Les 5 incontournables

Comités d’audit et gouvernance banque

#15

mazars

Édito

La pandémie de COVID-19 a engendré un choc macro-économique mondial sans précédent. Les institutions européennes et nationales s'organisent pour permettre aux banques de traverser au mieux la crise. Dans ce contexte de début de nouvelle année, encore très marqué par la persistance à l'échelle mondiale de la pandémie, nous vous proposons de faire un point sur les menaces induites par le recours massif au télé-travail, les premières conclusions du rapport commun AMF/ACPR sur les engagements climatiques des institutions financières ainsi que les modifications à venir sur l'arrêté sur le contrôle interne. Dans un second temps nous aborderons les enjeux clés liés au projet de règlement européen « DORA » – ***Digital Operational Resilience Act*** – ayant pour objectif d'améliorer la résilience opérationnelle informatique des acteurs financiers.

Très bonne lecture et bonne année !

Sommaire

04 Comité de Bâle : actualisation de ses orientations sur l'audit externe des banques

06 Nouvelles recommandations de l'AFA : l'engagement de l'instance dirigeante

08 Projet DORA : de la gestion du risque opérationnel vers la résilience opérationnelle informatique

10 Le télétravail : cible des pirates informatiques

12 Rapport commun ACPR-AMF : les engagements climatiques des institutions financières françaises

Le Comité de Bâle
Actualisation de ses orientations sur l'audit externe des banques

Le Comité de Bâle a publié une note additionnelle à ses orientations BCBS280 de 2014 relatives à l'audit externe des banques. Promouvoir un audit de haute qualité des banques constitue un point clé pour le Comité. En effet avec l'entrée en application de la norme IFRS9 en 2018 dans les juridictions concernées, le Comité de Bâle a estimé nécessaire de publier ce complément en ciblant particulièrement l'audit de l'estimation comptable de la perte de crédit attendue (ECL) dans le cadre de l'audit global des états financiers.

Contexte

Pour rappel le provisionnement des pertes de crédit constitue une question comptable centrale, puisque le passage sous IFRS9 rend obligatoire de provisionner dès l'octroi du crédit, i.e. en anticipation de pertes futures selon divers scénarii macroéconomiques. Mais également règlementaire, puisque ce provisionnement reflète en réalité l'évolution de l'exposition d'une banque au risque de défaut des emprunteurs, i.e. risque de crédit au sens de la règlementation, et va donc avoir un impact sur le capital réglementaire des banques et in fine sur leurs niveaux de ratios de solvabilité.

Portée

Cette note additionnelle décrit les attentes du Comité de Bâle en matière d'audit de haute qualité de l'application de IFRS9, en particulier de l'estimation des ECL. Les pratiques qui y sont décrites sont des moyens par lesquels les banques peuvent appliquer certains aspects des normes comptables, mais ne doivent pas être interprétées comme étant prescriptives. Sont visées les banques appliquant IFRS9, actives au niveau international et soumises à un audit des états financiers y compris celles appartenant à un groupe bancaire, ainsi que les sociétés holding dont les filiales sont principalement des banques actives à l'international.

Ainsi ces orientations n'ont pas la prétention de remplacer les normes comptables ou d'audit en vigueur, elles s'inscrivent plutôt dans le cadre du dialogue instauré entre les superviseurs bancaires et les auditeurs externes via les orientations originelles de 2002 sur ce thème.

Organisation du document

La partie 1 décrit les attentes du Comité à l'égard des auditeurs externes, à travers les questions que le comité d'audit devrait poser dans le cadre de son rôle de superviseur de ces derniers et de promoteur d'un audit bancaire de haute qualité. La partie 2 décrit, quant à elle, les attentes incombant aux auditeurs externes dans le contexte des éléments clés de l'ECL.

Principales attentes décrites dans le document

Le Comité de Bâle déroule un certain nombre de questions pertinentes que devraient poser le comité d'audit en lien avec les zones d'attention suivantes :

- la mise en place d'un environnement d'audit propice au scepticisme professionnel ;
- les facteurs qui ont poussé à la bonne compréhension des risques d'anomalies significatives ;
- le test de l'efficacité opérationnelle des contrôles internes sur lesquels s'appuie les auditeurs externes ;
- le profil des experts mobilisés par l'auditeur pour l'examen des ECLs ;
- les principales sources de preuve recueillies pour traiter les risques d'anomalies significatives.

Concernant les auditeurs externes, la déclinaison des attentes va concerner le scepticisme professionnel vis-à-vis des états financiers à auditer, l'évaluation du risque d'anomalie significative, les composantes clés ayant permis l'estimation des ECL, l'environnement de contrôle interne, le recours à des experts en modélisation, le niveau approprié de preuve attestant la qualité de l'audit. En effet, outre s'assurer de la compétence des équipes, les auditeurs doivent réunir suffisamment de preuve d'audit sur les facteurs de risques d'anomalie significative afin de démontrer le scepticisme professionnel, de comprendre le modèle d'affaires en particulier celui de prêts bancaires.

01

Les enjeux clés

- Le cadre des ECL soulève d'importants défis tant pour la direction d'une banque que pour les auditeurs
- L'estimation des ECL et des informations afférentes est un aspect important de l'information financière

Pour aller plus loin

Lettre réglementaire n°27 - Novembre 2020

Nouvelles recommandations de l'AFA
L'engagement de l'instance dirigeante

Contexte

En application de la loi Sapin II, l'Agence française anticorruption est chargée d'élaborer des recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits d'atteinte à la probité. Ces recommandations font l'objet d'un avis publié au Journal officiel de la République française le 12 janvier 2021. Les premières recommandations de l'AFA avaient été publiées le 22 décembre 2017.

L'AFA met notamment en évidence dans ses nouvelles recommandations, qu'un dispositif anticorruption repose nécessairement sur trois piliers indissociables :

- un engagement de l'instance dirigeante exempt d'atteintes à la probité,
- la connaissance des risques d'atteintes à la probité auxquels l'entité est exposée,
- ainsi qu'une gestion des risques.

Nous vous proposons d'approfondir le premier pilier d'un dispositif anticorruption : l'engagement de l'instance dirigeante.

L'obligation d'engagement de l'instance dirigeante

Pour rappel l'article 17 de la loi Sapin II impose à l'instance dirigeante « de prendre les mesures destinées à prévenir et détecter la commission, en France ou à l'étranger, de faits de corruption ou de trafic d'influence ». A défaut, sa responsabilité peut être engagée devant la commission des sanctions de l'AFA. Il est donc dans l'intérêt de l'instance dirigeante de veiller à la mise en œuvre d'un dispositif anticorruption adapté sur l'ensemble du périmètre d'intervention de l'entreprise.

Responsabilité de l'instance dirigeante

L'AFA recommande à l'instance dirigeante de mettre en œuvre une politique de tolérance zéro à l'égard de tout fait de corruption, de promouvoir et de diffuser une culture de la conformité anticorruption au sein de l'entreprise et vis-à-vis des tiers, en érigeant la prévention et la détection des faits de corruption à un niveau prioritaire. Ceci constitue un élément fondateur de la démarche de prévention et de détection de la corruption.

L'instance dirigeante définit la stratégie de gestion des risques et s'assure de sa mise en œuvre. A cet égard, elle veille à formaliser son approbation du dispositif et en particulier de la cartographie des risques de corruption. Elle s'assure de la mise en place d'un plan d'actions y afférent et des moyens adaptés pour l'exécuter et pour en assurer le suivi régulier. L'instance dirigeante vérifie, au moyen d'indicateurs et de rapports de contrôle et d'audit, que le dispositif anticorruption est organisé, efficace et à jour.

Elle doit également veiller à l'intégration de mesures anticorruption aux procédures et politiques, par exemple, de sa gestion des ressources humaines, de sa politique commerciale ou d'achat. L'instance dirigeante s'assure qu'un régime disciplinaire est mis en place et que des sanctions adéquates soient prises en cas de faits de corruption.

Les moyens dédiés

L'AFA insiste sur le fait que la mise en œuvre d'un dispositif anticorruption nécessite des moyens humains et financiers proportionnés au profil de risque de l'entreprise, mis à disposition par l'instance dirigeante.

Les moyens mis en place doivent couvrir notamment l'équipe chargée de la conformité anticorruption, le recours à des conseils ou prestataires externes, le cas échéant, et la mise en place d'outils. La mise en place du dispositif anticorruption incombe à l'instance dirigeante et nécessite d'en déléguer la mise en œuvre opérationnelle à un responsable de la conformité anticorruption, désigné « responsable de la conformité ».

L'instance dirigeante s'assure que le responsable de la conformité dispose des moyens lui permettant de réaliser ses missions, de coordonner les fonctions concernées et de lui rendre compte. Elle veille à ce que le responsable de la conformité bénéficie à tout moment d'un accès à toute information utile à l'exercice de ses fonctions, d'une indépendance et d'un accès à l'instance dirigeante, afin d'en obtenir l'écoute et le soutien. Il est primordial que le responsable de la conformité entretienne un lien direct et régulier avec l'instance dirigeante, ainsi qu'un accès facilité au conseil d'administration. L'instance dirigeante s'assure que le responsable de la conformité dispose des compétences requises.

La mise en place d'une politique de communication interne et externe adaptée est au cœur du dispositif anti-corruption. L'entreprise doit communiquer largement sur sa politique de prévention et de détection de la corruption, auprès de l'ensemble de son personnel et partenaires extérieurs.

02

Les enjeux clés

- S’assurer que l’établissement applique les nouvelles recommandations de l’AFA
- Mener un diagnostic pour s’assurer de la conformité du dispositif
- Mettre en place une politique de tolérance zéro à l’égard de tout fait de corruption
- S’assurer que la cartographie des risques de corruption est exhaustive et à jour

Pour aller plus loin

Mise en conformité Sapin II : s’auto-évaluer en 50 questions

Projet DORA

De la gestion du risque opérationnel vers la résilience opérationnelle informatique

La place centrale et stratégique des systèmes d'information dans le fonctionnement du système bancaire (digitalisation des processus, robotisation, IA, etc.) expose l'ensemble des institutions financières à un risque informatique (ou numérique) croissant pouvant affaiblir leur résilience opérationnelle, notamment dans un contexte de cyber-attaques de plus en plus sophistiquées.

Ces attaques peuvent atteindre les systèmes internes, cas d'usage des rançongiciels (« ransomware ») ou atteindre des infrastructures externes endommageant les services interbancaires ou en ligne. Par ailleurs, la mise en commun croissante de ressources techniques et opérationnelles élargit et intensifie les impacts d'une détérioration ou interruption de service et en complexifie la gestion des risques.

Cette situation est renforcée par le recours à l'externalisation auprès de prestataires, qui parfois opèrent pour de nombreuses autres institutions et deviennent ainsi des vecteurs de contamination en cas d'incident. L'amélioration de la résilience opérationnelle nécessite une évolution de la règlementation pour accompagner les institutions dans la gestion de leurs risques opérationnels, et en particulier sur le plan informatique.

Dans ce sens, le projet de règlement de la commission européenne « DORA » – *Digital Operational Resilience Act* - a pour objectif d'améliorer la résilience opérationnelle informatique des acteurs financiers.

L'importance d'une gouvernance forte sous la responsabilité de la Direction est explicitement inscrite dans le projet de règlement (cf article 4). Ainsi, les enjeux de la Direction seront de s'assurer de la mise en place d'une gestion efficace des risques liés aux technologies (ICT) se traduisant en particulier par :

- la détermination du niveau de tolérance aux risques liés aux technologies ;
- l'approbation, la surveillance et la revue périodique de la politique de continuité des activités et du plan de reprise d'activité liés aux technologies ;
- la revue périodique des plans d'audit couvrant les risques informatiques ;
- l'approbation et le suivi des contrats d'externalisation de services TIC, notamment en cas de modification des conditions ;
- l'allocation et le suivi périodique des budgets pour répondre aux besoins de résilience opérationnelle informatique ;
- le suivi des incidents informatiques et leurs impacts, ainsi que les réponses apportées, les mesures de rétablissement et de correction.

S'agissant d'un projet, les discussions entre les différentes instances européennes aboutiront probablement à une version finale du règlement DORA au cours des 12 prochains mois. Toutefois, cette proposition de la Commission européenne s'inscrit dans la continuité des récentes publications de l'EBA et l'EIOPA*, et concourt à la création d'un cadre réglementaire unifié et dédié à la gestion des risques informatiques.

Ce nouveau texte renforce la prise en compte de la dimension risque dans le pilotage des systèmes d'information des institutions financières (yc les investissements) et nécessite l'industrialisation des reporting à destination du Management et du Régulateur.

*** EBA/GL/2019/04 et EIOPA-BoS-20/600**

03

Les enjeux clés

- La gestion des risques informatiques (ICT *risk management framework*)
- La déclaration des incidents majeurs liés aux technologies
- Les tests de résilience opérationnelle informatique
- La gestion du risque de tiers avec notamment la supervision directe des prestataires de services « critiques »

Pour aller plus loin

COVID-19 - Réduire les risques et gérer les urgences de cybersécurité

Le télétravail,
Cible des pirates informatiques

2020 aura vu éclore un grand nombre de phénomènes dont le recours massif au télétravail et cela quelque soit la géographie ou le secteur d'activité. Ce nouveau mode de travail a nécessité de la part des entreprises et de leur direction des systèmes d'information (SI) une agilité importante pour déployer ou augmenter les capacités de collaboration à distance. Certains établissements étaient déjà préparés – par exemple suite au mouvement de grèves de fin 2019 en France – quand d'autres n'avaient pas encore déployé massivement de solutions pour leurs collaborateurs.

Dès le début du confinement, une question centrale est apparue pour le télétravail : comment assurer le même niveau de sécurité à distance qu'au sein des établissements ?

Les collaborateurs des établissements bancaires ont été sollicités ou ont été victimes, comme les autres, par des groupes de pirates ou soumis au même type de menaces. La presse se fait l'écho au quotidien d'attaques réussies rendant souvent indisponible une partie du système d'information et des opérations.

Pourquoi ces risques ont-ils été démultipliés depuis mars ? Même si les collaborateurs bénéficient d'un environnement de travail sécurisé : utilisation d'un VPN entre le PC et le SI pour chiffrer les données dans les communications à travers Internet, sécurisation du poste de travail pour limiter l'accès aux clés USB, utilisation de la double-authentification pour l'accès aux transactions sensibles, par exemple, la faille réside toujours dans les faiblesses de l'utilisateur.

Le Financial & Stability Institut a, dès avril 2020, alerté les institutions financières sur le risque lié à la combinaison de la pandémie et de la forte mobilisation des collaborateurs en télétravail et sur la nécessité de rester vigilant face aux menaces. D'autres organisations, par exemple la NASA, on fait paraitre des alertes début Avril 2020, sur l'augmentation des attaques cyber à destination des collaborateurs en télétravail. En juillet 2020, L'agence de notation financière Moody's fait paraitre une note indiquant des hausses massives d'attaques à destination des banques et des tentatives d'accès ou de récupération de données personnelles.

La réponse, bien intégrée par de nombreux Directeurs de la Cybersécurité, est la poursuite des chantiers de sensibilisation et de formation des utilisateurs. En effet, l'ajout de mécanismes techniques de sécurité seuls ne serait être suffisant pour diminuer les risques. La réussite et la résistance face aux attaques cyber – notamment dans ces temps de forte utilisation du télétravail, restent la mobilisation des collaborateurs et leur sensibilisation.

04

Les enjeux clés

- Poursuivre les chantiers de sensibilisation des collaborateurs aux risques de cybersécurité avec un focus particulier sur les menaces en télétravail
- Augmenter les solutions ou les services de détection des attaques
- Identifier, en fonction des organisations, les menaces spécifiques à l'établissement
- Evaluer régulièrement la maturité de la cybersécurité au sein de la banque

Pour aller plus loin

Télétravail : 4 règles d'or pour limiter les risques d'intrusion et d'infection virale de vos réseaux

Rapport commun ACPR-AMF
Les engagements climatiques des institutions financières françaises

Essentiel

Lors de la réunion de la Place de Paris du 2 juillet 2019, les institutions financières françaises avaient pris des engagements **en faveur de la lutte contre le changement climatique et de l'objectif de neutralité carbone à l'horizon 2050**. Ils ont également décidé que chaque année, un rapport sera rédigé par l'ACPR et l'AMF afin d'analyser les actions qui ont été menées sur ce sujet et de fournir une évaluation des engagements pris et les conditions de leur mise en œuvre. La prise de conscience du rôle attendu du secteur financier s'illustre par une implication croissante des plus hauts niveaux de gouvernance des institutions financières françaises sur les sujets climatiques et dans les engagements pris, même si des défis importants subsistent pour leur mise en œuvre effective. Le premier rapport sur ces engagements a été publié le 18 décembre 2020.

Méthodologie de suivi des engagements adoptée par l'ACPR et l'AMF

Pour mener à bien ce suivi, **des engagements ont été définis concernant** :

- la politique interne et empreinte carbone de l'entité dont relèvent les engagements portant par exemple sur des objectifs de réduction de gaz à effet de serre (GES) ;
- les stratégies de sortie des énergies fossiles ;
- les engagements en faveur de financements et d'investissements verts ou d'assurances d'activités vertes ;
- les engagements actionnariaux et tout autre engagement d'accompagnement des acteurs ;
- les engagements en vue d'une réduction des émissions de GES ou de l'alignement sur les objectifs de l'Accord de Paris ;
- la transparence de l'information relative à la prise en compte des enjeux climatiques.

L'ACPR et l'AMF ont retenu **trois types d'acteurs financiers** pour cette étude : les groupes bancaires, les groupes d'assurance et les sociétés de gestion de portefeuille. Pour chaque acteur, un **questionnaire tenant compte de ses spécificités a été transmis**.

Panorama des engagements climatiques pris par les acteurs financiers de la Place de Paris

L'ACPR et l'AMF dénombrent plus de **deux cents engagements pris par les groupes bancaires et d'assurance français. Pour les sociétés de gestion, on dénombre plus d'une centaine d'engagements**. Ces nombres reflètent la **mobilisation de ces acteurs pour lutter contre les risques climatiques**. La plupart des engagements sont, d'ailleurs, dotés d'indicateurs chiffrés renforçant leur traçabilité. Cependant, **des difficultés apparaissent en matière de convergences des méthodologies**. En effet, des différences d'interprétation des engagements peuvent avoir lieu notamment sur les engagements relatifs à l'alignement de portefeuilles concernant la part verte des financements, des investissements ou des expositions, des mesures d'impact, et enfin du périmètre des activités couvertes (scopes, type d'actifs, type d'opérations, taux de couverture, etc.). De plus, **le niveau de précision et de pédagogie dans les informations fournies peut-être divergent** selon les entités.

Les acteurs financiers de la Place de Paris et les politiques « charbon »

Pour rappel, le charbon est, d'après l'Agence Internationale de l'Energie, **le combustible qui a le plus contribué au réchauffement climatique.** Les établissements bancaires et financiers ont décidé d'agir afin de **limiter leurs empreintes carbones et de parvenir à la neutralité carbone d'ici 2050.** Une analyse portant sur quatre volets a été réalisée par l'ACPR et l'AMF afin d'évaluer l'efficacité des politiques « charbon » menées par les différents acteurs :

- une **comparaison qualitative des politiques** en vigueur et publiées au 31 juillet 2020 (critères et seuils retenus, champ d'application, stratégie de sortie définie, gouvernance, moyens et processus mis en œuvre pour le suivi) ;
- une **évaluation de l'exposition des banques, assureurs et fonds français** au charbon thermique au 31 décembre 2019 : cette analyse, réalisée à partir des déclarations des institutions et de leur exposition aux émetteurs identifiés en particulier par la *Global Coal Exit List* (GCEL), vise à réaliser un premier état des lieux de l'exposition agrégée de la Place et son évolution ;
- une **étude ligne à ligne de certaines expositions des plus gros gérants afin de vérifier la mise en œuvre des politiques** et de comprendre les raisons expliquant la présence d'émetteurs liés au charbon thermique en portefeuille (selon les seuils retenus par la GCEL) ;
- une **analyse des stratégies de sortie et de désengagement** du charbon thermique, au regard des informations fournies par les acteurs de l'échantillon.

L'ensemble des établissements a fait part de **l'existence d'une politique consacrée au charbon**. L'ACPR et l'AMF soulignent les **difficultés à mesurer l'exposition au « charbon »** ainsi que le fait que les engagements portent presque exclusivement sur **le « charbon thermique » et non sur le « charbon métallurgique »**. Des préconisations ont été émises en fonction de la catégorie des établissements.

05

Les enjeux clés

- Faciliter la traçabilité et la fiabilisation des engagements
- Renforcer l'effectivité des engagements en définissant des objectifs chiffrés, un échéancier clairement défini et un suivi de l'avancement
- Renforcer la transparence et la comparabilité des indicateurs et des méthodologies retenus
- Associer la gouvernance des entités et impliquer les dispositifs de contrôle pour assurer le suivi des engagements pris
- Prendre en compte les risques liés à la perte de biodiversité dans leurs engagements et les déclinaisons opérationnelles au niveau des lignes d'activités

Pour aller plus loin

S'engager dans la transition écologique

Contacts

Matthieu Ribes
Associé Co-responsable Secteur Banque
matthieu.ribes@mazars.fr
+33 (0)1 49 97 69 75

Alexandra Kritchmar
Associée Co-responsable Secteur Banque
alexandra.kritchmar@mazars.fr
+33 (0)1 49 97 64 19

Émilie Legroux
Associée contrôle interne et conformité
emilie.legroux@mazars.fr
+33 (0)1 49 97 37 58

Contributeurs
Inès de Bonneval, Consultante ; Matthieu Duponchel, Associé Audit IT ; David Labella, Directeur Responsable de la veille réglementaire bancaire ; Émilie Legroux, Associée Contrôle interne et conformité ; Michael Lemoigne, Consultant Secteur Banque ; David Luponis, Associé Cybersécurité.

Mazars est un groupe international et intégré spécialisé dans l'audit, la fiscalité et le conseil ainsi que dans les services comptables et juridiques*. Présents dans plus de 90 pays et territoires à travers le monde, nous nous appuyons sur l'expertise de plus de 42 000 professionnels – plus de 26 000 au sein de notre partnership intégré et plus de 16 000 via « Mazars North America Alliance » – pour accompagner les clients de toutes tailles à chaque étape de leur développement.
*Dans les pays où les lois en vigueur l'autorisent.

www.mazars.fr

mazars