MASTER EN SCIENCES DE GESTION À FINALITÉ SPÉCIALISÉE

La mission et le statut de la fonction compliance dans le modèle des trois lignes de défense, et la gestion des risques, dans le secteur bancaire

Bosi, Arnaud

Award date:
2018

Awarding institution:
Universite de Namur

UNIVERSITE DE NAMUR

Faculté des Sciences Economiques, Sociales et de Gestion

Année universitaire 2017-2018

La mission et le statut de la fonction compliance dans le modèle des trois lignes de défense, et la gestion des risques, dans le secteur bancaire

Arnaud Bosi

Mémoire présenté en vue de l'obtention du grade de Master 120 en sciences de gestion, à finalité spécialisée (horaire décalé)

Promoteur
Laurent Gatot

TABLE DES MATIÈRES

INTRODUCTION

Ce mémoire consiste en une relecture de la mission et du statut de la fonction compliance, au départ des principes de gouvernance, de gestion des risques et de contrôle interne appliqués au sein des banques. La fonction de compliance est devenue aujourd'hui un élément stratégique dans l'organisation et le bon fonctionnement des banques. Il est essentiel qu'elle soit prise en compte dans leur gouvernance générale. Elle doit être intégrée tant en amont dans leurs processus quotidiens, que sur le long terme dans leur vision stratégique.
Au côté du contrôle interne exercé quotidiennement sur les services opérationnels, et des autres fonctions de contrôle que sont les fonctions de gestion des risques et d'audit interne, la fonction de compliance participe activement au dispositif de maîtrise globale des risques encourus par les banques. Cet ensemble nécessite une coordination adéquate entre chacune des fonctions de contrôle. Le modèle des trois lignes de défense constitue un moyen d'y parvenir.

La première partie de ce mémoire sera consacrée à la description de la structure organisationnelle des banques. Nous commencerons pour cela par expliquer les principes généraux liés à la gouvernance, ainsi que le rôle de chacun des acteurs clés de la gouvernance. Nous parcourrons ensuite les éléments essentiels nécessaires à une organisation adéquate des banques, énumérés dans le *Manuel de gouvernance pour le secteur bancaire*, publié par la Banque Nationale de Belgique en septembre 2017. Parmi ces éléments, l'obligation pour les banques de disposer de fonctions de contrôle indépendantes, dont une fonction de compliance.

La seconde partie se concentre sur les fonctions de contrôle. D'une part nous expliquons en quoi consistent le contrôle interne et la gestion des risques. D'autre part, nous présentons les référentiels intégrés s'y rapportant : COSO I&III pour le contrôle interne et COSO II pour le management des risques. Nous terminons cette deuxième partie en expliquant l'utilité du modèle des trois lignes de défense, et en détaillant chacune de ces lignes représentées par les fonctions de contrôle.

La troisième et dernière partie porte exclusivement sur la fonction de compliance. Nous y abordons les missions qui lui sont attribuées, les domaines couverts par les textes légaux et réglementaires qu'elle est chargée de faire respecter, ainsi que l'obligation pour les banques de disposer d'une fonction de compliance indépendante, et ce que cela implique réellement. Nous clôturons cette partie en mettant en lumière les facteurs qui sont à l'origine de l'évolution du statut et de la mission de la fonction compliance, et comment cela se traduit concrètement dans les métiers de la compliance.

PARTIE I : STRUCTURE ORGANISATIONNELLE DES BANQUES

CADRE THÉORIQUE, LÉGAL ET RÉGLEMENTAIRE

CHAPITRE 1 : LA GOUVERNANCE

Pour réussir, toute organisation doit définir et suivre un cadre de référence pour ses décisions, qu'elles soient de long terme ou quotidiennes. Il faut pour cela appréhender la façon dont sont structurées les organisations et la manière dont elles opèrent pour atteindre leurs objectifs. La structure varie bien entendu d'une entité à une autre, mais toutes doivent disposer d'une structure de gouvernance d'ensemble, afin de parvenir aux objectifs fixés et aux besoins des différentes parties prenantes.

1.1 Définition

L'Organisation de Coopération et de Développement Economiques (OCDE) définit la gouvernance ou gouvernement d'entreprise comme ceci : « *Le gouvernement d'entreprise fait référence aux relations entre la direction d'une entreprise, son conseil d'administration, ses actionnaires et d'autres parties prenantes. Il détermine également la structure par laquelle sont définis les objectifs d'une entreprise, ainsi que les moyens de les atteindre et d'assurer une surveillance des résultats obtenus. »* [1]

Une autre définition est donnée par Le glossaire des Normes internationales pour la pratique professionnelle de l'audit interne de l'IIA (Institut of Internal Auditors), qui décrit la gouvernance comme « *le dispositif comprenant le processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs. »* [2]

1.2 Composantes et rôles clés dans la gouvernance

1.2.1 *Dispositions générales*

Le Conseil représente l'organe de gouvernance d'une organisation. Il peut s'agir d'un Conseil d'administration, d'un Conseil de surveillance, de l'organe délibérant d'un organisme public ou d'une association, ou de tout autre organe. [3]

---

[1] Organisation de Coopération et de Développement Economiques (2004). *Préambule aux Principes de gouvernement d'entreprise de l'OCDE*

[2] IIA & IFACI (2014). *Cadre de référence international des pratiques professionnelles de l'audit interne*. P.69

[3] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-5

Pour définir la structure de gouvernance d'une organisation, il convient d'appréhender son fonctionnement selon une perspective descendante ; Le Conseil dicte une orientation à la direction générale afin de la guider dans l'exécution des activités de gestion des risques, de contrôle ou des activités opérationnelles quotidiennes. La direction générale donne à son tour une orientation au management responsable d'activités et de contrôles spécifiques. Les managers intermédiaires rapportent les résultats de ces contrôles et activités à la direction générale. Finalement, la direction générale rend compte au Conseil de la réussite et de l'efficacité des activités.

1.2.2 Domaines de la gouvernance par le Conseil : supervision et orientation stratégique [4]

Pour aller plus loin dans la description de la gouvernance à charge du Conseil, deux domaines bien distincts et complémentaires sont à détailler.

Le premier domaine est celui de *l'orientation stratégique*.
Les priorités des parties prenantes ainsi que le modèle économique de l'organisation doivent concorder avec les objectifs clés de l'organisation, eux-mêmes définis par les lignes directrices et l'orientation stratégique. C'est au Conseil qu'il incombe de les définir et de les faire suivre au sein de l'organisation.
Les administrateurs du Conseil, de par leurs expériences et connaissances diverses et variées, disposent des informations nécessaires pour promouvoir la bonne orientation stratégique qui permettra à leur organisation de prospérer.
Il revient également au Conseil de tracer les limites dans lesquelles évoluer, selon la culture de l'organisation et son appétence au risque.
Enfin, le Conseil est en charge du suivi des objectifs de l'organisation et de l'avancée vers leur réalisation.

Le second domaine de la gouvernance concerne la *supervision*. Cela se rapporte au rôle du Conseil en matière de gestion et de pilotage des activités de l'organisation.
La supervision de la gouvernance pour l'ensemble de l'organisation revient au Conseil et à ses comités. Le Conseil doit rendre compte aux parties prenantes de l'organisation. Il doit pour cela définir l'ensemble des parties prenantes, et ensuite veiller à leur satisfaction. Nous y reviendrons plus en détail ci-après au point 2.3.
Le Conseil et ses comités confèrent une orientation à la direction générale, lui laissent prendre les mesures nécessaires pour y parvenir, et supervisent les résultats des opérations.
Au jour le jour, c'est le management qui se charge de la gouvernance.
La direction générale et les managers intermédiaires ont également un rôle important, notamment dans la gestion des risques.

[4] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-5

Les fonctions d'assurance internes (audit interne principalement) et externes (audit financier externe par exemple) fournissent au Comité et à la direction générale, l'assurance quant à l'efficacité des activités de gouvernance.

1.2.3 Acteurs dans la gouvernance et leurs rôles [5]

- Le Conseil et ses comités

Comme détaillé ci-dessus, la gouvernance relève de la responsabilité du Conseil même si dans bon nombre de cas, cela se fait par l'intermédiaire de ses différents comités (comité d'audit, comité de surveillance...).
L'une des premières responsabilités du Conseil est de déterminer les principales parties prenantes de l'organisation, c'est-à-dire toute partie ayant un intérêt direct ou indirect dans les activités de l'organisation.
Certaines parties prenantes participent directement au fonctionnement de l'organisation. C'est par exemple le cas des collaborateurs.
D'autres parties prenantes ne participent pas directement au fonctionnement de l'organisation, mais y ont un intérêt. Autrement dit, la réussite ou toute autre résultante de l'activité a un impact sur celles-ci. Prenons comme exemples les actionnaires qui ont un grand intérêt ou bien encore les clients/fournisseurs.
Enfin, certaines parties prenantes ne sont ni impliquées ni intéressées par la réussite des activités de l'organisation, mais peuvent toutefois avoir une influence sur certains aspects de l'organisation, et par extension, à leur réussite. C'est par exemple le cas de autorités de régulation et de supervision.
Une fois les parties prenantes identifiées, le Conseil doit déterminer quelles sont leurs attentes et leurs besoins. Les fournisseurs souhaiteront être payés dans les délais impartis, les actionnaires bénéficier de dividendes à hauteur de leur espérance.
Enfin, le Conseil doit évaluer les limites de ce qui peut être acceptable pour chacune des parties prenantes. Autrement dit, déterminer les seuils de tolérance de chacune selon le niveau d'appétence pour le risque de l'organisation. Ces seuils sont ensuite communiqués à la direction générale.
Le Conseil joue donc un rôle essentiel dans la gouvernance de l'organisation. Pour être pérenne, la gouvernance doit s'appuyer sur l'autorité, l'orientation et la supervision.

- La direction générale

Les seuils de tolérance déterminés par le Conseil, celui-ci délègue aux membres de la direction générale le pouvoir de gérer les différentes activités de l'organisation, dans les limites posées par ces seuils.

[5] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-6 à 3-15

L'une des principales responsabilités de la direction générale consiste à appliquer les orientations stratégiques dictées par le Conseil, afin de parvenir aux objectifs recherchés, à nouveau tout en respectant les seuils de tolérance établis.
Pour ce faire, la direction générale doit faire en sorte que toutes les orientations soient bien assimilées, et que la délégation des pouvoirs s'y rapportant soit bien comprise au sein de l'organisation. Cela n'est possible que si la direction générale a bien cerné les éléments que sont les attentes du Conseil en termes de gouvernance, le pouvoir que celui-ci lui a conféré, les seuils de tolérance, ainsi que les exigences de reporting envers le Conseil.
Un autre rôle essentiel de la direction générale est celui de la gestion des risques, vue de manière globale. Cela consiste à déterminer qui sont les « propriétaires de risques » (cfr infra), à gérer les risques pouvant aboutir à des évènements jugés inacceptables, ou bien encore à la manière de gérer ces risques. Cette fonction de la gestion des risques, composante clé de la gouvernance, sera vue plus en détail dans le chapitre V.
Enfin, la direction générale doit veiller à ce que les propriétaires de risques fournissent suffisamment d'informations afin que les exigences de reporting envers le Conseil soient respectées.

- Les propriétaires de risques

« Les propriétaires de risques sont les personnes qui ont la responsabilité, au quotidien, de veiller à ce que les activités de gestion des risques permettent de gérer efficacement les risques conformément aux seuils de tolérance au risque de l'organisation. » [6]
Ces personnes ont pour tâches l'identification, la mesure, la gestion et le pilotage des risques. Elles rendent ensuite compte à leur hiérarchie, en général aux membres de la direction. Parfois, les propriétaires de risques se situent à un niveau hiérarchique inférieur de l'organisation, auquel cas ils collaborent avec la direction générale afin que les activités de gestion des risques soient menées à bien.
Ils sont des acteurs essentiels de la gouvernance, puisque placés en première ligne de la gestion des risques. Leur rôle est d'une importance déterminante sur la capacité de l'organisation à faire face ou à échapper à des évènements jugés inacceptables.

- Les activités d'assurance (ou fonctions de contrôle)

« Par activité d'assurance, l'on entend l'examen objectif d'éléments probants, effectué en vue de fournir à l'organisation une évaluation indépendante des processus de gouvernement d'entreprise, de management des risques et de contrôle. » [7]

[6] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-13
[7] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-15

Ces activités d'assurance indépendantes constituent la dernière composante de la gouvernance de l'organisation. Elles ont donc pour rôle de donner au Conseil et à la direction générale, une évaluation objective de l'efficacité des activités de gouvernance et de gestion des risques. Ces activités peuvent être menées par diverses parties, appartenant ou non à l'organisation (audit interne, audit financier externe).
Nous développerons davantage cette partie sur les activités d'assurance dans la deuxième partie.

CHAPITRE 2 : LA GOUVERNANCE AU SEIN DES BANQUES

Comme pour tout autre secteur d'activité, une gouvernance efficace est primordiale au bon fonctionnement des établissements de crédit, et par extension, de l'économie dans son ensemble.
A la suite de la crise financière de 2008, l'une des préoccupations principales exprimées a été la nécessité d'une gouvernance adaptée au sein des établissements financiers.
En effet, les banques jouent un rôle crucial dans le système économique en amenant les fonds des épargnants et des déposants vers des activités qui contribuent au développement des entreprises et à la croissance économique.
La stabilité financière étant largement dépendante de la stabilité et de la solidité des banques, la manière dont celles-ci sont gérées est fondamentale pour le bon fonctionnement du système financier et pour la bonne santé de l'économie en général.
Ainsi, lorsque la gouvernance des banques n'est pas adaptée et présente de nombreux points de fragilité, c'est tout le système bancaire et l'ensemble de l'économie qui sont mis en péril. [8]

En septembre 2017, la Banque Nationale de Belgique (BNB) a publié un Manuel de gouvernance pour le secteur bancaire. [9] Il vise à rassembler l'ensemble des documents de politique applicables aux établissements de crédit en matière de gouvernance : loi bancaire, règlements, circulaires, règlementation européenne, normes internationales. Il est bien précisé que ce manuel ne porte aucunement préjudice aux compétences des autres autorités de contrôle, que peuvent être l'Autorité des Services et des Marchés Financiers (FSMA) ou bien encore la Banque Centrale Européenne (BCE), dans le domaine de la gouvernance. Outre la description des qualités requises pour les actionnaires, les associés, les dirigeants ou bien encore les fonctions de contrôle indépendantes, le manuel met en exergue le caractère approprié pour l'organisation des banques.
Cinq éléments importants y sont consacrés. Ils correspondent aux points de ce deuxième chapitre sur la gouvernance des banques.

2.1 Principes généraux de l'organisation de l'entreprise (bancaire)

L'article 21, § 1er de la loi bancaire, stipule que *« Tout établissement de crédit doit disposer d'un dispositif solide et adéquat d'organisation d'entreprise, dont des mesures de surveillance, en vue de garantie une gestion efficace et prudente de l'établissement. »* [10]
Il s'agit d'une disposition essentielle inhérente au statut légal des établissements de crédit, devant être respectée dans tous les cas.

[8] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks.* P. 3
[9] Banque Nationale de Belgique (2017). *Manuel de gouvernance pour le secteur bancaire*
[10] Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

La loi bancaire concrétise cette exigence à travers une liste d'éléments nécessaires à la mise en place de ce dispositif adéquat d'organisation d'entreprise [11] :

2.1.1 Une structure de gestion

Cette structure doit être transparente et refléter une gestion prudente et efficace.
La pierre angulaire de ce principe est la séparation claire entre les fonctions responsables de la direction effective et les fonctions de contrôle sur cette direction :
Ainsi, la *fonction de politique générale*, définissant la stratégie et la politique de l'organisation, est confiée aux administrateurs exécutifs et non exécutifs de l'organe légal d'administration.
NB : Organe légal d'administration et Conseil d'administration sont deux appellations équivalentes, qui seront toutes deux utilisées par la suite.
La *fonction de management*, qui dirige proprement dit l'activité de l'entreprise, est à charge des administrateurs exécutifs siégeant au comité de direction.
Et enfin la *fonction de surveillance*, contrôlant le management, est attribuée aux administrateurs non exécutifs, comme les membres des différents comités consultatifs de l'organe légal d'administration : comité d'audit, de la compliance, de la gestion des risques, des nominations, etc.

2.1.2 Une organisation administrative et comptable

En vue de disposer d'un processus de reporting financier fiable, l'établissement bancaire doit disposer d'une organisation administrative et comptable adéquate, ainsi qu'un contrôle interne efficace.

2.1.3 Des procédures en matière de risques

L'organe de direction doit connaître et comprendre pleinement la structure opérationnelle de l'établissement (principe de « connaissance de sa propre structure »), et s'assurer de sa compatibilité avec la stratégie et le profil de risque qui ont été adoptés. [12] En effet, lorsqu'un établissement crée de nombreuses entités au sein de son groupe, ce qui est monnaie courante dans le monde bancaire, leur nombre, leurs interconnexions et les transactions exécutées entre elles, peuvent poser des difficultés pour la conception du dispositif de gouvernance interne de l'établissement et pour la gestion et la surveillance des risques du groupe dans son ensemble, ce qui représente un risque en soi.

[11] Art. 21, § 1er, 1° à 9°, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[12] EBA European Banking Authority (2011). *Orientations de l'ABE sur la gouvernance interne (GL 44).* Principe 6

2.1.4 Des fonctions de contrôles indépendantes

Les banques doivent disposer de fonctions d'audit interne, de gestion des risques et de conformité (compliance) indépendantes, efficaces et permanentes.
Elles sont plus que nécessaires pour que la direction effective puisse réaliser ses tâches de manière optimale. Les avis et constats apportés par ces fonctions sont traduits par la direction sous forme de mesures visant à renforcer la structure de gestion, l'organisation ou le contrôle interne. Il est à noter qu'aucun domaine d'activité de l'établissement de crédit ne peut être écarté de la portée de ces fonctions de contrôle, notamment les activités off-shore.
Nous y reviendrons largement dans la deuxième partie.

2.1.5 Une politique d'intégrité

Les procédures, les mécanismes de contrôle et la structure de gestion ne suffisent pas à développer une bonne gouvernance. Elle s'acquière également en obtenant l'engagement et le dévouement de l'ensemble des collaborateurs. Pour cela, l'organe légal d'administration décide, fait communiquer et promouvoir, les valeurs de l'établissement, ses objectifs stratégiques, ou bien encore ses codes de conduite.
Selon l'expression « tone at the top », il est important que la direction montre le bon exemple.
La fonction de compliance joue un rôle essentiel dans le maintien de la politique définie par l'établissement, en veillant notamment sur les mesures nécessaires au respect des dispositions légales et réglementaires en matière d'intégrité et de conduite par les membres du personnel.

2.1.6 Une politique de rémunération

Le but étant que les objectifs personnels des membres du personnel et les intérêts à long terme de l'établissement de crédit soient alignés.
Pour cela, ce dernier doit faire en sorte qu'une politique et des pratiques en matière de rémunération soient mises en place et maintenues, ce qui permettra une maîtrise efficace en termes de risques.

2.1.7 Des mécanismes de contrôle et de sécurité dans le domaine IT

Les banques doivent disposer de mécanismes de contrôle et de sécurité appropriés dans le domaine informatique, aussi bien pour les domaines de l'externalisation, de la continuité des activités, mais également pour les services financiers via Internet (PC Banking, plateformes).

2.1.8 Un système d'alerte interne ; le régime « whistleblowing »

Il s'agit de canaux permettant aux collaborateurs de faire part en interne, de préoccupations à propos d'infractions aux valeurs de l'établissement, aux codes de conduite, ou bien à propos de comportements jugés contraires à l'éthique ou illégaux, et ce, pour des aspects de la compétence et du contrôle de la banque.
Ce régime doit être conforme à la législation en vigueur en matière de la protection de la vie privée
Les « whistleblowers » (dénonciateurs) doivent pouvoir porter plaintes sans passer par les canaux hiérarchiques normaux, soit directement à la direction, soit indirectement par l'intermédiaire de fonctions telles que médiateur, compliance ou audit interne.
La direction doit veiller à ce que l'information communiquée par les « whistleblowers » soit examinée, et que des mesures nécessaires soient prises, le cas échéant.

2.1.9 Des mesures de continuité de l'activité

L'établissement bancaire doit faire en sorte que sa gouvernance soit adaptée de telle manière à ce qu'en cas d'interruption sérieuse et non planifiée de ses activités, il puisse maintenir ou rétablir ses fonctions critiques le plus rapidement possible, et puisse de ce fait reprendre dans un délai raisonnable, l'exercice de ses activités normales et la fourniture de ses services habituels.

2.2 Mémorandum de gouvernance [13]

Il s'agit d'un document prudentiel faisant partie intégrante du dossier d'agrément, et qui par conséquent est confidentiel. Il reprend l'ensemble des modalités d'organisation interne de l'établissement de crédit, et est de la responsabilité de celui-ci. Il est approuvé et évalué au moins une fois par an par l'organe légal d'administration, et est adapté chaque fois que des modifications significatives influençant la structure de gestion et l'organisation de la banque ont lieu. Enfin, le mémorandum et ses modifications significatives sont communiqués à l'autorité de contrôle, et évalués par celle-ci.

Si la structure de gestion de la banque est jugée déficiente, l'autorité de contrôle utilisera les pouvoirs qui lui sont conférés par la loi bancaire, pour l'amener à mettre en place une organisation adéquate. Un modèle de mémorandum de gouvernance a été joint en annexe du Manuel de gouvernance, publié par la BNB en septembre 2017. [14]

[13] Art. 21, § 3 de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[14] Voir Annexe 1 - Modèle de mémorandum de gouvernance

2.3 Organe légal d'administration (Conseil d'administration) [15]

L'organe légal d'administration assume la responsabilité globale de l'établissement de crédit.

Comme déjà détaillé dans le point 2.2, deux fonctions principales sont du ressort du Conseil d'administration : la fonction de politique générale ou d'orientation stratégique, et celle de surveillance ou de supervision.

La *fonction de politique générale* consiste à définir la stratégie et l'orientation des activités de la banque. Cela concerne entre autres la politique commerciale, le profil de risque souhaité ainsi que la gestion et la maîtrise des risques, l'adéquation du capital interne, la sous-traitance, la continuité des activités, l'intégrité, l'acceptation de la clientèle ou bien encore les conflits d'intérêts.
Le seuil de tolérance au risque de la banque pour l'ensemble de ses activités est fixé par l'organe légal d'administration. En outre, il est responsable des décisions stratégiques en matière de risques ainsi que du contrôle continu du profil de risque de l'établissement et de son évolution. A cette fin, il doit disposer continuellement d'informations complètes et pertinentes, transmises notamment par les comités d'audit et de risques, sur les risques encourus par la banque.
Une autre compétence du Conseil d'administration, qui ne peut être déléguée à un comité spécialisé, est de préciser les critères déterminant si oui ou non une opération de crédit entraîne un risque de crédit ou de contrepartie majeur, et le cas échéant, s'y opposer.

La seconde grande responsabilité de l'organe légal d'administration est la *fonction de surveillance*. Elle doit s'étendre à l'ensemble des domaines d'activité de la banque, et incombe aux administrateurs non exécutifs (ne faisant pas partie du comité de direction).
Il s'agit de surveiller les activités et d'évaluer régulièrement la structure de gestion, l'organisation et les mécanismes de contrôle interne de l'établissement de crédit.
Ce contrôle porte également sur les membres du comité de direction et sur les dirigeants effectifs, grâce aux pouvoirs d'enquête conférés aux membres du Conseil d'administration, et au reporting sur l'évolution de l'activité de la banque.
L'organe légal d'administration doit aussi vérifier périodiquement, et au moins une fois par an, la bonne exécution des fonctions de contrôle indépendantes.
Pour cela, il s'appuie sur les nombreux contacts avec les membres de ces fonctions, ainsi que sur le rapport périodique rédigé par le comité de direction. Ce dernier a pour rôle de pallier aux manquement, le cas échéant.
De plus, il est responsable de la politique de rémunération (il peut s'appuyer sur un comité de rémunération, cfr infra), de la mise à jour et de la transmission du mémorandum de gouvernance à l'autorité de contrôle, ou bien encore de la fiabilité et de l'intégrité d'une série d'aspects relatifs au fonctionnement interne de la banque (domaines IT, publication, etc).

[15] Art. 23 ; 24 ; 56-58, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

Enfin, concernant la composition de l'organe légal d'administration, son président ne peut être la même personne que celui du comité de direction.
Par ailleurs, les membres non exécutifs ne faisant pas partie du comité de direction, au sein du Conseil d'administration doivent être majoritaires.

2.4 Comité de direction [16]

Tout établissement de crédit doit constituer, au sein de l'organe légal d'administration, un comité de direction. Ce dernier a pour vocation d'améliorer l'efficacité du contrôle dit bicéphale et la collégialité de la prise de décision concernant la bonne gestion de la banque.
Autrement dit, ce comité constitué au sein même de l'organe légal d'administration, n'entrave en rien l'attribution de responsabilités spécifiques (non exclusives) à ses membres.
Ainsi, en cas de conflits d'intérêt pouvant survenir dans le cadre de domaines d'activités différents, cette attribution de responsabilités en interne en permet une gestion efficace.
Cette attribution de domaines de compétences spécifiques, ou toute modification pouvant lui être apportée, doit être actée dans le mémorandum de gouvernance et communiquée à l'autorité de contrôle.
Comme déjà stipulé précédemment, tous les membres exécutifs du Conseil d'administration, et eux seuls, doivent faire partie du comité de direction, et à ce titre, sont responsables de la gestion journalière de la banque. De cette manière, la fonction de management est clairement distinguée de celles de surveillance et de contrôle, au sein de l'organe légal d'administration.

« Sans préjudice des pouvoirs dévolus à l'organe légal d'administration et sous sa surveillance, le comité de direction prend les mesures nécessaires pour assurer le respect de la mise en œuvre des dispositions de l'article 21. » [17](cfr point 3.1 - Principes généraux de l'organisation de l'entreprise (bancaire)).

Pour cela, « *le comité de direction fait rapport au moins une fois par an à l'organe légal d'administration, au commissaire agréé et à l'autorité de contrôle concernant l'évaluation de l'efficacité des dispositifs d'organisation visés à l'article 21 et les mesures prises le cas échéant pour remédier aux déficiences qui auraient été constatées. Le rapport justifie en quoi ces mesures satisfont aux dispositions légales et réglementaires ».*[18]
De la sorte, le comité de direction dirige les activités de la banque ainsi que la mise en place et le suivi de sa structure de gestion.
Il surveille le respect des compétences et des responsabilités attribuées aux membres de l'établissement de crédit, mais également l'information financière produite.
Il met en œuvre les mesures nécessaires pour assurer la maîtrise des risques.

[16] Art. 24-26 ; 59-60, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[17] Art. 59, § 1er, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[18] Art. 59, § 2, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

Il veille à ce que la politique de rémunération adoptée par l'organe légal d'administration soit correctement mise en œuvre.
Il doit également assurer l'organisation et l'évaluation des mécanismes et des procédures de contrôle interne, particulièrement les fonctions de contrôle indépendantes que sont celles de la gestion des risques, de la compliance et de l'audit interne.
Une organisation efficace du système de contrôle interne doit par ailleurs permettre un reporting interne fiable et une bonne communication de l'information financière, en vue d'assurer la conformité des comptes annuels avec la réglementation comptable en vigueur.
Enfin, pour que le Conseil d'administration puisse définir correctement la politique générale et la stratégie de l'établissement bancaire, le comité de direction lui confère des propositions et des avis, et lui fournit les informations nécessaires pour qu'il puisse prendre des décisions en toute connaissance de cause.

2.5 Comités [19]

Dans le but de renforcer l'efficacité du contrôle et de la surveillance des activités, du profil de risque et de l'organisation de la banque, l'organe légal d'administration doit constituer en son sein, quatre comités spécialisés que sont le comité d'audit, le comité des risques, le comité de rémunération et le comité de nomination.

Ce sont des comités consultatifs et spécialisés, chargés d'approfondir des domaines précis et de conseiller l'organe légal d'administration en la matière.

La prise de décision proprement dite est toujours à charge de l'organe légal d'administration, qui exerce ses pouvoirs en collège.

Seuls font partie de ces comités, les membres non exécutifs du Conseil d'administration, qui ne participent donc pas à la direction effective de l'établissement bancaire.
Ils viennent consolider la fonction de contrôle attribuée à l'organe légal d'administration.
Le comité d'audit est majoritairement composé de membres indépendants, alors que pour les autres comités, au moins un administrateur doit être indépendant. [20]
Afin de disposer d'une répartition équilibrée des responsabilités des membres non exécutifs de l'organe légal d'administration, et d'optimiser la disponibilité des administrateurs, un même membre non exécutif de l'organe légal d'administration ne peut siéger que dans trois comités différents.
Certaines mesures ont été prises afin d'assurer le bon fonctionnement des différents comités.
Tout d'abord, le président d'un comité ne peut être le président de l'organe légal d'administration.

[19] Art. 27-34, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[20] Au sens de l'article 526ter du Code des sociétés pour les critères d'indépendance

Chaque comité doit recevoir un mandat écrit, un règlement interne, de l'organe légal d'administration, définissant son champ d'activités, sa composition ou bien encore ses règles de fonctionnement. Ce mandat doit être rendu public dans un souci de transparence.
Le Conseil d'administration doit prévoir un système de rotation périodique des sièges et de la présidence de ces comités, afin d'éviter une concentration injustifiée des pouvoirs et de permettre l'expression de nouveaux points de vue. [21]
Des personnes externes aux comités peuvent participer aux réunions, pour en améliorer l'efficacité. Cela peut être le président, un membre du comité de direction, le commissaire agrée ou bien encore l'auditeur interne.
Il est à noter qu'en plus des quatre comités précités et détaillés ci-dessous, imposés par la législation, d'autres comités peuvent être mis en place comme le comité de compliance, le comité stratégique ou bien encore le comité d'investissement.

2.5.1 Le comité d'audit [22]

Le §1 de l'article 28 stipule que ; « *Les membres du comité d'audit disposent d'une compétence collective dans le domaine d'activités de l'établissement de crédit concerné et en matière de comptabilité et d'audit et au moins un membre du comité d'audit est compétent en matière de comptabilité et/ ou d'audit. »*
Le §2de l'article 28 énumère les missions principales confiées au comité d'audit.
Il doit tout d'abord superviser le processus de reporting financier (information financière) et veiller à son intégrité.
Il vérifie l'efficacité des mécanismes de contrôle interne et des fonctions de gestions des risques.
Il assure la surveillance des auditeurs internes et externes, tout en étant leur interlocuteur.
Il est en cela le destinataire des principaux rapports d'audit et doit s'assurer que la direction adopte immédiatement les mesures adéquates pour remédier aux insuffisances décelées par les auditeurs ou autres fonctions de contrôle.
Il est également chargé du suivi du contrôle légal des comptes annuels et des comptes consolidés (dans le cadre des groupes bancaires).
Enfin, il évalue et surveille l'indépendance du commissaire agréé, tout en discutant avec lui de questions importances ayant attrait au contrôle.

[21] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks.* P. 16
[22] Art. 28, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

2.5.2 Le comité des risques [23]

§1 de l'article 29 ; « *Les membres du comité des risques disposent individuellement des connaissances, des compétences, de l'expérience et des aptitudes nécessaires pour leur permettre de comprendre et d'appréhender la stratégie et le niveau de tolérance au risque de l'établissement.* »
En effet, au vu de la complexité du domaine, les membres du comité des risques doivent disposer d'un bagage professionnel ou académique suffisant pour acquérir l'esprit critique nécessaire à leurs responsabilités.
Le comité des risques fournit à l'organe légal d'administration des avis consultatifs sur l'appétence pour le risque actuelle et future de la banque.
Il surveille la mise en œuvre par la direction de la déclaration d'appétence pour le risque, rend compte de la culture du risque dans la banque, et est l'interlocuteur de la direction de la gestion des risques, dont il assure également la surveillance.

En outre, il est chargé de surveiller les stratégies de gestion de la liquidité et des fonds propres, mais également les stratégies relatives à tous les risques auxquels la banque est exposée, comme les risques opérationnels, de crédit, de marché et de réputation, afin de s'assurer de leur cohérence avec l'appétence pour le risque telle qu'établie.[24]
Le comité des risques doit aussi examiner la politique de tarification proposée aux clients, et faire en sorte que les prix des produits présentés à la clientèle tiennent compte des risques supportés par la banque, en conformité avec sa stratégie en matière de risques.

2.5.3 Le comité de rémunération [25]

§1 de l'article 30 ; « *Le comité de rémunération est composé de manière à lui permettre d'exercer un jugement pertinent et indépendant sur les politiques et les pratiques de rémunération et sur les incitants créés au regard de la maîtrise des risques, des besoins en fonds propres et de la position de liquidité.* »

Le comité de rémunération doit ainsi vérifier si les incitants créés par la politique de rémunération mise en place par l'organe légal d'administration, en ce y compris le système de promotion, ne vont pas engendrer des prises de risques excessives ou mener à des comportements poursuivant d'autres intérêts que celui de la banque et de ses parties prenantes (cfr point 2.3 - Acteurs dans la gouvernance et leurs rôles).

[23] Art. 29, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[24] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks.* P. 18
[25] Art. 30, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

A cette fin, le comité de rémunération travaille souvent en étroite collaboration avec le comité des risques, pour déterminer si les incitations générées par le système de rémunération tiennent bien compte des risques, des fonds propres, de la liquidité ou de la probabilité de gains et du moment de leur obtention. [26]

2.5.4 Le comité de nomination [27]

§1 de l'article 31 ; « *Le comité de nomination est composé de manière à lui permettre d'exercer un jugement pertinent et indépendant sur la composition et le fonctionnement des organes d'administration et de gestion de l'établissement, en particulier sur l'expertise individuelle et collective de leurs membres et sur l'intégrité, la réputation, l'indépendance d'esprit et la disponibilité de ceux-ci. »*

Selon l'environnement dans lequel évolue l'établissement, et son évolution, le comité de nomination doit identifier les besoins de l'organe légal d'administration, pour ensuite définir le profil adéquat recherché pour y répondre.
Il élabore pour cela une description des missions et des qualifications liées à une nomination donnée et évalue le temps à consacrer à ces fonctions.
Par ailleurs, il évalue périodiquement, et au moins une fois par an, divers éléments que sont la structure, la taille, la composition et les performances de l'organe légal d'administration, et lui soumet des recommandations en cas de nécessité de changements.
Il évalue également périodiquement les connaissances, les compétences, l'expérience ou le degré d'implication, notamment l'assiduité, des membres du Conseil d'administration, que ce soit sur le plan individuel ou collectif.
Il en va encore de même concernant les politiques de l'organe légal d'administration en matière de sélection et de nomination de ses membres exécutifs.
Le comité de nomination fixe également un objectif à atteindre en ce qui concerne la représentation du sexe sous-représenté au sein du Conseil d'administration, et élabore une politique en vue d'atteindre cet objectif.
Enfin, le comité de nomination doit veiller à ce que la prise de décision au sein de l'organe légal d'administration ne soit pas dominée par une personne ou un petit groupe de personnes, d'une manière qui soit préjudiciable aux intérêts de la banque dans son ensemble.

[26] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks.* P. 18
[27] Art. 31, §1, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

2.5.5 Dérogations [28]

L'obligation légale de mettre en place les quatre comités détaillés ci-dessus, au sein du Conseil d'administration, ne se justifie pas pour des établissements de crédit présentant un profil de risque réduit compte tenu de leur taille ou de la nature de leurs activités.

§1 de l'article 33 ; « *Les établissements de crédit qui ne sont pas d'importance significative sont dispensés de constituer, au sein de leur organe légal d'administration, les deux comités visés aux articles 30 (comité de rémunération) et 31 (comité de nomination).*
Ceux qui ne sont pas d'importance significative en application de l'article 3, 30°, b), peuvent, en outre, prévoir qu'un seul comité assure les missions dévolues aux comités visés aux articles 28 (comité d'audit) et 29 (comité des risques). »
Pour la définition légale d'un « établissement de crédit d'importance significative, il faut se référer à l'article 3, 30° de la loi bancaire. [29]

Ainsi, dans ces cas de figure précis, d'une part les banques sont dispensées de mettre en place les comités de nomination et de rémunération. Les fonctions attribuées à ces comités doivent alors être exercées par l'organe légal d'administration dans son ensemble (article 34).
Et d'autre part, elles peuvent fusionner les comités d'audit et des risques (lorsque le total du bilan est inférieur à 3 milliards d'euros – article 3,30°, b)).

[28] Art. 33-34, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[29] Art. 3, 30°, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse

PARTIE II : LES FONCTIONS DE CONTRÔLE

RÉFÉRENTIELS ET MODÈLE

Nous venons de mettre en exergue l'importance d'une gouvernance efficace et adéquate dans la poursuite des organisations à atteindre leurs objectifs.
Nous avons détaillé le rôle des acteurs de la gouvernance au sein des banques, ainsi que les responsabilités et les obligations légales de chacun d'entre eux, régies en grande partie par la loi bancaire.
Cependant, il ne suffit pas de mettre en place des mécanismes de gouvernance, en attribuant des rôles et en énumérant les tâches de chaque organe, comité, fonction de contrôle, etc. Encore faut-il le faire de façon adaptée et contrôlée.

Le Code belge de gouvernance d'entreprise de 2009 (le Code 2009) recommande au conseil d'administration de décrire les principales caractéristiques de contrôle interne et de gestion des risques dans sa déclaration de gouvernance d'entreprise.
En effet, les systèmes de contrôle interne et de gestion des risques ont un rôle essentiel dans le pilotage des activités et dans la maîtrise des risques permettant aux sociétés d'atteindre les objectifs fixés. Ils permettent de mieux maîtriser et de mieux contrôler l'ensemble des risques auxquels la société est confrontée (risques stratégiques, risques financiers, respect des lois et de la réglementation,…). En outre, ces systèmes visent aussi à assurer une publication fidèle des informations financières (reporting financier). [30]

Pour ce faire, le Code 2009 recommande au conseil d'administration d'approuver un cadre référentiel de contrôle interne et de gestion des risques, adapté aux particularités de la société ainsi qu'aux risques auxquels la société est sujette et qu'elle a acceptés de prendre. [31]
Un tel cadre référentiel doit être clair, définir la signification du « contrôle interne » et de la « gestion des risques » et aider le management exécutif à mettre en œuvre un système de contrôle interne et de gestion de risques. [32] Ce cadre doit contenir des systèmes d'identification, d'évaluation, de gestion et de suivi des risques financiers et autres. [33]

[30] Commission Corporate Governance. Fondation Privée (2011). *Contrôle interne et gestion des risques. Lignes directrices dans le cadre de la loi du 6 avril 2010 et du Code Belge de gouvernance d'entreprise 2009*. P. 3
[31] Commission Corporate Governance. Fondation Privée (2009). *Le code belge de gouvernance d'entreprise 2009.* Disposition 1.3
[32] Commission Corporate Governance. Fondation Privée (2009). *Le code belge de gouvernance d'entreprise 2009.* Ligne de conduite de la disposition 1.3
[33] Commission Corporate Governance. Fondation Privée (2009). *Le code belge de gouvernance d'entreprise 2009.* Disposition 6.5

De manière générale, « un cadre de référence (ou référentiel) est un ensemble de principes directeurs qui forment une matrice par rapport à laquelle les organisations peuvent évaluer une multitude de pratiques. Ces pratiques se composent de divers concepts, valeurs, hypothèses et pratiques dont le but est de fournir une référence pour évaluer une structure, un processus ou un environnement, ou encore un groupe de pratiques ou de procédures. » [34]
Pour utiliser ces cadres de référence, l'Institut des Auditeurs Internes (IIA) donne les orientations suivantes : « En général, un cadre de référence fournit une structure schématique permettant de comprendre la relation entre un ensemble de connaissances et une ligne directrice. En tant que système cohérent, le cadre de référence permet d'uniformiser l'élaboration, l'interprétation, l'application des concepts er des méthodologies ainsi que els techniques utilisées dans un domaine ou une profession donnée. » [35]
Il existe plusieurs référentiels de contrôle interne et de gestion des risques reconnus au niveau mondial [36] :

- *Référentiels de contrôle interne* :

- *Le référentiel intégré de contrôle interne*, publié par le COSO (Committee of Sponsoring Organizations of the Treadway Commission) en 1992 (COSO I) et actualisée en 2013 (COSO III) ;
- *Recommandations sur le contrôle*, souvent appelé le cadre CoCo, publié en 1995 par l'Institut canadien des comptables agréés (ICCA) ;
- *Internal Control : Revides Guide for Directors on the Combined Code*, connu sous le nom de raport Turnbull, publié par le Financial Reporting Council en 1999 et actualisé en 2005 ;
- *Le cadre de référence de l'AMF*, publié en 2007 sous l'égide de l'Autorité des marchés financiers et actualisé en 2007

- *Référentiels relatifs au management des risques de l'entreprise* :

- *Le management des risques de l'entreprise (ERM), Cadre de référence – Techniques d'application*, publié par le COSO en 2004 (COSO II) ;
- *Australian/New Zealand Standard Risk Management publié en 1995 ;*
- *Management du risque – Principes et lignes directrices (norme ISO 31000)*, publié par l'Organisation internationale de normalisation (ISO), Suisse, en 2009

[34] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-2
[35] IIA & IFACI (2014). *Cadre de référence international des pratiques professionnelles de l'audit interne*. P. 45
[36] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-3

Nous nous intéressons plus particulièrement aux cadres de références publiés par le COSO aussi bien pour le contrôle interne (COSO I & III) que pour le management des risques (COSO II). Il s'agit de référentiels qui sont parmi les plus reconnus et les plus couramment utilisés par les organisations et notamment les banques.

CHAPITRE 3 : CONTRÔLE INTERNE ET LE RÉFÉRENTIEL INTÉGRÉ COSO I & III

3.1 Définitions et concepts fondamentaux

Historiquement, l'élaboration et le développement outre-Atlantique des référentiels de gestion des risques sont liés à une volonté institutionnelle de lutte contre la fraude.
Les scandales financiers intervenus aux Etats-Unis dans les années 1970 ont renforcé la législation en matière de lutte contre la corruption et la fraude, avec l'adoption en 1977 du *Foreign Corrupt Practice Act*, imposant des dispositifs de contrôle interne aux entreprises, ceux-ci n'étant auparavant définis que par les normes d'audit externe édictées par l'AICPA (*American Institute of Certified Public Accountants).* [37]
En 1985, la *National Commission on Fraudulent Financial Reporting* (appelée Treadway Commission) est créée suite à l'alliance de cinq associations professionnelles aux Etats-Unis.[38]
Par la suite, la Treadway Commission s'est à nouveau réunie afin de réfléchir à la construction d'un cadre commun de contrôle interne, qui a vu le jour en 1992 sous le nom de Committee *of Sponsoring Organizations* (COSO).

Le COSO définit le contrôle interne en ces termes : « Un processus mis en œuvre par le Conseil d'administration, le management et les collaborateurs d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité. » [39]

De cette définition générale, il est important de détailler certains de ses aspects. [40]
Tout d'abord, le contrôle interne est basé sur la réalisation d'objectifs provenant d'une ou plusieurs catégories qui se recoupent : objectifs liés aux opérations proprement dites, objectifs liés au reporting ou bien encore objectifs liés à la conformité.

---

[37] Pierandrei, L. (2015). Risk Management. *Gestion des risques en entreprise, banque et assurance.* Dunod. Section 1 Référentiels de la gestion du risque. 1.1 COSO

[38] Accounting Association (AAA), The American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), The National Association of Accountants maintenant appelée The Institute of Management Accountants (IMA)

[39] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-9

[40] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 30

Ensuite, le contrôle interne est un processus qui repose sur la mise en œuvre de tâches et d'activités communes. A cet égard, il constitue un moyen et non une fin en soi.
Il est assuré par des personnes, œuvrant à tous les niveaux de l'organisation et ne peut par conséquent se cantonner à un ensemble de règles, à des manuels de procédures, à des documents ou des systèmes.
Il permet au Conseil d'administration et à la direction générale d'obtenir une assurance raisonnable et non une assurance absolue.

Enfin, le contrôle interne est adaptable à la structure de toute organisation., Il permet ainsi une certaine souplesse d'application pour l'ensemble de l'organisation ou une filiale d'un groupe, une division, une unité opérationnelle ou un processus métier en particulier.
Il est applicable dans différents types d'organisations, de secteurs d'activités ou de zones géographiques.
Cela laisse la possibilité à toute organisation de se focaliser sur son système global de contrôle interne, ou bien de se concentrer sur des contrôles visant des unités ou des activités spécifiques, ou bien encore de se cantonner par exemple uniquement au contrôle interne relatif au reporting ou à la conformité aux lois et règlements.

Avant de présenter le référentiel COSO I et sa mise à jour COSO III à proprement parler, en voici la définition générale donnée par le COSO :
« Un référentiel intégré de contrôle interne permet aux organisations de développer, de manière efficace et efficiente, des systèmes de contrôle interne qui s'adaptent aux évolutions de l'environnement économique et opérationnel et qui visent à maîtriser les risques en les ramenant à des niveaux acceptables. Ils permettent ainsi une prise de décision éclairée et une bonne gouvernance. » [41]

3.2 Le référentiel COSO I (1992) et son évolution vers COSO III (2013)

Avant tout chose, il est important de signaler que nous ne présentons pas successivement en détail les référentiels COSO I puis COSO III.
La raison est que COSO III est essentiellement une mise à jour plutôt qu'une refonte. Notamment la définition, les composantes et les concepts clés restent les même que ceux du référentiel d'origine COSO I datant de 1992.[42]
C'est pourquoi la description des concepts fondamentaux (cube COSO, objectifs, composantes : cfr supra) englobe déjà les mises à jour de 2013 du référentiel COSO I.
Nous discuterons ensuite de la raison de cette mise à jour du référentiel d'origine.
Enfin, nous mettrons en exergue les principales évolutions entre les deux référentiels.

[41] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 31
[42] Vilepet, S. (2013). IFACI. Dossier Audit & Contrôle internes n°215. *Le COSO 2013 : une mise à jour du référentiel d'origine pour mieux maîtriser les évolutions*

3.2.1 Le cube COSO

Selon le COSO : « Il existe un lien direct entre les objectifs que l'organisation cherche à atteindre, les composantes du contrôle interne nécessaires à leur réalisation, et la structure de cette organisation (ses unités opérationnelles, ses entités juridiques,etc). » [43]

Ce lien est représenté dans le cube ci-après ;

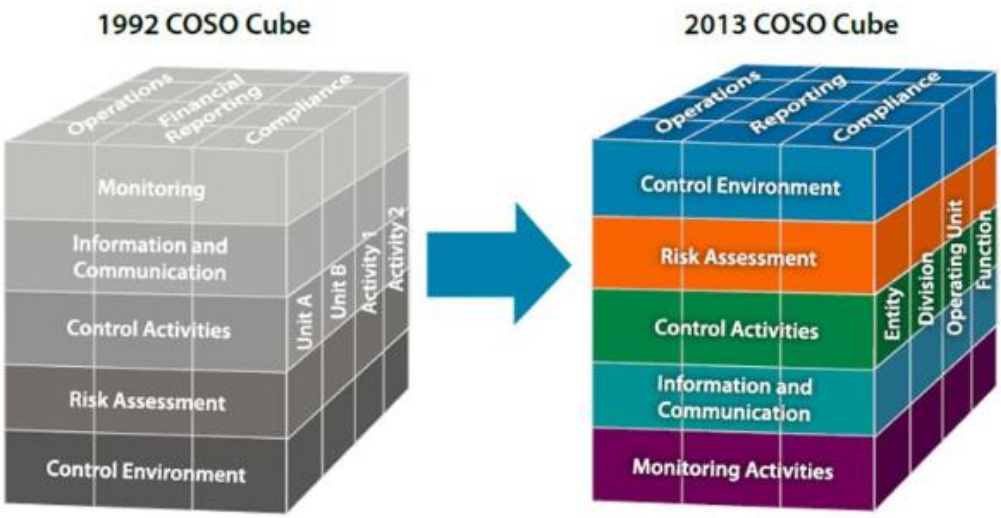

Figure 1 – Le cube COSO
Source : Committee of Sponsoring Organizations of the Treadway Commission

Le modèle du cube COSO est donc basé sur une architecture à trois plans :

- Les colonnes représentent les trois catégories d'objectifs ;
- Les lignes, les cinq composantes du contrôle interne ;
- La troisième dimension se réfère aux unités de l'organisation (entité/division/unité opérationnelle/fonction).

[43] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 39

3.2.2 Les objectifs [44]

Le référentiel COSO établit trois catégories d'objectifs, ce qui permet aux organisations de prendre en compte différents aspects du contrôle interne :

- *Les objectifs liés aux opérations :* ils concernent l'efficacité et l'efficience des opérations. Il s'agit par exemple des objectifs de performance financière ou opérationnelle, ou bien encore la sauvegarde des actifs ;

- *Les objectifs liés au reporting (information financière)* : ils concernent le reporting interne et externe, financier et extra-financier. [45]
  Ils peuvent englober la fiabilité, les délais, la transparence ou d'autres aspects demandés par les régulateurs, les organismes de normalisation ou les instructions internes ;

- *Les objectifs liés à la conformité* : ils concernent le respect des lois et règlements applicables.[46]

En outre le COSO recommande ceci : « un système de contrôle interne devrait fournir à une organisation un niveau d'assurance raisonnable quant à la réalisation des objectifs liés au reporting externe et à la conformité aux lois et règlements.
La réalisation de ces objectifs, qui sont principalement fondés sur des lois, règlements et normes établis par les législateurs, les régulateurs et les organismes de normalisation, dépend de la façon dont sont conduites les activités relevant du périmètre de responsabilité de l'organisation.
En règle générale, le management et/ou le conseil d'administration auront plus de latitude pour définir les objectifs liés au reporting interne qui ne sont pas directement régis par des tiers. Néanmoins, l'organisation peut choisir d'aligner ses objectifs liés au reporting interne et externe afin que le reporting interne étaye mieux le reporting externe de l'organisation. » [47]

[44] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-11
[45] Le reporting extra-financier consiste à rendre compte de la performance sociétale de l'entreprise, à travers un rapport de développement durable. Il s'agit d'une nouveauté de COSO III. Sur le cube COSO, l'objectif « Financial Reporting » est devenu « Reporting », englobant le reportant financier et extra-financier (Voir Figure 1 – Evolution du cube COSO)
[46] [47] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P.31

3.2.3 Les composantes [48]

Pour atteindre ses objectifs, le COSO indique que « l'organisation peut s'appuyer sur cinq composantes du contrôle interne :

- L'environnement de contrôle ;
- L'évaluation des risques ;
- Les activités de contrôle ;
- L'information et la communication ;
- Les activités de pilotage.

Ces composantes du contrôle interne s'appliquent à l'échelle de l'organisation, à ses filiales, ses divisions ou unités opérationnelles, ses fonctions ou tout autre subdivision. » [49]
Cela est représenté sur le cube de COSO (cfr infra - Figure 1) par le lien entre la troisième dimension représentant la structure de l'organisation, et les lignes du cube représentant les cinq composantes du contrôle interne.
De façon simplifiée, *l'environnement de contrôle* constitue le milieu dans lequel les personnes accomplissent leurs tâches et assument leurs responsabilités en matière de contrôle.
Il sert de base pour les autres éléments du contrôle interne.
Dans cet environnement, les dirigeants *évaluent les risques* susceptibles de mettre en cause la réalisation d'objectifs spécifiques.
Les *activités de contrôle* sont mises en place pour permettre à la direction de s'assurer que ses directives visant à traiter ces risques ont été exécutées.
Entre-temps, les *informations* pertinentes sont recueillies et *communiquées* à l'ensemble de l'organisation.
Le processus complet fait l'objet d'un *pilotage* et de modifications le cas échéant.
Les cinq composantes sont expliquées plus en détail ci-après :

- L'environnement de contrôle [50]

Cette composante est fondamentale car elle crée le contexte dans lequel existent les autres composantes du contrôle interne. En effet, l'environnement de contrôle d'une organisation en imprègne tous les services et influence la manière dont les personnes abordent le contrôle interne.

---

[48] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-13
[49] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P.38
[50] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-13

Le COSO en donne une définition très complète : « L'environnement de contrôle est l'ensemble des normes, des processus et des structures qui constituent le socle de la mise en œuvre du contrôle interne dans toute l'organisation.
Le conseil et la direction générale font preuves d'exemplarité en ce qui concerne l'importance du contrôle interne, et notamment les normes de conduites attendues
Le management répercute et précise ces attentes aux différents niveaux de l'organisation.
L'environnement de contrôle englobe l'intégrité et les valeurs éthiques de l'organisation, les éléments permettant au conseil d'exercer ses responsabilités en matière de surveillance, la structure organisationnelle ainsi que l'attribution des pouvoirs et des responsabilités, le processus de recrutement, de formation et de fidélisation de personnes compétentes, et la robustesse des indicateurs, des mesures d'incitation et des gratifications favorisant le devoir de rendre compte de la performance.
L'environnement de contrôle a un impact déterminant sur l'ensemble du système de contrôle interne. » [51]
La culture d'entreprise et l'histoire de l'organisation influencent directement l'environnement de contrôle. Les objectifs de l'organisation sont atteints, en partie, grâce à l'environnement de contrôle qui, s'il est mis en œuvre efficacement, conduit à une culture d'entreprise qui valorise l'intégrité et met l'accent sur la sensibilisation au contrôle.
Pour parvenir à un tel environnement de contrôle, cela nécessite une exemplarité au plus haut niveau et par des règles et procédures appropriées, qui s'accompagnent souvent d'un code de conduite.
Ainsi, ces éléments favorisent l'adhésion aux valeurs de l'organisation et le travail en équipe pour atteindre les objectifs fixés.

- L'évaluation des risques [52]

Toutes les organisations sont confrontées à des risques, c'est-à-dire à des menaces qui pèsent sur la réalisation de leurs objectifs. Tous les risques, externes et internes, doivent être évalués.

Le COSO définit la notion de risque et décrit les étapes nécessaires à son évaluation :
« Toute organisation est confrontée à une diversité de risques, provenant de sources externes et internes. Un risque est défini comme la possibilité qu'un évènement survienne et ait un impact défavorable sur la réalisation des objectifs.
L'évaluation des risques implique un processus dynamique et itératif d'identification et d'analyse des risques susceptibles d'affecter la réalisation des objectifs.
Ces risques sont envisagés au regard des seuils de tolérance au risque. Pour déterminer la manière dont les risques seront gérés, il convient donc de commencer par les évaluer.

[51] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 75
[52] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-14

Pour pouvoir procéder à cette évaluation, il est nécessaire d'avoir préalablement définit des objectifs cohérents aux différents niveaux de l'organisation.
Le management spécifie des objectifs liés aux opérations, au reporting et à la conformité avec suffisamment de clarté pour pouvoir identifier et analyser les risques susceptibles d'affecter la réalisation de ces objectifs. Le management tient également compte de la pertinence des objectifs pour l'organisation. L'évaluation des risques nécessite par ailleurs que le management tienne compte de l'impact d'éventuelles évolutions dans l'environnement externe et dans son propre modèle économique, susceptibles de rendre le contrôle interne inefficace. » [53]
Une évaluation efficace des risques nécessite donc préalablement d'identifier et d'analyser ces risques. Ces deux aspects seront davantage détaillés dans le chapitre 4, lors de la présentation du cadre de référence relatif au management des risques de l'entreprise (ERM) publié par COSO en 2004.
Par ailleurs, la condition préalable à une identification des risques, à leur analyse, à leur évaluation et à leur traitement, est l'établissement d'objectifs clairs.
Il faut d'abord définir les objectifs dans l'optique de déterminer une stratégie, avant que le management puisse identifier les risques susceptibles d'empêcher la réalisation de ces objectifs et prendre les mesures nécessaires pour gérer les risques.
En conséquence, la fixation des objectifs est une condition préalable du contrôle interne et facilite son efficience et sa pertinence.

- Les activités de contrôle [54]

Les activités de contrôle sont les mesures prise par la direction générale, le Conseil et d'autres parties afin de maîtriser les risques et d'accroître la probabilité que les objectifs et buts fixés seront atteints. Les managers planifient, organisent et dirigent la mise en œuvre de mesures suffisantes pour donner une assurance raisonnable que les objectifs et buts seront atteints.

Le COSO rajoute ceci : « Les activités de contrôle sont réalisées à tous les niveaux de l'organisation et à divers stades des processus métier.
Elles peuvent également être mises en œuvre par l'intermédiaire des systèmes d'information.
Il peut s'agir de contrôles préventifs ou détectifs, incluant diverses activités manuelles et automatisées, comme des autorisations et des approbations, des vérifications, des rapprochements et des revues de performance opérationnelle. » [55]

[53] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 107
[54] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-15/16
[55] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 141

Tout comme les objectifs qu'elles sont censées permettre d'atteindre, les activités de contrôle peuvent être classées selon les trois catégories suivantes : opérations, reporting et conformité. Cependant, les activités de contrôle sont souvent conçues pour maitriser des risques multiples pouvant menacer les objectifs dans plus d'une catégorie.
Bien entendu, la catégorie à laquelle appartient un contrôle importe moins que la capacité de ce dernier à maîtriser le ou les risques auxquels elle correspond.

Il existe néanmoins un concept fondamental commun à tous les contrôles, ce que le COSO définit comme la séparation des tâches. Celui-ci consiste à répartir ou discriminer les tâches liées à l'autorisation des transactions, au traitement de ces transactions et à l'accès physique aux actifs liés à ces transactions sous-jacents. Exemple : les tâches liées à l'autorisation d'achat d'une marchandise, celles liées à l'exécution de l'achat et enfin celles liées à la réception et au stockage de la marchandise doivent être séparées. Lorsqu'il n'est pas possible de séparer des tâches, le management sélectionne et développe des activités de contrôle alternatives. [56]
L'objectif premier de la séparation des tâches entre différentes personnes est la réduction du risque d'erreur ou d'action inappropriée de la part d'une personne.

Dans un système de contrôle interne bien conçu, outre la séparation des tâches, de nombreuses activités de contrôle communément admises sont mises en place, telles que des évaluations de la performance et des activités de suivi, des autorisations (validations), des contrôles d'accès aux systèmes d'information, une documentation rigoureuse et détaillée, des contrôles relatifs à l'accès physique, des contrôles applicatifs des systèmes d'informations (entrées, traitements, sorties), ou bien encore des vérifications et rapprochements indépendants.

- L'information et la communication [57]

Une information de qualité doit être communiquée de façon appropriée. C'est en raison de l'interdépendance de ces deux notions que le COSO les regroupe.
Des informations pertinentes, exactes et opportunes doivent être disponibles pour les personnes qui en ont besoin, à tous les niveaux d'une organisation, pour la faire fonctionner efficacement.
L'information doit être au service des utilisateurs concernés, de sorte que ces derniers puissent assumer leurs responsabilités liées aux opérations, au reporting et à la conformité.
De plus, la communication doit également être élargie à d'autres aspects importants, tels que les attentes et les responsabilités des personnes et des groupes.

[56] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-16
[57] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-17

La communication avec les tiers (clients, fournisseurs, prestataires de services, régulateurs, auditeurs externes ou bien encore les actionnaires) est également importante et peut apporter des informations essentielles au fonctionnement des contrôles.
Il est essentiel de veiller à ce que l'information reste alignée sur les besoins de l'organisation pendant les périodes de changement. Il convient également de veiller à ce que cette information soit communiquée en temps opportun à toutes les parties intéressées.

De nombreux moyens de communications sont à la disposition d'une organisation.
Il peut s'agir de moyens matériels tels que des manuels, des notes d'information ou des panneaux d'affichage situés dans les lieux où les personnes se réunissent.
La communication peut aussi prendre la forme de réunions en face à face ou se faire de manière électronique via les courriels, les sites intranet, la vidéo-conférence ou bien encore les panneaux d'affichage électroniques.
La forme de communication optimale est déterminée par la culture de l'organisation et le contenu de l'information à partager. Etant donné que chaque personne reçoit et traite l'information différemment, la plupart des organisations utilisent divers outils pour que toutes les personnes puissent traiter et comprendre l'information qui leur est apportée.
Les actions du management reflètent fortement les valeurs de l'organisation, car les actes en disent plus long que les paroles.
Ainsi, la culture d'entreprise joue un rôle prépondérant dans la manière dont l'organisation communique ses priorités. C'est pourquoi les organisations ayant mis en place une culture de l'intégrité et de la transparence ont plus de facilité à communiquer que les autres.

- Les activités de pilotage [58]

Les systèmes de contrôle interne doivent être pilotés pour rester fiables.
COSO définit le pilotage comme étant des « évaluations continues, qui sont intégrées au cœur des processus métier à tous les niveaux de l'organisation, et qui permettent de disposer d'informations en temps voulu. Les évaluations ponctuelles, réalisées périodiquement, varient généralement en termes de périmètre et de fréquence, en fonction de l'évaluation des risques, de l'efficacité des évaluations continues et d'autres considérations d'ordre managérial.Les constats sont établis selon les critères définis par les régulateurs, les organismes de normalisation, le management et le conseil. Le cas échéant, les déficiences sont communiquées au management et au conseil. » [59]

Le pilotage est plus efficace lorsque l'on met en œuvre une approche à plusieurs niveaux :

[58] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 6-18/19/20
[59] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P.185

Le premier niveau englobe les évaluations continues concernant les activités quotidiennes exécutées par la direction d'un secteur donnée.
Le second niveau concerne les évaluations ponctuelles, distinctes des évaluations non indépendantes de premier niveau. Il s'agit d'une démarche d'auto-évaluation des contrôles par le management. Ces évaluations visent à donner l'assurance que toutes les déficiences existantes ont été identifiées et réglées en temps opportun.
Selon le COSO, « une déficience peut correspondre à une insuffisance observée, potentielle ou réelle, ou représenter une opportunité de renforcer le système de contrôle interne, afin d'accroître la probabilité d'atteindre les objectifs de l'organisation ».
Et enfin, le troisième niveau reprend les évaluations indépendantes effectuées par un service ou une fonction extérieure, souvent l'audit interne [60], dans le but de valider la fiabilité et l'exactitude de l'auto-évaluation, réalisée par le management, à propos de l'efficacité des contrôles dans le secteur concerné.
Grâce à cette approche multiniveaux, l'organisation sait que le système de contrôle interne reste efficace, et que ses déficiences peuvent être identifiées et éliminées en temps opportun.
Cette stratégie est souvent désignée comme un modèle de « lignes de maîtrise multiples » dont l'exemple classique est le « modèle des trois lignes de défense » que nous verrons en détail au chapitre 4.
Comme déjà explicité dans le chapitre sur la gouvernance, la direction générale est la première responsable de l'efficacité du système de contrôle interne de l'organisation, y compris du pilotage. Lorsque certains contrôles relèvent de niveaux hiérarchiques supérieurs, la supervision traditionnelle devient plus délicate.
Les activités de pilotage effectuées par les subordonnés sont nettement moins efficaces que celles réalisées par les supérieurs.
Lorsque la direction générale exécute les contrôles, il peut être judicieux que d'autres membres de la direction générale pilotent ces contrôles.
Lorsqu'il y a un risque de contournement des contrôles par la direction générale, il peut être nécessaire que ce soit le Conseil d'administration qui effectue le pilotage.
In fine, c'est bien le Conseil d'administration qui est chargé de vérifier que la direction générale a mis en place un système de contrôle interne efficace.
Par conséquent pour remplir cette mission, il doit bien comprendre les risques pesant sur l'organisation, ainsi que la manière dont la direction générale les maîtrise à un niveau acceptable.

[60] D'autres parties prenantes fournissent également une certaine forme d'assurance : les services chargés de l'environnement et de la sécurité, les acteurs de l'assurance qualité, les services de contrôle des transactions, etc.

3.2.4 Nécessité d'une mise à jour du référentiel COSO I

Le référentiel intégré de contrôle interne COSO I, publié en 1992, a défini les fondamentaux du contrôle interne.
Cependant, pour mieux tenir compte de l'évolution de l'environnement économique réglementaire dans lequel évoluent les organisations, une mise à jour du référentiel a vu le jour le 14 mai 2013. Il s'agit de COSO III.
En effet, l'objectif de cette adaptation est de prendre du recul par rapport aux évolutions des vingt dernières années, depuis la parution du référentiel d'origine. En particulier [61] :

- Les risques nouveaux qui émergent et qui sont autant de nouveaux enjeux de contrôle interne (la cyber-criminalité, le cloud-computing,etc) ;
- Le rôle toujours plus important de la technologie (performance, sécurité, continuité,etc) ;
- Le recours intensifié à l'externalisation, avec un enjeu de bonne définition des attentes en matière de contrôle interne vis-à-vis des prestataires ;
- Les attentes accrues en matière de gouvernance, notamment les rôles des comités du conseil mais aussi de la direction générale sur des enjeux importants comme les risques, la conformité, etc ;
- Les responsabilités du personnel à tous les niveaux de la hiérarchie et dans toutes les entités de l'organisation ;
- La nécessité de s'adapter en permanence à un environnement interne et externe en mutation ;
- L'efficacité et l'efficience du dispositif du contrôle interne (articulation entre les opérationnels, les fonctions support et l'audit interne) ;
- Les exigences de reporting au-delà de la communication financière (développement durable, environnement, qualité,etc).

3.2.5 Principales évolutions de COSO I à COSO III

C'est par le biais de 17 nouveaux principes structurants que le COSO III définit les éléments essentiels en matière de contrôle interne pour aider les organisations, quels que soient leur taille ou leur domaine d'activité, à faire face dans un monde qui devient de plus en plus complexe. [62]

[61] IFACI & PWC (2013). Pocket Guide. COSO 2013. *Une opportunité pour optimiser votre contrôle interne dans un environnement en mutation*
[62] Vilepet, S. (2013). IFACI. Dossier Audit & Contrôle internes n°215. *Le COSO 2013 : une mise à jour du référentiel d'origine pour mieux maîtriser les évolutions*

Ces 17 principes correspondent aux concepts fondamentaux associés aux cinq composantes intégrées du contrôle interne. A ce propos, COSO précise que « tous ces principes étant directement dérivés des différentes composantes, une organisation peut mettre en œuvre un contrôle interne efficace en les appliquant tous. L'ensemble des principes s'applique aux objectifs liés aux opérations, au reporting et à la conformité. » [63]
Nous ne voyons pas en détail chacun de ces 17 principes. [64] Ils ont d'ailleurs été évoqués lors de la présentation des cinq composantes au point 3.2.3. Par contre, voici les principales évolutions qui en découlent : [65]

- Tout d'abord l'élargissement du domaine d'application au-delà du reporting financier. L'on parle dans ce cas de reporting extra-financier (cfr point 3.2.2 – objectifs liés au reporting). Par exemple la responsabilité sociale et environnementale ;
- Le renforcement des attentes en matière de gouvernance. Par exemple le rôle des comités et l'alignement avec le business model ;
- La gestion des collaborateurs clés du contrôle interne. Par exemple les plans de successions pour la direction générale ;
- L'articulation des 3 « lignes de maîtrise » dans l'organisation : les opérationnels, les fonctions support et l'audit interne. Nous y reviendrons largement au chapitre 5 ;
- Le rapprochement entre risque, performance et rémunération. Notamment le principe portant sur la responsabilisation pour le contrôle interne ;
- L'articulation du « tone at the top » avec les comportements à travers l'organisation (« tone in the middle »). Autrement dit, même si l'engagement de la direction reste primordial, celui du le middle management est aussi déterminant pour faire évoluer la culture de la gestion des risques et du contrôle interne ;
- La prise en compte des sous-traitants et des autres intervenants clés. Par exemple leur adhésion au code de conduite ;
- L'exigence de l'adaptabilité et l'adéquation du dispositif par rapport à l'évolution de l'organisation, liée par exemple à la mise en place de nouveaux processus, rôles, structures, systèmes d'information, centres de services partagés, périmètre d'activité, etc.

[63] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 123
[64] Voir Annexe 2 - Les 17 principes structurants du COSO III pour un contrôle interne efficace
[65] IFACI & PWC (2013). Pocket Guide. COSO 2013. *Une opportunité pour optimiser votre contrôle interne dans un environnement en mutation.*

CHAPITRE 4 : GESTION DES RISQUES ET LE RÉFÉRENTIEL INTÉGRÉ COSO II

4.1 Définitions et concepts fondamentaux

Le COSO a publié en 2004 *Enterprise Risk Management – Integrated Framework* (ERM), référentiel relatif au management des risques de l'entreprise, surnommé COSO II.

Il a perçu la nécessité d'établir un cadre de référence solide permettant d'aider les organisations à identifier, évaluer et gérer efficacement le risque. [66]

Le COSO définit le risque de la manière suivante : « la possibilité qu'un évènement survienne et ait un impact défavorable sur la réalisation des objectifs. » [67]

En outre, voici la définition que donne le COSO sur le management des risques de l'entreprise : « Processus mis en œuvre par le Conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les évènements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation. » [68]

De cette définition ressortent certains concepts fondamentaux [69] :
Tout d'abord, le management des risques est un processus permanent qui irrigue toute l'organisation. Il est mis en œuvre par l'ensemble des collaborateurs, à tous les niveaux de l'organisation. Il est également mis en œuvre à chaque niveau et dans chaque entité de l'organisation.
Ensuite, le management des risques est pris en compte dans l'élaboration de la stratégie. Il permet d'obtenir une vision globale de l'exposition aux risques à l'échelle de l'organisation, d'identifier les évènements potentiels susceptibles d'affecter l'organisation, et de gérer les risques en fonction de l'appétence pour le risque de l'organisation.
Enfin, le management des risques donne à la direction générale et au Conseil d'administration une assurance raisonnable quant à la réalisation des objectifs. Par ailleurs il est orienté vers l'atteinte d'objectifs appartenant à une ou plusieurs catégories indépendantes susceptibles de se recouper.

---

[66] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-5

[67] IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles. P. 21

[68] COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*

[69] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-5/6

4.2 Le référentiel COSO II (2004)

4.2.1 Le cube COSO ERM

Tout comme le référentiel intégré pour le contrôle interne, le cadre de référence relatif au management des risques de l'entreprise est représenté graphiquement au moyen d'un cube. Ce dernier illustré ci-dessous, montre qu'il existe une relation entre les différentes catégories d'objectifs, les éléments du management des risques de l'entreprise et la structure de l'organisation.

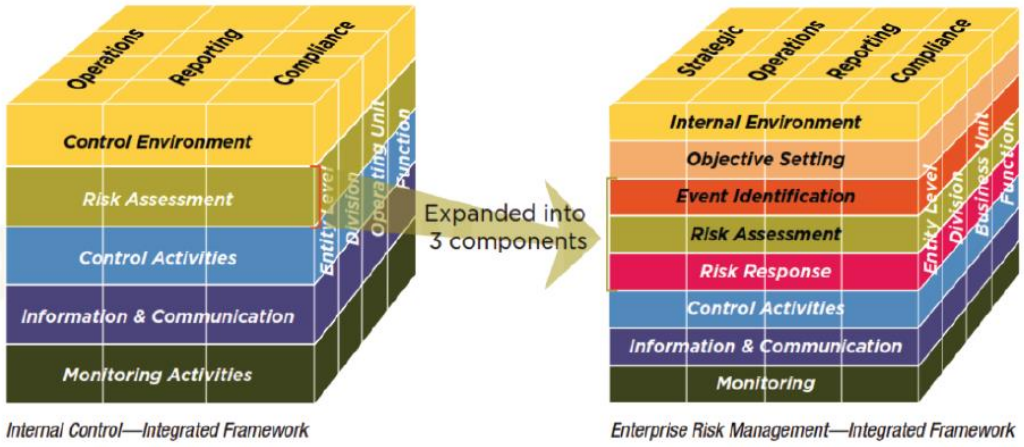

Figure 2 – Le cube COSO ERM
Source : Committee of Sponsoring Organizations of the Treadway Commission

Comme nous allons le voir par la suite, et comme illustré sur la Figure 2 ci-dessus, les différences principales sont d'une part, la prise en compte d'une catégorie d'objectif supplémentaire liées à la stratégie, et d'autre part, la composante relative à l'évaluation des risques est complétée par trois éléments que sont la fixation des objectifs, l'identification des événements et le traitement des risques. Les autres composantes déjà présentés pour le COSO I & III sont adaptées au management des risques.

4.2.2 Les catégories d'objectifs

Lorsque l'organisation se dote d'une mission et d'une vision, le management fixe également divers objectifs visant qui favorisent la réalisation de la mission, qui soient cohérents et qui se déploient dans toute l'organisation.[70]

[70] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-7

COSO II répartit les objectifs d'une organisation en quatre catégories :
Outre les trois objectifs détaillés dans le point 3.2.2 que sont ceux lés aux opérations, au reporting et à la conformité, le COSO II met en avant les objectifs liés à la stratégie.
Il s'agit des objectifs de haut niveau, c'est-à-dire liés à la stratégie de l'organisations. Ils sont en ligne avec sa mission et la soutienne.

Le COSO décrit ainsi la réalisation des objectifs de la manière suivante : « L'organisation ayant le contrôle sur les objectifs relatifs à la fiabilité du reporting et à la conformité aux lois et aux règlements, il est légitime d'attendre du processus de management des risques une assurance raisonnable quant à l'atteinte de ces objectifs. En revanche, l'atteinte des objectifs stratégiques et opérationnels dépend parfois d'évènements extérieurs qui peuvent échapper au contrôle de l'organisation. Par conséquent, dans ce cas, le management des risques ne peut donner qu'une assurance raisonnable que la direction et le Conseil d'administration, dans son rôle de supervision, sont informés en temps utile de l'état de progression de l'organisation vers l'atteinte de ses objectifs. » [71]

4.2.3 Les éléments du management des risques de l'organisation

COSO II comprend huit éléments, huit composantes pour reprendre le même terme que COSO I et III. Ils traduisent la façon dont l'organisation est gérée et sont intégrés au processus de gestion. Les huit éléments sont expliqués plus en détail ci-après :

- L'environnement interne [72]

Le COSO en donne une définition précise : « La direction expose sa conception en matière de management des risques et détermine l'appétence de l'organisation pour le risque. L'environnement de contrôle interne englobe la culture et l'esprit de l'organisation.
Il pose les bases qui vont déterminer la façon dont les risques et les contrôles sont appréhendés et considérés par les collaborateurs de l'organisation. Les collaborateurs (avec leurs qualités individuelles, notamment l'intégrité, les valeurs éthiques, la compétence) et l'environnement dans lequel ils travaillent sont au cœur de toute organisation.
L'environnement interne constitue le fondement structurel de tous les autres éléments du dispositif de management des risques. Il exerce une influence sur la façon dont les stratégies et les objectifs sont définis, sur la façon dont les activités sont structurées et les risques identifiés, évalués et gérés.

[71] COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*
[72] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-8

Il a également une influence sur la conception et le fonctionnement des activités de contrôle, sur les systèmes d'information et de communication ainsi que sur le suivi des opérations. »[73]

Ainsi, la culture de l'organisation et son histoire influencent son environnement interne, et ce au travers de bon nombre d'éléments tels que la culture du risque, l'appétence pour le risque[74], le rôle du Conseil d'administration, l'intégrité et les valeurs éthiques, l'engagement de compétence et donc des aptitudes et connaissances, la structure organisationnelle, la délégation de pouvoirs et de responsabilités ou bien encore la politique de ressources humaines mise en place au sein de l'organisation.

- La fixation des objectifs [75]

Comme déjà expliqué dans le point 4.2.2, les objectifs opérationnels, de reporting et de conformité, découlent des objectifs définis au niveau stratégique. Le COSO poursuit : « Chaque organisation est confrontée à une grande variété de risques d'origines externes et internes. La condition préalable pour pouvoir identifier les opportunités et les menaces, les évaluer et y répondre efficacement est la fixation d'objectifs. » [76]

Pour que cela puisse se faire efficacement, les objectifs doivent être alignés sur l'appétence pour le risque de l'organisation, c'est-à-dire le niveau de risque global qu'elle accepte de prendre pour atteindre ses objectifs.
En outre, la tolérance au risque, autrement dit le niveau de risque et d'écart entre les objectifs et la performance réelle, doit être en adéquation avec l'appétence au risque de l'organisation.

- L'identification des évènements [77]

COSO recommande la démarche suivante : « Le management identifie les évènements potentiels qui, s'ils se réalisent, pourront affecter l'organisation. Il détermine s'ils représentent une opportunité ou s'ils sont susceptibles de nuire sérieusement à la capacité de l'entité à mettre en œuvre, avec succès, sa stratégie et à atteindre ses objectifs.
Les évènements ayant un impact négatif constituent des risques qui demandent une évaluation du management et un traitement.

[73] COSO/PwC/IFACI (trad.), Le management des risques de l'entreprise : Cadre de référence -Techniques d'application, p. 32 et 40
[74] L'appétence pour le risque désigne le niveau de risque global qu'une organisation est prête à accepter en vue de ma réalisation de ses objectifs
[75] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-9
[76] COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*
[77] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-9

Les évènements ayant un impact positif représentent des opportunités que le management doit intégrer à la stratégie et au processus de définition des objectifs.
Lors de la phase d'identification des évènements, le management prend en compte, à l'échelle de l'organisation dans sa globalité, différents facteurs externes et internes pouvant se traduire par des menaces et des opportunités. » [78]

Parmi les facteurs externes, nous pouvons citer les facteurs économiques (fluctuations de prix, disponibilité des capitaux), les facteurs environnementaux (inondations, incendies), les facteurs politiques (nouvelles lois et règlements), les facteurs sociaux (évolutions démographiques, coutumes sociales) ou bien encore les facteurs technologiques (nouveaux modes de commerce électronique, de stockage ou de traitement).

Comme facteurs internes, nous retrouvons l'infrastructure (augmentation des capitaux alloués au centres d'appels), le personnel (accidents de travail fraudes), les processus (modification ou erreurs d'exécution des processus) ainsi que la technologie (augmentation des ressources pour la sécurité informatique).

- L'évaluation des risques

Cette composante a déjà été décrite en détail au point 3.2.3.
Il est cependant nécessaire de préciser que cette composante a été complétée par les deux précédentes que sont la fixation des objectifs et l'identification des évènements, ainsi que par la suivante, le traitement des risques.

- Le traitement des risques [79]

Selon le COSO : « Une fois les risques évalués, le management détermine quels traitements appliquer à chacun de ces risques. Les différentes solutions possibles sont : l'évitement, la réduction, le partage et l'acceptation. En fonction de la solution retenue, il convient de considérer l'effet des différentes solutions en termes de probabilité et d'impact, ainsi que de coûts et bénéfices. Le choix doit porter sur une solution ramenant le risque résiduel en deçà du seuil de tolérance souhaité par la direction. Les opportunités potentielles sont également identifiées. Les risques et opportunités sont appréhendés de manière transversale ou agrégés de façon à déterminer si le risque résiduel global correspond à l'appétence de l'organisation pour le risque. » [80]

Quatre modalités de traitement ont été abordées dans la définition ci-dessus.

[78] COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*
[79] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 4-11
[80] COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*

Tout d'abord l'évitement, qui consiste à cesser les activités à l'origine du risque. Par exemple en décidant de ralentir une expansion prévue sur un nouveau marché géographique.
Ensuite la réduction, qui se traduit par la prise de mesures afin de réduire la probabilité d'occurrence, ou l'impact du risque, ou bien les deux à la fois. Cela peut être la mise en place de contrôles.
La troisième modalité de traitement est le partage, c'est-à-dire diminuer la probabilité ou l'impact d'un risque en le transférant ou en le partageant. Par exemple l'externalisation d'une activité.
Et enfin l'acceptation, autrement dit ne prendre aucune mesure pour modifier la probabilité d'occurrence du risque et son impact.
Dans la pratique, étant donné les ressources nécessaires aux autres modalités de traitement, les organisations préfèrent souvent accepter le risque à son niveau actuel.

- Les activités de contrôle (voir point 3.2.3)

- Information et communication (voir point 3.2.3)

- Les activités de pilotage (voir point 3.2.3)

CHAPITRE 5 : LE MODÈLE DES TROIS LIGNES DE DÉFENSE

Comme évoqué précédemment dans la description de la composante relative aux activités de contrôle pour les deux référentiels de contrôle interne et de gestion des risques (point 3.2.3), la mise en place d'une approche à plusieurs niveaux permet de renforcer l'efficacité des activités de contrôle et de rassurer les organisations quant à la performance de leurs systèmes de contrôle interne et de management des risques.
Cette stratégie à multi-niveaux est souvent désignée comme un modèle de « lignes de maîtrise multiples », dont l'exemple classique, celui que nous allons aborder, est le « modèle des trois lignes de maîtrise » ou « modèle des trois lignes de défense ».

5.1 Rôle du modèle [81]

Afin d'aider leur organisation à gérer ses risques, bon nombre d'acteurs sont amener à interagir et à coopérer, qu'il s'agisse d'experts en gestion des risques, en conformité, en contrôle interne, en contrôle qualité, d'auditeurs internes ou d'autres professionnels en matière de contrôle et de risques.
Chacun de ces spécialistes dispose d'un point de vue particulier et possède des compétences spécifiques pouvant être une aide précieuse pour leur organisation.
Cependant, les tâches afférentes au contrôle et à la gestion des risques sont de plus en plus souvent réparties au sein de différents départements et divisions, et requièrent de ce fait une coordination rigoureuse afin d'assurer le bon fonctionnement des processus de contrôle et de gestion des risques.
En effet, il ne suffit pas que ces différentes fonctions de contrôle et de gestions des risques existent. Il faut leur assigner des rôles précis et mettre en place une coordination efficiente entre ces groupes afin d'éviter des manquements dans les contrôles ou des redondances dans les fonctions. Leurs responsabilités doivent donc être clairement définies de façon à ce que chaque groupe puisse appréhender son périmètre de responsabilités et son positionnement dans le système global de gestion des risques et de contrôle de l'organisation.

Dans le cas contraire, cela peut mener à des situations dans lesquelles des risques significatifs sont mal gérés voire non identifiés, ou bien à une mauvaise utilisation des ressources, déjà limitées, destinées aux fonctions de contrôle et de gestion des risques.
Dans certains cas, il peut même arriver que la relation entre les différents groupes en charge du contrôle et de la gestion des risques ne se limite à un débat permanent sur leurs attributions respectives et leur rôle vis-à-vis d'une tâche en particulier.
Ces cas de figure peuvent apparaître dans n'importe quelle organisation, y compris dans celles utilisant un référentiel formalisé de gestion des risques.
Ces référentiels permettent d'identifier efficacement les risques mais ne se concentrent pas sur les modalités d'attribution et de coordination des tâches nécessaires à leur mise en œuvre.

[81] IIA (2013). Prise de position de l'IIA. *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces. P. 1*

Dans cette optique, le modèle des trois lignes de maitrise permet justement d'améliorer la communication et la coordination en matière de contrôle et de gestion des risques en précisant les rôles et les activités essentiels s'y rapportant. Il convient à toute organisation, quelle qu'en soit la taille, la complexité ou la structure organisationnelle, y compris dans celles ne disposant pas de référentiel de gestion des risques.

5.2 Présentation du modèle

« « L'image des quatre lignes de défense (l'audit externe et le régulateur constituant la quatrième ligne) est dérivée du domaine de la stratégie militaire. Plusieurs lignes de défense successives doivent empêcher un adversaire d'atteindre l'objectif de son attaque. Si un ennemi parvenait à faire tomber la première ligne de défense, il resterait encore d'autres obstacles pour le retenir. L'efficacité des lignes de défense en aval augmente si chacune dispose de ses propres moyens spécifiques. Ainsi, avec l'apparition des lourds canons à poudre au début des temps modernes, les fortifications des châteaux et des villes ont été équipées successivement, dans toute l'Europe, de différentes lignes de défense telles que des douves, des remparts, des chemins de ronde couverts, des citadelles et d'autres bâtiments permettant de repousser l'ennemi à une distance adéquate pour l'artillerie. » [82]

En termes de gestion des risques, la parallèle entre la stratégie militaire et les trois (+1) lignes de défense est approprié car de nouveaux risques émergent constamment et à un rythme toujours plus effréné (cfr point 3.2.4), et les organisations doivent pouvoir s'adapter en conséquence.

Voici ci-dessous (Figure 3) une représentation type du modèle des trois lignes de défense.

Avant de décrire chacune des lignes de défense, il est important de rappeler le rôle essentiel des organes de gouvernance dans le bon fonctionnement des organisations (cfr chapitres 1 et 2 sur la gouvernance en général et la gouvernance dans les banques pour plus de précisions). En effet, bien que le Conseil d'administration, le comité d'audit et la direction générale se distinguent des trois lignes de maîtrise (voir Figure 3), toute approche globale des systèmes de gestion des risques implique préalablement la prise en compte des responsabilités de ces organes de gouvernance.
D'une part ce sont les principales parties prenantes auxquelles les trois lignes de maîtrise apportent leur appui. D'autre part, ce sont elles qui sont le plus à même d'intégrer le modèle des trois lignes de défense dans les processus de gestion des risques et de contrôle de l'organisation.
Autrement dit, le modèle des trois lignes de maîtrise sera d'autant plus efficace que les organes de gouvernance soutiennent activement son déploiement, et donnent des consignes dans ce sens aux autres parties prenantes.

[82] Bernet, A. & Genequand, E. (2015). PWC. Disclose. Gros plan sur la gestion des risques. *Contrôle coordonnée : le modèle des « quatre ligne de défense ».*

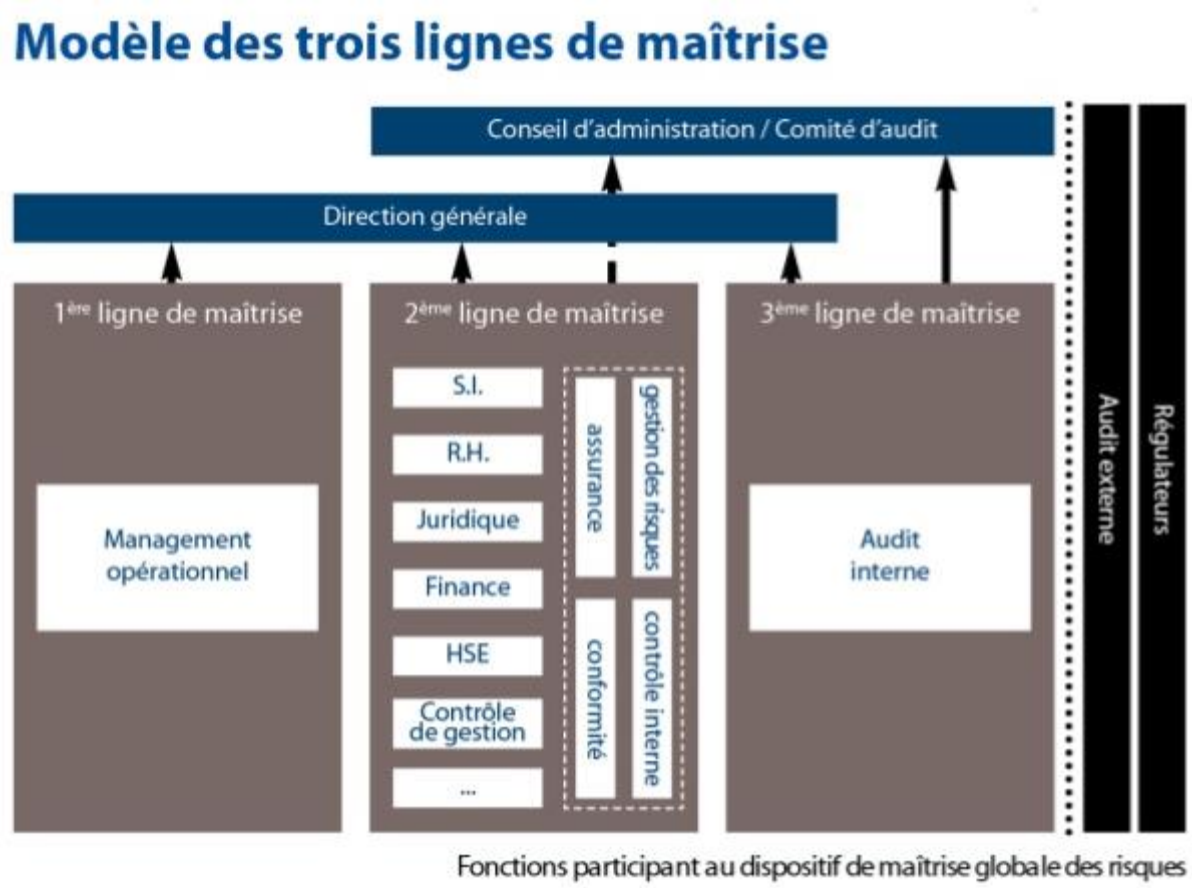

Figure 3 - Modèle des trois lignes de maîtrise
Source : Institute of Internal Auditors (IIA), traduit en français par l'Institut français des auditeurs et des contrôleurs internes (IFACI)

Plusieurs groupes de fonctions sont impliquées dans la maîtrise globale des risques.
Il y a dans un premier temps les fonctions qui endossent et gèrent les risques, c'est la première ligne de défense. Les fonctions qui assurent le suivi des risques constituent la deuxième ligne de défense. Et enfin, la troisième ligne de défense est composée des fonctions qui fournissent une assurance indépendante aux deux premières lignes.[83]
Pour mettre en place efficacement une structure organisationnelle en trois lignes de maîtrise, il est donc nécessaire de recenser préalablement les rôles et les responsabilités des fonctions qui concourent aux mécanismes de contrôles et au dispositif global de gestion des risques.

5.2.1 La première ligne de défense : les managers et le contrôle interne

En tant que première ligne de défense, les managers opérationnels endossent et gèrent les risques. Plus précisément, les tâches de cette première ligne sont réalisées par les collaborateurs et le management qui est directement responsable des contrôles.

[83] Bernet, A. & Genequand, E. (2015). PWC. Disclose. Gros plan sur la gestion des risques. *Contrôle coordonnée : le modèle des « quatre ligne de défense ». P.3*

Les managers sont responsables de la mise en place des dispositifs de contrôle interne efficaces portant sur les processus dont ils ont la charge. Ces activités de contrôle interne permettent de superviser et de surveiller les activités opérationnelles quotidiennes.
Les managers sont également chargés de la mise en œuvre au jour le jour de procédures de gestion des risques et de contrôle, en évaluant, en contrôlant et en gérant les risques, mais aussi en élaborant et en mettant en place des règles et des procédures internes qui visent à assurer que les activités sont bien compatibles avec les objectifs fixés.
Cette notion de contrôle interne et les différents aspects s'y rapportant, ont été vus en détail au chapitre 3.

Par ailleurs, en cas de déficiences des procédures, des règles, des processus ou des contrôles, ce sont eux qui doivent apporter les mesures correctives permettant d'y remédier.
Cette première ligne permet ainsi la maîtrise des activités au jour le jour en mettant en œuvre les pratiques les plus efficaces de gestion des risques au niveau de chaque processus et en communicant les informations appropriées à la deuxième ligne de défense. [84]
Etant assurée par les collaborateurs et les managers, elle constitue la ligne de maîtrise la moins indépendante et la moins objective des trois.[85]

5.2.2 La deuxième ligne de défense : les fonctions de gestion des risques et de conformité

La deuxième ligne est constituée des services fonctionnels responsables de domaines d'expertise et des fonctions dédiées à l'animation du dispositif global de maîtrise des risques. Ces services disposent d'une expertise et d'un savoir-faire uniques pour l'analyse des organisations et de compétences essentielles en matière d'activités de contrôle. [86]
Il incombe au management de mettre en place différentes fonctions spéciales de gestions des risques, de contrôle et de conformité. Leurs tâches consistent à surveiller les mesures conçues pour la première ligne de défense.

A cette fin, la fonction de conformité est chargée de surveiller des risques bien spécifiques tels que le non-respect des lois et règlementations en vigueur.
Cette fonction de conformité peut également couvrir d'autres domaines tels que la sécurité et la santé, l'environnement ou bien la qualité. Il est fréquent que ces diverses fonctions de conformité coexistent au sein de la même organisation.

[84] [85] AMRAE & IFACI (2013). *Trois lignes de Maîtrise pour une meilleure performance. Fiabiliser la stratégie par une gestion organisée des risques*.
[85] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-18

La fonction de gestion des risques doit faciliter et surveiller la mise en place de dispositifs efficaces de gestion des risques par les managers, mais également assister le management dans la définition du seuil de tolérance aux risques et dans la communication d'informations adéquates au sein de l'ensemble de l'organisation. Cette notion gestion des risques et les différents aspects s'y rapportant, ont été vus en détail au chapitre 4.
Une fonction de contrôle de gestion peut également être instaurée afin de veiller au suivi des risques financiers et du reporting financier.

Le management instaure donc ces fonctions pour s'assurer que la première ligne de maîtrise soit bien conçue, soit effective et fonctionne comme prévu.
Ces fonctions sont réalisées par des collaborateurs rattachés à des niveaux hiérarchiques différents de celui qui est directement responsable des activités de contrôle interne.
Ce sont donc par nature des fonctions support du management, pour lesquelles les collaborateurs exercent souvent d'autres responsabilités de gestion en sus de leurs responsabilités d'assurance.[87]
Elles bénéficient malgré tout, dans une certaine mesure, d'une indépendance par rapport à la première ligne de maîtrise.

5.2.3 La troisième ligne de défense : l'audit interne

Les auditeurs internes constituent la troisième ligne de défense. En tant qu'instance de conseil et de contrôle indépendante, l'audit interne est un instrument du Conseil d'administration.
En effet, il fournit aux organes de gouvernance une assurance globale fondée sur un plus haut degré d'indépendance organisationnelle et d'objectivité.
Il confère une assurance sur l'efficacité de la gouvernance, de la gestion des risques et du contrôle interne, y compris sur l'atteinte des objectifs de gestion des risques et de contrôle par les deux premières lignes de maîtrise.
« La mise en place d'un audit interne faisant preuve de professionnalisme devrait figurer parmi les règles de gouvernance de toute organisation. Ce point est important non seulement pour les organisations de grande dimension ou de taille moyenne, mas également pour les entités de taille plus modeste, qui peuvent être confrontées à des environnement aussi complexes sans disposer d'une structure organisationnelle aussi formalisée et robuste pour s'assurer de l'efficacité de leurs processus de gouvernance et de gestion des risques. » [88]

[87] Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne. *Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles. chap. 3-18
[88] [89] IIA (2013). Prise de position de l'IIA. *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces.* P. 5

L'Institut des Auditeurs Internes (IIA) recommande certaines bonnes pratiques en la matière.[89]Les organisations doivent mettre en place et maintenir une fonction d'audit interne indépendante, dotée de ressources et de compétences adéquates.
D'autres recommandations sont à prendre en considération. Tout d'abord en appliquant les normes internationales généralement admises pour la pratique de l'audit interne. Ensuite, en veillant à ce que l'auditeur interne soit rattaché à un niveau suffisamment élevé dans l'organisation pour pouvoir assurer ses responsabilités de manière indépendantes. Enfin, en faisant en sorte que l'auditeur interne ait une relation étroite et effective avec le Conseil d'administration ou l'organe de gouvernance équivalent.

Ci-dessous, un récapitulatif sur le rôle fondamental de chacune des trois lignes de défense :

PREMIÈRE LIGNE DE MAÎTRISE	DEUXIÈME LIGNE DE MAÎTRISE	TROISIÈME LIGNE DE MAÎTRISE
Propriétaires des risques / Managers	Gestion des risques et conformité	Assurance globale relative à l'efficacité de la gestion des risques
• Management	• Indépendance limitée • Rend compte principalement au management	• Audit interne • Plus grande indépendance • Rend compte aux organes de gouvernance (direction générale et Conseil)

Figure 4 – Rôle fondamental de chaque ligne de maîtrise
Source : Institute of Internal Auditors (IIA), traduit en français par l'Institut français des auditeurs et des contrôleurs internes (IFACI)

5.2.4 La « quatrième » ligne de défense : auditeurs externes et régulateurs

Les auditeurs externes [90], les régulateurs (la BNB ou la FSMA par exemple comme autorités de contrôle belge des secteur bancaires, financiers et des assurances) ou d'autres organes externes, peuvent également jouer un rôle important dans le dispositif global de de gouvernance et de contrôle des organisations. C'est principalement le cas dans des secteurs fortement réglementées comme les services financiers, bancaires ou d'assurances.
Ainsi dans certains cas, les régulateurs ont des exigences visant à renforcer les contrôles au sein des organisations, et procèdent pour cela à des revues indépendantes et objectives pour évaluer en tout ou partie les première, deuxième ou troisième ligne de défense. [91]

[90] Cabinet d'experts-comptables agréé, chargé par le Conseil d'administration ou la direction générale de l'organisation de procéder à un audit des états financiers et donner une assurance sous la forme d'une attestation écrite, indiquant son opinion quant à la sincérité des états financiers et à leur conformité aux principes comptables généralement admis
[91] IIA (2013). Prise de position de l'IIA. *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces.* P. 6

C'est dans cette optique que les auditeurs externes et régulateurs peuvent être considérés comme une quatrième ligne de défense, fournissant une assurance aux organisations et à l'ensemble des parties prenantes, notamment les actionnaires, ou le marché.

CHAPITRE 6 : LES TROIS LIGNES DE DÉFENSE DANS LE SECTEUR BANCAIRE

Dans le chapitre 2 relatif à la gouvernance au sein des banques, nous avons parcouru les principaux points d'attention du Manuel de gouvernance pour le secteur bancaire, publié par la Banque Nationale de Belgique en septembre 2017.
Il y est indiqué qu'afin de garantir une gestion efficace et prudente de l'établissement de crédit, la loi bancaire préconise certains éléments nécessaires à la mise en place d'un dispositif solide et adéquat d'organisation d'entreprise.[92] Nous nous intéressons à deux éléments, qui font le lien entre la règlementation bancaire et le modèle des trois lignes de défense vu au chapitre précédent :

Tout d'abord le besoin de disposer d'un contrôle interne adéquat. [93] Cela correspond à la *première ligne de maîtrise*.

Ensuite, la nécessité pour les établissements de crédit de disposer de fonctions de contrôles indépendantes d'audit interne, de gestion des risques et de conformité (compliance).[94]
Plus précisément, comme le stipule le §1 de l'article 35 de la loi bancaire ;
« *Les établissements de crédit prennent les mesures nécessaires pour disposer en permanence des fonctions de contrôle indépendantes adéquates suivantes : a) conformité (compliance) ; b) gestion des risques ; c) audit interne, dont les personnes qui en assurent l'exercice sont indépendantes des unités opérationnelles de l'établissement et disposent de prérogatives nécessaires au bon accomplissement de leurs fonctions.* »
Ces fonctions forment les *deuxièmes et troisièmes lignes de défense*.

Par ailleurs, le modèle des trois lignes de défense est directement évoqué dans le Manuel de gouvernance de la Banque Nationale de Belgique [95] :

« Les relations entre, d'une part, les unités commerciales et d'exploitation et, d'autre part, les fonctions de contrôle indépendantes sont parfois définies comme formant le modèle des trois lignes de défense de l'établissement de crédit :

[92] Art. 21, § 1er, 1° à 9°, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[93] Art. 21, § 1er, 2°, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[94] Art. 21, § 1er, 4°, de la Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse
[95] Banque Nationale de Belgique (2017). *Manuel de gouvernance pour le secteur bancaire*. P. 15

- les unités commerciales et d'exploitation (y compris le front office) forment la première ligne de défense de l'établissement, à laquelle il revient d'identifier les risques posés par chaque opération et de respecter les procédures et les limites posées;
- la seconde ligne de défense comprend les fonctions de contrôle que sont la fonction de gestion des risques et la fonction de compliance, qui sont chargées de s'assurer que les risques ont été identifiés et gérés par les unités commerciales et d'exploitation (et le front office), selon les règles et procédures prévues;
- la troisième ligne de défense est constituée de l'audit interne qui s'assure, entre autres, du respect des procédures par les première et deuxième lignes de défense. »

Nous ne nous attarderons pas à détailler à nouveau le rôle de chacune des lignes de défense, ni les fonctions qui les composent. Pas plus que le rôle des organes de gouvernance, du Conseil d'administration et des différents comités dans la bonne mise en œuvre du modèle et dans leur fonction de surveillance du système global de gestion des risques.

Ces points ont déjà été largement traités lors des chapitres précédents. Mis à part pour la gouvernance, tous ces éléments ont été expliqués pour les organisations en général.

Les rôles et responsabilités des fonctions liées au contrôle interne et à la gestion des risques, vus en détail dans les chapitres 3 et 4, s'appliquent également aux banques.
Même constat en ce qui concerne le rôle et les responsabilités attribués aux auditeurs internes, décrits (certes succinctement) lors de la présentation de la troisième ligne de défense dans le chapitre 5.
Pour plus de précisions concernant l'organisation et le fonctionnement de la fonction d'audit interne, la Banque Nationale de Belgique a publié la circulaire NBB_2015_21 du 13 juillet 2015 concernant le contrôle interne et la fonction d'audit interne, consultable sur le site de la BNB. [96]

Par contre, la fonction de compliance, appréhendée de manière très rapide dans la présentation de la deuxième ligne de défense, sera entièrement consacrée par la troisième et dernière partie.

[96] https://www.nbb.be/fr/supervision-financiere/controle-prudentiel/domaines-de-controle/etablissements-de-credit/circulair-7

PARTIE III : LA FONCTION COMPLIANCE

Au vu du contexte économique et financier de cette dernière décennie, les différentes règles et bonnes pratiques en matière de bonne gouvernance des banques ont été adaptées et renforcées, comme présenté dans la première partie. Tout d'abord par les autorités de contrôle via notamment les nouvelles orientations du Comité de Bâle sur le contrôle bancaire [97] ou bien celles de l'Autorité Bancaire Européenne sur la gouvernance interne. [98] Ensuite au niveau de la règlementation belge, avec en autre la mise à jour de la loi bancaire en 2014.[99]
Une attention toute particulière a été portée sur la gestion des risques et les rôles et responsabilités respectifs des opérationnels et des fonctions de contrôle indépendantes. Nous avons consacré la seconde partie à décrire les mécanismes de contrôle interne et de gestion des risques, tout en présentant les référentiels intégrés s'y rapportant.
Le modèle des trois lignes de défense, présenté également dans la deuxième partie, permet de mettre en exergue et d'optimiser la coordination nécessaire entre les lignes de défense représentées par ces fonctions de contrôle. Au sein de la deuxième ligne de défense, au côté notamment de la fonction de gestion des risques, la fonction de compliance a énormément évolué ces dernières années et a pris une place de plus en plus importante au sein des établissements financiers, entre autres.
C'est cette évolution, ce rôle accru de la fonction compliance dans la pratique d'une bonne gouvernance et d'une gestion des risques adéquate, que nous voulons mettre en avant dans cette troisième partie. Nous présentons dans un premier temps les points importants de la circulaire consacrée à la fonction de compliance, et les éléments caractéristiques propres à cette fonction.

CHAPITRE 7 : ÉLÉMENTS CARACTÉRISTIQUES DE LA FONCTION COMPLIANCE

La circulaire sur la fonction compliance [100] a été rédigée conjointement par la Banque Nationale de Belgique (BNB) et l'Autorité des Services et Marchés Financiers (FSMA) en décembre 2012. Outre la spécification du champ d'application de la circulaire et quelques définitions clés, la circulaire présente une série de principes sur base desquels la BNB et la FSMA *évaluent le caractère adéquat du fonctionnement et de l'organisation de la fonction de compliance,* dans le cadre de leur contrôle respectif.

[97] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks*
[98] EBA European Banking Authority (2011). *Orientations de l'ABE sur la gouvernance interne (GL 44).*
[99] Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse.
[100] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. Disponible sur le site : https://www.nbb.be/fr/articles/circulaire-nbb201214-fonction-de-compliance

7.1 Définition des concepts

7.1.1 Compliance et conformité

La *conformité* représente l'objectif à atteindre. « *Elle définit jusqu'où aller pour garantir la sécurité des opérations de la banque et préserver son image, sa réputation, la mise en jeu de sa responsabilité civile et* pénale ». [101]

La *compliance* est un véritable changement de paradigme axé sur la sécurité, et qui permet d'assurer une performance plus solide et plus pérenne. Sa mise en œuvre nécessite d'une part, la compréhension de la stratégie globale, et d'autre part que les comportements de tous les collaborateurs soient alignés avec les outils permettant d'être conforme.
Il s'agit véritablement d'une culture d'entreprise basée sur le respect des règles et accordant une place importante à des valeurs telles que l'intégrité, se traduisant par une conduite honnête, fiable et crédible. Il est important d'insister sur le fait que toutes les parties prenantes doivent être sensibilisées à cette culture et adopter un comportement responsable en ce sens, comme le stipule l'article 36, § 1er de la loi bancaire ; *« Les établissements de crédit disposent d'une fonction de compliance destinée à assurer le respect, par l'établissement, les membres de son organe d'administration, ses dirigeants effectifs, ses salariés, ses mandataires et agents liés, des règles légales et réglementaires d'intégrité et de conduite qui s'appliquent à l'activité bancaire. »*

La circulaire sur la fonction compliance décrit également ce que doit représenter une « compliance effective ». Elle « *implique que les valeurs défendues par l'établissement sont intégrées dans la manière de conduire les affaires. »* [102] Pour cela, elle nécessite non seulement une conduite intègre de la part des collaborateurs et de l'établissement financier, mais également la prise en compte des intérêts des clients, qui ne doivent pas être mis de côté par les propres intérêts de l'établissement. La protection du consommateur financier est un rôle clé de la compliance : « *les clients doivent toujours être traités de façon honnête, équitable et professionnelle ».* [103]

7.1.2 Le risque de compliance

Le Comité de Bâle défini le risque de compliance (ou risque de non-conformité) comme « *un risque de sanction judicaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, du fait de l'absence de respect des dispositions législatives et réglementaires, des normes et usages professionnels et déontologiques, propres aux activités des banques. »* [104]

---

[101] Cordier, B. (2016). Société Française des Analystes Financiers. Focus Métiers. *La compliance, une fonction en pleine évolution*
[102] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 9
[103] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 8
[104] Bank for International Settlements (2003). Basel Commitee on Banking Supervision. Consultative Document. *The compliance function in banks*

Ces dispositions peuvent notamment porter sur la lutte contre le blanchiment des capitaux et le financement du terrorisme, la protection de la vie privée et des données, la conduite des activités bancaires et financières dont fait par exemple partie la problématique des conflits d'intérêts, que nous verrons par la suite dans le point sur l'indépendance de la fonction compliance.

Portons une attention particulière à un élément de la définition qu'est le risque d'atteinte à la réputation de l'établissement. La réputation d'une banque est primordiale car elle est directement liée à sa crédibilité aux yeux des consommateurs, des Autorités de Contrôle, du marché ou bien du secteur financier. Elle constitue donc l'un des principaux actifs d'une banque mais est également l'un des plus fragiles.
La perte de réputation peut notamment provenir d'un non-respect de la politique interne mise en place dans l'établissement. Ou bien directement en raison des valeurs et des règles de conduite véhiculées au sein de l'établissement.
A ce propos, le Comité de Bâle recommande la mise en place d'un comité spécialisé en la matière, le comité d'éthique et de conformité qui va justement veiller *à ce que la banque dispose des moyens requis afin que la prise de décision soit adéquate, que les risques d'atteinte à la réputation de la banque soient dûment pris en considération et que la législation, la réglementation et les règles internes soient respectées.*[105]

Notons que le risque de compliance ainsi défini ne porte pas sur la responsabilité des établissements financiers vis-à-vis de leurs obligations contractuelles, mais bien sur le non-respect des règles et des conséquences qui en découlent. Le risque de compliance doit donc être distingué du risque juridique de litige, pour lequel il y a une contrepartie.[106]

7.2 Missions de la fonction compliance

La compliance et le risque de compliance ainsi définis dans le point 7.1, la fonction de compliance fait référence à *« une fonction indépendante au sein de l'établissement financier, axée sur le respect des règles qui sont liées à :*

- *l'intégrité des activités de l'établissement ; et*
- *la maîtrise du risque de compliance de l'établissement. »* [107]

[105] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks* Principle 3
[106] Bank for International Settlements (2003). Basel Commitee on Banking Supervision. Consultative Document. *The compliance function in banks*
[107] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 9

A côté de cette définition générale, le principe 1 de la circulaire sur la fonction compliance décrit bon nombre de facettes du métier de compliance, en énumérant les tâches et responsabilités leur étant attribuées : [108]

- **Identification et évaluation du risque de compliance ;** il s'agit donc d'identifier, de mesurer, de documenter et d'évaluer les risques compliance au sein de la banque, en utilisant les résultats de mesure pour proposer des solutions visant à réduire ces risques. La fonction compliance évalue également les différents contrôles, procédures et directives mis en place dans la banque, et propose des modifications en cas de défaillances.

- **Conseil** ; la fonction compliance conseille et communique les évolutions à propos des lois, des règlements, des normes et des codes relevant de sa mission. Ces conseils et communications sont destinés aussi bien à la direction qu'aux services opérationnels. Elle conseille également la direction quant à l'élaboration d'une politique d'intégrité et à sa mise à jour continue. Cela concerne les directives, le code de déontologie, les procédures ou bien encore les politiques et instructions administrées au sein de l'établissement. Le rôle de conseil de la fonction compliance consiste aussi à identifier, documenter et évaluer les risques de compliance lorsque l'organisation de la banque est modifiée, lorsque la banque souhaite lancer de nouveaux produits/services ou intégrer un nouveau marché, ou également en matière de règles de publicité.

- **Surveillance et tests** ; en utilisant les résultats des contrôles apportés par la première ligne de défense, constituée par le contrôle interne des services opérationnels, la fonction de compliance veille à ce que les règles légales et/ou règlementaires d'intégrité et de conduite, soient bien appliquées au sein de l'établissement. Elle communique ensuite les résultats de cette surveillance aux services concernés, et veille à ce qu'ils les prennent bien en considération. Différentes techniques, différents tests, peuvent être utilisés pour faciliter ce rôle de surveillance, telles que la réalisation de sondages des opérations réalisées et l'évaluation des échantillons obtenus, la mise à jour et le suivi d'indicateurs de risque comme le nombre de plaintes et d'infraction, ou bien encore en organisant des entretiens avec les collaborateurs.

- **Sensibilisation, point de contact et formation** ; la fonction compliance veille dans un premier temps à ce que tous les collaborateurs de la banque soient sensibilisés sur les questions d'évaluation et de maîtrise des risques de compliance. Elle sert ensuite de point de contact pour les collaborateurs pour toute question ayant attrait à la compliance. Enfin, elle assiste la direction pour organiser la formation des collaborateurs sur des matières liée à la compliance.

[108] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 12-14

- **Élaboration d'un plan d'action** ; le responsable de la fonction compliance élabore un plan d'action par écrit, qui est ensuite approuvé par la direction, et finalement confirmé par le Conseil d'administration. Il comprend tout d'abord la description des missions qui seront effectuées par la fonction compliance sur une période spécifiée (nature et fréquence de ces missions). Il comporte ensuite une analyse méthodique du risque couvrant toutes les activités et entités de la banque, comprenant non seulement des données antérieures pertinentes, mais également les innovations et les évolutions attendues, en matière de compliance. Le plan d'action doit en outre préciser les ressources humaines (nombre de personnes et compétences) et matérielles requises pour mener à bien les missions à effectuer. Enfin, le plan d'action doit être réaliste, en prévoyant par exemple du temps pour les formations ou autres tâches non répertoriées dans le plan.

- **Suivi et interprétation des législations et réglementations dans les domaines de compliance** ; en collaboration avec la fonction juridique, la fonction compliance « *dresse un inventaire et assure la surveillance et un suivi permanent des réglementations nationales et internationales, des codes de conduite et normes de bonne pratique applicables, des règlements, circulaires et directives des autorités de contrôle nationales et internationales ayant trait aux risques de compliance, ainsi que toutes les règles dont l'objectif est de promouvoir le traitement honnête, équitable et professionnel de ses clients et des parties intéressées et de leur interprétation pour chacune des activités de l'entreprise.* »

Au-delà de ces tâches spécifiques, la fonction de compliance est le point de contact clé des deux autorités de contrôle que sont la Banque Nationale de Belgique et l'Autorité des Services et Marchés Financiers. Elle entretien des relations avec l'ensemble des services de l'établissement, en tentant de les sensibiliser un maximum sur les risques de compliance.
La fonction compliance doit également bénéficier d'une relation étroite et régulière avec le comité de direction et le conseil d'administration, pour pouvoir assumer ses responsabilités.
Afin d'avoir un rôle crédible dans ces relations, et pour mener à bien ses missions, la fonction de compliance doit être indépendante des services opérationnels et avoir un accès privilégié à l'organe exécutif. Nous décrivons davantage cette notion d'indépendance de la fonction de compliance au point 7.4.

Un autre rôle essentiel de la mission de compliance, que nous avons déjà évoqué, est celui de la protection du client. La relation entre la banque et le client est d'autant plus forte lorsque le client a confiance dans sa banque. Cette confiance est renforcée par le durcissement des règles en matière de protection du client mises en place par la banque. En effet, « *le plus important pour les clients est de savoir qu'ils peuvent compter sur une banque qui prône l'intégrité et qui est soucieuse de la protection du client dans le respect de la règlementation*. »

[109] Parmi ces règlementations, les banques ne sont par exemple pas autorisées à fournir certains instruments financiers à n'importe quel client. Chaque client doit être traité distinctement. A ce propos, le respect des règles de conduites MiFID (Directive sur les marchés d'instruments financiers) [110] est suivi de près par la FSMA, dans sa qualité d'autorité de contrôle. Les règles MiFID imposent par exemple aux banques de soumettre un questionnaire aux clients, qui va déterminer leur profil de risque. Leurs connaissances doivent être testées en matière de produits d'investissement. C'est pour cela que certains clients ne peuvent pas investir dans certains produits financiers complexes, s'ils ne disposent pas des connaissances nécessaires en la matière. A cette fin, certaines banques mettent en place des programmes de formation dans lesquels sont expliquées les caractéristiques des différents produits financiers, notamment en termes de risque.

7.3 Domaines de travail de la fonction compliance [111]

La mission principale de la fonction compliance est d'analyser et de faire respecter l'ensembles des textes légaux et réglementaires auxquels les banques doivent se conformer. Il convient maintenant de spécifier les domaines couverts par ces différents textes. Certains sont du ressort de la Banque Nationale de Belgique (BNB), certains de l'Autorité des Services et Marchés Financiers (FSMA), certains des deux autorités de contrôle, et d'autres encore pour lesquels ni la BNB ni la FSMA n'ont de compétences.
La BNB exerce un contrôle prudentiel et veille en tant que tel, au respect des conditions d'agrément et d'exercice des banques.
La FSMA agit comme autorité de contrôle pour les règles de conduite, et veille pour cela à *l'organisation de la fonction compliance sous l'angle du respect des règles de conduite destinées à assurer un traitement honnête, équitable et professionnel des parties intéressées.*

Nous énumérons ci-dessous l'ensemble des domaines repris dans la circulaire compliance. Cela peut paraître fastidieux à la lecture, mais cela permet toutefois de se rendre compte de l'étendue des compétences et connaissances requises dans l'exercice de la fonction compliance, et des nombreuses tâches qui lui incombent. Cela confirme également le fait que la fonction compliance doit être indépendante et disposer de suffisamment de ressources, tant humaines que matérielles, pour mener à bien sa mission.

[109] *Zurstrassen, M. (2016) Puilaetco Dewaay Private Bankers. Compliance : Une fonction clé dans un univers bancaire toujours plus réglementé*
[110] Intégrées dans la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers
[111] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 3-8

Voici dans un premier temps les domaines dans lesquels la BNB est habilitée :

- *Le respect du devoir de vigilance à l'égard de la clientèle, la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et du financement du terrorisme, ainsi que la prévention du financement de la prolifération des armes de destruction massive ;*
- *La politique de prévention dans le domaine fiscal et les mécanismes particuliers (c'est-à-dire lorsque qu'une banque a connaissance du fait qu'un établissement de crédit a mis en place un mécanisme particulier ayant pour but ou pour effet de favoriser la fraude fiscale par des tiers).*
- *Le respect des règles légales en matière d'incompatibilité des mandats ou des règles fixées en la matière dans le code de déontologie de l'établissement.*

Les domaines dans lesquels la FSMA est habilitée :

- *Le respect des règles de conduite figurant au chapitre II de la loi du 2 août relative à la surveillance du secteur financier et aux services financiers, notamment : les règles de conduite MiFID, les règles en matière d'abus de marché ou les dispositions réglementaires visant à favoriser un traitement honnête, équitable et professionnel des parties intéressées ;*
- *Le respect des règles de conduite relatives à l'intermédiation en services bancaires et en services d'investissement, mais aussi à la distribution et à l'utilisation d'instruments financiers ;*
- *Application de la loi sur le crédit hypothécaire ;*
- *Le suivi du traitement des plaintes ;*
- *Le respect des règles en matière de publicité (par exemple à propos des offres publiques d'instruments de placement ou à certaines formes de gestion collective de portefeuilles d'investissement).*

Domaines pour lesquels ni la BNB ni la FSMA ne disposent de compétences directes :

- *Le respect de la législation sur la vie privée ;*
- *Le respect des dispositions relatives à la législation anti-discrimination ;*
- *Pratiques du marché et à la protection du consommateur ;*
- *Le respect de dispositions spécifiques pour le secteur bancaire, notamment les codes de conduite de Febelfin (Fédération belge du secteur financier) et Beama (Association belge des gestionnaires d'actifs) ;*
- *Le respect des valeurs et règles d'intégrité internes.*

Domaines dans lesquels tant la BNB que la FSMA sont habilitées :

- *Le statut et le contrôle des établissement de crédit ;*
- *Le respect des principes en matière de bonne politique de rémunération.*

D'autre domaines et activités peuvent également être couverts par la fonction compliance. La direction mène une analyse de risque et décide des autres matières à regarder de près par la fonction de compliance, notamment :

- Le crédit à la consommation (coûts, taux, durée et modalités de remboursement) ;
- Le respect d'embargos spécifiques, en ce compris le gel d'avoirs de certaines personnes et entités ;
- La législation étrangère ayant une incidence sur les domaines de compliance.

7.4 Indépendance de la fonction compliance

La disposition permanente d'une fonction de compliance indépendante est une condition (posée par les lois de contrôle) d'agrément et d'exercice pour les banques. Le Comité de Bâle précise dans ses orientations de gouvernance des banques que *« la fonction compliance est indépendante de la direction, afin d'éviter toute influence indue et tout obstacle à l'exercice de ses responsabilités. Elle doit rendre directement compte au conseil d'administration des efforts déployés par la banque dans les domaines susmentionnés et de la gestion, par la banque, du risque de non-conformité*. » [112]

La circulaire sur la fonction de compliance met en avant quatre éléments clés pour assurer cette indépendance : [113]

- **Statut formel de la fonction compliance au sein de l'établissement** ; une charte présentée à tous les collaborateurs doit décrire le statut formel de la fonction compliance au sein de la banque. La charte doit contenir au minimum certaines précisions sur la fonction de compliance, notamment :

[112] Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks. Principle 9*
[113] Circulaire FSMA_2012_21 du 4/12/2012 sur la fonction compliance. P. 20-23

- L'organisation et la place de la fonction de compliance au sein de l'établissement ainsi que ses compétences et ses responsabilités ;
- L'objectif et la portée de la fonction compliance (voir point 7.2) ;
- Le principe « *comply or explain* », c'est-à-dire que toute recommandation faite par la fonction de conformité doit être respectée, ou dans le cas contraire, la motivation de ce non-respect doit être expliquée ;
- Le droit d'initiative de la fonction de compliance ;
- La procédure dite « d'escalade » qui confère à la fonction compliance la possibilité de remettre en cause des décisions prises par d'autres services en matière de compliance, et ce à un niveau hiérarchique supérieur ;
- Les relations, les incompatibilités et la coordination avec les autres fonctions de contrôle constituant les trois lignes de défense de la banque ;
- Afin de pouvoir mener à bien sa mission en menant directement des entretiens avec les collaborateurs, la direction habilite la fonction de compliance à avoir accès à toutes les activités, à tous les documents, fichiers et informations de l'établissement (y compris les PV des organes consultatifs et décisionnels) ;
- L'obligation de reporting de la fonction de compliance envers la direction et le conseil d'administration ;
- La possibilité pour le responsable de la fonction compliance de contacter directement le président du conseil d'administration, le commissaire agrée ou les autorités de contrôle, sans en informer préalablement la direction.

- **Désignation d'un responsable de la fonction compliance** ; un responsable de la fonction compliance doit être désigné au sein de chaque établissement, et doit être placé à un niveau hiérarchique suffisamment haut pour pouvoir rapporter directement à la personne compétente en matière de compliance faisant partie de la direction.
  Le responsable de la fonction compliance doit idéalement disposer d'un agrément octroyé par la FSMA.[114]
  C'est lui qui établit le plan d'action (voir point 7.2), au moins une fois par an, ainsi que la charte (cfr supra) définissant le statut formel de la fonction compliance.
  Enfin, lorsque le responsable de la fonction compliance est démis de ses fonctions (uniquement par l'organe légal d'administration), la BNB et la FSMA doivent être prévenues sans délai, et doivent recevoir de la part de la direction, les motivations de cette décision.

[114] Article 87bis de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers

- **Conflits d'intérêts** ; l'indépendance du responsable et des autres collaborateurs de la fonction compliance peut être menacée lorsque ceux-ci se retrouvent confrontés à des conflits d'intérêts. En effet, certaines autres tâches de la fonction compliance peuvent rentrer en conflit avec leur mission proprement dite de compliance. Pour pallier à cela, les banques doivent mettre en œuvre et maintenir des politiques efficaces pour identifier et éviter des conflits d'intérêts potentiels ou réels. Parmi ces politiques, la mise en place d'une structure de gestion adéquate (l'un des principes généraux de la loi bancaire pour l'organisation des banques), ou bien l'instauration du modèle des trois lignes de défense, permet aux banques de disposer d'une séparation adéquate des fonctions et d'un dispositif cohérent dans l'attribution des responsabilités.

- **Accès aux informations et aux collaborateurs** ; il s'agit d'un élément précisé dans la charte conférant un statut formel à la fonction de compliance, à savoir le droit de mener directement des entretiens avec tous les collaborateurs, et avoir accès à toutes les activités, à tous les documents, fichiers et informations de l'établissement (y compris les PV des organes consultatifs et décisionnels). Et ce, dans la mesure requise pour l'exercice de la mission.

CHAPITRE 8 : ÉVOLUTION DE LA FONCTION COMPLIANCE

Lors du chapitre précédent, nous avons pu observer toute l'étendue de la fonction de compliance, tant au niveau des domaines qu'elle est amenée à traiter que des nombreuses tâches et responsabilités qui lui sont attribuées. Sa position privilégiée auprès de l'organe légal d'administration, la nécessité de son indépendance vis-à-vis des services opérationnels et autres fonctions de contrôle, mais aussi dans une certaine mesure à l'égard de la direction, prouve que la fonction compliance va bien au-delà du respect de la conformité.

Cela n'a pas toujours été le cas, les prescriptions sur la conformité avaient été à l'origine définies afin de répondre aux exigences légales minimales. D'ailleurs *la profession de Compliance Officer* (la personne exerçant la fonction de compliance) *ne s'est développée que dans la seconde partie des années 90*. [115] Ce n'est que par la suite que cette fonction a réellement émergé et est devenue un acteur stratégique incontournable dans les banques (entre autres), qui évoluent dans un secteur très réglementé. Le renforcement des règlementations financières et bancaires constitue d'ailleurs l'un des points de départ de cette mutation de la fonction compliance.

[115] *Zurstrassen, M. (2016) Puilaetco Dewaay Private Bankers. Compliance : Une fonction clé dans un univers bancaire toujours plus réglementé.*

Dans ce chapitre, nous commençons ainsi par discuter des facteurs qui sont à l'origine de cette mutation. Nous poursuivons en décrivant les enjeux auxquels font face et feront face les métiers de la compliance.

8.1 Facteurs d'évolution de la fonction compliance

L'évolution de la fonction compliance est étroitement liée à l'environnement dans lequel ont évolué les banques. Pour avoir une idée plus précise de la période durant laquelle nous faisons référence, nous décrivons cet environnement via une étude du Rapport annuel de la Commission bancaire française de 2003.[116] Ainsi, avant 2003, l'on pouvait observer les éléments suivants :

- *Une diversification des métiers au sein des grands groupes du fait de rapprochements, de partenariats, d'acquisitions ;*
- *Un enrichissement de l'offre de produits proposés aux différentes catégories de clients ;*
- *Un développement des opérations complexes. Les opérations de financement structuré comme celles de titrisation pour compte de tiers faisant appel à des véhicules ad hoc se sont ainsi multipliées ; l'usage de nouveaux instruments sophistiqués s'est fortement développé au cours des dernières années ;*
- *Une expansion géographique des implantations et des risques pris par les établissements ;*
- *Une multiplication des agents économiques avec lesquels les établissements sont amenés à traiter, du fait par exemple de l'émergence au cours des dernières années de l'externalisation d'activités ;*
- *Une intensification de la concurrence entre les établissements, ce qui se traduit par un renforcement des contraintes de rentabilité.*

Tous ces éléments ont eu pour conséquence d'accroître et de diversifier les risques auxquels faisaient face les banques. Elles ont donc dû maîtriser davantage de réglementations et de techniques afin de pouvoir disposer d'une politique de gestion des risques adaptée et suffisamment robuste. Par conséquent, ce contexte a obligé les banques à porter une attention toute particulière à la conformité de leurs opérations. Elles ont progressivement dû mettre en place des outils permettant de veiller à l'évolution des règlementations (rôle actuel de la compliance). Les banques ont également été amenées à améliorer les connaissances de la réglementation par leurs collaborateurs. Les procédures de contrôle de la conformité des décisions à la réglementation ont dû être davantage formalisées.

[116] Rapport consultable via le lien : https://acpr.banque-france.fr/sites/default/files/media/2017/11/06/cb_ra_2003.pdf

Les banques ont été contraintes de mettre tout cela en place, non seulement par nécessité, mais également sous l'impulsion des autorités de contrôle. En Belgique par exemple, la Commission bancaire, financière et des assurances, la CBFA (remplacée par la suite par la BNB et la FSMA) a publié en 2001 la circulaire D1 2001/13, définissant les principes auxquels devait répondre la fonction de compliance. Tout un cadre réglementaire autour de la fonction compliance a été mis en œuvre par la suite. Nous en avons d'ailleurs décrit les grandes lignes dans le chapitre précédent, en présentant la circulaire FSMA_2012_21 sur la fonction compliance, publiée en 2012.

Les règlementations financières et bancaires se sont encore sensiblement renforcées suite à la crise financière et bancaire de 2007-2008. En conséquence, le rôle et l'importance de la fonction compliance, ainsi sur les exigences à son égard, ont suivi cette même tendance.
En effet, les exigences en termes de conformité se sont multipliées mais sont aussi plus détaillées et plus approfondies. Pour y répondre, les banques doivent désormais produire beaucoup plus de documents, multiplier les tests et apporter davantage de preuves du respect des règles en vigueur.
Plusieurs études confirment cette tendance : la plupart des établissements financiers prévoient une nette augmentation des coûts liés à l'application des exigences de conformité. [117]
En outre, les amendes infligées aux banques par les régulateurs sont très élevées en cas de non-respect des exigences légales et réglementaires.
Malgré tout, la conformité peut également s'avérer utile, et ne constitue pas uniquement une contrainte à respecter. *Lorsqu'une banque se positionne bien en matière de conformité réglementaire et que ce bon positionnement est visible pour les investisseurs, cela peut contribuer à améliorer ses résultats.*[118]

Dans ce contexte, les responsabilités de la fonction compliance se sont sensiblement accrues. D'ailleurs en Belgique, les *Compliance Officers* sont maintenant tenus d'être agréés auprès des autorités de contrôle que sont la BNB et la FSMA. [119] Cela distingue la fonction compliance des autres métiers de la banque, et en fait un acteur clé.
Les métiers de compliance sont véritablement devenus des partenaires stratégiques en réponse à la multiplication et à la diversification des risques et des réglementations. Ils contribuent à anticiper les exigences en matière de conformité avant même que celles-ci ne freinent la banque dans la bonne mise en œuvre de sa stratégie. Cela peut permettre également à la banque de convertir des risques en opportunités et à s'en servir pour se développer et se distinguée de la concurrence.

[117] [118] Gassmann, P. (2015). PWC. Disclose. Gros plan sur la gestion des risques. *Le rôle de la fonction de Compliance dans la gestion des risques bancaires*

[119] Article 87bis de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers + Règlement de la FSMA du 27 octobre 2011 relatif à l'agrément des Compliance Officers et à l'expertise des responsables de la fonction de compliance

En alignant ainsi la compliance sur les enjeux stratégiques de la banque, la fonction compliance participe à l'amélioration de sa performance globale.[120]

8.2 Enjeux pour la fonction compliance

Comme nous venons de l'expliquer, la mission de la fonction compliance n'est plus uniquement de faire en sorte que les banques soient conformes aux lois et règlements, même si cette mission reste toujours au cœur de la fonction. Elle doit non seulement s'adapter aux réglementations de plus en plus complexes, mais également à des exigences en internes de plus en plus fortes. Il suffit de voir pour cela la multitude des missions qui lui sont confiées (voir point 7.2). La fonction compliance doit donc constamment s'adapter et se réinventer.
Deloitte a publié en 2017 un article intitulé « *New Horizons – Compliance 2020 and beyond »*.
[121]

Cet article met en lumière les enjeux majeurs auxquelles sont confrontées les métiers de la compliance, et comment la fonction de compliance est amenée à évoluer. Nous discutons des points essentiels qui en ressortent. Cela permet notamment de se rendre compte du profil recherché des personnes amenées à exercer la fonction de compliance. C'est ce point que nous souhaitons mettre en avant.

La fonction compliance au sein des banques nécessite aujourd'hui de nouvelles compétences, de nouveaux profils capables de faire le lien entre la conformité et le business proprement dit. Les collaborateurs en compliance doivent avoir des connaissances en gestion des risques, en économie, et comprendre parfaitement les activités bancaires. En outre, au vu de la densité des réglementations, des sujets précis tels que l'imposition ou les sanctions doivent être maîtrisés. Pour cela, les banques ont besoin de faire appel à des spécialistes en la matière. En plus de spécialistes dans de nombreux domaines, la fonction de compliance requière également des personnes ayant une expérience et des compétences suffisantes pour pouvoir synthétiser les choses. L'ancienneté des collaborateurs a aussi de l'importance dans la communication d'égal à égal avec d'autres acteurs clés de la banque. La discussion de points problématiques est ainsi plus aisée et mieux acceptée.

[120] Cordier, B. (2016). Société Française des Analystes Financiers. Focus Métiers. *La compliance, une fonction en pleine évolution*
[121] Deloitte (2017). New horizons. *Compliance 2020 and beyond*

Un passage d'un article décrit très bien la personnalité, le profil idéal d'une personne amenée à exercer dans le domaine de la compliance : *Le Compliance Officer sera doté d'une grande faculté d'adaptation et d'une bonne sensibilité à l'évolution des règles et à l'éthique. C'est un esprit à la fois ouvert et curieux, indépendant, rigoureux, intègre avec un fort leadership. Il lui faudra être communicant et pédagogue, humain mais ferme. Ses compétences et ses qualités humaines lui permettront de conseiller, former, sensibiliser les salariés et les parties prenantes de l'entreprise à la compliance, à l'éthique des affaires, à la conformité, notamment dans le contexte de la responsabilité sociale et environnementale. C'est aussi un capteur et un veilleur que les salariés n'hésiteront pas à interroger lors d'un dossier sensible.*[122]
Il en ressort qu'en plus de savoir élaborer des règles, des procédures ou des politiques, le Compliance Officer doit être un genre de facilitateur. Autrement dit capable de convaincre, d'influencer ou bien de communiquer le rôle essentiel de la compliance dans le bon fonctionnement des banques, et comment parvenir à la mettre en œuvre correctement.

Un autre point mis en avant dans l'article de Deloitte est le fait que la *compliance se caractérise traditionnellement par une approche en silos*. C'est-à-dire que la compliance est abordée de manière spécifique par chaque fonction, qui a donc ses propres méthodes. Pour être plus efficace en termes de compliance, il faut mettre en place des programmes de compliance de plus en plus intégrés, comme c'est par exemple le cas pour le contrôle interne ou la gestion des risques, avec l'utilisation des référentiels COSO (voir partie 2). Cela peut se faire par le partage des connaissances et du savoir-faire, ou bien en coordonnant davantage les équipes (l'utilisation du modèle des trois lignes de défense présenté dans les chapitres 5 peut être utile à cette fin).
Enfin, un enjeu majeur à prendre également en considération est celui de l'attention particulière qui doit être portée à la culture d'entreprise et aux principes éthiques. *La définition de règles et de procédures permet de se protéger des risques prévus et connus, mais ne couvre par tous les scénarios et toutes les éventualités. Seules une culture éthique forte et des pratiques d'entreprise exemplaires peuvent garantir à l'organisation une certaine résilience face à des risques imprévus et non anticipés.*

[122] Cordier, B. (2016). Société Française des Analystes Financiers. Focus Métiers. *La compliance, une fonction en pleine évolution*

CONCLUSION

Une structure organisationnelle adéquate fondée sur une gouvernance efficace est essentielle pour que les banques puissent évoluer et prospérer dans un secteur aussi compétitif et confronté à un nombre sans cesse croissant de risques en tout genre. Dans ce contexte, il est essentiel de disposer d'organes de gouvernance efficaces.
La responsabilité globale de la banque et confiée à son conseil d'administration. En tant que tel, ce dernier doit d'une part définir la stratégie globale de la banque et l'orientation des activités, et d'autre part, exercé sa fonction de surveillance à l'égard de l'ensemble des domaines d'activités de la banque (uniquement les membres non exécutifs). C'est lui qui veille à ce que la banque dispose en permanence d'une fonction de compliance indépendante adéquate.
Au sein de ce conseil d'administration, les banques doivent désigner un comité de direction. Il se compose donc des membres exécutifs du conseil d'administration. Ils sont responsables de la gestion journalière de la banque ainsi que de la maîtrise du risque de compliance.
Enfin l'organe légal d'administration doit également constituer en son sein, quatre comités spécialisés que sont le comité d'audit, le comité des risques, le comité de rémunération et le comité de nomination. Ils sont chargés de conseiller le conseil d'administration dans leur domaine respectif. A ce titre, le comité d'audit doit notamment vérifier l'efficacité des mécanismes de contrôle interne et des fonctions de gestion des risques.

Nous avons ensuite vu qu'il était vivement conseillé aux banques de mettre en place des systèmes robustes de contrôle interne et de gestion des risques. A cette fin, l'utilisation de référentiels intégrés constitue une solution, voire une obligation. Ils doivent contenir des systèmes d'identification, d'évaluation, de gestion et de suivi des risques. Nous avons présenté les référentiels COSO I et son évolution COSO III pour le contrôle interne, et COSO II pour le management des risques.
En parallèle, les fonctions de contrôle doivent être clairement définies, et des rôles spécifiques doivent leurs être assignés. Sans quoi peuvent surgir des manquements dans les contrôles et des redondances dans les fonctions, ce qui peut s'avérer fort coûteux. Elles doivent également être parfaitement coordonnées et communiquer efficacement entre elles. C'est le but de la mise en œuvre du modèle des trois lignes de défense. Nous avons mis en avant le rôle essentiel des organes de gouvernance pour que le modèle soit correctement appliqué dans les processus de gestion des risques et de contrôle de la banque. Les membres des organes de gouvernance sont les mieux placés, de par leur statut hiérarchique, et sont justement les principales parties prenantes à qui les trois lignes de maîtrise apportent leur appui.

En tant que fonction de contrôle de la deuxième ligne de défense, au côté des fonctions de gestion des risques, la fonction compliance est devenue un acteur stratégique incontournable dans les banques.

Ayant à l'origine pour but de répondre uniquement aux exigences légales minimales, ses responsabilités se sont considérablement accrues. Nous avons vu que la transformation de l'environnement dans lequel évoluaient les banques en était la cause principale. Le renforcement sans cesse croissant des réglementations financières et bancaires a obligé les banques à durcir leurs exigences en matière de conformité, conférant ainsi un rôle central à la fonction de compliance dans le dispositif de maîtrise globale de gestion des risques. Elle est désormais le point de contact clé des autorités de contrôle et bénéficie d'une relation étroite et régulière avec les organes de gouvernance, tout en conservant son indépendance. La fonction de compliance n'est plus vue, ou ne doit plus être vue, comme une contrainte, un « mal nécessaire », destinée uniquement à rester conforme. Elle est ou devrait être perçue comme une alliée avec laquelle composer car elle peut également participer à l'amélioration de la performance globale des banques lorsqu'elle est correctement alignée sur leurs enjeux stratégiques. Elle peut faire de la conformité un atout, transformer les risques de conformité en opportunités, et s'en servir pour que les banques puissent se développer.

Ce développement de la fonction compliance se traduit également par une évolution dans les profils, les personnalités de ceux ou celles qui sont amenés à l'exercer. En plus d'être compétents dans l'élaboration et le suivi de règles et de procédures, les compliance officers doivent aussi pouvoir convaincre, influencer et faire comprendre à l'ensemble du personnel l'importance et le rôle clé occupé par la compliance. Ils doivent en plus constamment faire face à de nouveaux enjeux comme par exemple celui de la conformité à l'égard de tout ce qui concerne les technologies ou les outils d'analyse de données.

Ainsi, bien que la fonction de compliance ait déjà assisté à une profonde évolution de son statut et de sa mission, elle est encore amenée à s'adapter et à se réinventer afin d'être à la hauteur des responsabilités qui lui sont confiées.

BIBLIOGRAPHIE

AMRAE & IFACI (2013). *Trois lignes de Maîtrise pour une meilleure performance. Fiabiliser la stratégie par une gestion organisée des risques*. En ligne sur le site : https://chapters.theiia.org/montreal/ChapterDocuments/Trois%20lignes%20de%20ma%C3%AEtrise%20pour%20une%20meilleure%20performance%20%28IFACI%20-%20AMRAE%29.pdf

Bank for International Settlements (2015). Basel Commitee on Banking Supervision. Guidelines. *Corporate governance principles for banks*. En ligne sur le site : https://www.bis.org/bcbs/publ/d328.pdf

Bank for International Settlements (2003). Basel Commitee on Banking Supervision. Consultative Document. *The compliance function in banks*. En ligne sur le site : https://www.bis.org/publ/bcbs103.pdf

Banque Nationale de Belgique (2017). *Manuel de gouvernance pour le secteur bancaire*. En ligne sur le site : https://www.nbb.be/doc/cp/fr/2015/governancemanual.pdf

Bernet, A. & Genequand, E. (2015). PWC. Disclose. Gros plan sur la gestion des risques. *Contrôle coordonnée : le modèle des « quatre ligne de défense ».* En ligne sur le site : https://disclose.pwc.ch/21/fr/article-focus--02/

Commission Corporate Governance. Fondation Privée (2011). *Contrôle interne et gestion des risques. Lignes directrices dans le cadre de la loi du 6 avril 2010 et du Code Belge de gouvernance d'entreprise 2009*. En ligne sur le site : https://www.corporategovernancecommittee.be/sites/default/files/generated/files/page/2011_01_10_controle_interne_fr.pdf

Commission Corporate Governance. Fondation Privée (2009). *Le code belge de gouvernance d'entreprise 2009.* En ligne sur le site : https://www.corporategovernancecommittee.be/sites/default/files/generated/files/page/corporategovfrcode2009.pdf

Cordier, B. (2016). Société Française des Analystes Financiers. Focus Métiers. *La compliance, une fonction en pleine évolution.* En ligne sur le site : http://www.sfaf.com/la-compliance-une-fonction-en-pleine-evolution/

COSO Commitee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management. Integrated Framework*. En ligne sur le site : https://www.coso.org/Pages/erm-integratedframework.aspx

Deloitte (2017). New horizons. *Compliance 2020 and beyond.* En ligne sur le site : https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_compliance-2020-and-beyond.pdf

EBA European Banking Authority (2011). *Orientations de l'ABE sur la gouvernance interne (GL 44).* En ligne sur le site : https://www.eba.europa.eu/documents/10180/103861/EBA_2012_00210000_FR_COR.pdf

Gassmann, P. (2015). PWC. Disclose. Gros plan sur la gestion des risques. *Le rôle de la fonction de Compliance dans la gestion des risques bancaires.* En ligne sur le site : https://disclose.pwc.ch/21/media/pdf/pwc_disclose_1501_f.pdf

IFACI & PWC (2013). Pocket Guide. COSO 2013. *Une opportunité pour optimiser votre contrôle interne dans un environnement en mutation.* En ligne sur le site : http://fichiers.ifaci.com/tmp_fichiers/AD_Pocket_Guide_Coso_Juillet2013_Draft3.pdf

IFACI & PWC (2014). COSO Commitee of Sponsoring Organizations of The Treadway Commission (2014). *Référentiel intégré de contrôle interne. Principes de mise en œuvre et pilotage*. Eyrolles

IIA (2013). Prise de position de l'IIA. *Les trois lignes de maîtrise pour une gestion des risques et un contrôle efficaces.* En ligne sur le site : https://na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20French.pdf

IIA & IFACI (2014). *Cadre de référence international des pratiques professionnelles de l'audit interne*.

Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse (dite « **loi bancaire** »). En ligne sur le site web de la Banque Nationale de Belgique : https://www.nbb.be/doc/cp/moniteur/2018/201803_wet_20140425.pdf

Organisation de Coopération et de Développement Economiques (2004). *Préambule aux Principes de gouvernement d'entreprise de l'OCDE*. En ligne sur le site : https://www.oecd.org/fr/daf/ae/principesdegouvernementdentreprise/31652074.PDF

Pierandrei, L. (2015). Risk Managment. *Gestion des risques en entreprise, banque et assurance.* Dunod

Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, M.S. & Riddle, C. (2015). IFACI. The IIA Research Foundation. Manuel d'audit interne*. Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques*. Eyrolles.

Vilepet, S. (2013). IFACI. Dossier Audit & Contrôle internes n°215. *Le COSO 2013 : une mise à jour du référentiel d'origine pour mieux maîtriser les évolutions.* En ligne sur le site : http://fichiers.ifaci.com/tmp_fichiers/Dossier_COSO_Revue215.pdf

Zurstrassen, M. (2016) Puilaetco Dewaay Private Bankers. *Compliance : Une fonction clé dans un univers bancaire toujours plus réglementé.* En ligne sur le site : https://www.puilaetcodewaay.be/fr/articles/economie-finance-7/compliance-une-fonction-cle-dans-un-univers-bancaire-toujours-plus-reglemente-188

ANNEXES

Annexe 1 – Modèle de mémorandum de gouvernance

ANNEXE: MODELE DE MEMORANDUM DE GOUVERNANCE

1. Structure de l'actionnariat
2. Structure de groupe si applicable (structure juridique et fonctionnelle; organigramme)
3. Politique en matière de composition et de fonctionnement des organes de gestion (avec éventuellement une description de l'impact du groupe)
   (a) nombre, durée du mandat, rotation, âge, suivi, ...
   (b) critères de sélection;
   (c) procédure de proposition (nouveaux mandats/reconduction) et de démission/non-reconduction;
   (d) administrateurs indépendants;
   (e) politique de rémunération
      I. membres exécutifs de l'organe légal d'administration
      II. membres non exécutifs de l'organe légal d'administration
4. Structure de gestion et organigramme (avec éventuellement une description de l'impact du groupe)
   (a) organe légal d'administration (en l'espèce, le conseil d'administration)
      I. composition
      II. fonctionnement (règlement d'ordre intérieur)
      III. répartition interne éventuelle
      IV. comités spécialisés
         - composition
         - fonctionnement
   (b) comité de direction
      I. composition
      II. fonctionnement (règlement d'ordre intérieur)
      III. répartition interne des tâches des membres
   (c) direction effective (niveau « CD-1 »)
      I. composition
      II. répartition interne des tâches des dirigeants effectifs
   (d) autres comités
5. Fonctions-clés (avec éventuellement une description de l'impact du groupe)
   (a) Fonctions d'encadrement (secrétaire général, questions juridiques, personnel, communication)
   (b) fonctions de contrôle indépendantes
      I. audit interne;
      II. compliance
      III. gestion des risques
      IV. actuaire désigné
6. Structure organisationnelle (avec éventuellement une description de l'impact du groupe)
   (a) structure opérationnelle, *business lines*, *matrix management* et attribution des compétences et des responsabilités
   (b) sous-traitance
   (c) gamme des produits et services
   (d) périmètre géographique de l'activité
      I. libre prestation de services
      II. succursales
      III. filiales, coentreprises, ...
   (e) utilisation de centres off-shore
7. Politique de rémunération
   (a) Gouvernance
   (b) Politique globale applicable à tous les collaborateurs
   (c) *Identified Staff*
      I. Processus de sélection

      II. Règles spécifiques (alignement des risques, reports, instruments, ...)
8. Politique d'intégrité (avec éventuellement une description de l'impact du groupe)
   (a) objectifs stratégiques et valeurs d'entreprise
   (b) codes et règlements internes, politique de prévention, ...
   (c) politique en matière de conflits d'intérêt
   (d) procédure de *whistleblowing*
   (e) traitement des plaintes de clients
9. Politique en matière de publicité des principes appliqués
10. Statut du mémorandum de gouvernance et date
   (a) établissement
   (b) dernière adaptation
   (c) dernière évaluation
   (d) approbation par l'organe légal d'administration

Annexe 2 – Les 17 principes structurants du COSO III pour un contrôle interne efficace

Environnement de contrôle	**1. L'organisation démontre son engagement en faveur de l'intégrité et de valeurs éthiques.** **2. Le conseil d'administration fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.** **3. La direction, agissant sous la surveillance du conseil d'administration, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs.** **4. L'organisation démontre son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs.** **5. L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.**
Evaluation des risques	6. L'organisation **spécifie les objectifs** de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs. 7. L'organisation identifie les risques associés à la réalisation de ses objectifs dans **l'ensemble de son périmètre de responsabilité** et elle procède à leur analyse de façon à déterminer les **modalités de gestion des risques appropriées.** 8. L'organisation intègre le **risque de fraude** dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs. 9. L'organisation **identifie et évalue les changements** qui pourraient avoir un impact significatif sur le système de contrôle interne.
Activités de contrôle	10. L'organisation **sélectionne et développe les activités de contrôle** qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs. 11. L'organisation sélectionne et développe des activités de contrôle général en matière de **système d'information** pour faciliter la réalisation des objectifs. 12. L'organisation met en place les activités de contrôle par le biais de **directives** qui précisent les objectifs poursuivis, et de **procédures** qui mettent en œuvre ces directives.
Information et communication	13. L'organisation obtient ou génère puis utilise des **informations pertinentes et de qualité** pour faciliter le fonctionnement des autres composantes du contrôle interne. 14. L'organisation **communique en interne** les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne. 15. L'organisation **communique avec les tiers** au sujet des facteurs qui affectent le bon fonctionnement des autres composantes du contrôle interne.
Pilotage	16. L'organisation sélectionne, met au point et réalise des **évaluations continues et/ou ponctuelles** afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent. 17. L'organisation **évalue et communique les faiblesses de contrôle interne en temps voulu** aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration.