que le superviseur et le fournisseur ont des approches divergentes. Dans ce cas, DORA stipule qu'au niveau européen, nous aurions le pouvoir d'indiquer aux autorités nationales de développer une approche cohérente. C'est toujours l'entité financière et son superviseur national qui réaliseront le suivi des exigences vis-à-vis des prestataires critiques. Ce n'est que la supervision qui est réalisée au niveau européen. La société et le superviseur discuteront ensemble avec le fournisseur critique pour comprendre les raisons de son refus. Si les conséquences de ce refus impliquent un risque considéré par le superviseur comme un risque important, alors sont prévues les possibilités de modifier, de résilier, de terminer partiellement ou totalement le contrat. Mais ce cas devrait rester exceptionnel, d'autant plus qu'il n'est pas dans l'intérêt du fournisseur de mettre fin à ses services.

Christophe LEBLANC

La difficulté est opérationnelle, car résilier rapidement un contrat avec un fournisseur n'est pas possible en général. Et je pense qu'un refus de remédiation n'est pas dans l'intérêt du fournisseur.

Une intervenante (3)

Aujourd'hui, j'interviens chez un client qui travaille avec un prestataire qualifié comme critique important dans le cadre de la réglementation luxembourgeoise CF 22 826.

Nous avons déposé le dossier cloud auprès du régulateur. La réglementation CF 22 826 est encadrée par un *guideline* OBA sur l'*outsourcing*. Ainsi, existe-t-il une adhérence entre DORA et les *guidelines* sur l'*outsourcing* ?

Ruxandra-Gabriela ADAM

Il s'agit de deux éléments différents : d'une part, le rapport entre un prestataire critique qui serait désigné sur la base d'une réglementation nationale, et d'autre part, le prestataire de critique qui serait désigné sur la base de DORA pour un éventuel effet systémique au niveau européen.

Au sujet de l'*outsourcing*, ou un prestataire sera désigné comme critique sur la base d'une réglementation nationale, DORA ne s'occupe pas d'une situation qui intervient uniquement au niveau national, parce que les critères DORA servent à désigner un fournisseur qui est critique pour les sociétés en vue de son impact systémique pour l'Union européenne.

En revanche, quelle est la procédure s'il existe au niveau national un superviseur financier qui a le pouvoir d'intervenir auprès des prestataires désignés comme critiques à la fois par une réglementation nationale et par DORA ? Dans ce cas, DORA prévoit que les régimes en place doivent permettre une coordination. Dès lors qu'un prestataire est défini comme critique sur la base des critères DORA, c'est le règlement européen qui l'emporte. Un superviseur national doit donc coordonner sa démarche avec le régulateur européen. Si, par exemple, le prestataire est désigné seulement au niveau national, mais pas au niveau européen, DORA n'est pas concerné.

Niamkey ACKABLE

Les internautes demandent combien de tiers critiques les régulateurs pensent être en mesure de superviser. Quelle coordination au niveau européen est-elle prévue pour ces prestataires multinationaux ?

Emmanuel ROCHER

Le nombre de prestataires critiques et les noms individuels seront désignés par le cadre européen de surveillance, lequel n'est pas encore en place. Certains critères seront précisés par les textes de niveau 2. Toutefois, il est nécessaire d'identifier de manière précise les activités qui sont critiques. Il en est de même pour les prestataires critiques. Le nombre de prestataires devrait être limité et concerner des acteurs de taille mondiale spécifiquement critique pour les acteurs financiers européens. Bien qu'il n'existe pas véritablement de coordination pour la désignation des prestataires critiques, nous identifierons vraisemblablement les mêmes noms que les dispositifs non européens déjà en place avec des problématiques identiques.

Niamkey ACKABLE

Je tiens à remercier l'ensemble des panélistes pour leur présence et leur disponibilité. J'espère pour l'audience que nous avons pu vous apporter des éclaircissements sur ce projet de loi.

CLUB BANQUE

Le rendez-vous mensuel
des professionnels
de la banque et de la finance

Cyber-résilience opérationnelle

Jeudi 17 novembre 2022

18 h 00 à 20 h 00
Auditorium de la FBF
18, rue La Fayette
75009 Paris

REVUE BANQUE

Partenariat officiel TNP

En partenariat avec kyndryl

Programme

Cyber-résilience opérationnelle

Président de séance :
Niamkey ACKABLE, ***Deputy Core Practice Leader Security & Resiliency***
KYNDRYL

Règlement sur la résilience opérationnelle numérique du secteur financier

Ruxandra-Gabriela ADAM, ***Legal and Policy Supervisor,*** **DG FISMA, Commission Européenne**

Mise en œuvre de DORA: principaux enjeux pour les banques et les superviseurs

Emmanuel ROCHER, directeur des affaires internationales, ACPR

Table ronde :

Christophe LEBLANC, ***Head of the Group Operational Resilience Mission,*** **Société Générale**
Romain ELIOT, CISO Groupe adjoint, Responsable des Relations Institutionnelles et Analyses Stratégiques, Crédit Agricole SA
Niamkey ACKABLE, ***Deputy Core Practice Leader Security & Resiliency***
Emmanuel ROCHER, directeur des affaires internationales, ACPR
Ruxandra-Gabriela ADAM, ***Legal and Policy Supervisor,*** **DG FISMA, Commission Européenne**

Questions/réponses

CLUB BANQUE

Programme

Président de séance

Niamkey ACKABLE

Deputy Core Practice Leader Security & Resiliency

kyndryl

CLUB BANQUE

Programme

Règlement sur la résilience opérationnelle numérique du secteur financier

Ruxandra-Gabriela ADAM, *Legal and Policy Supervisor,* DG FISMA

Commission européenne

CLUB BANQUE

Contexte

- Discussions niveau international (G7,CSF, Comité de Bâle)
- 2018: **Plan d'action pour les technologies financières**: → 2019 **Avis techniques conjoints** des 3 ASE
  - Dispositions relatives à la sécurité informatique dans le secteur financier: disparités législatives et approches inégales (nationales et UE)
  - Directive NIS - couverture partielle
  - Risque posé par les tiers prestataires de services informatiques
  - 2019: Début processus au niveau européen - consultation publique, analyse d'impact
- Septembre 2020: **Proposition** de la Commission - Règlement + Directive DORA sur la résilience opérationnelle numérique

Début négociations Conseil (Octobre 2020) - Approche générale Conseil (Novembre 2021) - Rapport final PE (Décembre 2021)

Trilogues politiques (2022) - Accord politique (Mai 2022) - Trilogues techniques (Février - Juin 2022) – Finalisation juridique et linguistique (Juillet - Octobre)

- **Adoption** Novembre 2022
- Dates estimées d'entrée en vigueur et d'application: début 2023 et respectivement début 2025

European Commission

Champ d’application

- **Grande majorité** des entités financières soumises à réglementation européenne, par ex: les établissements de crédit, de paiement et de monnaie électronique, les entreprises d'investissement; les prestataires de services sur crypto-actifs; les dépositaires centraux de titres; les contreparties centrales; les plates-formes de négociation; les référentiels centraux; les gestionnaires de fonds d'investissement alternatifs et les sociétés de gestion; les prestataires de services de communication de données; les entreprises d'assurance et réassurance; les intermédiaires d'assurance, réassurance et 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

- **Exemptions**

  - Catégories exemptées en vertu du régime dérogatoire (par ex: gestionnaires de fonds d'investissement alternatifs; entreprises d'assurance, réassurance sous les seuils des Directives AIFMD et Solvency)

  - Catégories exemptées en vertu de leur taille (intermédiaires d'assurance, réassurance et d'assurance à titre accessoire qui sont des micro, petites ou moyennes entreprises)

  - Possibilité des États Membres d’exempter les établissements visés à l'article 2, paragraphe 5, points (4) à (23), de la directive CRD

  Régime allégé

  Les articles 5 à 15 DORA ne s'appliquent pas aux petites entreprises d'investissement non interconnectées; aux établissements de paiement exemptés en vertu de la directive (UE) 2015/2366; aux établissements exemptés en vertu de la directive 2013/36/UE pour lesquels les États membres ont décidé de ne pas appliquer l'option visée à l'article 2, paragraphe 4 DORA, aux établissements de monnaie électronique exemptés en vertu de la directive 2009/110/CE; et aux petites institutions de retraite professionnelle. Ces entités appliqueront un cadre simplifié de gestion des risques informatiques - Article 16 DORA

Gestion des risques informatiques

- Gouvernance et organisation (principes pour l'organe de direction)
- Cadre de gestion des risques informatiques (y compris la partie physique) et stratégie de résilience opérationnelle numérique
- Règles de principe sur les systèmes, protocoles et outils informatiques

- Identification
- Protection et prévention
- Détection
- Réponse et rétablissement
  - continuité des fonctions critiques ou importantes
  - activation sans retard des plans de réponse et rétablissement
  - politiques et procédures de sauvegarde, procédures et méthodes de restauration et de rétablissement
  - objectifs en matière de délai et de point de rétablissement pour chaque fonction fixés par les entités financières (pas par DORA)
- Apprentissage et évolution
- Communication

Gestion, classification et notification des incidents liés à l'informatique

- Règles générales
  - gestion des incidents liés à l'informatique
  - classification des incidents et des cybermenaces - normes techniques de réglementation et d'exécution (critères DORA à détailler par les ASE; contenu des rapports de notification; formulaires de notification)
  - Tout incident opérationnel ou de sécurité lié au paiement (PSD) passe sous DORA

Notification des incidents **majeurs** liés à l'informatique et notification volontaire des cybermenaces importantes

- à l'autorité compétente pertinente

États membres peuvent toutefois décider que certaines / toutes leurs entités financières fournissent également les notifications / rapports aux autorités compétentes NIS ou aux centres nationaux de réponse aux incidents de sécurité informatique (CSIRT)

- notification initiale + rapport intermédiaire + rapport final
- autorités compétentes transmettent les détails aux autorités NIS / CSIRTs/ autorités de résolution / ASEs / BCE

Tests de résilience opérationnelle numérique (1)

- Tests de base
- Tests avancés d'outils, de systèmes et de processus informatiques - tests de pénétration fondés sur la menace (TPFM)
  - Entités financières désignées par les autorités compétentes suivant des critères DORA
    - facteurs d'incidence (criticité/ l'importance des fonctions liées aux services /activités de l'entité financière)
    - stabilité financière (caractère systémique niveau de l'Union /national)
    - profil de risque informatique spécifique, niveau de maturité informatique
  - Reconnaissance mutuelle
  - TIBER - EU

Tests de résilience opérationnelle numérique (2)

- Couverture
  - plusieurs, voire la totalité, des fonctions et services critiques ou importants d'une entité financière
  - systèmes de production en direct qui appuient ces fonctions
  - possibilité TPFM associant plusieurs entités financières (test ‘groupé’) auxquelles le tiers prestataire de services informatiques fournit des services informatiques
  - exigences applicables aux testeurs aux fins du déploiement des TPFM
    - testeurs internes possibles sur agrément des autorités compétentes

Gestion des risques liés aux tiers prestataires de services informatiques (1)

- Principes de base
  - Les entités financières restent responsables du respect et exécution des obligations découlant du DORA et du droit applicable aux services financiers
  - Stratégie en matière de risques liés aux tiers prestataires de services informatique - base individuelle et consolidée
  - registre d'informations - accords contractuels sur l'utilisation de services informatiques fournis par des tiers prestataires de services informatiques
  - Évaluation préliminaire du risque de concentration informatique au niveau de l’entité

Gestion des risques liés aux tiers prestataires de services informatiques (2)

Dispositions contractuelles

- description exhaustive des services informatiques /fonctions fournis par le tiers prestataire de services informatiques
- indication des lieux - régions ou pays - où les services informatiques / la sous-traitance seront fournis et les données seront traitées
- indications des dispositions assurant la confidentialité, disponibilité, l'intégrité ou l'authenticité des données
- dispositions sur la garantie de l'accès/récupération/restitution, dans un format facilement accessible, des données à caractère personnel et autres données traitées par l'entité financière, si insolvabilité/résolution/ cessation des activités commerciales du tiers prestataire de services informatiques /résiliation des accords contractuels
- descriptions des niveaux de service, mises à jour et révisions
- l'obligation du tiers de fournir à l'entité financière, sans frais supplémentaires ou à un coût déterminé ex ante, assistance si incident lié à l'informatique en rapport avec le service
- droits de résiliation + délai de préavis minimal pour la résiliation des accords, conformément aux attentes des autorités compétentes et des autorités de résolution
- coopération du tiers avec les autorités compétentes et de résolution de l'entité financière

Gestion des risques liés aux tiers prestataires de services informatiques (3)

- Dispositions plus détaillées des services informatiques appuyant des fonctions critiques /importantes
  - descriptions complètes des niveaux de service + objectifs de performance quantitatifs et qualitatifs pour le suivi par l'entité financière des risques + mesures correctives si niveaux de service pas atteints;
  - délais de préavis et obligation de notification l'entité financière - tout développement susceptible d'avoir une incidence significative sur la capacité du tiers à fournir les services
  - obligation du prestataire de mettre en œuvre / tester des plans d'urgence / mesures et outils de sécurité informatique d'un niveau approprié de sécurité
  - suivi permanent - droits illimités d'accès, inspection et d'audit par l'entité financière / tierce partie désignée/ autorité compétente / droit de prendre copie des documents pertinents sur place
  - obligation du prestataire de coopérer pleinement lors des inspections sur place et audits des autorités compétentes, superviseur principal, l'entité financière ou une tierce partie désignée
  - stratégies de sortie, fixation d'une période de transition adéquate obligatoire

Cadre de supervision des tiers prestataires critiques de services informatiques (1)

- Supervision continue – Objectif: stabilité financière
- Désignation des tiers prestataires critiques de services informatiques par les AES - critères DORA
- AES désignées comme superviseur principal pour chaque tiers prestataire critique
- Gouvernance
  - Forum de supervision - sous-comité du Comité mixte
  - approche cohérente + évaluation collective des conclusions des activités de supervision menées pour l'ensemble des tiers prestataires critiques + coordination et atténuation des transferts de risques intersectoriels

Cadre de supervision des tiers prestataires critiques de services informatiques (2)

- Un superviseur principal pour chaque tiers prestataire critique de services informatiques
  - détermine si chaque tiers prestataire critique a mis en place des règles, procédures, mécanismes et des dispositifs complets, solides et efficaces pour gérer les risques informatiques qu'il est susceptible de faire peser sur les entités financières
  - équipe d'examen conjoint
  - pouvoirs de mener des enquêtes et inspections générales, demander des informations et des rapports formuler des recommandations
  - En cas de non-respect total /partiel des mesures de *transparence et coopération* : astreintes
  - Exercice de certains pouvoirs aussi en dehors de l'Union
  - Suivi par les autorités compétentes

European Commission

Dispositifs de partage d'informations

- **Mécanisme volontaire**
  - entités financières peuvent échanger des informations / renseignements sur les cybermenaces
    - indicateurs de compromis, tactiques, techniques, procédures, alertes de cybersécurité et outils de configuration
  - communautés d'entités financières de confiance
  - protection de la nature potentiellement sensible des informations partagées - confidentialité des affaires, protection des données à caractère personnel et respect de la politique de concurrence
  - protocoles pour fixer les condition de participation + le cas échéant modalités de participation des autorités publiques + aspects opérationnels - utilisation de plateformes informatiques spécialisées

Relation avec la Directive NIS

- DORA lex specialis
- Liens avec écosystème NIS
  - Participation des AES / autorités DORA au Groupe de Coopération NIS
  - Autorités NIS / CSIRTs reçoivent indirectement les détails des incidents majeurs
  - Autorités NIS
    - impliqués dans la governance du cadre de supervision des tiers critiques
    - sur requête des autorités DORA, peuvent être consultées dans l’exercice du cadre de supervision et dans son suivi

Programme

Mise en œuvre de DORA: principaux enjeux pour les banques et les superviseurs

Emmanuel Rocher, directeur des Affaires internationales

ACPR
BANQUE DE FRANCE

CLUB BANQUE

BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

MISE EN ŒUVRE DE DORA : PRINCIPAUX ENJEUX POUR LES BANQUES ET LES SUPERVISEURS

EMMANUEL ROCHER
DIRECTEUR DES AFFAIRES INTERNATIONALES, SG ACPR

CLUB BANQUE – 17 novembre 2022

BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

Sommaire

BANQUE DE FRANCE
EUROSYSTÈME

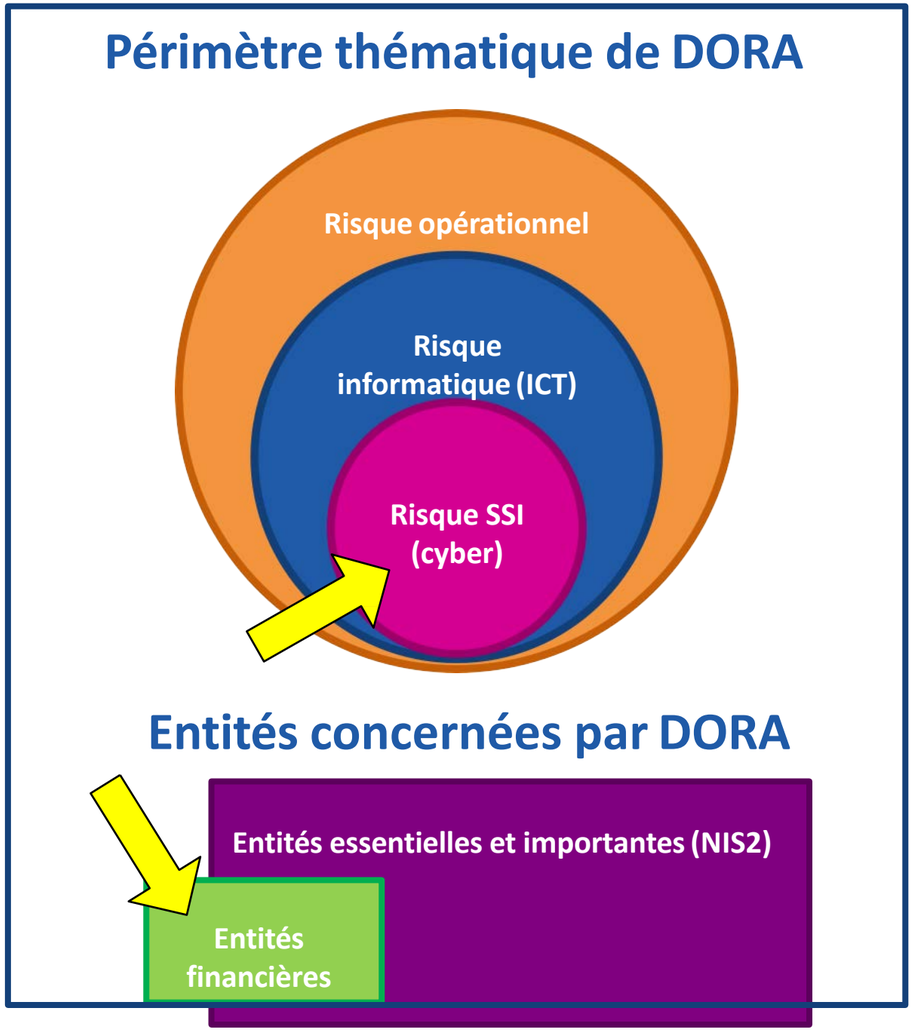
PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

1. Objectifs et apports de DORA

LES OBJECTIFS DE DORA

- DORA renforce le **versant numérique de la résilience opérationnelle** du secteur financier par des mesures portant sur la **sécurité des réseaux et des systèmes d'information**
- 4 grands thèmes :
  - Gestion du risque
  - *Reporting* des incidents
  - Tests (dont TLPT)
  - Risque de tiers (dont surveillance des prestataires critiques)



LES APPORTS DE DORA

- Pour les établissements
  - Un référentiel de **règles harmonisées** (gouvernance, *reporting*, tests, risque de tiers) pour toutes les activités financières dans l'UE
    - » Simplification pour les groupes internationaux ou trans-sectoriels
    - » Moins de barrière à l'entrée et à la croissance pour les petits établissements
  - **Pas de changement règlementaire majeur** en substance
- Pour le superviseur
  - Un **cadre juridique sécurisant** (règlement et règlements délégués au lieu d'orientations et de textes nationaux)
  - Approche par la **résilience** plus que par les exigences en fonds propres : accompagner la place vers une meilleure gouvernance
  - Un cadre de surveillance européen des **prestataires critiques** pour limiter les risques systémiques et renforcer la confiance

BANQUE DE FRANCE
EUROSYSTÈME

PÔLE
STABILITÉ
FINANCIÈRE

ACPR
BANQUE DE FRANCE

2. Incidences sur la supervision bancaire du risque cyber

DORA CONFORTE LES RÈGLES DE GOUVERNANCE EN VIGUEUR

- Le risque cyber est une **priorité aux niveaux français et européen** depuis le milieu des années 2010
  - Le Collège de l'ACPR a inscrit la cybersécurité dans les priorités du contrôle **chaque année depuis 2015**
  - Révision de **l'arrêté « contrôle interne »** du 3 novembre 2014 **en février 2021**
  - Les AES ont proposé des **orientations** sectorielles successives (les textes de l'EBA en vigueur ont été adoptés en 2019-2021)
- **DORA consacre une nouvelle approche** : viser la résilience opérationnelle et non la seule maîtrise du risque opérationnel
- **Le niveau cible** de gouvernance du risque cyber sous DORA est **comparable** à celui que consolide la notice ACPR du 7 juillet 2021 relative à la gestion du risque informatique

DORA SUIT UNE DÉMARCHE CONSTRUCTIVE

- Un objectif central d'**harmonisation** des normes
  - Mais pas de révolution des pratiques
- DORA reflète une **priorité croissante** du risque cyber pour le législateur comme pour les superviseurs
  - Une singularité qui justifie une harmonisation entre secteurs
  - Des outils de gouvernance dédiés
  - Un *reporting* particulier
- DORA promeut une **relation de confiance** avec les autorités
  - *Reporting* volontaire des menaces
  - Encouragement à utiliser des clauses contractuelles standard (lorsqu'elles existent)
  - Réduction du risque de tiers pour les entités financières grâce à la surveillance des prestataires critiques par les AES et les superviseurs

EXEMPLE DU CADRE DE GESTION DU RISQUE DE TIERS

- Aucun des principes introduits par DORA n'est inédit
  - L'entité financière reste la **responsable** du risque
  - Le risque doit être géré de **manière proportionnelle**
  - Les entités financières doivent établir une **stratégie** relative au risque de tiers
  - Les entités financières doivent maintenir un **registre d'information** et **signaler** au superviseur lorsqu'un contrat porte sur des fonctions critiques ou importantes
  - **Évaluation du risque** préalablement à la signature du contrat, **sécurité et accès aux données** et **stratégies de sortie**
- Les bonnes pratiques contractuelles sont réaffirmées
  - Clarté des obligations réciproques
  - Accords de niveau de service
  - Clauses de réversibilité…
- Mais DORA harmonise des termes, des périmètres et des pratiques
  - « risque de tiers » plutôt qu'« externalisation »
  - Une approche commune partagée avec les filiales et concurrents français et européens, des secteurs de la banque et de l'assurance…

3. Mise en œuvre de DORA

DES ENJEUX ESSENTIELS POUR L'ACPR

- **2022-2024** : Participer aux travaux sur les textes de niveau 2
  - DORA attribue **13 mandats aux AES** à remplir d'ici à la mi-2023 : un défi collectif pour les autorités européennes et nationales
    - 10 textes de niveau 2 (RTS/ITS)
      - » Cadre de gestion des risques : le niveau 1 contient l'essentiel pour le régime général mais le niveau 2 le précisera et sera clé pour le régime simplifié
      - » *Reporting* des incidents : seuils et modalités à déterminer
      - » Tests : modalités de mise en œuvre du TLPT à établir
      - » Risque de tiers : des précisions à apporter au cadre général et le fonctionnement concret du cadre européen de surveillance à arrêter
    - 2 textes de niveau 3 (orientations) et 1 rapport de faisabilité
  - Les autorités nationales de supervision ont une **expertise** à faire valoir
  - L'ACPR souhaite promouvoir **l'efficacité** et la **qualité** de la gouvernance et éviter le formalisme
- **D'ici à 2025** : Préparer la mise en œuvre de DORA avec les AES et le MSU
  - **Renforcer les compétences** dans le domaine cyber qui restera une **priorité stratégique** pour les activités de contrôle de l'ACPR
  - Être prêt à contribuer à la **surveillance des prestataires critiques**
  - Mettre en place les **nouveaux *reportings***

QUE PEUVENT ATTENDRE LES ENTITÉS FINANCIÈRES DU CADRE EUROPÉEN DE SURVEILLANCE DES PRESTATAIRES CRITIQUES ?

DES EFFETS DIRECTS LIMITÉS

- Pas de contrainte réglementaire particulière
- Droit de suite des ANC auprès des entités financières si des risques particuliers sont constatés lors de la surveillance

DES EFFETS INDIRECTS POSITIFS

- Une plus grande sensibilisation des prestataires critiques aux préoccupations des superviseurs financiers (et des établissements)
- Une réduction du risque de tiers par une amélioration de la résilience des principaux prestataires informatiques de la place

PRÉPARER LA TRANSITION VERS DORA

EC, EP, EME, EI (cl. 1 et 2)

- **Orientations actuelles** de l'ABE ont inspiré le texte de niveau 1
- **Peu de proportionnalité dans DORA** (sauf éventuelles microentreprises)
- 2 projets d'**harmonisation de *reporting*** à prévoir en 2024 (incidents et registre des prestataires) proches des travaux actuels du MSU

Autres entités financières

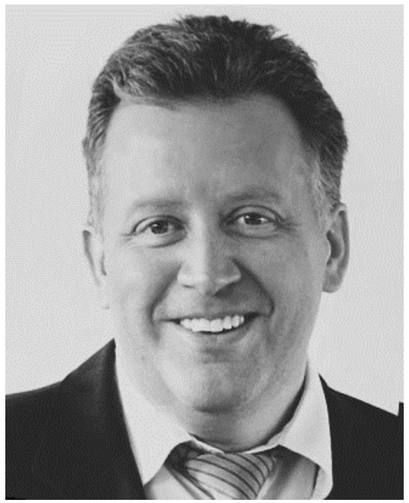
- **Périmètre large** (y compris PSAN du régime MICA, agences de notation…)
- Des règlementations sectorielles **déjà comparables** pour l'assurance et les services d'investissement
- **Large proportionnalité dans DORA**
  - assureurs « solvabilité 1 » exclus
  - obligations simplifiées pour les EI de classe 3
  - traitement particulier des microentreprises
  - obligations supplémentaires pour CCP, CSD…

Renforcer la gouvernance dans le cadre actuel est la meilleure préparation à DORA

Table ronde

Christophe Leblanc,
Head of the Group Operational Resilience Mission

SOCIETE GENERALE



Romain ELIOT,
CISO Groupe adjoint, Responsable des Relations Institutionnelles et Analyses Stratégiques

CRÉDIT AGRICOLE

Niamkey ACKABLE
Deputy Core Practice Leader Security & Resiliency

kyndryl

Emmanuel Rocher, directeur des Affaires internationales

ACPR
BANQUE DE FRANCE

Ruxandra-Gabriela ADAM, *Legal and Policy Supervisor,*
DG FISMA

Commission européenne

CLUB BANQUE

à venir

Les prochains événements

Reporting extra-financier

Jeudi 24 novembre 2022

Reporting réglementaire : le projet IReF

Mardi 6 décembre 2022

Forum Des Auteurs : Politique monétaire, taux, inflation, jusqu'où irons-nous ?

Lundi 12 décembre 2022

Retrouvez tous nos séminaires sur http://evenement.revue-banque.fr/seminaires/

CLUB BANQUE

à venir

Profitez du Club Banque toute l'année avec l'adhésion !

Inscription et renseignements :

clubbanque@revue-banque.fr

01.48.00.54.04

CLUB BANQUE