



Analyse prospective des métiers du risque et du contrôle dans la banque

3.1 Enjeux organisationnels, économiques et réglementaires

Les mutations s'accroissent dans le secteur bancaire, ce qui se traduit notamment par d'importantes réorientations stratégiques, des réorganisations d'activités et de processus. Les banques sont également victimes de nouveaux risques et doivent se doter de nouveaux métiers afin de maîtriser ces nouveaux enjeux.

Les métiers du Risque et du Contrôle dans la banque doivent faire face à de nouvelles problématiques, telles que la couverture du risque systémique, le développement du Cloud computing ou de la banque sur mobile (« le nomadisme technologique »), l'émergence des « class actions »⁵⁰, ...

⁵⁰ Actions de groupe : assignation de la banque par un groupe de clients



3.1.1 La couverture du risque systémique

Depuis Bâle I, la sécurité des opérations et plus largement, la gestion des risques se trouvent au cœur des préoccupations des banques et le risque systémique constitue un risque majeur. Afin d'assurer la pérennité du système bancaire et le préserver d'une crise systémique, la nouvelle réglementation Bâle III vient renforcer l'encadrement du risque systémique ⁵¹ en identifiant et en surveillant plus particulièrement des acteurs dits systémiques.

Les établissements bancaires qui ont une « importance systémique mondiale (EBIS) ⁵² doivent se conformer à toutes les exigences de Bâle III et doivent disposer d'une plus grande capacité d'absorption des pertes ». Ces banques doivent donc redéfinir le risque systémique, le mesurer et le contrôler.

Ainsi, les métiers du Risque et du Contrôle, au cœur de la stratégie des banques, vont devoir veiller à la prise en compte de ce risque dans le système glo-

bal de gestion des risques. Cette prise en compte ne donnera pas forcément lieu à la création d'une fonction dédiée. Il s'agit davantage d'une nouvelle dimension que les métiers du Risque et du Contrôle doivent appréhender (élargissement du domaine de compétence). En effet, ce sont des métiers qui doivent sans cesse se renouveler, s'adapter à un environnement de risque en perpétuel mouvement, afin d'éviter toute déperdition de maîtrise du risque.

A noter également, concernant le reporting à l'ACPR, que « dans une optique de prévention, les banques doivent lui fournir des plans de résolution établis à l'avance, qui leur permettent, en cas de difficulté, de se restructurer rapidement afin de préserver les activités critiques pour le financement de l'économie » (source ACPR).

3.1.2 Le «nomadisme technologique» et le Cloud computing

Les banques doivent faire face également à de nouveaux enjeux générés par le « nomadisme technologique » et le Cloud computing.

Le « nomadisme technologique » désigne l'évolution des techniques de l'information et de la communication qui tendent vers le tout numérique et spécifiquement vers un tout numérique «nomade». Sont ici visés, les possibilités de connexions à distance et des opérations qu'il est possible de réaliser. Ceci à partir de l'ensemble de différents supports (ordinateur portable, tablette numérique, smartphone). Ces connexions pouvant s'établir soit par une liaison filaire ou sans fil (principe même de la mobilité connectée).

La notion de « cloud computing » renvoie également à la mobilité connectée. Il s'agit de rendre accessible via un réseau de télécommunications, à la demande et en libre-service, des ressources informatiques partagées configurables.

Ces nouvelles technologies impliquent de nouveaux usages : pouvoir accéder aux informations numériques, les modifier, réaliser des transactions, quel que soit l'endroit où l'on se trouve. Pour le secteur bancaire, cette forme de nomadisme virtuel pose de nouvelles questions de sécurité, de confidentialité, de conformité des modalités de commercialisation...

⁵¹ CF. définition risque systémique au sein de la partie 1.3.1 Un environnement de risques de plus en plus marqué

⁵² EBIS : Etablissements bancaires avec une importance systémique

a/ Le nomadisme technologique

Les banques ont pris conscience de l'importance des technologies mobiles dans l'intégration de leurs activités. Le « nomadisme technologique » se manifeste à travers le développement des outils de communication du professionnel de la banque : tablette numérique, smartphone, micro-ordinateur, etc., a des impacts notoires pour la banque.

Les banques, dont l'activité est inéluctablement dépendante des systèmes d'information, se doivent d'évoluer au rythme des nouvelles techniques d'information et de communication. L'enjeu est de permettre aux salariés d'accéder à leur boîte mail professionnelle, à leur outils d'aide à la vente, de gestion, à tout moment et en tout lieu, de manière ponctuelle ou sans interruption, et ce en toute sécurité que ce soit pour les données consultées ou échangées. On comprend que cette sécurité peut être remise en cause par des attaques cybercriminelles.

b/ Le Cloud computing

Le Cloud computing est « un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients»⁵³.

En faisant appel à un prestataire de Cloud computing, la banque se trouve confronter à des risques spécifiques, tels que le risque d'atteinte à la confidentialité des données, l'indisponibilité des données, ... Le Cloud computing amène donc les banques à repenser leur sécurité informatique de manière holistique, au sein d'un environnement mutualisé, virtualisé, avec une informatique de

La communication et les offres proposées via ces modes de communication sont extrêmement normées et nécessitent un encadrement bien particulier. Ces nouveaux canaux de distribution exposent la banque à de nouveaux risques que ce soit en termes de connaissance client et de conseil ou encore de lutte contre le blanchiment et le financement du terrorisme.

La banque doit ainsi faire face à de nouveaux enjeux et de nouvelles contraintes de l'informatique mobile : terminaux variés et en perpétuelle évolution ; support et modes de connexion intermittents ; accès à toutes les informations de la banque (e-mail, applications métier, portail, applications spécifiques). Dans ce contexte de « nomadisme technologique », la sécurité des systèmes d'information s'intègre encore davantage dans le dispositif de gestion des risques global. Ceci afin d'assurer la sécurité des activités réalisées par l'ensemble des collaborateurs de la banque, mais également des transactions réalisées par les clients.

plus en plus développée vers le réseau. La banque devra prendre en compte ce risque généré par cette évolution informatique, « l'Informatique en nuage », en mettant en place des contrôles et des procédures visant à protéger l'intégrité des systèmes d'information de la banque, et leurs données sensibles (dont les exigences réglementaires en termes de confidentialité et de modalités de conservation sont fortes).

Les directeurs de la conformité se retrouvent de plus en plus interpellés par les Responsables de la Sécurité des Systèmes d'Information (RSSI) afin de traiter ensemble les problématiques soulevées par des projets de cloud computing ou de big data (utilisation de données non structurées issues d'internet ou de différentes natures de capteurs).

⁵³ Vocabulaire de l'informatique et de l'internet, publié au Journal Officiel de la République Française n° 129 du 6 juin 2010



C/ Le risque de cybercriminalité

Si les nouvelles technologies d'informations et de communication contribuent au développement des activités bancaires, elles en augmentent également l'exposition au risque de fraude, aux attaques informatiques malveillantes.

Ces nouvelles technologies ont permis de développer certaines méthodes : phishing⁵⁴, usurpation d'identité, piratage des applications des banques disponibles sur tablettes numériques ou smartphone... les réseaux internationaux des fraudes rivalisent d'imagination pour développer de nouvelles techniques de fraudes bancaires. Face au nombre croissant d'attaques piratages, les banques doivent rapidement s'adapter et renforcer leurs mesures de sécurité. Par exemple, pour les transactions sur Internet, certains sites marchands ne cryptent pas leurs données et par conséquent, celles-ci peuvent être interceptées. Si les clients désireux de faire leurs achats en ligne doivent faire preuve de bon sens, il revient à la banque de sécuriser ces transactions.

La cybercriminalité représente un coût, non seulement en termes de fraude, mais également en termes de charge interne pour la résolution des attaques. Les attaques, qu'elles relèvent d'une tentative de fraude ou d'un déni de service par l'exploitation d'une faille sur Internet provoquent une charge de gestion du risque importante. Si les attaques classiques par virus ou malware peuvent se régler en moins d'une semaine, les plus dangereuses, qui impliquent l'injection de codes malveillants ou la complicité interne, demandent plus d'un mois, une fois détectées, pour être résolues⁵⁵.

Ainsi, la gestion des risques liés à la cybercriminalité oblige la banque à renforcer ses forces vives, que ce soit d'un point de vue purement informatique, que comportementale comme l'est par exemple, l'analyse comportementale de la fraude à la monétique lors des paiements en ligne. Sur ce point, un métier spécifique voit progressivement le jour : le « fraud risk manager ». Son rôle vise à définir les scénarios de fraudes envisageables ou les comportements anormaux (« red flag »), à accompagner leur implémentation dans des systèmes dédiés et à investiguer les cas nécessitant une analyse approfondie avant un éventuel dépôt de plainte.

3.1.3 L'E-réputation

La cybercriminalité est également une problématique qui affecte l'image, la réputation des banques. Les cyber-attaques génèrent non seulement des dommages matériels, mais peuvent également impacter l'image et la réputation des banques. Ce phénomène ne cesse de prendre de l'ampleur depuis ces dernières années, aidé en cela par l'évolution des nouvelles technologies de l'information et de la communication. La perte de données confidentielles (objet d'une cyber-attaque) représenterait un coût conséquent, et une atteinte à la crédibilité des banques quant à leur capacité à assurer la confidentialité des informations détenues.

Au-delà des risques issus de la cybercriminalité, une banque mise en cause pour tout type de dysfonctionnement (ex : double prélèvement des paiements CB à débit différé) peut connaître une détérioration sensible de son image et subir un impact commercial important et durable en impactant directement la fidélité de ses clients.

L'e-réputation est une notion apparue depuis quelques années et fait référence à la représentation des banques que les internautes, qu'ils soient clients ou prospects, se constituent en fonction des flux d'informations qu'ils rencontrent sur internet.

⁵⁴ Le phishing consiste à envoyer des mails frauduleux de la part d'une banque (usurpation d'identité de la personne morale) et qui invitent à se connecter sur un site grâce à un lien hypertexte à partir duquel seront piratées des informations, dont les données bancaires. La méthode du pharming est plus élaborée que celle du phishing. L'utilisateur va saisir la bonne adresse mais va être redirigé sur un faux site. Comme pour le phishing, le pirate va avoir accès aux données confidentielles du client.

⁵⁵ Cf Revue Banque n°765

Le web social, joue un rôle de démultiplicateur des risques de réputation. En libérant la parole des collaborateurs, des experts, des journalistes et bien entendue des clients, la « Toile » démultiplie la probabilité d'une mise en cause publique de Banque.

Aussi, la maîtrise du risque de réputation et spécifiquement de l'e-réputation fait aujourd'hui partie du périmètre global de la gestion des risques,

nécessitant sa prise en compte par l'ensemble de ses acteurs. L'étude du CIGREF « Etude des risques et opportunités liés à l'e-réputation des entreprises » illustrent bien l'importance grandissante de la veille proactive sur sa réputation qui est aujourd'hui nécessaire. Les connexions entre la gestion des risques et la conformité et les nouvelles fonctions de « social media manager » ou « community manager » sont évidentes.

3.1.4 La position stratégique des métiers liés à la conformité face aux «class actions» à la française

Aujourd'hui, les banques doivent faire face à un enjeu réglementaire crucial : la protection de la clientèle. Les banques doivent répondre à des problématiques de conformité en matière de pratiques commerciales et plus particulièrement en matière de devoir de conseils.

Par exemple, un manquement, par le chargé de clientèle, le chargé d'affaires (communément appelé « le banquier ») à ses obligations précontractuelles, telles que le conseil en matière d'octroi de crédit, d'investissements financiers, peut aboutir à une assignation de la banque, non plus individuelle comme c'est encore le cas aujourd'hui, mais collectivement, par le biais d'actions de groupe, les « class actions »⁵⁶. Les « class actions » permettront à un grand nombre de clients, victimes d'un même préjudice, d'intenter une action en justice commune. L'objectif affiché est de permettre au «consommateur d'agir collectivement contre

des professionnels alors qu'ils n'auraient pas agi individuellement, du fait de la faiblesse des montants en jeu, du coût et de la lourdeur des procédures» (source : « Paroles d'experts », janvier 2014). Ces actions de groupe sanctionneront alors plus particulièrement les défauts de conformité ayant des incidences individuelles de faibles montants mais majorées à grande échelle. Ces actions de groupe pourront entraîner en outre des impacts en termes de dégradation de l'image de marque.

C'est pourquoi, les métiers du Risque et du Contrôle, en particulier les métiers liés à la conformité (responsable de conformité, chargé de conformité, ...) vont voir leur importance croître au sein des banques. En effet, le développement des métiers lié à la conformité offre une véritable opportunité aux banques pour les accompagner en termes de sécurité de l'activité et in fine de protection du client.

3.2 L'avenir des métiers du risque et du contrôle dans la banque

Les perspectives de carrière et d'évolution sont multiples : il est possible, soit d'évoluer au sein des lignes métiers Risque ou Finance, du Contrôle Interne ou de l'Audit, auprès du siège ou des entités du Groupe, soit de rejoindre les fonctions commerciales ou support, généralement à des postes à responsabilités. Ceci grâce à l'acquisition de la vision transverse et stratégique des activités de la banque.

Généralement de formation supérieure, (école de commerce, d'ingénieurs ou troisième cycle universitaire en Banque, Finance, Audit et/ou Comptabilité). Les professionnels des métiers du Risque et du Contrôle disposent d'expériences significatives acquises soit dans une autre famille de métiers du Risque et du Contrôle, soit par des fonctions « terrains » exercées dans les différentes activités de la banque.

⁵⁶ Les « class actions » à la française ou actions de groupe : un projet de loi adopté en 1ère lecture le 14 septembre 2013



3.2.1 L'avenir des métiers de l'Inspection générale et de l'Audit interne

Véritables fonctions de passage, ces métiers constituent un très bon vivier de potentiels pour de futurs postes d'encadrement, que ce soit dans des activités commerciales ou opérationnelles.

Dès lors, si l'on ne peut pas parler de croissance ou d'une tendance forte au recrutement pour ces métiers, le renouvellement est de fait, nécessaire et indispensable.

3.2.2 L'avenir des métiers du risque

Contrairement aux métiers d'audit interne (Inspection générale comprise), les métiers liés à la gestion des risques ont tendance à se spécialiser de plus en plus. C'est le cas notamment pour les analystes de risque (tout type de risque confondu). Les banques s'inscrivent dans une démarche de spécialisation, de renforcement de l'expertise des filières risques

ce qui les amène à poursuivre leur recrutement, mais de façon plus ciblée.

Les fonctions du risque et les fonctions d'audit interne se rejoignent dans leur développement à l'international avec l'anglais comme langue quasi-obligatoire.

3.2.3 L'avenir des métiers liés à la conformité

Les métiers liés à la conformité sont en développement au sein des banques aujourd'hui. Ce métier a considérablement évolué au fil des évolutions réglementaires. Cette fonction fait partie des postes à pourvoir dans le cadre du déploiement de la filière conformité et de sa spécialisation de plus en plus forte par métier. Les chiffres en témoignent : les métiers de la conformité, pris au sens large, représentent environ 5% des effectifs des banques ⁵⁷.

Les banques ont le choix aujourd'hui entre deux profils :

- des profils « seniors » ayant une réelle expertise dans le domaine de la conformité et une véritable appétence pour ce métier ;
- des profils « juniors » ayant fait ce choix de métier en suivant une formation via des masters spécialisés dédiés aux problématiques de conformité ⁵⁸.

3.2.4 Les métiers du Risque et du Contrôle face à la lutte contre le blanchiment de capitaux et le financement du terrorisme

Face à l'évolution des textes réglementaires encadrant la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), les banques doivent aiguïser leur capacité à identifier leurs clients et à parfaire la connaissance qu'elles en ont (profilage). Pour ce faire, le Responsable Conformité fait appel à un réseau de correspondants spécifiquement dédiés aux processus de connaissance

client (KYC ⁶⁰). Un nouveau métier est donc en train de prendre forme, celui d'« Analyste KYC ». L'analyste KYC est en charge notamment de la mise en place de nouveaux Workflow KYC. Ils complètent les informations collectées par les commerciaux et procèdent à des recherches complémentaires selon le niveau de risque pressenti en ayant recours à des outils d'analyse spécifiques.

⁵⁷ Estimations du Centre de formation de la profession bancaire

⁵⁸ CF. ANNEXES - Fiches métiers – La famille professionnelle « Conformité »

⁵⁹ « KYC » pour Know Your Customers : Connaître son client

3.3 L'attractivité des métiers du Risque et du Contrôle

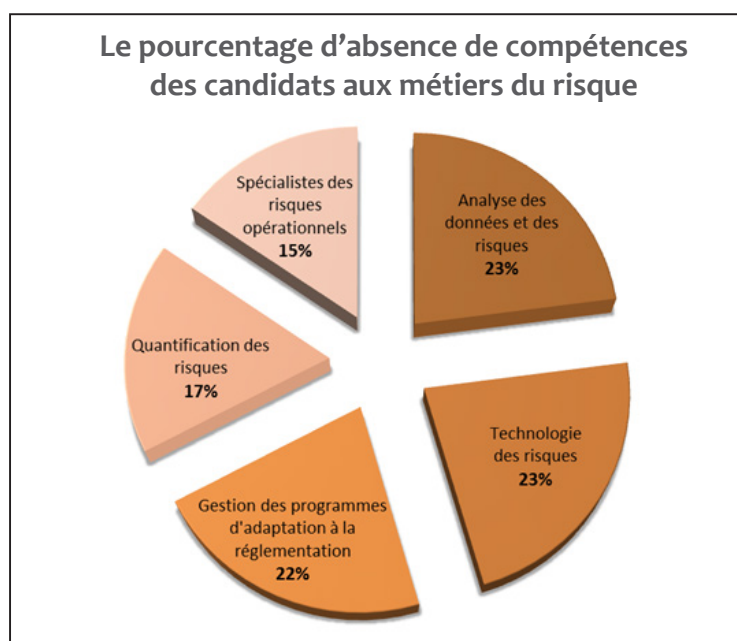
L'éventail de métiers de la banque, en particulier les métiers du Risque et du Contrôle, est en constante évolution sous l'influence de l'évolution de l'activité, des réglementations, du progrès technologique.

Les contrôles s'intensifient, des métiers se spécialisent et de nouveaux métiers se développent au sein des banques afin de répondre à ces nouveaux enjeux.

3.3.1 Les métiers du risque en «vogue» au sein des banques

Dans une économie réglementée en perpétuel changement, avec de nouvelles exigences telles que Bâle III, les banques, sont à la recherche de nouvelles compétences en matière de gestion des risques et continuent de recruter.

Mais une vraie difficulté réside : un candidat sur deux ne répond pas au profil attendu par les banques. Les banques ont en effet constaté une vraie carence pour certaines compétences⁶⁰ :



Source : Etude mondiale « Risk Management for an Era of Greater Uncertainty », Accenture, 2013

Même si certaines compétences sont toujours recherchées, les banques ont augmenté leurs investissements dans la gestion des risques et ne cessent de recruter des Responsables des risques. Les chiffres en témoignent : le pourcentage d'entreprises ayant pourvu ce poste représentait 78% en 2011 contre 96% en 2013. La gestion et la maîtrise des risques sont fondamentales pour la survie

des banques. Ainsi, l'implication du directeur des risques, appelé aussi Risk Manager, est essentielle dans la mise en œuvre d'une gestion globale des risques au sein de la banque. C'est un acteur clé dans la mesure où il permet de diffuser plus largement la culture de la gestion des risques dans le groupe bancaire.

⁶⁰ CF. Etude mondiale « Risk Management for an Era of Greater Uncertainty », Accenture, 2013



3.3.2 Les facteurs d'évolution des métiers du Risque et du Contrôle

Depuis quelques décennies déjà les métiers du Risque et du Contrôle évoluent en s'adaptant à l'activité des banques et aux grandes tendances plus générales des métiers du risque comme l'approche ERM.

Sans prendre le risque de se tromper, nous pouvons affirmer qu'un certain nombre de facteurs vont contribuer demain à la poursuite de ces évolutions.

a/ Les facteurs d'évolution économique

Les périodes de difficultés économiques rendent les acteurs bancaires particulièrement sensibles. Les marges se réduisent face à une concurrence plus forte. Or, une meilleure maîtrise des risques permet une meilleure maîtrise du coût du risque et donc des marges. Par ailleurs, ce contexte économique laisse moins de droit à l'erreur.

Aussi, la maîtrise de ses processus, un contrôle interne solide et une conformité des produits permettent d'éviter nombre de pertes opérationnelles.

C'est en cela que les métiers du risque et du contrôle sont également amenés à se renforcer en période de non-croissance.

b/ Les facteurs réglementaires

Pour se conformer, s'adapter à l'élargissement et à la complexification toujours plus forte du terrain réglementaire sur lequel les banques exercent leurs activités, contexte associé à une évolution toujours plus sophistiquée des produits et services proposés, elles se doivent de renforcer leurs compétences en matière de gestion des risques.

La banque est donc dans l'obligation d'accroître ses effectifs dédiés à la gestion du risque avec des compétences techniques renforcées (maîtrise de la réglementation bancaire, des techniques de contrôle interne, de l'évaluation des risques, ...). C'est notamment le cas des métiers liés à la conformité.

c/ Les évolutions technologiques

Comme précisé en amont, les évolutions technologiques, notamment celles portant sur les nouvelles technologies de l'information et de la communication et la dématérialisation de la relation client/banquier via la banque à distance, amènent de facto, à une refonte du panel des métiers du Risque et du Contrôle.

La banque est donc dans l'obligation d'accroître ses effectifs dédiés à la gestion du risque avec des compétences techniques renforcées (maîtrise de la réglementation bancaire, des techniques de contrôle interne, de l'évaluation des risques, ...). C'est notamment le cas des métiers liés à la conformité.

Les risques générés par ces nouvelles technologies sont principalement juridiques, financiers et opérationnels. En effet, les banques, comme c'est le cas dans une relation directe, doivent s'assurer de la capacité de leurs clients à effectuer les opérations proposées sur le site (condition d'âge ou de capa-

Face à l'émergence de ces nouveaux risques, la banque à recourt à des profils davantage spécialisés ou étendent les domaines de compétences des fonctions existantes.