ifaci

institut français de l'audit et du contrôle internes

Cahier de la Recherche

De la cartographie des risques au plan d'audit

Réalisé par le Groupe Professionnel Banque

L'IFACI est affilié à The Institute of Internal Auditors

Dans la même collection

- **La cartographie des risques – 2ème édition,** Groupe Professionnel « Assurance » *(septembre 2013)*
- **L'audit du versement des subventions aux associations,** Groupe Professionnel « Collectivités Territoriales » *(février 2013)*
- **Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet,** Unité de Recherche Informatique IFACI *(décembre 2012)*
- **L'accès et la conservation des dossiers relatifs aux missions d'audit,** Unité de Recherche IFACI *(octobre 2012)*
- **La délégation de gestion en assurance de personnes : pistes pour un contrôle interne efficace,** Unité de Recherche IFACI *(juin 2012)*
- **Les variables culturelles du contrôle interne,** Unité de Recherche IFACI *(décembre 2011)*
- **Des clés pour la mise en œuvre et l'optimisation du contrôle interne,** Unité de Recherche IFACI *(octobre 2011)*
- **Transposition des normes professionnelles de l'audit interne et bonnes pratiques : Edition spéciale Administrations d'Etat,** Groupe Professionnel « Administrations de l'Etat » *(septembre 2011)*
- **Transposition des normes professionnelles de l'audit interne et bonnes pratiques : Edition spéciale Collectivités Territoriales,** Groupe Professionnel « Collectivités territoriales » *(avril 2011)*
- **La fraude : Comment mettre en place un dispositif de lutte contre la fraude ?** Unité de Recherche de l'IFACI *(décembre 2010)*
- **La création de valeur par le contrôle interne,** Unité de Recherche de l'IFACI *(octobre 2010)*
- **Prise de Position du Groupe Professionnel Banque pour un urbanisme du contrôle interne efficient,** Groupe Professionnel « Banque » *(Avril 2010)*
- **L'audit de la fraude dans le secteur bancaire et financier,** Unité de Recherche de l'IFACI *(janvier 2010)*
- **Création et gestion d'une petite structure d'audit interne,** Unité de Recherche IFACI *(janvier 2009)*
- **Une démarche d'audit de plan de continuité d'activité,** Unité de Recherche IFACI *(juillet 2008)*
- **Guide d'audit du développement durable : comment auditer la stratégie et les pratiques de développement durable ?,** Unité de Recherche IFACI *(juin 2008)*
- **Contrôle interne et qualité : pour un management intégré de la performance,** Unité de Recherche IFACI *(mai 2008)*
- **Evaluer et développer les compétences des collaborateurs,** Antenne régionale Aquitaine IFACI *(novembre 2007)*
- **Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement – 2ème Edition,** Groupe Professionnel « Banque » *(janvier 2007)*
- **L'audit interne et le management des collectivités territoriales,** Unité de Recherche IFACI *(mai 2006)*
- **Une démarche de management des connaissances dans une direction d'audit interne,** Unité de Recherche IFACI *(mai 2006)*
- **L'auto-évaluation du contrôle interne,** Unité de Recherche IFACI *(octobre 2005)*
- **Cartographie des Risques,** Groupe Professionnel « Immobilier Locatif » *(septembre 2005)*
- **Étude du processus de management et de cartographie des risques,** Groupe Professionnel « Industrie et commerce » *(janvier 2004)*
- **Pour un bon audit du dispositif de lutte contre le blanchiment des capitaux,** Groupe Professionnel « Banque » *(février 2004)*
- **L'efficacité des Comités d'audit – Les meilleures pratiques,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Gouvernement d'entreprise et Conseil d'administration,** PwC – The IIA Research Foundation – Traduction IFACI – PwC *(mai 2002)*
- **Évaluation de la compétence dans la pratique de l'audit interne,** Prise de position de l'ECIIA – Traduction IFACI *(2001)*
- **Management des risques,** IIA UK – Traduction Unité de Recherche IFACI *(2001)*
- **Le rôle de l'auditeur interne dans la prévention de la fraude,** Prise de position de l'ECIIA – Traduction IFACI *(2000)*

Pour plus d'informations : www.ifaci.com

Remerciements

L'IFACI tient tout particulièrement à remercier toutes les personnes qui ont contribué aux différentes étapes de ce cahier :

- **Conception et rédaction :**
  Bruno BURESI, *Inspecteur principal, Barclays*
  Christophe DEBOUDT, *Directeur de l'audit, Groupe COFIDIS Participations*
  Edwige DUTERRAGE-BAUDIN, *Responsable du pôle Ressources & prospectives, La Banque Postale*
  Isabelle FALET-MANGIN, *Auditeur senior, Groupe COFIDIS Participations*
  Benjamin HACKNEY, *Auditeur interne, CDC*
  Christiane LEGAT, *Directeur de l'audit interne, GE Corporate Finance Bank, Animateur de l'unité de recherche*
  Vincent LUNEAU, *Responsable audit filiales, Crédit Foncier*
  Christian MASCLE-ALLEMAND, *Inspecteur principal, BPCE*
  Arlette RAIMBAULT, *Chargée des affaires internes et de l'appui aux missions, Pôle Ressources & prospectives, La Banque Postale*
  Frédéric SERVRANCKX, *Responsable du Risk Assessment, Direction du Contrôle périodique, Société Générale*
  Beatrice VEDRENNE-ROBSON, *Directeur de l'Inspection générale, Barclays*

- **Comité de rédaction composé de :**
  Annie BRESSAC, *Consultante*
  Christophe DEBOUDT, *Directeur de l'audit, Groupe COFIDIS Participations*
  Benjamin HACKNEY, *Auditeur interne, CDC*
  Béatrice KI-ZERBO, *Directeur de la Recherche, IFACI*
  Christiane LEGAT, *Directeur de l'audit interne, GE Corporate Finance Bank*
  Christian MASCLE-ALLEMAND, *Inspecteur principal, BPCE*

- **Relecture :**
  Groupe Professionnel « Banque » de l'IFACI présidé par **Frédéric GEOFFROY,** *Responsable de l'audit interne, Banque de financement et d'investissement de la Société Générale (SGCIB) et directions fonctionnelles.*

- **La révision a été assurée par :**
  Julie FERRE, *Chargée de projets Recherche, IFACI*

Philippe MOCQUARD, *Délégué Général, IFACI*

Sommaire

Introduction **7**

1- Pourquoi une cartographie des risques par l'audit interne ? **9**

1.1- Les exigences et attentes des parties prenantes 11

1.1.1- Les exigences des régulateurs 11

1.1.1.1- Les exigences relatives à la cartographie globale des risques 11

1.1.1.2- Des cartographies de risques spécifiques 17

1.1.2- Les attentes des organes de gouvernance 19

1.2- Bénéfices attendus de la cartographie des risques par l'audit interne 20

1.2.1- Un outil pour répondre aux exigences des Normes Professionnelles de l'Audit Interne 20

1.2.2- Une réponse à d'autres besoins 20

2- L'établissement d'une cartographie des risques exhaustive **23**

2.1- Choix méthodologiques 24

2.1.1- Périmètre et granularité de la cartographie 24

2.1.1.1- Principe de l'exhaustivité du périmètre à couvrir 25

2.1.1.2- Granularité de la cartographie 25

2.1.1.3- Les différentes approches 26

2.1.2- Nature des risques à couvrir 27

2.2- Réalisation de la cartographie des risques 28

2.2.1- Sources d'information pour l'audit interne 29

2.2.1.1- Les directions fonctionnelles 30

2.2.1.2- Les organes de gouvernance et les comités techniques 31

2.2.1.3- Les autres cartographies existantes 34

2.2.1.4- La prise en compte des résultats du contrôle permanent 36

2.2.2- Analyse et évaluation des risques 37

2.3- Mise à jour de la cartographie 38

2.3.1- Périodicité 39

2.3.2- La prise en compte des résultats des audits réalisés en cours d'année 39

3- De la cartographie des risques au plan d'audit 41
3.1- Pourquoi un plan d'audit ? 42
3.1.1- Une nouvelle recommandation 42
3.1.2- Une exigence réglementaire 42
3.1.3- Une norme professionnelle 43
3.1.4- Une saine pratique de gestion 43
3.2- Autres contributions au plan d'audit 43
3.3- Passage de la cartographie des risques au plan d'audit 45
3.3.1- Exigence préalable 45
3.3.2- Etapes successives 45
3.4- Communication du plan d'audit et des résultats de la cartographie 47

Conclusion 49

Glossaire 51

Annexes 55
Annexe 1 : Extraits du Règlement CRBF 97-02 56
Annexe 2 : Prudential sourcebook for Banks, Building Societies and Investment Firms 60
Annexe 3 : International convergence of capital measurements and capital standards 62
Annexe 4 : Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing 63
Annexe 5 : Convergence internationale de la mesure et des normes de fonds propres 64
Annexe 6 : Exemple de Fiche d'objet auditable 68

Bibliographie 71

Avertissement aux lecteurs

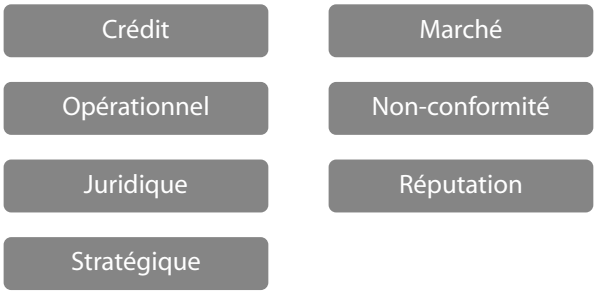
Ce cahier de la recherche a été réalisé à partir de contributions de professionnels de l'audit et du contrôle internes. Ce travail collectif, réalisé sous l'égide de l'IFACI, fournit un état des lieux des pratiques professionnelles et des pistes d'amélioration qui n'engagent pas les établissements représentés.

ISBN : 978-2-915042-53-5 – ISSN : 1778-7327

Introduction

Le terme de « cartographie » est couramment associé à la notion de risques. Utilisé dans des domaines aussi variés que la géopolitique (cartographie des risques pays), la météorologie ou la santé publique, la cartographie est naturellement très présente dans l'univers bancaire, où le risque constitue le cœur de métier.

A l'heure de la mondialisation des marchés de capitaux, le terme d'établissement de crédit, comme celui de banque, recouvre une multitude d'activités. L'image traditionnelle de l'agence de quartier n'est plus suffisante pour traduire l'étendue des activités désormais concernées. Sous la dénomination d'établissement de crédit, on trouve des organisations complexes, souvent internationales, qui regroupent des succursales, des filiales, éventuellement soumises à des réglementations différentes, et qui font appel à des prestataires externes. Toutefois, même si les activités financières sont soumises à un nombre important de risques, ces derniers peuvent être regroupés au sein d'un nombre restreint de catégories. Par exemple, l'unité de recherche a retenu la nomenclature ci-après.



Un des apports de la cartographie des risques est qu'elle constitue une grille de lecture commune, qui peut être reprise aussi bien dans les politiques du Groupe que dans les descriptions de l'environnement de contrôle de chaque filiale et succursale.

Pour le contrôle périodique, elle revêt une importance capitale pour la définition du programme de chaque mission, ainsi que pour l'élaboration du plan d'audit. En effet, les normes professionnelles de l'audit interne[1] demandent que le plan d'audit soit fondé sur une évaluation des risques.

La réglementation ne fournit pas de cadre méthodologique, et encore moins de « modèle » de cartographie des risques. De même, elle n'impose pas explicitement à l'audit interne de réaliser une cartographie des risques.

[1] *Cadre de Référence International des Pratiques Professionnelles de l'audit interne, IIA-IFACI, 2013*

L'objectif de ce cahier de la recherche est de présenter ***pourquoi et comment***, au sein des banques représentées dans le groupe de travail, la cartographie des risques élaborée par l'audit interne peut constituer un outil efficace pour l'élaboration du plan d'audit.

Précisons que ces travaux ont été inscrits dans ***le contexte du seul métier bancaire,*** et excluent donc les activités d'assurances.

Soulignons également que ce cahier traite de la ***cartographie des risques établie par l'audit interne.*** Au-delà de la volonté de respecter le principe d'indépendance de la fonction, la cartographie des risques mise en œuvre par l'audit interne présente des spécificités qui la distinguent de celles élaborées par d'autres fonctions telles que la direction des risques ou de la conformité.
En effet :

- le périmètre doit être global, voire exhaustif ;
- la granularité de l'analyse doit correspondre à la « maille » des objets auditables et des missions ;
- la périodicité et le niveau de l'évaluation peut différer de ceux requis par une surveillance permanente.

Le groupe de travail a été lancé en avril 2012. Au-delà des réglementations bancaires, il s'est appuyé sur :

- Les référentiels COSO *(« Committee of Sponsoring Organization of the Treadway Commission »)* en matière de gestion des risques et de contrôle interne, notamment la composante « Evaluation des risques ».
- Les normes professionnelles de l'audit interne (Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne).

L'ambition du cahier est de mettre en évidence les bénéfices d'une cartographie des risques réalisée par l'audit interne et de proposer des bonnes pratiques pour son élaboration et son utilisation.

- la première partie analyse les exigences réglementaires et les attentes auxquelles la cartographie des risques permet de répondre ;
- la deuxième partie développe l'approche méthodologique que l'audit interne peut mettre en œuvre pour construire une cartographie des risques exhaustive ;
- la troisième partie précise comment l'on s'appuie sur la cartographie pour élaborer le plan d'audit.

Partie 1

Pourquoi une cartographie des risques par l'audit interne ?

La cartographie des risques est une démarche dynamique d'identification et d'évaluation des risques qui permet d'en donner une représentation synthétique et visuelle. Elle constitue ainsi un outil de mise en évidence des risques à couvrir en priorité.

Définition proposée par l'unité de recherche

Le périmètre potentiel des risques bancaires génériques est bien connu : risque de crédit, risque de marché et risque opérationnel (fraude, sécurité au travail, pratiques commerciales, dommages aux actifs physiques, interruption de l'activité et lacune de traitement des transactions, etc.). L'exercice de cartographie doit permettre d'analyser leurs causes, leurs conséquences potentielles, et d'en évaluer l'impact et la probabilité de survenance.

Cette démarche est complexe. Elle soulève en effet des questions :

- de méthode, comment définir :
  - le « catalogue des risques »,
  - le degré de granularité,
  - les conventions de description,
  - les échelles de cotation
  - etc.
- de forme, quelle(s) représentation(s) retenir :
  - tableau,
  - axes de la carte,
  - diagrammes,
  - etc.
- de finalité, comment arbitrer, articuler les différents objectifs de la cartographie des risques :
  - outil de pilotage de l'organisation ou d'une activité, elle est aussi le point d'entrée des démarches d'audit et de contrôle interne,
  - comment répondre à différentes exigences ou attentes des parties prenantes ; en particulier des régulateurs, et des organes de gouvernance.

L'audit interne peut lui-même mettre en œuvre sa propre démarche de cartographie des risques afin de disposer d'un outil :

- qui lui permette de répondre aux exigences des Normes Professionnelles de l'audit interne liées à la planification de ses activités ;
- qui soit adapté aux caractéristiques de sa mission et en particulier à son indépendance.

1.1 Les exigences et attentes des parties prenantes

1.1.1 Les exigences des régulateurs

Dans l'environnement bancaire, la cartographie des risques résulte d'obligations règlementaires. Pour un établissement de droit français, il s'agit notamment :

- du règlement CRBF 97-02 modifié, en tant qu'établissement de crédit opérant sur le territoire français ;
- des textes émanant du comité de Bâle.

Certaines réglementations étrangères apportent des éclairages complémentaires qui, s'ils ne s'appliquent pas obligatoirement aux entités intervenant à France, peuvent constituer des bonnes pratiques. A titre d'exemple, il est intéressant de prendre connaissance :

- des dispositions de la Financial Services Authority (FSA), applicables aux établissements succursales d'une banque britannique ;
- des exigences de la Réserve fédérale américaine (FED) applicables aux sociétés américaines installées en France.

1.1.1.1 Les exigences relatives à la cartographie globale des risques

1.1.1.1.1 La vision du règlement CRBF 97-02 : la cartographie des risques comme pilier du dispositif de contrôle

La cartographie des risques est explicitement évoquée dans l'article 17 (Cf. annexe 1) du règlement CRBF 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement. Cet article fondateur constitue le corps du titre IV relatif aux systèmes de mesure des risques et des résultats. Nous en citons ci-dessous le début :
« Les entreprises assujetties mettent en place des ***systèmes d'analyse et de mesure des risques*** *en les adaptant à la nature et au volume de leurs opérations afin d'appréhender les risques de différentes natures auxquels ces opérations les exposent, et notamment les risques de crédit, de marché, de taux d'intérêt global, d'intermédiation, de règlement et de liquidité ainsi que le risque opérationnel ».*

L'arrêté du 19 janvier 2010 modifie le règlement CRBF 97-02 en y insérant les articles 17 quater et 17 quinquies ci-dessous qui le rendent encore plus explicite sur le sujet de la cartographie :
Article 17 quater
« Les entreprises assujetties mettent en place des systèmes et procédures permettant d'appréhender globalement l'ensemble des risques associés aux activités bancaires et non bancaires de l'établissement, notamment de crédit, de marché, de taux d'intérêt global, d'intermédiation, de règlement, de liquidité et opérationnels.

Les systèmes et procédures doivent permettre aux établissements de disposer d'une ***cartographie des risques*** *qui identifie et évalue les risques encourus au regard de facteurs internes (notamment la complexité de l'organisation, la nature des activités exercées, le professionnalisme des personnels et la qualité des systèmes) et externes (notamment les conditions économiques et les évolutions réglementaires). Cette cartographie :*

a) Prend en compte l'ensemble des risques encourus ;

b) Est établie par entité et/ou ligne de métier, au niveau auquel est exercée, le cas échéant, la surveillance consolidée ou complémentaire ;

c) Evalue l'adéquation des risques encourus par rapport aux orientations de l'activité ;

d) Identifie les actions en vue de maîtriser les risques encourus, par :

- *Le renforcement des dispositifs de contrôle permanent ;*
- *La mise en œuvre des systèmes de surveillance et de maîtrise des risques définis au titre V ;*
- *La définition des plans de continuité de l'activité prévus à l'article 14-1. »*

Article 17 quinquies

« L'ensemble des systèmes visés aux articles 17 à 17 quater doivent faire l'objet d'une ***actualisation et d'une évaluation régulières****. »*

La cartographie évoquée ici est un croisement dynamique des risques-clés par rapport au contexte de l'organisation traitée, c'est-à-dire son marché, ses activités et ses processus. Il s'agit ici de mener une réflexion de fond destinée à poser à plat les risques susceptibles de toucher l'organisation. C'est un travail lourd et minutieux. En effet, il ne s'agit pas d'une simple analyse prospective.

La règlementation détaillée dont fait l'objet le secteur financier offre une première base de travail utile pour aborder le chantier d'une cartographie : les risques-clés sont connus et d'ailleurs cités dans le règlement CRBF 97-02.

La cartographie des risques est par ailleurs directement suggérée dans trois autres articles comme un outil central du dispositif de traitement des risques liés à l'activité bancaire :

N° article	Mention associée	Explications
1	*« […] Ce contrôle interne comprend notamment :* *a) un système de contrôle des opérations et des procédures internes,* *b) une organisation comptable et du traitement de l'information,* *c) des* ***systèmes de mesure des risques*** *et des résultats,* *d) des systèmes de surveillance et de maîtrise des risques,* *e) un système de documentation et d'information,* *f) un dispositif de surveillance des flux d'espèces et de titres. […] »*	**La cartographie est évoquée implicitement ici à travers sa finalité d'appui à la maîtrise progressive des risques.**
10	*« **Les entreprises assujetties s'assurent que le système de contrôle s'intègre dans l'organisation, les méthodes et les procédures de chacune des activités** et que les dispositifs mentionnés au b de l'article 6 s'appliquent à l'ensemble de l'entreprise, y compris ses succursales, ainsi qu'à l'ensemble des entreprises contrôlées de manière exclusive ou conjointe. »*	La couverture exhaustive de la cartographie et la nécessité de ses interactions avec les processus opérationnels de l'organisation sont mentionnées ici.
26	*« Pour la mesure des risques de marché, les entreprises assujetties veillent à appréhender de manière complète et précise* ***les différentes composantes du risque****.[...] »*	Nouveau rappel de la couverture exhaustive de la cartographie. C'est l'un des rôles de la cartographie que d'offrir une vision synthétique des différentes composantes du risque de marché (risque de pertes encourues en cas d'évolution défavorable des prix ou des paramètres de marché (taux, actions, marges de crédit et change) affectant le portefeuille de négociation, risque de taux d'intérêt global, risque de liquidité, risque de règlement, risque d'intermédiation.) (cf. partie 2.1.2).

1.1.1.1.2 Les préconisations du comité de Bâle

Les exigences du règlement CRBF 97-02, notamment suite aux différents arrêtés de 2009 et 2010 (Cf. annexe 6), ont adopté, voire renforcé, certaines des préconisations du Comité de Bâle, relatives à la mesure des risques, et plus ou moins explicitement à la cartographie des risques. En effet, le dispositif d'adéquation des fonds propres, adopté par le Comité de Bâle en juin 2004[1], prévoyait une couverture plus complète des risques bancaires et incitait les établissements à améliorer leur gestion interne des risques.

[1] *L'accord sur la convergence internationale de la mesure et des normes de fonds propres, dit « Bâle II » a été transposé en droit communautaire par les directives 2006/48 et 2006/49 du 14 juin 2006 applicable dans les pays européens à partir de 2007.*

Le dispositif « Bâle II » repose sur trois piliers :

- une exigence minimale de fonds propres que chaque banque devra respecter afin de couvrir le risque de crédit, les risques de marché et le risque opérationnel générés par ses activités ;
- une surveillance prudentielle individualisée adaptable selon le profil de risque des établissements ;
- de nouvelles exigences en matière de communication financière.

La validation des approches internes de mesure des risques est l'un des enjeux majeurs de la mise en œuvre de Bâle II. La cartographie des risques apparaît ici encore comme un outil indispensable de réponse à la règlementation. En effet, c'est elle qui donne l'une des meilleures visions des risques et de leurs interactions dans l'entreprise.
Nous voyons que l'accord de Bâle II a explicitement visé les trois grandes catégories de risques suivants :

- crédit
- marché
- opérationnel

La cartographie des risques (désignée sous le terme *risk mapping*) est évoquée en tant qu'outil pour circonscrire spécifiquement le risque de crédit. Il est attendu que le processus de cartographie *(mapping process)* aboutisse à une pondération des risques cohérente avec le niveau de risque de crédit :
« Il incombe aux autorités de contrôle d'affecter les évaluations des OEEC[1] reconnus aux pondérations existantes dans le cadre de l'approche standard, c'est-à-dire d'établir à quelle pondération correspond chaque catégorie d'évaluation de crédit. Cette mise en correspondance doit être objective et faire coïncider de façon cohérente la pondération et le niveau de risque de crédit indiqué dans les tableaux ci-dessus, et ce pour toute l'échelle des pondérations. »[2] (cf. annexe 3)

La construction effective de la cartographie fait par ailleurs l'objet de l'annexe 2 du texte du Comité de Bâle, (cf. annexe 5) intitulée : « Standardised Approach – implementing the mapping process ». Les travaux de pondération des risques traités dans la cartographie y font l'objet d'un développement spécifique. Les textes du Comité de Bâle attachent en effet une importance particulière à la pondération des risques, appelant ainsi à en préciser l'analyse. Il ne suffit pas de dresser une liste des risques auxquels il est estimé que l'organisation est soumise, il faut également classer ces risques les uns par rapport aux autres.

La publication en décembre 2010 par le comité de Bâle des accords dits « Bâle III » entraîne des évolutions significatives suivantes par rapport à l'ancien texte :

- amélioration de la qualité des fonds propres ;
- renforcement du niveau des fonds propres ;

[1] *Organisme Externe d'Evaluation de Crédit*
[2] *Paragraphe 92 de Bâle II – Convergence Internationale de la mesure et des normes de fonds propres, Comité de Bâle, juin 2006*

- maîtrise de l'effet de levier (maîtrise de la croissance des bilans) ;
- amélioration de la gestion de la liquidité (à court et long terme) ;
- couverture des risques du portefeuille de négociation.

Loin de remettre en cause l'importance de la cartographie des risques, Bâle III en souligne au contraire l'intérêt en insistant sur les risques fondamentaux des organisations bancaires (risque en fonds propres, risque de liquidité, de portefeuille). Ils fournissent également des outils permettant d'en accroître la précision (ratios de liquidité court/long terme) et vont dans le sens d'une amélioration du contrôle du risque de contrepartie. Ils appellent finalement à une analyse plus fine, plus poussée dans la réalisation de la cartographie.

1.1.1.1.3 La vision de la FSA[1] : la cartographie des risques comme outil d'analyse initial

La cartographie des risques est clairement évoquée dans le FSA Handbook.

- Dans le chapitre 6 du *Prudential sourcebook for Banks, Building Societies and Investment Firms* relative au risque opérationnel, les points § 6.4.10 et § 6.4.11 (Cf. annexe 2) invitent à la construction d'une cartographie. Ils exigent le développement et la formalisation des politiques et critères spécifiques pour cartographier les processus métiers et activités dans le cadre de l'approche standardisée.

La compréhension des mécanismes d'affaires, c'est-à-dire des processus, des marchés et des environnements économiques, est un préalable nécessaire à la constitution d'une cartographie solide et durable dont la vision est sous-jacente à la proposition du FSA Handbook.
Ce texte donne par ailleurs des clés pour amorcer la construction effective de la cartographie. En particulier, il indique que toutes les activités doivent être cartographiées par lignes métier tout en permettant une vision d'ensemble.

Ce chapitre précise en outre que « *Le processus de cartographie des lignes de métier doit être soumis à des revues indépendantes* ». Ceci fait directement référence au rôle de l'audit interne qui, s'il s'appuie sur la cartographie au lancement de chaque mission ou pour l'élaboration du plan d'audit, a également pour rôle d'en revoir périodiquement l'exhaustivité et la pertinence (cf. annexe 2).

---

[1] *Début 2013, la FSA a été scindée en deux autorités distinctes :*
- Le FCA pour "Financial Conduct Authority" (www.fca.org.uk)
- Le PRA pour "Prudential Regulation Authority" (www.bankofengland.co.uk)
Le FSA Handbook, auquel on se réfère dans cette partie, a été scindé en deux parties rattachées respectivement à chacune des deux entités créées.

- **Deux autres parties du FSA Handbook développent également la nécessité d'une structuration de l'environnement de contrôle et de la gouvernance d'un établissement :**

  - **SYSC Section du FSA Handbook**
    On retrouve dans cette partie du FSA Handbook la nécessité d'un travail de fond destiné à une formalisation synthétique des risques essentiels de l'organisation. Là aussi, cette formalisation n'aura de sens que si elle est exprimée au travers du prisme des activités et des processus-clés.
    Ce texte introduit le concept clé de la gouvernance de la structure avec *« une organisation claire incluant des règles de responsabilités formelles, transparentes et cohérentes, des processus effectifs destinés à identifier, gérer, contrôler et assurer le reporting des risques potentiels et avérés, des mécanismes de contrôle interne incluant des procédures administratives et comptables adéquates ainsi que les moyens ad hoc de sauvegardes des systèmes informatiques ».*
    Une gouvernance efficace permettra une exploitation maximale de la cartographie des risques. A long terme, en permettant une circulation fluide et structurée de l'information relative aux risques anticipés, détectés et traités, elle sera également l'une des garantes de la dynamique de la cartographie.

  - **FSA Handbook Principles**
    La deuxième partie du Handbook *(Principles for Businesses)* propose 11 principes génériques parmi lesquels le principe n°3 selon lequel *« Une société doit prendre toutes les mesures suffisantes afin d'assurer un contrôle responsable et effectif de ses opérations via un système adéquat de management des risques. »*
    Ce point renvoie implicitement à la cartographie des risques, dont les caractéristiques naturelles (organisation, rationalisation, dynamique) en font un élément clé du système de management des risques.
    Là-encore, le texte suggère que l'analyse des risques n'est pas complète sans prise en compte de la diversité des activités et des processus-métier de l'organisation.

Il est à noter ici qu'une continuité existe entre les exigences du règlement CRBF 97-02 et celles du régulateur britannique. Cela apparaît comme un gage de lisibilité et de cohérence des travaux, utile dans le contexte actuel d'une industrie financière résolument internationalisée.

- **Les apports de la cartographie des risques au contrôle permanent des risques opérationnels**
  La FSA commande aux établissements relevant de son périmètre de supervision la construction d'une cartographie des risques. Si cet exercice s'avère nécessaire en amont de toute démarche efficace de contrôle périodique, elle est également très importante pour soutenir l'effort constant du contrôle permanent. (Cf. annexe 2)

L'idée de fond est la même dans le règlement CRBF 97-02 et le FSA Handbook, à savoir proposer une vision détaillée des processus de l'entreprise et des risques associés afin de structurer l'approche du contrôle interne et externe. En revanche, l'analyse approfondie des textes fait ressortir des différences d'approches assez nettes :

- Une notion d'obligation forte dans le FSA Handbook, moins marquée dans le règlement CRBF 97-02.
- L'exigence d'une autoévaluation de la cartographie dans le FSA Handbook, qui n'apparait pas dans le règlement CRBF 97-02.
- La focalisation du FSA Handbook sur le seul risque opérationnel, qui n'est pas exclusivement visé par le règlement CRBF 97-02.

1.1.1.1.4 La vision de la Réserve Fédérale américaine

La Réserve Fédérale américaine (FED) a publié le 23/01/2013 (Cf. annexe 4), un complément à sa politique d'origine relative à la fonction d'audit interne et à son externalisation. Ce document suggère notamment le renforcement de plusieurs pratiques d'audit et notamment celles relatives à la cartographie des risques. A cet égard, le document indique :

- que la compréhension que les auditeurs internes ont des activités significatives de l'établissement et des risques associés est documentée au travers d'une évaluation des risques revue au moins une fois par an ;
- que toute évolution des risques pourra alimenter la revue du plan d'audit afin, s'il y a lieu, d'étendre ou de réduire le périmètre des missions planifiées.

La cartographie des risques apparaît ici comme un outil de l'audit interne, outil fondamental et dynamique destiné à la structuration du plan d'audit. La capacité de la cartographie des risques à alimenter les travaux de l'audit interne est ici évoquée plus explicitement que dans les textes précédents.

Si son objectif est la formalisation de la compréhension par l'audit des activités et des risques clés, la cartographie réalisée par l'audit interne devient un élément incontournable auquel les cartographies établies par d'autres acteurs ne peuvent se substituer.

1.1.1.2 Des cartographies de risques spécifiques

Outre la cartographie des risques globale, il existe des cartographies spécifiques (protection de la clientèle, prestations externalisées, etc.) sur lesquelles l'audit interne peut s'appuyer dans le cadre de certaines missions ou pour alimenter sa propre démarche d'évaluation des risques.

Tel est le cas par exemple pour l'analyse du risque de blanchiment qui, avec le « *misselling* » (risque de vente abusive), est l'un des principaux risques règlementaires auxquels est confronté

aujourd'hui un établissement de crédit. Sa probabilité élevée d'occurrence, ainsi que la gravité de ses impacts potentiels en font l'un des enjeux d'une cartographie des risques efficace.

A ce titre, une cartographie des risques spécifique à la lutte contre le blanchiment et le financement du terrorisme (LAB/FT) est explicitement évoquée dans l'article 11-7 du règlement CRBF 97-02.

« Les entreprises assujetties se dotent […] d'une classification des risques de blanchiment des capitaux et de financement du terrorisme. […] [Celle-ci] évalue le niveau de risque des différents produits ou services offerts, des modalités ou des conditions particulières des opérations effectuées, des canaux de distribution utilisés ainsi que des caractéristiques de la clientèle ciblée. [Elle] est mise à jour selon une fréquence régulière et à la suite de tout événement affectant significativement les activités, les clientèles ou les implantations de l'entreprise assujettie. »

Il est important de noter que la construction et la mise à jour de la cartographie dédiée à la LAB/FT appartient au responsable LAB/FT et non à l'audit interne. Ce dernier, soucieux de considérer l'ensemble des risques de l'entreprise, doit en effet se concentrer sur une cartographie globale dont la LAB/FT ne représentera qu'une composante.
Pour un établissement de crédit, la cartographie spécifique dont il est fait état ici s'appuie sur un nombre réduit mais incompressible de notions règlementaires :

- la connaissance de la clientèle à l'entrée en relation et lors du suivi de la relation d'affaires ;
- le monitoring des transactions financières ;
- le monitoring des relations d'affaires par rapport aux listes de sanctions internationales ;
- la formation adéquate des contrôleurs des niveaux 1 (opérationnels), 2 (contrôle permanent) et 3 (contrôle périodique).

Ces éléments sont également les axes-clé d'un audit sur la thématique du blanchiment. A l'image de ce qui est proposé par la FED (Cf. Partie 1.1.1.1.4), cette cartographie peut alimenter les travaux de l'audit.

L'audit interne peut aussi s'appuyer sur la cartographie des risques opérationnels préconisée dans le « *Principles for the Sound Management of Operational Risk* » du Comité de Bâle : *"The Business process mappings identify the key steps in business processes, activities and organisational functions. They also identify the key risk points in the overall business process."*

L'exercice de cartographie des risques opérationnels est également présent dans le paragraphe 6.4.10 du « *Prudential sourcebook for Banks, Building Societies and Investment Firms* » dans le FSA (Cf. Partie 1.1.1.1.3 et annexe 2) où il est précisé d'une part que le risque opérationnel fait partie intégrante de l'exercice d'évaluation des risques et, d'autre part, que l'élaboration d'une cartographie des risques est un principe nécessaire.

Par ailleurs, selon la position de l'AMF n° 2012-17, le **risque de non-conformité** doit également être *« évalué pour déterminer l'angle de travail des activités de contrôle et de conseil de la fonction conformité ».* Cette dernière peut donc s'appuyer sur une cartographie pour *« élaborer sur cette base ses objectifs et son programme de travail ».*

La revue des différents textes réglementaires qui ont été présentés dans cette partie fait apparaitre plusieurs points de convergence. L'un d'entre eux nous parait devoir être souligné, puisqu'il explique et justifie une des options prises pour la rédaction de ce cahier de la recherche. En effet, les textes réglementaires mettent en avant la nécessité de prendre en compte, non seulement le contexte, mais aussi les activités spécifiques de chaque organisation. Une cartographie ne sera significative que pour l'organisation dans laquelle elle a été bâtie. C'est pourquoi ce cahier de la recherche ne contient pas de modèle de cartographie, afin d'éviter toute tentation d'appliquer de manière indifférenciée un même modèle quelle que soit l'organisation. La construction de la cartographie des risques est un exercice long et complexe, mais enrichissant et utile à condition de rester introspectif.

1.1.2 Les attentes des organes de gouvernance

L'évolution légale a étendu explicitement, pour les sociétés cotées, le rôle de surveillance du conseil d'administration et du comité d'audit au suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques.

Pour le secteur bancaire, le règlement CRBF 97-02 inscrit dans le rôle du comité d'audit celui de *« porter une appréciation sur la qualité du contrôle interne, notamment la cohérence des systèmes de mesure de surveillance et de maîtrise des risques […] ».* (art 4 c)

Il prévoit que *« le responsable de la filière « risques » rend compte de l'exercice de ses missions à l'organe exécutif et l'alerte de toute situation susceptible d'avoir des répercussions significatives sur la maîtrise des risques ».* Il peut également rendre compte à l'organe délibérant ou au comité d'audit. (art 11.8)

Par ailleurs, dans son article 37, le règlement CRBF 97-02 précise que « *pour les informations destinées à l'organe exécutif, au comité des risques, à l'organe délibérant, et le cas échéant au comité d'audit, les entreprises assujetties doivent élaborer des états de synthèse adaptés ».*

Ainsi, les besoins d'information des organes de gouvernance en matière de maîtrise des risques sont de plus en plus importants. La cartographie des risques permet de disposer d'un outil approprié pour élaborer un reporting adapté à ces attentes.

1.2 Bénéfices attendus de la cartographie des risques par l'audit interne

1.2.1 Un outil pour répondre aux exigences des Normes Professionnelles de l'Audit Interne

Le Cadre de Référence des Pratiques Professionnelles de l'audit interne (CRIPP) donne des lignes directrices sur l'utilisation des risques dans le cadre de la planification. Ainsi, la Norme IIA/IFACI 2010 relative à la planification demande au responsable d'audit interne « *d'établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation* ». Il est précisé (Norme 2010.A1) que « *le plan d'audit interne doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois par an* ». De plus, les Modalités Pratiques d'Application (MPA) 2010-1[1] et 2010-2[2] apportent des bonnes pratiques sur l'utilisation du management des risques dans le cadre de la planification de l'audit interne.

En établissant la cartographie des risques sur l'ensemble du périmètre auditable, l'audit interne dispose d'une base solide et formalisée pour élaborer son plan d'audit.

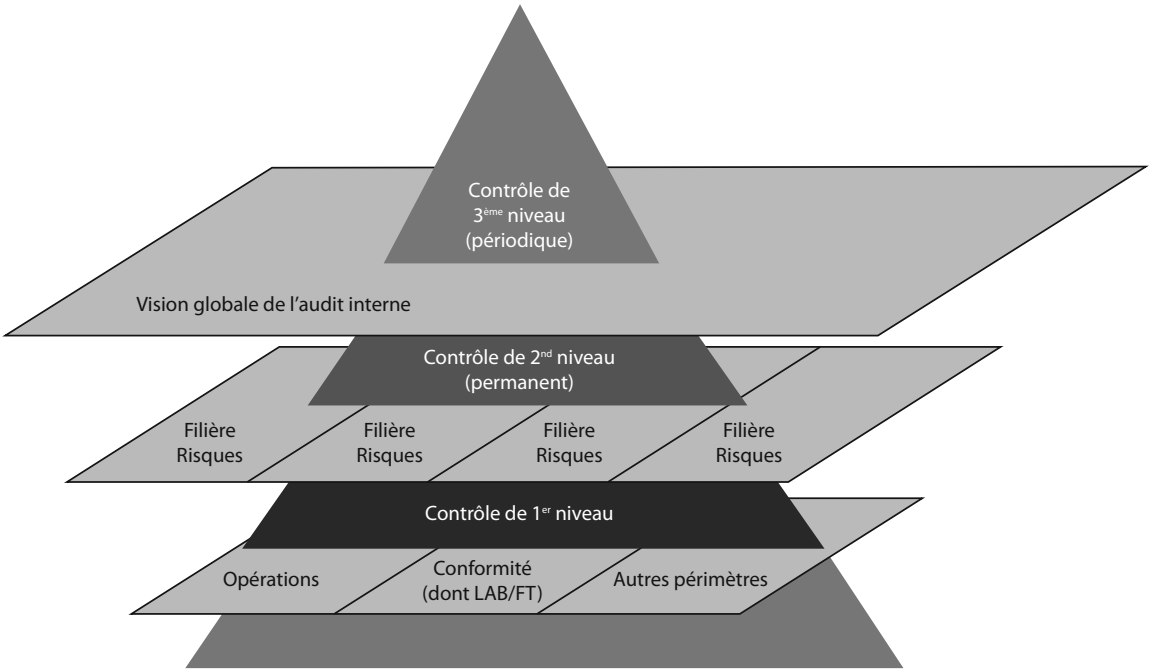
Dans la Norme 2060 et la MPA 2060-1, il est précisé que le responsable de l'audit interne doit communiquer avec la direction générale et le Conseil, notamment de l'exposition aux risques significatifs.

1.2.2 Une réponse à d'autres besoins

S'il existe déjà des cartographies des risques établies par d'autres fonctions, la réalisation d'une cartographie par l'audit interne n'en présente pas moins une valeur ajoutée :

- la démarche permet d'acquérir et de formaliser une connaissance approfondie des activités et du fonctionnement de l'établissement ;
- l'analyse et l'évaluation des risques peuvent être conduites de manière indépendante vis-à-vis des métiers ;
- la granularité des cartographies existantes peut ne pas correspondre au niveau de maille des missions d'audit ;
- le champ couvert par ces cartographies est souvent partiel alors que la démarche conduite par l'audit interne permet d'avoir une vision globale de l'établissement et du périmètre auditable ;
- cette vision globale fait de la cartographie de risques réalisée par l'audit interne un outil de dialogue avec les autres prestataires d'assurance. (Cf. Partie 3).

[1] *La prise en compte des risques et des menaces pour l'élaboration du plan d'audit*
[2] *La prise en compte du management des risques dans la planification de l'audit interne*


Contrôle de
3ème niveau
(périodique)
Vision globale de l'audit interne
Contrôle de 2nd niveau
(permanent)
Filière
Risques
Filière
Risques
Filière
Risques
Filière
Risques
Contrôle de 1er niveau
Opérations
Conformité
(dont LAB/FT)
Autres périmètres

Partie 2

L'établissement d'une cartographie des risques exhaustive

Afin d'évaluer le degré de maîtrise des risques et d'en rendre compte aux autorités de tutelle, aux actionnaires, aux instances de gouvernance et à la direction générale, un plan pluriannuel d'audit doit être élaboré par l'audit interne.

La Norme 2010 de l'IIA demande que « *le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation.* »

La cartographie des risques auditables hiérarchise et permet d'organiser la couverture d'audit de l'ensemble des activités de l'entité à travers la segmentation des missions, le choix de leur périodicité ainsi que l'évaluation de leur charge en termes de jours d'audit.

Sur quel périmètre, à partir de quelles sources d'information et comment l'audit interne doit-il procéder pour élaborer cette cartographie des risques ?

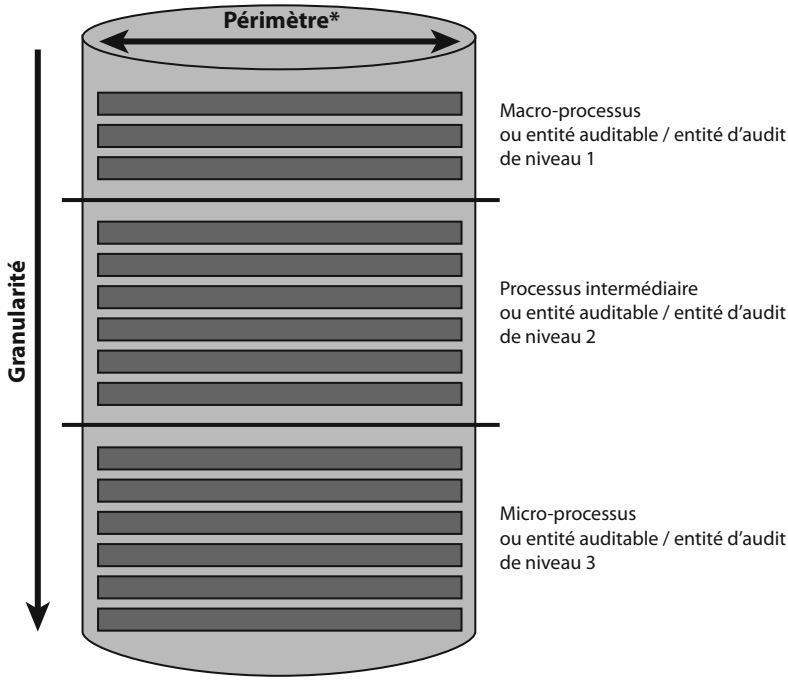
2.1 Choix méthodologiques

2.1.1 Périmètre et granularité de la cartographie

Le périmètre d'audit correspond à l'ensemble des « objets auditables » identifiés au sein de l'établissement concerné et qui relève du champ de responsabilités de l'audit interne tel qu'il est défini dans la charte. En fonction du degré de précision souhaité, il s'agira d'une unité d'affaires *(Business Unit)* ou d'un ensemble d'activités élémentaires (par exemple, les processus métiers) sur lequel portera une mission d'audit.

Il convient également de définir la granularité, c'est-à-dire le niveau de profondeur de l'analyse des risques.

La granularité (niveau de profondeur) de la cartographie des risques reste à la main du responsable de l'audit interne en fonction de son positionnement dans la structure organisationnelle (groupe, filiale), de ses objectifs et de ses ressources.



** La couverture du périmètre doit être impérativement exhaustive.*

Schéma représentatif des différents niveaux de granularité et du périmètre

2.1.1.1 Principe de l'exhaustivité du périmètre à couvrir

Pour élaborer la cartographie, la première question à se poser est celle de la définition de l'**univers d'audit** qui peut varier d'un établissement à l'autre.

Ainsi, le périmètre à couvrir sera différent selon le niveau où l'on se situe : cartographie d'une entité au sein d'un groupe ou cartographie d'un groupe constitué de plusieurs entités, y compris des *joint-ventures*.

De plus, l'univers d'audit pourra être construit uniquement sur les subdivisions organisationnelles ou « unités d'affaires » (filiales / directions / service, etc.), ou prendre appui sur cette structure et la croiser soit avec les grands risques de l'établissement financier, les objectifs du plan stratégique, les grands projets, etc.

L'univers correspond à l'ensemble des objets qui devront être audités sur le cycle retenu par l'établissement. La cartographie correspond quant à elle à une présentation structurée des objets auditables, identifiés par l'audit interne comme porteurs de risques et classés en fonction de leur criticité. La cartographie des risques est ainsi calquée sur la structure de l'univers d'audit.

La cartographie doit identifier l'exhaustivité des risques du périmètre d'audit qui, en général, est identique au périmètre de contrôle interne décrit dans le rapport annuel, y compris les Prestations de Services Essentielles Externalisées (P.S.E.E.).

Le principe « d'absence de sanctuaire » doit s'appliquer. Toutes les activités présentant un risque pour l'entité sont à auditer et donc à intégrer à la cartographie.

Les objets auditables qui donneront éventuellement lieu à des missions d'audit déléguées, soit à une autre unité (ex : un holding ou une maison-mère), soit à un tiers (cabinet externe), font partie de la cartographie.

2.1.1.2 Granularité de la cartographie

Le niveau de précision dans l'analyse des risques doit être adapté à la structure et aux objectifs de la fonction audit. Ainsi, pour un audit Groupe, les missions inscrites au plan d'audit seront exprimées au niveau de l'établissement. C'est donc à ce niveau que l'analyse des risques sera réalisée. En revanche, les fonctions audit des entités décentralisées interviendront au niveau des macro processus (par exemple « Crédit Clientèle ») voire des processus (par exemple analyse des dossiers clients, décision, versement des fonds, intérêts, etc.) : la granularité de l'analyse des risques devra être plus fine.

Au plan pratique, le choix de la granularité est un exercice essentiel. S'il faut prendre garde à ne pas rester à un niveau trop général qui ferait perdre à la cartographie tout intérêt, il faut également veiller à ne pas s'astreindre à un niveau de profondeur trop important. En effet, plus les processus ou les entités auditables seront détaillés ou nombreux, plus le nombre de missions sera important. Dans ce cas, la programmation risque de ne pas être respectée, faute de ressources nécessaires. En outre, la mise à jour de la cartographie s'avérera compliquée en raison d'une base trop complexe à réactualiser régulièrement.

2.1.1.3 Les différentes approches

Après avoir défini le périmètre et la granularité de la cartographie des risques, il faut déterminer l'approche de construction. Trois grandes options sont envisageables :

- **Approche « unités opérationnelles » :** l'audit établit des priorités d'investigation principalement en fonction des « unités opérationnelles » qu'il identifie comme plus ou moins porteuses de risques : par exemple, une unité en charge d'une nouvelle activité au sein de l'établissement ou une unité née d'une acquisition (« audit post-acquisition »).

- **Approche « risques majeurs » de l'établissement :** les risques majeurs de l'entreprise sont définis par la direction des risques et validés au plus haut niveau de l'organisation. L'audit interne peut choisir de les utiliser comme angle d'attaque de sa cartographie : le risque de fraude en est une bonne illustration.

- **Approche « processus » :** Un processus est une représentation d'un enchaînement ordonné d'activités reliées les unes aux autres dont l'objectif est la délivrance d'un service ou d'un produit : exemple, le processus « souscription d'un produit bancaire ».

Chaque processus (pilotage, métiers, supports) peut être décliné en niveaux plus fins (processus généraux ou macro-processus / processus intermédiaire / micro-processus, etc.).

Ceci étant, pour l'élaboration de sa cartographie, l'audit interne pourra opter alternativement pour les différentes approches présentées ci-avant. De même, pour l'élaboration d'une cartographie à un niveau plus macro, l'audit interne reste libre de choisir l'approche la plus adaptée, comme par exemple l'approche « unités opérationnelles ». Si elle est utilisée, on vérifie que les objets auditables couvrent l'ensemble de l'organisation, au travers des référentiels utilisés.

Les différentes approches présentées ci-dessus doivent être considérées comme des « angles d'attaque » de la cartographie et à ce titre peuvent être croisées les unes avec les autres. L'approche « processus » peut être privilégiée dans la mesure où elle est transverse et permet d'investiguer à la fois les « unités d'affaires » qui portent une partie du processus mais également les risques

induits spécifiquement par ce processus. Ainsi, le processus « souscription d'un produit bancaire » permet d'auditer les front, middle et back offices en tant qu'unités d'affaires et aussi de focaliser sur les risques induits par ce processus. Les angles d'attaque peuvent donc être combinés.

2.1.2 Nature des risques à couvrir

Les risques identifiés dans l'article 4d et suivants du règlement CRBF 97-02 modifié étant inclus dans Bâle II, l'approche retenue par l'unité de recherche est celle de Bâle II et de ses trois grandes familles de risques (crédit, marché, opérationnel). Dans certains établissements, le risque de non-conformité et le risque juridique peuvent être distingués des autres risques opérationnels.
Les risques identifiés peuvent être décrits comme suit (Cf. Glossaire) :

- **Le risque de crédit** (ou risque de contrepartie) est le risque de perte sur une créance à l'échéance convenue.

- **Le risque de marché** regroupe notamment les risques définis par le règlement CRBF 97-02 modifié (la taille, l'activité de l'établissement peuvent l'amener à regrouper ces différents risques dans le risque de marché ou à les évaluer séparément) : risque de marché, risque de pertes encourues en cas d'évolution défavorable des prix ou des paramètres de marché (taux, actions, marges de crédit, et change) affectant le portefeuille de négociation, risque de taux d'intérêt global, risque de liquidité, risque de règlement, risque d'intermédiation, l'ensemble regroupé par souci de clarté sous le vocable de « Risque financier ».

- **Le risque opérationnel** est le risque résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes ou à des événements extérieurs.

Selon les établissements, les natures de risques suivantes peuvent faire l'objet d'une typologie distincte s'ils ne sont pas intégrés par l'établissement dans le risque opérationnel :

- **Le risque de non-conformité** est le risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, du fait de l'absence de respect de dispositions législatives et réglementaires propres aux activités bancaires et financières, de normes professionnelles et déontologiques, ainsi que d'orientations de l'organe délibérant ou d'instructions de l'organe exécutif.
  Les risques liés au blanchiment de capitaux et au financement du terrorisme font partie du risque de non-conformité (Cf. Partie 1.1.1.2)

- **Le risque juridique** est le risque, tel que défini par le règlement CRBF 97-02 modifié, de tout litige avec une contrepartie, résultant de toute imprécision, lacune ou autre insuffisance susceptible d'être imputable à l'entreprise au titre de ses opérations.

- **Le risque de réputation** (défini dans le risque de non-conformité dans le règlement CRBF 97-02) se définit comme le risque résultant d'une perception négative de la part des clients, des contreparties, des actionnaires, des investisseurs ou des régulateurs qui peut affecter défavorablement la capacité d'une banque à maintenir ou engager des relations d'affaires et la continuité de l'accès aux sources de financement.

- **Le risque stratégique** se définit comme le risque représenté par les choix stratégiques des instances dirigeantes (c'est-à-dire l'opportunité de la décision stratégique) ou le risque résultant de la déclinaison de la stratégie au sein de l'organisation. En fonction de la maturité de l'établissement et de l'audit interne, la couverture de ce type de risque est parfois confiée à un cabinet externe.

L'objectif est de déterminer, pour chaque objet auditable, les risques qui peuvent s'y rapporter, puis d'apprécier l'importance relative de ces risques.

Pour évaluer les niveaux de risque, deux notions sont communément utilisées par les établissements de la place : le niveau de risque inhérent et le niveau de risque résiduel. Cette double évaluation est l'approche conseillée par le présent cahier de la recherche. Selon le COSO II, le risque inhérent (ou risque brut) est celui auquel une entité est exposée en l'absence de mesures correctives prises par le management pour en modifier la probabilité d'occurrence ou l'impact. C'est le risque intrinsèque de l'objet auditable. Pour chaque objet auditable, il est déterminé un niveau de risque global, résultant de l'identification et de la cotation des différents risques, classés par nature.

Le risque résiduel est le risque subsistant après les mesures de prévention et de réduction d'impact.

Si c'est bien le risque inhérent que l'on décrit dans la cartographie, c'est l'évaluation du risque résiduel (risque final ou risque net) qui sert à déterminer la fréquence des audits.

2.2 Réalisation de la cartographie des risques

L'objectif de la cartographie est de constituer un appui pour la programmation de l'année suivante. L'élaboration d'une première cartographie des risques de l'audit interne se fait nécessairement ex nihilo en amont de la programmation. Une fois établie, elle pourra être mise à jour soit à l'issue de chaque mission, soit en fin d'exercice de la programmation.

2.2.1 Sources d'information pour l'audit interne

L'audit interne va s'appuyer sur une documentation interne et externe pour élaborer la cartographie des risques auditables. Ces sources diverses apportent une information relative aux objectifs de l'organisation, à sa structure organisationnelle, à ses risques (inhérents et résiduels), ainsi qu'à leur degré de maîtrise. Les sources sont de deux natures :

- **Sources internes à l'audit :**
  - Rapports produits suite aux missions réalisées ;
  - Suivi des recommandations ;
  - Etc.
- **Sources externes à l'audit :**
  - Plan stratégique ;
  - Organigramme ;
  - Arborescence du diagramme des flux des processus ;
  - Cartographie des risques majeurs et opérationnels ;
  - Travaux du contrôle permanent et de la conformité ;
  - Incidents opérationnels ;
  - Réclamations clientèles ;
  - Analyses des procès-verbaux des principaux comités ;
  - Résultats des interventions / inspections des régulateurs ;
  - Travaux des commissaires aux comptes et du comité inter inspections générales (CIIG) ;
  - Etc.

Selon qu'il s'agira de sa première cartographie ou d'une mise à jour annuelle, ou selon l'approche retenue, ces sources seront plus ou moins pertinentes.

Dès lors que l'approche « processus » est privilégiée, notamment parce que les organisations changent plus vite que les processus, il conviendra – pour une première cartographie – de s'appuyer sur la cartographie des processus de l'établissement, si elle existe, sur la cartographie des risques majeurs (élaboré à partir des risques Bâle II) et celle des risques opérationnels. Cette dernière existe normalement dans tous les établissements.

Pour sa cartographie de l'année en cours, le responsable de l'audit interne pourra choisir de ne pas procéder à une analyse approfondie des risques d'une entité ou d'une activité spécifique, dans la mesure où celle-ci est soumise à une évolution forte à court terme. Il identifiera néanmoins le risque global dont il reporte l'analyse une fois que l'activité ou l'entité sera stabilisée.
Les autres cartographies pourront être utilisées pour l'évaluation du niveau des risques auditables (exemples : cartographie des risques de non-conformité, cartographie des risques juridiques).

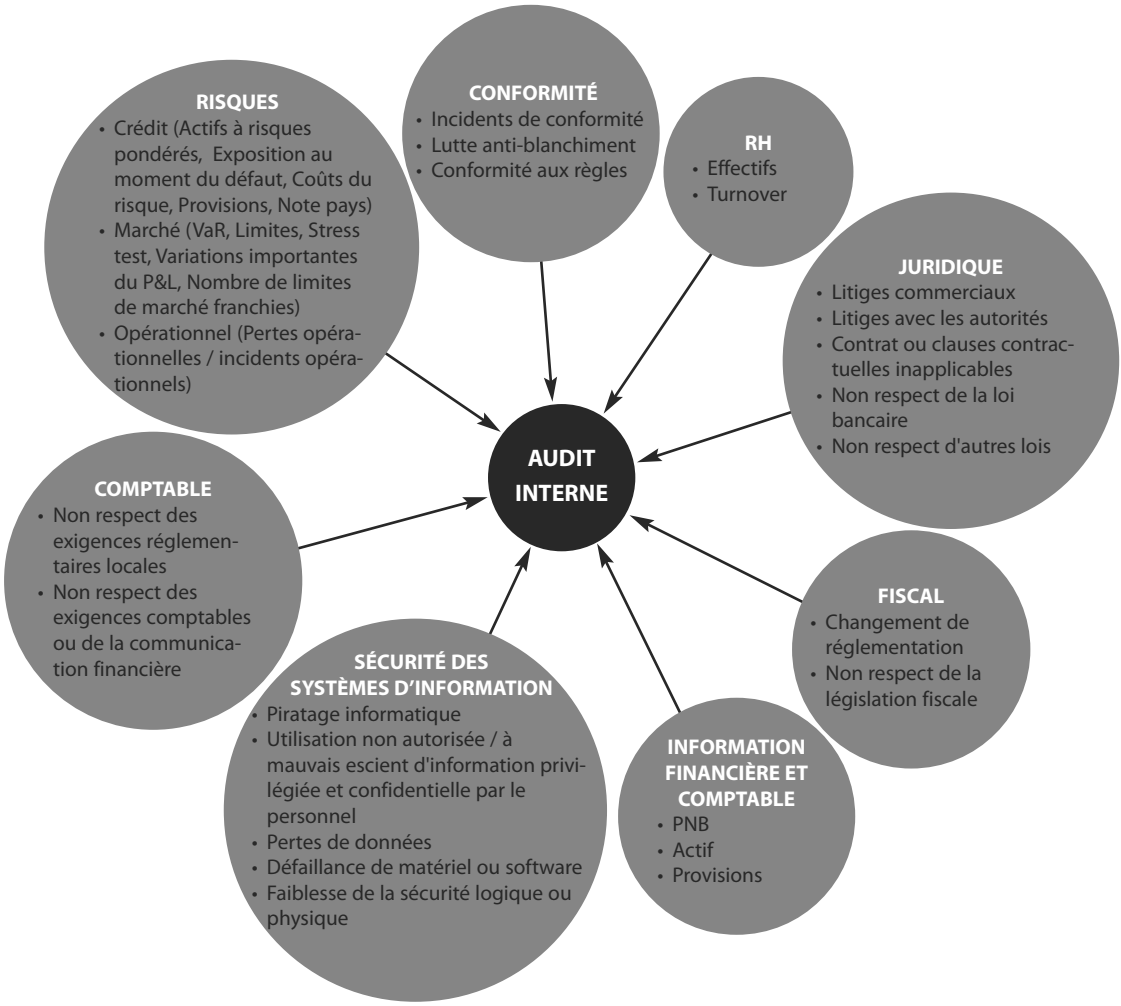
Si l'approche « unité opérationnelle » est utilisée, il convient de s'appuyer sur les référentiels de l'organisation (référentiels organisationnels, organigrammes, référentiels des entités juridiques du

groupe, etc.). Le cas échéant, les autres cartographies mentionnées ci-dessus peuvent être également utilisées pour déterminer la granularité.

Afin d'établir une cartographie des risques complète et pertinente, l'audit interne collecte des données quantitatives et qualitatives auprès des directions fonctionnelles, des départements, des comités, et des cartographies des risques disponibles auprès de chaque filière risque. (Cf. Partie 1.2.2)

2.2.1.1 Les directions fonctionnelles

Les directions fonctionnelles sont en charge de la production d'indicateurs spécifiques qui peuvent être schématisées de la manière suivante (liste non exhaustive) :



Par ailleurs, les préconisations et les notes des rapports ainsi que les réserves de l'audit externe sont également à prendre en compte.

2.2.1.2 Les organes de gouvernance et les comités techniques

Les instances de gouvernance et les comités sont sources d'information pour l'exercice d'évaluation des risques.

2.2.1.2.1 Les organes délibérants

Au sens de l'article 4b du règlement CRBF 97-02, les organes délibérants sont le conseil d'administration, le conseil de surveillance, l'assemblée des associés ou le conseil d'orientation selon la forme juridique des établissements bancaires. Les décisions qui y sont prises sont susceptibles d'être communiquées par les organes exécutifs et les comités d'audit aux responsables de l'audit interne.

2.2.1.2.2 Les organes exécutifs

L'audit interne peut être amené à y participer et devrait avoir accès aux comptes rendus de ces comités élargis parfois appelés « COMEX » ou « EXCOM ». C'est une instance de discussion qui intègre la direction générale et les principaux dirigeants de la banque et traite de sujets transversaux.

L'audit interne peut collecter les comptes rendus de ces organes pour alimenter sa cartographie en informations stratégiques (réorganisations, cessions, acquisitions, etc.).

Selon le règlement CRBF 97-02 :
4.a) Organe exécutif : *« les personnes qui, conformément aux articles L. 511-13 et L. 532-2, point 4 et au b du II de l'article L. 522-6 du code monétaire et financier susvisé, assurent la détermination effective de l'orientation de l'activité de l'entreprise, la personne qui dans le cas d'établissement de paiement hybride, est déclarée responsable de la gestion des activités de services de paiement, ainsi que les personnes qui assurent les mêmes fonctions ».*

Selon le code monétaire et financier - Article L511-13 :
« La détermination effective de l'orientation de l'activité des établissements de crédit doit être assurée par deux personnes au moins qui doivent satisfaire à tout moment aux conditions prévues à l'article L. 511-10 ».

Selon le code monétaire et financier - Article L532-2 :
« Pour délivrer l'agrément à une entreprise d'investissement, l'Autorité de contrôle prudentiel vérifie si celle-ci est dirigée effectivement par deux personnes au moins possédant l'honorabilité nécessaire et l'expérience adéquate à leur fonction, en vue de garantir sa gestion saine et prudente ».

2.2.1.2.3 Le comité d'audit

C'est un comité spécialisé qui est une émanation de l'organe délibérant.

Les comités d'audit sont une source d'informations pour l'audit interne sur les travaux du contrôle de deuxième niveau ainsi que sur les données financières qui y sont présentées.

Conformément à **la directive 2006/43/CE**[1], à la réglementation bancaire et à la **recommandation AMF du 22 Juillet 2010**[2], le comité d'audit est chargé d'examiner le niveau de contrôle des risques de l'établissement. Ce comité examine les procédures de contrôle des risques de marché, des risques structurels et de taux d'intérêt, et est consulté pour la fixation des limites de risque. Il émet en outre une opinion sur la politique de provisionnement globale de l'établissement ainsi que sur les provisions spécifiques de montants significatifs. Il examine également le rapport annuel sur le contrôle interne qui est remis au conseil d'administration et à l'Autorité de Contrôle Prudentiel et de Résolution (ACPR).

Les comités d'audit revoient les contrôles de deuxième niveau des banques (annexe II du document de Bâle de Juin 2012 *« The internal audit function in banks »*).
« Le comité d'audit de la banque s'assure que la direction générale établit et maintient un processus et un système de contrôle interne adéquat et efficace. Le système et le processus devraient être établis de manière à garantir les informations dans le domaine du reporting (financier, opérationnel, risque), du contrôle de conformité avec les lois, régulations, et procédures internes, de l'efficacité des opérations et de la conservation des actifs. »

2.2.1.2.4 Les comités de coordination

Cette instance peut exister sous différentes dénominations. Il peut s'agir notamment du comité de coordination du contrôle interne (CCCI) qui permet de collecter et d'analyser les principales anomalies identifiées au sein du dispositif de contrôle interne, et de coordonner toutes les initiatives transversales entreprises ou à entreprendre dans le but de corriger ces anomalies ou d'améliorer le dispositif de contrôle permanent. Le CCCI pilote la cohérence et l'efficacité de l'ensemble du dispositif du contrôle interne. Il passe en revue le dispositif de contrôle (conformité, finance) et de maîtrise des risques du deuxième niveau et examine les résultats de ces contrôles.

L'IFACI préconise dans sa prise de position sur l'urbanisme du contrôle interne[3], recommandation numéro 3 sur la coordination des acteurs :
« […]Que un ou plusieurs comités de coordination soient créés et animés aux niveaux pertinents à chaque

[1] *La directive 2006/43/CE du 17 mai 2006 relative au contrôle légal des comptes annuels et consolidés pose, dans son article 41, le principe de la mise en place obligatoire d'un « comité d'audit » dans certaines sociétés et structures, mettant en exergue dans son préambule le fait que l'existence de comités d'audit et de systèmes efficaces de contrôle interne « contribue à minimiser les risques financiers, opérationnels et de non-conformité » et « accroît la qualité de l'information financière » Cf. 24ème considérant du préambule de la directive.*

[2] *Les dispositifs de gestion des risques et de contrôle interne, AMF, 22 Juillet 2010*

[3] *Prise de position – L'urbanisme du contrôle interne, IFACI, 2008*

organisation, incluant non seulement les responsables opérationnels et fonctionnels mais également les responsables des activités de contrôle permanent ou périodique [afin de] partager et échanger sur la cartographie des risques ; identifier les risques nouveaux et les mesures qu'ils appellent ».

2.2.1.2.5 Les comités nouveaux produits

L'audit interne ne participe pas aux comités nouveaux produits. Il peut seulement y assister en tant qu'observateur.

Le Comité de Bâle précise que « *Les banques devraient, avant de lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent* » (Voir principe 4 : Gestion du risque).

Ainsi, les directions opérationnelles soumettent leurs nouveaux produits à une procédure de validation. Cette procédure s'assure qu'avant tout lancement :

- tous les types de risques induits ont été identifiés, compris, et correctement évalués ;
- toutes les fonctions supports ont été mobilisées et n'ont pas, ou plus, de réserve non satisfaite ;
- la conformité a été appréciée au regard des lois et règlements en vigueur, des règles de bonne conduite professionnelle et des risques d'atteinte à l'image et à la réputation de l'établissement. En particulier, la conformité doit valider les nouveaux produits et émettre ses réserves, le cas échéant. (Article 11 du règlement CRBF 97-02 modifié : « *Les entreprises assujetties prévoient des procédures spécifiques d'examen de la conformité.* » Il s'agit notamment « *des procédures d'approbation préalable systématique, incluant un avis écrit du responsable en charge de la conformité ou d'une personne dûment habilitée par ce dernier à cet effet, pour les produits nouveaux ou pour les transformations significatives opérées sur les produits préexistants, pour cette entreprise ou pour le marché.* »)

Le comité nouveaux produits doit valider le produit en fonction du risque que l'établissement accepte de supporter en fonction des seuils autorisés d'appétit au risque (rapport gain/risque).

Exemple des types de procédures nouveaux produits :
Le comité qui a avalisé le produit *(Product Owner)* peut demander une revue dans un délai donné. Le comité peut également donner une autorisation provisoire, suivie éventuellement par une autorisation définitive.
Le comité peut donner une validation avec réserves, avec un suivi des préconditions, avant le lancement du produit et des post conditions par la suite. La post-condition est une réserve à respecter lorsque le nouveau produit est mis en place ; elle concerne par exemple une limitation de volume d'opérations, une période de temps limitée, etc. le contrôle permanent peut être en charge du suivi de la mise en œuvre du respect des conditions.

2.2.1.2.6 Comité actif / passif (ou comité ALM)

Le comité de gestion actif/passif (ou ALM) est l'instance qui fait les propositions en matière de gestion des risques de taux d'intérêt et de change contenus dans le bilan. De cette manière, en évaluant, en contrôlant et en approuvant les pratiques relatives à un risque dû à des déséquilibres dans la structure du capital, le comité de gestion actif/passif (ou ALM) est une source d'information pour l'audit interne sur les programmes de couverture.

2.2.1.3 Les autres cartographies existantes

Pour réaliser l'exercice d'évaluation des risques, l'audit interne peut collecter les cartographies de risques disponibles. Ces interactions ont lieu en amont de l'exercice d'évaluation des risques pour compléter la cartographie des risques faite par l'audit, et en aval, pour présenter au management une cartographie indépendante.

2.2.1.3.1 La filière risque

- **Il s'agit de la filière « risques » au sens du règlement CRBF 97-02**

  C'est auprès de la filière « risques » que peuvent être collectées les cartographies utiles à l'audit interne, et plus particulièrement celles des risques opérationnels.

  Elle collecte les informations sur tous les risques de l'établissement et contrôle notamment le respect des seuils fixés et de l'appétence pour le risque. La filière « risques » définit ou valide les méthodes et procédures d'analyse, de mesure, d'approbation et de suivi des risques ; et met en œuvre le dispositif de pilotage et de suivi de ces risques, y compris transversaux. Pour ce faire, elle doit disposer des moyens nécessaires en termes de personnel (qui doit disposer de suffisamment d'expérience et de qualification pour exercer ses contrôles au sein de l'établissement), de système d'information et d'accès aux informations. La filière « risques » informe son comité de direction pour lui permettre de vérifier si la réalité des opérations correspond à l'appétence pour le risque et prendre les mesures correctives éventuelles.
  Elle **établit régulièrement des rapports sur la nature et l'ampleur à destination de la direction générale, du conseil d'administration et des autorités de supervision bancaire.** Le comité d'audit est informé des situations susceptibles d'avoir des répercussions significatives sur la gestion des risques.

- **Une cartographie de la filière « risques » particulièrement utile pour l'audit interne : le rapport défini à l'article 43 du règlement CRBF 97-02**

  Dans le cadre du pilier 2 de Bâle 2, le processus ICAAP *(Internal Capital Adequacy Assesment Process)* introduit une procédure réglementaire qui permet de s'assurer que les banques

évaluent au mieux leurs fonds propres pour couvrir l'ensemble des risques auxquels elles sont exposées. Ce processus d'évaluation se construit sur les procédures de calculs et de stress test sur les risques majeurs.

Dans la réglementation française, cette procédure se retrouve dans le règlement CRBF 97-02 à l'article 17 bis, qui oblige les entreprises assujetties à disposer de systèmes et procédures pour évaluer et conserver en permanence les types ainsi que la répartition de capital interne qu'elles jugent appropriés compte tenu de la nature et du niveau de risques auxquels elles sont ou pourraient être exposées.

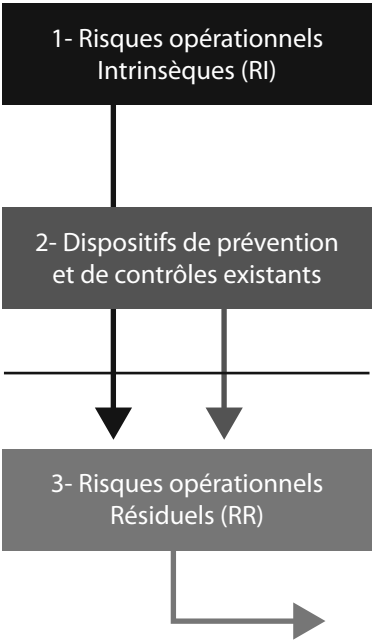
Selon l'article 43 du règlement CRBF 97-02 : *« Au moins une fois par an, les entreprises assujetties et les compagnies financières surveillées sur une base consolidée élaborent un rapport sur la mesure et la surveillance des risques qui permet d'appréhender globalement et de manière transversale l'ensemble des risques, en y intégrant les risques associés aux activités bancaires et non bancaires. »*

2.2.1.3.2 L'exemple du risque opérationnel

- **Que collecte l'audit interne dans ces différentes cartographies de risques opérationnels ?**

  Afin de permettre l'identification des risques, la collecte des informations suivantes peut être réalisée par l'audit interne :
  - les éléments quantitatifs et qualitatifs issus des dispositifs de risques opérationnels de l'établissement (par exemple : analyse des résultats des contrôles issus de la surveillance permanente, exercices d'autoévaluation des risques précédents, niveaux des pertes financières avérées, indicateurs clés tels que volumes de transactions, dépassements de limites, analyse de scénarios etc.) ;
  - l'appréciation qualitative des facteurs d'environnement (par exemple, la complexité des produits et environnement légal) et du dispositif de prévention et de contrôle des risques ;
  - l'audit peut vérifier l'exhaustivité de sa cartographie en la croisant avec celle des risques opérationnels : l'ensemble des risques opérationnels se trouvent-ils bien identifiés dans la cartographie de l'audit ?

- **En particulier la cartographie issue de l'autoévaluation des risques :**
  L'autoévaluation des risques a pour but d'évaluer la qualité du dispositif de prévention et de contrôle afin de quantifier l'exposition de l'établissement aux risques opérationnels. Il permet à l'audit interne de disposer d'une cartographie sur tout le périmètre des risques opérationnels. Pour cela, il s'agit:



- **d'identifier et d'évaluer les risques intrinsèques** auxquels est exposée chaque activité de l'établissement. Ces risques inhérents à la nature d'une activité sont déterminés en faisant abstraction de son environnement de prévention et de contrôle ;
- **d'évaluer la qualité** (existence et efficacité) **des dispositifs de prévention et de contrôle en place permettant de réduire ces risques** et leurs impacts financiers ;
- **de déduire l'exposition aux risques résiduels** de chaque activité de l'établissement (après prise en compte de l'environnement de prévention et de contrôle mais sans prise en compte des couvertures d'assurance) ;
- Pour identifier les zones de faiblesse des mesures de prévention et de contrôle et mettre en œuvre **des plans d'actions correctrices.**

2.2.1.4 La prise en compte des résultats du contrôle permanent

L'audit interne peut obtenir les résultats issus du contrôle permanent pour affiner sa cartographie des risques, tout en gardant son autonomie de jugement sur la nature et la gravité des risques identifiés.

Il s'agit, en particulier, d'analyser les anomalies et les mesures correctives mises en place, issues de la surveillance permanente qui est réalisée par les directions opérationnelles et fonctionnelles de l'établissement.

2.2.2 Analyse et évaluation des risques

Une fois l'approche choisie, l'univers d'audit est décomposé en « éléments porteurs d'un ou plusieurs risques », les objets auditables, dont il conviendra d'apprécier l'importance relative, en termes de niveau de risque.

Pour chacun de ces objets, il faut identifier précisément les risques (cf. Partie 2.1.2) :

Objet auditable	Risques						
	Crédit	Marché	Opérationnel	Non-conformité	Juridique	Réputation	Stratégique
Sécurité financière			X	X			

On distingue ensuite le risque inhérent et le risque résiduel.

Pour chaque risque inhérent, il est nécessaire d'indiquer le dispositif de maîtrise de risque associé, d'en évaluer la qualité afin de déterminer et de coter l'impact du risque résiduel. Dans le dispositif de maîtrise des risques, la qualité du contrôle permanent est à prendre en compte. Elle concourt à la cotation du risque final.

Pour procéder à la cotation – autrement dit à l'évaluation de la criticité (le niveau de risque) – on croise l'impact du risque (gravité) et sa probabilité de survenance (fréquence). Ainsi, un risque « R » pourra avoir une gravité cotée 2 et une fréquence 1, d'où une cotation globale 2x1=2. Ces évaluations s'appuient sur les indicateurs, et font appel au jugement professionnel.

Selon les établissements, une échelle plus ou moins détaillée pourra être retenue, par exemple, une échelle à 3 positions (faible – moyen – élevé).

Objet auditable	Risques opérationnel / Non-conformité			
	Risque(s) inhérent(s)	Dispositif de maîtrise de risques (résultat des contrôles)	Risque résiduel	Cotation du risque final (criticité)
LSF	Qualité des contrôles permanents	- Procédures liées au blanchiment des capitaux et financement du terrorisme - Profession à risques		3

Une fois l'ensemble des champs ci-dessus renseignés pour chacun des objets auditables, la cartographie est considérée comme complète.
A l'issue de cette étape, l'audit interne peut mettre en place une fiche d'identité / de synthèse (Cf. annexe 6) qui présente l'avantage de donner des éléments détaillés d'analyse de risque constitutifs d'une première approche de mission. L'ensemble des fiches constitue une déclinaison de la cartographie. Les éléments suivants peuvent y être retrouvés :

- un descriptif synthétique de l'objet (unité d'affaires ou processus) et de la nature du/des risques qu'il porte ; l'unité d'affaires concernée (Direction / service, etc.) ;
- le périmètre d'audit concerné ;
- un descriptif du risque inhérent (aléa dont la survenance pourrait affecter la réalisation des objectifs de l'entreprise) justifiant l'évaluation de son impact et de sa probabilité de survenance ;
- les conclusions des précédentes missions d'audit ;
- les recommandations non éteintes échues et non échues ;
- des points d'attention éventuels d'intervenants externes.

2.3 Mise à jour de la cartographie

La mise à jour va concerner :

- les objets auditables : nouveaux objets auditables (par exemple, nouvelles « unités d'affaires » par croissance externe), objets auditables existants mais porteurs de nouveaux risques ;
- et d'autre part, les risques identifiés dans la précédente cartographie dont la criticité devra être minorée ou majorée.

La mise à jour va donc s'opérer à la fois au niveau de la cartographie mais également au niveau des fiches d'objet auditable, si elles existent, qui pourront être enrichies à l'issue des missions. Il sera utile de distinguer les fiches qui auront fait l'objet d'une mise à jour (par un numéro de version par exemple).

Lors de l'actualisation de la cartographie, les audits réalisés en cours d'année sur l'exercice d'évaluation des risques seront pris en compte en enrichissant les fiches d'objet auditable à deux moments : Pré et Post Audit. A la fin de la mission, la fiche peut être réévaluée par rapport aux constats et préconisations émises afin de vérifier, et le cas échéant actualiser, les risques résiduels sur les entités/processus concernés.

Par conséquent, la méthode de mise à jour doit suivre à l'identique la méthode de construction de la cartographie initiale.

2.3.1 Périodicité

La cartographie doit être mise à jour sur une base annuelle en année N pour constituer le support de l'élaboration du plan d'audit en année N+1. Cette mise à jour peut être faite à l'issue des vagues de missions d'audit ou sur une période définie (par exemple, fin septembre). La mise en place d'un retro-planning s'impose dans la mesure où il est nécessaire d'aboutir avant la fin de l'année civile à la validation du plan annuel.

Cette réactualisation devrait en principe s'effectuer en amont de l'établissement du plan annuel pour l'exercice suivant, elle ne peut donc pas intégrer les résultats de la dernière vague de missions (celles conclues sur le dernier quadrimestre), qui seront alors intégrés dans la réactualisation de l'année suivante.

Les sources internes et externes sont les mêmes que lors de la construction initiale de la cartographie. On pourra néanmoins juger utile de s'appuyer plus avant sur certaines d'entre elles pour enrichir l'évaluation des risques. Ainsi, la synthèse annuelle du contrôle permanent peut être utilisée pour mettre à jour des zones de risques identifiées précédemment ou pour en relever de nouvelles.

2.3.2 La prise en compte des résultats des audits réalisés en cours d'année

Les missions réalisées en cours d'année permettent d'actualiser la cartographie de l'audit interne à deux niveaux :

- **au démarrage de la mission**

Lors du démarrage de la mission, les auditeurs collectent des données plus à jour que celles utilisées pendant l'exercice annuel de cartographie, et les vérifient en fonction de leurs contrôles.

- **à la remise du rapport**

A la fin de la mission, la cartographie peut être réévaluée par rapport aux constats et préconisations émises afin de vérifier, et le cas échéant, actualiser les risques résiduels de la cartographie de l'audit interne sur les entités/processus concernés. Il s'agit de réaliser un **exercice d'évaluation des risques au fil de l'eau.**

Une cartographie des risques de l'audit interne est donc un instrument de pilotage et de planification de l'utilisation des ressources, aussi souple et réactif que possible, qui ne doit pas conduire à figer les programmes d'audit, ceux-ci devant s'adapter en permanence aux besoins de l'entreprise et à l'évolution des risques.

Partie 3

De la cartographie des risques au plan d'audit

3.1 Pourquoi un plan d'audit ?

Un plan d'audit annuel et/ou pluriannuel, fondé sur une cartographie des risques de l'entreprise, permet au responsable du contrôle périodique de définir ses priorités, de planifier son activité et d'évaluer les moyens nécessaires à ses audits, enfin de justifier les budgets proposés aux organes exécutif et délibérant. Le plan d'audit constitue à la fois une recommandation ou une exigence des autorités de tutelle (Cf. Partie 1.1), un standard professionnel et une saine pratique de gestion.

3.1.1 Une nouvelle recommandation

Le Comité de Bâle a publié en septembre 2012 un document traduit de l'anglais sur les nouveaux *« Principes fondamentaux pour un contrôle bancaire efficace ».* Le cinquième critère essentiel du principe n° 26 (Contrôle interne et audit) préconise à ses alinéas e) et f) les diligences qui doivent s'appliquer en matière de supervision bancaire :

« L'autorité de contrôle établit que la fonction d'audit interne :

e) s'appuie sur une méthodologie permettant d'identifier les risques significatifs encourus par la banque ;

f) prépare et réexamine régulièrement un plan d'audit reposant sur sa propre évaluation du risque et répartit ses ressources en conséquence ».

3.1.2 Une exigence réglementaire

De facture plus ancienne, l'article 9 du règlement CRBF 97-02 introduit deux horizons en termes de planification :

- Plan pluriannuel **« pour mener un cycle complet d'investigations de l'ensemble des activités sur un nombre d'exercices aussi limité que possible »** ;
- Programme de missions de contrôle **« établi au moins une fois par an en intégrant les objectifs annuels de l'organe exécutif et de l'organe délibérant en matière de contrôle ».**

La notion du « nombre d'exercices aussi limité que possible » pose une difficulté d'interprétation, mais on observe généralement que :

- les établissements raisonnent et communiquent généralement en durée maximale entre deux audits (selon le niveau de risque de leurs principales activités), et non pas en moyenne sur le cycle ;
- si les pratiques peuvent être différentes en fonction des pays, la durée communément admise en France n'excède pas cinq ans ;
- pour certaines problématiques spécifiques, le cycle est ramené à un an (homologation Bâle II, lutte contre le blanchiment et le financement du terrorisme, etc.).

Rappelons aussi que la FED (Cf. Partie 1.1.1.1.4) fait explicitement référence à la cartographie comme élément d'alimentation du plan d'audit.

3.1.3 Une norme professionnelle :

Comme prévu par la norme 2010 « Planification » de l'IIA *(Institute of Internal Auditors)*, l'audit interne doit *« établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation ».* En outre, la norme 2010.A1 – *« Le plan d'audit interne doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois par an. Les points de vue de la direction générale et du Conseil doivent être pris en compte dans ce processus ».*

A titre d'illustration, on notera que les standards de l'ISACA (*Exposure draft* de 2012) prévoient également explicitement le recours à une cartographie des risques pour construire un plan d'audit (Standard 1202 – *Use of Risk Assessement in Audit Planning*) : *« The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources ».*

3.1.4 Une saine pratique de gestion

L'élaboration d'un plan d'audit permet de donner aux instances de gouvernance une vision globale des risques et de la manière dont les missions d'audit en assurent une couverture appropriée.

Le plan d'audit permet au responsable de l'audit interne de rationnaliser l'utilisation de ses ressources : il peut ainsi calibrer ses moyens, planifier son activité et justifier le budget alloué (Cf. Partie 3.3.2)

3.2 Autres contributions au plan d'audit

Le plan d'audit (pluriannuel ou annuel) doit couvrir en général la grande majorité des missions d'audit, à l'exception de celles « hors plan » résultant par construction d'évènements non prévisibles au moment de l'élaboration du plan d'audit. Ainsi, peuvent être considérées comme missions « hors plan », les missions initiées suite à détection d'un incident majeur mis en évidence par les contrôles permanents, création de nouvelles activités ou opération d'acquisition, perspectives de cession, ou toute autre mission spéciale non prévisible, cette liste ne se voulant pas exhaustive.

Outre la cartographie des risques, les autres contributions au plan d'audit sont les suivantes (par ordre de priorité observée) :

- l'évolution de la stratégie du Groupe (restructuration, migration informatique, cession, etc.) s'accompagne régulièrement de demandes spécifiques de missions à intégrer dans le plan d'audit en plus du cycle d'audit pluriannuel (qui intègre les structures concernées) et indépendamment de ce qui peut être identifié au travers de la cartographie des risques ;
- en fonction des pratiques de chaque établissement, certaines missions d'audits transverses ou réglementaires sont inscrites au plan sans être cartographiées du fait de la nécessaire régularité de ces missions (prestations de services essentielles externalisées, homologation Bâle II, lutte contre le blanchiment et le financement du terrorisme, etc.) ;
- l'audit de suivi des recommandations est devenu un point d'attention du régulateur, ce qui peut amener à programmer régulièrement des missions de suivi des recommandations au travers de missions dédiées ;
- la réalisation d'audits mutualisés qui peut amener à positionner une mission dans le plan, en fonction de la disponibilité des différents intervenants plutôt qu'en fonction d'une lecture stricte de la cartographie des risques ;
- dans l'élaboration de son plan, l'audit tient compte des attentes spécifiques des organes délibérants ou exécutifs, notamment dans le cas de prise de fonctions d'un nouveau dirigeant ;
- la prise en compte des contraintes justifiées de l'entité auditable peut être intégrée dans le cadre de la construction du plan d'audit notamment par le décalage de la mission à un moment plus opportun pour les audités ; toutefois, cette faculté doit demeurer une exception et ne pourrait amener à décaler une mission d'audit sur les années suivantes du plan pluriannuel ;
- enfin, du fait de son expérience et son expertise sur les modalités de construction du plan, le responsable de l'audit interne peut être amené à procéder à des arbitrages et à modifier le plan d'audit initial.

Sur cette base, le plan d'audit peut être constitué à condition de tenir compte de deux contraintes complémentaires dans la planification qui conditionnent la faisabilité du plan d'audit en tenant compte de la réalité des organisations :

- Les ressources disponibles qui constituent une contrainte à part entière, une source de flexibilité pour répondre aux besoins ponctuels mais aussi une contrainte dans la planification des missions (prise de congés, rythme des missions, volume d'inter-mission, compétences techniques disponibles, etc.) ;
- Les budgets alloués à l'audit vont aussi guider la constitution du plan d'audit en permettant de calibrer les besoins, de confronter ce calibrage au budget réellement alloué et enfin d'aborder les arbitrages possibles entre les budgets alloués aux différentes missions du plan. Rappelons qu'une information doit être donnée au comité d'audit quant aux missions d'audit qui n'ont pu être réalisées faute de ressources et aux arbitrages réalisés.

3.3 Passage de la cartographie des risques au plan d'audit

3.3.1 Exigence préalable

L'objectif du plan d'audit pluriannuel est de positionner les objets auditables constituant le périmètre d'audit (Cf. Partie 2.1.1) sur un calendrier de missions. Il est préférable que le découpage du périmètre d'audit en objets auditables, utilisé dans la cartographie des risques et dans le plan d'audit, soit d'un niveau de granularité identique. En effet, un découpage différent ne permettrait pas de prendre en compte directement les résultats de la cartographie dans le plan d'audit et nécessiterait des retraitements spécifiques, parfois complexes, pour faire le lien entre les deux.
Ce principe général de cohérence entre la cartographie des risques et le plan d'audit souffre toutefois quelques exceptions, dont certaines ont été détaillées ci-dessus : il s'agira bien sûr des missions effectuées hors plan d'audit, ou de nouveaux objets auditables (par exemple, une activité lancée depuis peu, ou une entité récemment acquise) qui peuvent être intégrés au plan d'audit avant d'avoir fait l'objet d'une cartographie complète des risques.

3.3.2 Etapes successives

La construction du plan d'audit à partir de la cartographie des risques se fait généralement au travers de quatre étapes successives.

La première étape dans le passage de la cartographie des risques au plan d'audit est de traduire le niveau de risque attribué à l'objet auditable par la cartographie des risques en une fréquence d'audit cohérente.
Quel que soit le mode d'expression du résultat de la cartographie des risques (couleur, chiffre, lettre, etc.), il conviendra de bâtir une grille de passage permettant la transposition de ce niveau de risque en fréquence. A titre d'exemple, sur la base d'une évaluation du risque sur 4 positions (où le niveau 1 représenterait le risque le plus faible et 4 le plus élevé) dans la cartographie, cette grille pourrait être la suivante :

- Risque de niveau 1 : audit tous les 5 ans ;
- Risque de niveau 2 : audit tous les 4 ans ;
- Risque de niveau 3 : audit tous les 3 ans ;
- Risque de niveau 4 : audit tous les 2 ans.

A chaque mise à jour du plan d'audit pluriannuel (par exemple en fin d'année), toute modification du niveau de risque issu de la cartographie entraînera ainsi logiquement une révision de la date du prochain audit par rapport au précédent passage, voire un positionnement au plus tôt dans le calendrier de missions en cas de dégradation particulièrement importante et soudaine du niveau de risque.

La deuxième étape dans la construction du plan d'audit est la prise en compte des objets auditables dont le niveau de risque n'a pas été évalué au moyen de la cartographie (cf. Partie 3.2).

Faute de pouvoir disposer comme indiqué ci-dessus d'un niveau de risque issu de la cartographie pour la détermination de la date à laquelle positionner ces objets auditables dans le plan d'audit, la date sera alors fixée en fonction d'autres critères nécessairement plus subjectifs. A titre d'exemple, une entité récemment acquise sera souvent auditée dans l'année qui en suit la prise de contrôle, alors qu'une nouvelle activité pourra nécessiter un délai d'un à deux ans avant de pouvoir disposer du recul suffisant pour en effectuer un bilan pertinent.

La troisième étape consiste en l'évaluation des moyens humains nécessaires pour la réalisation des missions positionnées dans le plan d'audit.

Ce dimensionnement, à la fois quantitatif et qualitatif, sera fonction de différents critères tels que par exemple : la taille des équipes auditées, le niveau de complexité de l'activité ou de l'organisation de l'objet auditable, le besoin de compétences spécifiques en matière technique ou linguistique, le contexte de la mission, etc.
En complément des facteurs énumérés ci-dessus, le niveau de risque issu de la cartographie des risques peut également constituer un bon indicateur pour évaluer le dimensionnement de l'équipe d'audit : les missions sur des objets auditables à risque élevé pourront ainsi être confiées à des auditeurs plus expérimentés et/ou plus nombreux.

Enfin, **la dernière étape** dans la construction du plan d'audit sera de mettre en cohérence les besoins théoriques déterminés ci-dessus avec les ressources réellement disponibles, tant au niveau quantitatif que qualitatif.

En cas de déséquilibre important entre les deux, sur une ou plusieurs années du plan pluriannuel, les arbitrages suivants pourront être demandés ou mis en œuvre :

- obtenir des moyens supplémentaires pour la réalisation du plan d'audit ;
- reporter certaines missions dans le temps afin de rétablir l'équilibre global entre besoins et ressources, si certaines années du plan sont plus chargées que d'autres du fait des fréquences d'audit retenues ;
- revoir ponctuellement le périmètre des travaux prévus, par exemple en retirant du périmètre d'audit une activité ou une direction de l'objet auditable jugée moins risquée que les autres. A noter que ce type d'arbitrage ne saurait être utilisé de façon durable, car il introduit une distorsion entre la vision des risques donnée par la cartographie des risques et celle retenue pour la planification des missions. A terme, il serait donc préférable de revoir le découpage du périmètre d'audit en objets auditables, afin de restaurer une nécessaire cohérence entre la cartographie des risques et le plan d'audit ;

- recourir à une sous-traitance externe pour une partie des travaux envisagés[1]. Cette externalisation pourra notamment être réalisée pour les raisons suivantes : besoin de compétences particulières pour l'audit (par exemple des actuaires, des statisticiens ou des auditeurs informatiques), connaissance spécifique d'un contexte local ou d'une réglementation étrangère, mutualisation des travaux avec d'autres établissements notamment lors des audits « de Place » des prestations de services essentielles externalisées (PSEE), exigence réglementaire locale (cas de l'audit des diligences en matière de lutte anti-blanchiment en Espagne, par exemple), etc.

Quelle qu'en soit la raison, le recours à une sous-traitance externe de travaux d'audit suppose toutefois :

- un cadrage des travaux du prestataire, puis un suivi rigoureux de leur réalisation, par l'audit interne. Ce dernier doit en effet s'approprier le diagnostic produit afin de pouvoir ensuite vérifier par lui-même la correcte mise en œuvre des recommandations émises ;
- l'existence d'une ligne budgétaire dédiée à ce type de prestations, que l'audit interne pourra utiliser à tout moment en fonction de ses besoins.

Une fois le plan pluriannuel d'audit élaboré, il pourra être, en fonction de l'organisation interne de l'établissement, décliné en plan annuel voire en vagues ou campagnes successives de missions d'audit à réaliser en cours d'année.
Cela permettra notamment de matérialiser l'alternance des missions d'audit et des périodes de formation ou de prise de congés des auditeurs, afin de faciliter la gestion interne du service d'audit interne.

3.4 Communication du plan d'audit et des résultats de la cartographie

En général prévue dans la charte d'audit interne, la communication aux organes exécutifs, délibérants ou leur émanation peut porter :

- d'une part sur la cartographie de l'audit, notamment pour expliquer les choix effectués pour bâtir le plan d'audit et donc assurer la couverture des risques principaux ;
- et d'autre part sur le plan d'audit pour en obtenir la validation d'ensemble (et non pas mission par mission), ce qui permet de donner un caractère officiel au dispositif. En effet, la Norme Professionnelle 2020 prévoit que « *Le responsable d'audit doit communiquer à la Direction générale et au Conseil son plan d'audit et ses besoins pour examen et approbation* ».

[1] *Comme prévu à l'alinéa 6 de l'article 7 du règlement CRBF 97-02, « […] lorsque des circonstances particulières le justifient, une entreprise assujettie peut confier des tâches d'exécution des contrôles prévus à l'article 6 à des prestataires extérieurs de services[…] ».*

En termes de niveau de détail, la communication de la cartographie pourra porter uniquement sur les résultats (par exemple, détail des risques majeurs uniquement ou niveau de risque résiduel de l'ensemble des objets auditables).

Pour ce qui concerne la communication du plan d'audit, celle-ci pourra prendre la forme d'une présentation de la programmation des missions sur le cycle d'audit avec un focus sur le plan de l'année à venir.
Les éventuelles remarques de ces instances sont prises en compte dans la cartographie et le plan d'audit.
La communication avec les métiers est nécessairement plus restreinte en fonction des pratiques internes :

- pour des questions d'indépendance lié à la fonction, la cartographie de l'audit ne fait pas l'objet d'un processus contradictoire avec les unités auditées ;
- il ne peut y avoir communication du plan d'audit aux audités afin de préserver la confidentialité des missions à venir.

La communication avec les autres fonctions de contrôles sera intégrée aux échanges réguliers selon les principes en vigueur dans chaque établissement.

Conclusion

Qu'ils soient bancaires ou de portée plus générale, les référentiels analysés dans ce cahier de la recherche mettent en évidence l'utilité d'une cartographie des risques. Elle apparait comme un outil clé pour leur évaluation.

La réalisation d'une cartographie des risques par l'audit interne, si elle n'est pas exigée ni même prévue explicitement par les textes réglementaires, présente plusieurs avantages :

- Pour l'audit, cette démarche constitue la meilleure base pour construire le plan d'audit annuel et/ou pluriannuel qui couvre l'intégralité des zones d'enjeux prioritaires de l'organisation et qui permet d'optimiser l'affectation des ressources. En outre, la cartographie des risques documente l'analyse qui sous-tend le choix des missions. Elle en améliore ainsi la traçabilité.
- Pour l'établissement de crédit, la cartographie des risques réalisée par l'audit interne offre une représentation à la fois globale et indépendante de l'exposition aux risques.
- Pour les instances de gouvernance, les caractéristiques de cette représentation : globalité et indépendance, font de la cartographie des risques de l'audit interne un outil qui répond efficacement à leur besoin de surveillance des risques.

Une démarche de cartographie des risques auditables exige une méthodologie rigoureuse. Même si elle peut s'appuyer sur diverses sources disponibles au sein de l'établissement, elle demande un investissement initial important. A cet égard, le choix de la granularité de l'analyse est déterminant.

GLOSSAIRE

Clossaire

BIPRU : *Prudential sourcebook for Banks, Building Societies and Investment Firms* – règlementation de la FSA s'appliquant notamment aux banques.

Cartographie des risques auditables : La cartographie des risques auditables, est une présentation des risques hiérarchisés de l'ensemble des activités de l'entité, ou, si l'on se situe au niveau d'un groupe, la présentation des risques des entités d'un groupe. La cartographie sert de fondement à l'organisation du contrôle périodique (organisation de la couverture par l'audit du périmètre considéré) et permet de justifier l'établissement d'un plan pluri annuel, à travers la segmentation des missions, le choix de leur périodicité ainsi que l'évaluation de leur charge prévisible (en termes de jours d'audit).

Filière risque : *« Cette filière inclut les agents et unités en charge de la mesure, de la surveillance et de la maîtrise des risques. Les entreprises assujetties désignent un responsable en charge de la filière "risques", dont elles communiquent l'identité à la Commission bancaire. »* (97-02 modifié).

FSA : Autorité britannique de régulation des marchés financiers.

MiFID : Directive concernant les services d'investissement – Directive concernant les marchés d'instruments financiers (MiFID). La Commission adopte une proposition de Directive concernant les marchés d'instruments financiers abrogeant la Directive 2004/39/EC du Parlement Européen et du Conseil, et de Règlement concernant les marchés d'instruments financiers modifiant le Règlement [EMIR] sur les produits dérivés négociés de gré à gré, les contreparties centrales et les référentiels centraux.

Normes de Bâle : Les normes dites de Bâle constituent un dispositif prudentiel destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie et les exigences en fonds propres. Ces directives ont été préparées depuis 1988 par le Comité de Bâle, sous l'égide de la Banque des règlements internationaux.

Objet auditable : correspond à une unité d'affaires *(Business Unit)* ou à une activité élémentaire (ex : processus métier) sur lequel portera un audit. La totalité de ce périmètre doit être audité.

Risque de crédit (ou risque de contrepartie) : Risque de perte sur une créance à l'échéance convenue. Ce risque est fonction de trois paramètres : le montant de la créance, la probabilité de défaut et la proportion de la créance qui ne sera pas recouvrée en cas de défaut.

Risque inhérent : Risque auquel une entité est exposée en l'absence de mesures correctives prises par le management pour en modifier la probabilité d'occurrence ou l'impact.

Risque de marché : Ce risque regroupe notamment les risques définis par le règlement français 97-02 modifié : risque de marché, risque de pertes encourues en cas d'évolution défavorable des prix ou des paramètres de marché (taux, actions, marge de crédit, et change) affectant le portefeuille de négociation, risque de taux d'intérêt global (risque encouru en cas de variation défavorable des taux d'intérêt du fait de l'ensemble des opérations de bilan et hors bilan, à l'exception, le cas échéant, des opérations soumises aux risques de marché visés ci-dessus) , risque de liquidité (risque de ne pas pouvoir faire face à ses obligations - exemple : retrait massif des dépôts clients – ou de ne pas pouvoir dénouer ou compenser une position en raison de la situation de marché), risque de règlement (risque de pertes encourues au cours de la période qui sépare le moment où l'instruction de paiement ou de livraison d'un instrument financier vendu ne peut être annulée unilatéralement et la réception définitive de l'instrument financier acheté ou des espèces correspondantes), risque d'intermédiation (risque de pertes encourues en cas de défaillance d'un donneur d'ordre ou d'une contrepartie à l'occasion d'une transaction sur instruments financiers dans laquelle la Banque apporte sa garantie de bonne fin).

Risque opérationnel : Ce risque désigne les risques de pertes résultant de l'inadéquation ou de la défaillance de procédures, de personnes et de systèmes ou résultant d'évènement extérieurs.

Risque de non-conformité : Risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, du fait de l'absence de respect de dispositions législatives et réglementaires propres aux activités bancaires et financières, de normes professionnelles et déontologiques, ainsi que d'orientations de l'organe délibérant ou d'instructions de l'organe exécutif. Les risques liés au blanchiment de capitaux et au financement du terrorisme font partie du risque de non-conformité.

Risque juridique : Risque de tout litige avec une contrepartie, résultant de toute imprécision, lacune, ou autre insuffisance susceptible d'être imputable à l'entreprise au titre de ses opérations.
Risque de réputation : Le risque de réputation peut être défini comme le risque résultant d'une perception négative de la part des clients, des contreparties, des actionnaires, des investisseurs ou des régulateurs qui peut affecter défavorablement la capacité d'une banque à maintenir ou engager des relations d'affaires et la continuité de l'accès aux sources de financement (par exemple via les marchés interbancaires ou de titrisation). Le risque de réputation est multidimensionnel et reflète la perception d'autres acteurs du marché. En outre, il est présent dans toute l'organisation. L'exposition à ce risque dépend de l'adéquation des processus internes de gestion des risques de la banque, mais aussi de la manière et de l'efficacité avec laquelle la direction réagit à des influences externes sur ses opérations bancaires.

Risque résiduel : Risque subsistant après le traitement du risque, ou le risque subsistant après que des mesures de prévention aient été prises.

Risque stratégique : Risque représenté par les choix stratégiques des instances dirigeantes (c'est à dire l'opportunité de la décision stratégique) ou le risque résultant de la déclinaison de la stratégie au sein de l'organisation. En fonction de la maturité de l'établissement, la couverture de ce type de risque pourra être effectuée par un cabinet externe.

SYSC : *Senior Management Arrangements, Systems and Controls :* partie du FSA handbook qui définit les exigences s'appliquant au management en termes d'organisation et de contrôles.

Annexes

Annexe 1 : Extraits du Règlement CRBF 97-02

Article 1

[…] Ce contrôle interne comprend notamment:

a) un système de contrôle des opérations et des procédures internes,
b) une organisation comptable et du traitement de l'information,
c) des systèmes de mesure des risques et des résultats,
d) des systèmes de surveillance et de maîtrise des risques,
e) un système de documentation et d'information,
f) un dispositif de surveillance des flux d'espèces et de titres. […]

Article 7

[…] 6. Dans les conditions prévues au 3 du présent article ou lorsque des circonstances particulières le justifient, une entreprise assujettie peut confier des tâches d'exécution des contrôles prévus à l'article 6 à des prestataires extérieurs de services sous la responsabilité des personnes désignées au titre du 1 du présent article et dans les conditions prévues à l'article 37-2 du présent règlement. […]

Article 9

Les entreprises assujetties s'assurent que le nombre et la qualification des personnes mentionnées à l'article 6, ainsi que les moyens mis à leur disposition, en particulier les outils de suivi et les méthodes d'analyse de risques, sont adaptés aux activités, à la taille et aux implantations de l'entreprise.

Les moyens affectés au contrôle périodique au titre des dispositifs mentionnés au b de l'article 6 doivent être suffisants pour mener un cycle complet d'investigations de l'ensemble des activités sur un nombre d'exercices aussi limité que possible ; un programme des missions de contrôle doit être établi au moins une fois par an en intégrant les objectifs annuels de l'organe exécutif et de l'organe délibérant en matière de contrôle.

Article 9-1

Les entreprises assujetties définissent des procédures qui permettent :

a) de vérifier l'exécution dans des délais raisonnables des mesures correctrices qui ont été décidées par les personnes compétentes dans le cadre du dispositif de contrôle interne ;
b) au responsable du contrôle périodique d'informer directement et de sa propre initiative le comité d'audit de l'absence d'exécution des mesures correctrices décidées.

Article 10

« Les entreprises assujetties s'assurent que le système de contrôle s'intègre dans l'organisation, les méthodes et les procédures de chacune des activités et que les dispositifs mentionnés au b de l'article 6 s'appliquent à l'ensemble de l'entreprise, y compris ses succursales, ainsi qu'à l'ensemble des entreprises contrôlées de manière exclusive ou conjointe.

Article 11-8

Les entreprises assujetties désignent un responsable en charge de la filière "risques", dont elles communiquent l'identité à la Commission bancaire. Cette filière inclut les agents et unités en charge de la mesure, de la surveillance et de la maîtrise des risques.

Lorsqu'il n'est pas membre de l'organe exécutif, le responsable de la filière "risques" est directement rattaché à cet organe et ne doit effectuer aucune opération commerciale, financière ou comptable.

Le responsable de la filière "risques" rend compte de l'exercice de ses missions à l'organe exécutif et l'alerte de toute situation susceptible d'avoir des répercussions significatives sur la maîtrise des risques. Lorsque ce dernier ou l'organe délibérant l'estiment nécessaire, il rend également directement compte à l'organe délibérant ou, le cas échéant, au comité d'audit.

Lorsque la taille d'une entreprise assujettie ou les circonstances le justifient, le responsable du contrôle permanent assure la coordination de tous les dispositifs qui participent à la filière "risques".

Lorsqu'une entreprise appartient à un groupe au sens de l'article 1er du règlement n°2000-03 susvisé ou relève d'un organe central, la responsabilité de la filière "risques" peut être assurée au niveau d'une autre entreprise du même groupe ou affiliée au même organe central, après accord des organes délibérants des deux entreprises concernées.

Lorsque l'entreprise est une entreprise d'investissement, les responsabilités prévues au premier alinéa du présent article peuvent être confiées aux personnes en charge des contrôles prévus par le règlement général de l'AMF.

Article 11-9

Le responsable de la filière "risques" s'assure de la mise en œuvre des systèmes de mesure et de surveillance des risques et des résultats visés au titre IV et des systèmes de surveillance et de maîtrise des risques visés au titre V. Il s'assure que le niveau des risques encourus par l'entreprise assujettie est compatible avec les orientations de l'activité fixées par l'organe délibérant et les limites mentionnées à l'article 33.

Article 11-10

Les entreprises assujetties dotent la filière "risques" de moyens suffisants en termes de personnel, de systèmes d'information et d'accès aux informations internes et externes nécessaires à l'exercice de ses fonctions. Elles s'assurent que le personnel de la filière "risques"

dispose de suffisamment d'expérience, de qualification et d'un positionnement adéquat pour exercer ses missions au sein de l'entreprise.

Article 17

Les entreprises assujetties mettent en place des systèmes d'analyse et de mesure des risques en les adaptant à la nature et au volume de leurs opérations afin d'appréhender les risques de différentes natures auxquels ces opérations les exposent, et notamment les risques de crédit, de marché, de taux d'intérêt global, d'intermédiation, de règlement et de liquidité ainsi que le risque opérationnel.

Les entreprises assujetties et les compagnies financières mentionnées à l'article 2 doivent également disposer de systèmes de mesure adaptés à la nature et au volume de leurs opérations leur permettant d'appréhender les risques de crédit, de marché, de liquidité, de taux d'intérêt global et de règlement ainsi que le risque opérationnel sur une base consolidée.

Article 17bis

Les entreprises assujetties doivent disposer de systèmes et procédures fiables, efficaces et exhaustives pour évaluer et conserver en permanence les montants, les types ainsi que la répartition de capital interne qu'elles jugent appropriés compte tenu de la nature et du niveau des risques auxquels elles sont ou pourraient être exposées.

Ces systèmes et procédures doivent faire l'objet d'un contrôle interne régulier, visant à assurer qu'elles restent exhaustives et proportionnées à la nature, à la taille et à la complexité de leurs activités.

Article 17ter

Les systèmes d'analyse et de mesure des risques prévus à l'article 17 doivent prévoir les critères et seuils permettant d'identifier comme significatifs les incidents révélés par les procédures de contrôle interne au sens de l'article L. 511-41 du Code monétaire et financier. Ces critères doivent être adaptés à l'activité de l'établissement et couvrir les risques de perte, y compris lorsque celle-ci ne s'est pas matérialisée.

Est réputée à cet effet significative toute fraude entraînant une perte ou un gain d'un montant brut dépassant 0,5 % des fonds propres de base. Ce montant ne peut être inférieur à dix mille euros.

Article 17 quater

Les entreprises assujetties mettent en place des systèmes et procédures permettant d'appréhender globalement l'ensemble des risques associés aux activités bancaires et non bancaires de l'établissement, notamment de crédit, de marché, de taux d'intérêt global, d'intermédiation, de règlement, de liquidité et opérationnels.

Les systèmes et procédures doivent permettre aux établissements de disposer d'une cartographie des risques qui identifie et évalue les risques encourus au regard de facteurs internes

(notamment la complexité de l'organisation, la nature des activités exercées, le professionnalisme des personnels et la qualité des systèmes) et externes (notamment les conditions économiques et les évolutions réglementaires). Cette cartographie :

c) Prend en compte l'ensemble des risques encourus ;

d) Est établie par entité et/ou ligne de métier, au niveau auquel est exercée, le cas échéant, la surveillance consolidée ou complémentaire ;

e) Evalue l'adéquation des risques encourus par rapport aux orientations de l'activité ;

f) Identifie les actions en vue de maîtriser les risques encourus, par :

- le renforcement des dispositifs de contrôle permanent ;
- la mise en œuvre des systèmes de surveillance et de maîtrise des risques définis au titre V ;
- la définition des plans de continuité de l'activité prévus à l'article 14-1.

Article 17 quinquies

L'ensemble des systèmes visés aux articles 17 à 17 quater doivent faire l'objet d'une actualisation et d'une évaluation régulières.

Article 26

Pour la mesure des risques de marché, les entreprises assujetties veillent à appréhender de manière complète et précise les différentes composantes du risque. […]

Annexe 2 : Prudential sourcebook for Banks, Building Societies and Investment Firms

Extrait du chapitre 6 « Risques Opérationnels » du *Prudential sourcebook for Banks, Building Societies and Investment Firms :*

Principles for business lines mapping

6.4.1
(1) To be eligible for the standardised approach, a firm must meet the qualifying criteria set out in this rule, in addition to the general risk management standards set out in • SYSC 4.1.1 R to • SYSC 4.1.2 R and • SYSC 7.1.16 R.
(2) A firm must have a well-documented assessment and management system for operational risk with clear responsibilities for the system assigned within the firm. The system must identify the firm's exposures to operational risk and track relevant operational risk data, including material loss data.
(3) A firm's operational risk assessment and management system must be subject to regular independent review.
(4) A firm's operational risk assessment system must be closely integrated into the firm's risk management processes. Its output must be an integral part of the process of monitoring and controlling the firm's operational risk profile.
(5) A firm must implement a system of management reporting that provides operational risk reports to relevant functions within the firm. A firm must have procedures in place for taking appropriate action in response to the information contained in such reports.
[…]

6.4.10
A firm must develop and document specific policies and criteria for mapping the relevant indicator for current business lines and activities into the framework for the standardised approach. The criteria must be reviewed and adjusted for new or changing business activities and risks as appropriate.

6.4.11
(1) The principles for business line mapping that a firm must meet are set out in this rule.
(2) All activities must be mapped into the business lines in a mutually exclusive and jointly exhaustive manner.
(3) Any activity which cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports. If more than one business line is supported through the ancillary activity, an objective mapping criterion must be used (e.g., proportional allocation of the indicators).

(4) If an activity cannot be mapped into a particular business line then the business line yielding the highest charge for the firm must be used. The same business line equally applies to any associated ancillary activity.
(5) A firm may use internal pricing methods to allocate the relevant indicator between business lines.
(6) The mapping of activities into business lines for operational risk capital purposes must be consistent with the definitions of business lines used by the firm for credit and market risks.
(7) Senior management must be responsible for the mapping policy.
(8) The mapping process to business lines must be subject to independent review.

Annexe 3 : International convergence of capital measurements and capital standards

Extrait de *International convergence of capital measurements and capital standards (Basel Committee on banking supervision)*

92. Supervisors will be responsible for assigning eligible ECAIs' assessments to the risk weights available under the standardised risk weighting framework, i.e. deciding which assessment categories correspond to which risk weights. The mapping process should be objective and should result in a risk weight assignment consistent with that of the level of credit risk reflected in the tables above. It should cover the full spectrum of risk weights.

93. When conducting such a mapping process, factors that supervisors should assess include, among others, the size and scope of the pool of issuers that each ECAI covers, the range and meaning of the assessments that it assigns, and the definition of default used by the ECAI. In order to promote a more consistent mapping of assessments into the available risk weights and help supervisors in conducting such a process, Annex 2 provides guidance as to how such a mapping process may be conducted.

94. Banks must use the chosen ECAIs and their ratings consistently for each type of claim, for both risk weighting and risk management purposes. Banks will not be allowed to "cherry-pick" the assessments provided by different ECAIs.

95. Banks must disclose ECAIs that they use for the risk weighting of their assets by type of claims, the risk weights associated with the particular rating grades as determined by supervisors through the mapping process as well as the aggregated risk-weighted assets for each risk weight based on the assessments of each eligible ECAI.

Annexe 4 : Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing

Board of Governors of the Federal Reserve (23 janvier 2013)

Extrait du chapitre « *Internal Audit Risk Assessment* »

*"**A risk assessment should document the internal audit staff's understanding of the institution's significant business activities and the associated risks.** These assessments typically analyze the risks inherent in a given business line or process, the mitigating control processes, and the resulting residual risk exposure to the institution. […]The risk assessments should also consider thematic control issues, risk tolerance, and governance within the institution. Risk assessments should be revised […] no less than annually. When the risk assessment indicates a change in risk, the audit plan should be reviewed to determine whether the planned audit coverage should be increased or decreased to address the revised assessment of risk."*

« Une évaluation des risques doit documenter la compréhension que les auditeurs internes ont des activités significatives de l'établissement et des risques-clé associés. Ces évaluations intègrent une analyse des risques inhérents à une ligne de métier donnée ou à un processus, les dispositifs de maîtrise associés, et le risque résiduel auquel est exposée la structure. […] Les évaluations de risques devraient également prendre en considération les contrôles thématiques, la tolérance au risque ainsi que la gouvernance de la structure. Les évaluations des risques doivent être revues […] annuellement a minima. Toute évolution de l'environnement des risques pourra alimenter les travaux de revue du plan d'audit afin de déterminer si le périmètre des audits planifiés doit être étendu ou réduit pour prise en compte des évolutions. »

Annexe 5 : Convergence internationale de la mesure et des normes de fonds propres

Comité de Bâle – juin 2004

Annexe 2

Approche standard : conversion des évaluations de crédit

1. Les autorités de contrôle seront chargées de définir le mode de conversion en coefficients de pondération (dans l'approche standard) des évaluations de crédit attribuées par les OEEC reconnus ; elles devront donc prendre en compte divers éléments qualitatifs et quantitatifs leur permettant de différencier les niveaux relatifs de risque exprimés par chaque évaluation. Les éléments qualitatifs peuvent englober notamment l'ensemble des émetteurs couvert par chaque organisme, l'échelle des notations attribuées et la signification de chacune ainsi que la définition du défaut utilisée.

2. Des paramètres quantifiables peuvent favoriser une plus grande homogénéité du processus de conversion. Cette annexe récapitule les propositions du Comité destinées à aider les autorités de contrôle à cet égard. Les paramètres présentés ci-dessous visent à leur servir de guide ; ils ne sont pas destinés à s'ajouter ni à se substituer aux actuels critères de reconnaissance des OEEC

   Appréciation des Taux de Défaut Cumulés (TDC) : deux mesures proposées

3. Pour s'assurer qu'une pondération particulière corresponde bien à une évaluation donnée du risque de crédit, le Comité recommande aux autorités de contrôle d'apprécier le taux de défaut cumulé (TDC) sur trois ans de l'ensemble des émissions de même notation, en recourant à deux mesures distinctes.
   - Pour se doter d'une perspective de long terme sur les défauts de paiement, elles devraient se référer à une moyenne sur une période de dix ans, lorsque c'est possible, du TDC sur trois ans[1]. Dans le cas d'une agence de notation nouvelle ou ayant compilé des données de défaut sur moins de dix ans, elles pourraient lui demander d'estimer cette moyenne ; elles la tiendront responsable de la fiabilité de l'estimation, par la suite, dans la pondération des créances qu'elle note.
   - En second lieu, elles devraient examiner le TDC sur trois ans le plus récent pour chaque évaluation de crédit d'un OEEC.

[1] *Pour 2002, par exemple, les autorités de contrôle calculeraient la moyenne des TDC sur trois ans de chaque groupe d'émetteurs de même notation (« cohorte ») pour chacune des dix années de 1990 à 1999.*

4. Les deux mesures seraient comparées aux taux historiques de défaut agrégés compilés par le Comité pour les évaluations de crédit jugées représenter un niveau équivalent de risque.

5. Les TDC sur trois ans des OECC étant supposés disponibles, les autorités de contrôle devraient pouvoir comparer l'historique des défauts correspondant aux évaluations d'un organisme de notation spécifique avec celui de ses pairs, notamment les grandes agences, pour une même population.

6. Pour aider les autorités de contrôle à déterminer les pondérations applicables aux notations d'un OEEC, chacune des mesures de TDC indiquées ci-dessus pourrait être comparée aux valeurs de référence suivantes.
   - Pour chaque échelon de notation de l'OEEC, la moyenne sur dix ans du TDC sur trois ans serait comparée à un TDC de référence sur trois ans représentant l'historique des défauts au niveau international.
   - Il en serait de même pour les deux TDC sur trois ans les plus récents. Cette analyse comparative servirait à déterminer si les évaluations de crédit récentes de l'OEEC se maintiennent dans les normes de référence prudentielles.

7. Le tableau 1 ci-dessous illustre l'ensemble du processus de comparaison.

Tableau 1

Comparaison des TDC[1]

Historique international (découlant de l'historique agrégé des grandes agences de notation)	à comparer avec	Organisme externe d'évaluation du crédit
Recommandation définie par le Comité de Bâle		Calcul des autorités de contrôle nationales sur la base des chiffres de défaut de l'OEEC
TDC de référence sur longue période	⟷	Moyenne sur dix ans du TDC sur trois ans
TDC de référence	⟷	Les deux TDC sur trois ans les plus récents

1. Comparaison de la moyenne à long terme du TDC sur trois ans d'un OEEC avec le TDC de référence sur longue période

[1] *Il convient de noter que chacune des grandes agences de notation serait soumise à ce processus comparant ses résultats propres avec l'historique international agrégé.*

8. Pour chaque catégorie de risque relevant de l'approche standard dans le présent dispositif, le TDC de référence sur longue période renseignerait les autorités de contrôle sur le niveau historique international des défauts correspondants. La moyenne sur dix ans d'un OEEC donné n'est pas censée concorder exactement avec ce taux de référence ; celui-ci constitue un guide à l'intention des autorités de contrôle et non un objectif à atteindre par les OEEC. Le tableau 2 ci-après présente les TDC de référence sur longue période recommandés pour chaque catégorie de risque de crédit, sur la base des observations du Comité concernant l'expérience des grandes agences de notation sur le plan international.

Tableau 2
TDC de référence sur longue période (proposition)

S&P *(Moody's)*	AAA-AA *(Aaa-Aa)*	A *(A)*	BBB *(Baa)*	BB *(Ba)*	B *(B)*
Moyenne sur vingt ans du TDC sur trois ans	0,10%	0,25%	1,00%	7,50%	20,00%

2. Comparaison du TDC sur trois ans le plus récent aux TDC de référence

9. Les TDC de l'OEEC ne sont pas censés correspondre exactement aux TDC de référence ; il importe donc d'indiquer plus clairement les TDC plafonds acceptables pour chaque évaluation et, partant, pour chaque pondération.

10. Dans l'ensemble, le Comité estime que les TDC plafonds devraient servir de guide aux autorités de contrôle, sans constituer nécessairement des exigences absolues. En cas de dépassement, l'autorité de contrôle ne va pas nécessairement augmenter le coefficient de pondération appliqué à une évaluation donnée, surtout si elle est convaincue que ce dépassement est dû à un phénomène passager et non à des critères d'évaluation déficients.

11. Pour aider les autorités de contrôle à déterminer si un TDC s'inscrit dans une fourchette acceptable pour qu'une notation corresponde à une pondération donnée, deux références seraient établies pour chaque évaluation : niveau de suivi et niveau de seuil.
    a) Niveau de suivi

12. Si le TDC dépasse le niveau de suivi, cela signifie que les résultats actuels d'un OEEC en matière de défaut pour une notation donnée sont sensiblement plus élevés que l'historique international. Même si l'évaluation reste généralement considérée acceptable pour le coefficient de pondération correspondant, l'autorité de contrôle devrait interroger l'OEEC concerné sur la raison de cet écart. Si elle le juge attribuable à des critères d'évaluation du risque de crédit déficients, elle devrait affecter l'évaluation de cet OEEC à une

catégorie de risque supérieure.

b) Niveau de seuil

13. Si le TDC dépasse le niveau de seuil, cela signifie que les résultats de l'OEEC en matière de défaut pour une notation donnée sont beaucoup plus élevés que les antécédents internationaux. Il est donc présumé que ses critères sont trop faibles ou ne sont pas appliqués de manière appropriée. Lorsque le TDC observé sur trois ans dépasse le niveau de seuil deux années consécutives, l'autorité de contrôle devrait affecter la notation à une catégorie de risque moins favorable. Si elle estime que l'écart n'est pas attribuable à des critères d'évaluation du risque déficients, elle peut toutefois, sur la base de son jugement, décider de conserver la pondération d'origine[1].

14. Dans tous les cas où l'autorité de contrôle décide de laisser la catégorie de risque inchangée, elle peut, au titre du deuxième pilier du présent dispositif, inciter les banques à accroître provisoirement leurs fonds propres ou à constituer des réserves plus importantes.

15. Lorsque l'autorité de contrôle a relevé la catégorie de risque, un retour en arrière est possible si l'OEEC peut démontrer que son TDC sur trois ans s'est inscrit en baisse et reste en deçà du niveau de suivi deux années consécutives.

c) Calibrage des TDC de référence

16. Après avoir examiné diverses méthodologies, le Comité a décidé d'utiliser des simulations Monte-Carlo pour calibrer les niveaux de suivi et de seuil correspondant à chaque notation. En particulier, le niveau de suivi proposé repose sur l'intervalle de confiance correspondant au 99e centile et le niveau de seuil au 99,9e centile. Les simulations reposent sur les données historiques de défauts publiées par les grandes agences de notation internationales. Le tableau 3 ci-après présente les niveaux ainsi obtenus, arrondis à la première décimale.

Tableau 3

TDC de référence sur trois ans (proposition)

S&P *(Moody's)*	AAA-AA *(Aaa-Aa)*	A *(A)*	BBB *(Baa)*	BB *(Ba)*	B *(B)*
Niveau de suivi	0,8%	1,0%	2,4%	11,0%	28,6%
Niveau de seuil	1,2%	1,3%	3,0%	12,4%	35,0%

[1] *Si, par exemple, l'autorité de contrôle juge qu'il s'agit d'un phénomène temporaire résultant peut-être d'un choc passager ou exogène comme une catastrophe naturelle, alors la pondération de risque proposée dans l'approche standard pourrait encore s'appliquer. De même, le dépassement simultané du niveau de seuil par plusieurs OEEC peut indiquer une modification passagère du marché ou une influence exogène, et non une détérioration des critères. Dans l'un ou l'autre cas, l'autorité de contrôle se devrait de surveiller les évaluations de l'OEEC pour s'assurer qu'il n'y a pas relâchement des critères d'évaluation du risque de crédit.*

Annexe 6 : Exemple de Fiche d'objet auditable

XX_ Définir, suivre et piloter la conformité aux exigences réglementaires et mettre en œuvre les principes de contrôle interne : Sécurité Financière

MàJ 20XX		5	3	2
Importance	+ +			2 ans
	- +		3 ans	
	- -	5 ans		
Prévision : 20XX		+ +	+ -	- -
		Niveau de maîtrise actuel		

1. Périmètre d'audit

Le périmètre d'audit couvre le pilotage de la sécurité financière et notamment :

2. Mesure des risques inhérents

Typologie de risque	Cotation	Eléments de contexte (constats, dispositifs de maîtrise des risques, réglementations...)
Crédit		
Marché		
Opérationnel		Ex : Un risque de non respect de procédures peut subvenir et avoir des impacts importants (blanchiment de capitaux, financement du terrorisme). Le non respect de la réglementation (contrôle sur les PPE, professions à risques, liste des terroristes) entraîne un risque juridique. Le non respect des règles relatives à l'exploitation des listes terroristes peut conduire l'établissement à financer un terroriste ou à participer aux blanchiments de capitaux.
Risques inhérents		
Qualité des Contrôles Permanents		

3. Conclusions des précédentes missions d'audit

4. Suivi des recommandations sur les 5 dernières années

5. Points d'attention éventuels

6. Avis éventuels des intervenants externes : CAC, Missions d'expertise de consultants externes, actionnaires, ACPR

7. Détermination du risque résiduel et de la périodicité d'audit :

Le niveau de risque résiduel est évalué à …

Une périodicité d'audit de …N ans est retenue.

8. Thèmes d'audit possibles

Bibliographie

Bibliographie

Réglementation

- Bâle III : dispositif réglementaire mondial visant à renforcer la résilience des établissements et systèmes bancaires : décembre 2010 (document révisé juin 2011) / Comité de Bâle sur le contrôle bancaire. - Banque des Règlements Internationaux, 2010.
- Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement. Modifié par les arrêtés du 31mars 2005, du 17 juin 2005, des 20 février et 2 juillet 2007, du 11 septembre 2008, du 14 janvier 2009, du 5 mai 2009, deux arrêtés du 29 octobre 2009, les arrêtés du 3 novembre 2009, du 19 janvier 2010, du 25 août 2010 et par l'arrêté du 13 décembre 2010.
- Directive 2006/48 du Parlement européen et du Conseil du 14 juin 2006 concernant l'accès à l'activité des établissements de crédit et son exercice.
- Directive 2006/49 du 14 juin 2006 du Parlement européen et du Conseil du 14 juin 2006 sur l'adéquation des fonds propres des entreprises d'investissement et des établissements de crédit.
- Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil.
- Directive 2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers, modifiant les directives 85/611/CEE et 93/6/CEE du Conseil et la directive 2000/12/CE du Parlement européen et du Conseil et abrogeant la directive 93/22/CEE du Conseil.

Référentiel

- Cadre de Référence International des Pratiques Professionnelles de l'audit interne / IIA ; IFACI. – 2013.
- Internal Control-Integrated Framework / COSO. – 2013. [version française attendue pour début 2014]
- IS Audit and Assurance Standards : Exposure Draft / ISACA. – 2012.
- Convergence Internationale de la mesure et des normes de fonds propres : dispositif révisé / Comité de Bâle sur le contrôle bancaire. - Banque des Règlements Internationaux, 2006.
- Le Management des risques de l'entreprise : Cadre de référence - techniques d'application : COSO II report / IFACI ; PWC ; Landwell & Associés. – Ed. d'organisation, 2005.

Ouvrages

- FSA Handbook [updated 2013] / Financial Services Authority. – 2013.
- Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing / Board of Governors of the Federal Reserve System. – 2013.
- Position AMF n° 2012-17 : Exigences relatives à la fonction de vérification de la conformité/ – AMF, 2012.
- The internal audit function in banks / Basel Committee on Banking Supervision. – Bank for International Settlements, 2012.
- Principes fondamentaux pour un contrôle bancaire efficace / Comité de Bâle sur le contrôle bancaire. – Banque des Règlements Internationaux, 2012.
- Principles for the Sound Management of Operational Risk / Basel Committee on Banking Supervision. – Bank for International Settlements, 2011.
- Pour un urbanisme du contrôle interne efficient : [Prise de position] / Groupe Professionnel "Banque". – IFACI, 2010.
- Recommandation AMF n° 2010-16 : Cadre de référence des dispositifs de gestion des risques et de contrôle interne. – AMF, 2010.
- International convergence of capital measurements and capital standards / Basel Committee on Banking Supervision. – Bank for International Settlements, 2006.
- Prudential sourcebook for Banks, Building Societies and Investment Firms / FSA. – 2006.
- Standardised Approach – implementing the mapping process [Annex 2] / Basel Committee on Banking Supervision. – Bank for International Settlements, 2004.
- Etude du processus de management et de cartographie des risques : Conception, mise en place et évaluation / Commerce et Services « Groupe Professionnel Industrie ». – IFACI, 2003.
- A glossary of terms used in payments and settlement systems / Committee on Payment and Settlement Systems. – Bank for International Settlements, 2003.

Réalisation : Ebzone Communication (www.ebzone.fr)