

L'AUTEUR

Marie-Agnès NICOLET est Présidente de *Regulation Partners* qu'elle a fondé en septembre 2011. Elle est diplômée d'HEC (promotion 1989) et a plus de 25 ans d'expérience dans les domaines du contrôle, des risques et de la conformité auprès des institutions bancaires et financières, tout d'abord en tant que responsable du contrôle interne d'une banque de 1991 à 1998, puis en tant que dirigeante d'un cabinet de conseil spécialisé dans ces matières. Elle a dirigé de nombreuses missions de diagnostic et mise en conformité des dispositifs réglementaires pour des sociétés de gestion d'actifs, des établissements de crédit, des entreprises d'investissement, des sociétés de financement, des établissements de paiement et de monnaie électronique, des mutuelles...

Elle anime des conférences et formations sur les sujets réglementaires (enjeux de la régulation, gestion des risques, titrisation, lutte contre le blanchiment, chambres de compensation, risque de liquidité...) ainsi que des formations pour les administrateurs d'établissements de crédit, sociétés de financement et d'assurance. Elle enseigne dans le cadre d'un cursus certifiant sur le contrôle interne et gestion des risques au CNAM depuis 2012.

Elle est par ailleurs membre du conseil d'administration du Centre des professions financières, et préside le Club des marchés financiers depuis 2011. Dans ce cadre, elle a piloté deux études avec la SFAF sur le financement des entreprises (cotées et non cotées) et organise des séminaires sur les modes alternatifs de financement de l'économie et l'évolution des marchés (conférence sur les financements des entreprises en mars 2014 et octobre 2015, conférences sur le *crowdfunding* en 2013 et 2014, sur l'obligataire PME en 2013, plusieurs conférences sur la titrisation et les fonds de dettes...) et des ateliers permettant de faire dialoguer la recherche et le monde de l'industrie financière (sur l'analyse comportementale et les *robo-advisors*, le 18 janvier 2017, sur la *blockchain* en mars 2017).

Elle est membre de comités de labellisation du pôle Finance innovation qui donnent leur avis pour la labellisation des projets innovants.

SOMMAIRE

Liste des sigles et abréviations.....	13
Introduction.....	15

Chapitre 1

La fonction Conformité	19
-------------------------------------	-----------

1.1 Une fonction permettant de limiter le risque de réputation	19
1.2 Le contexte international.....	20
1.3 La fonction Conformité en France.....	24
1.3.1 La fonction Conformité dans les établissements bancaires	24
1.3.2 La fonction de vérification de la conformité dans les sociétés d'assurance, réassurance et mutuelles.....	25
1.3.3 La fonction Conformité dans l' <i>Asset Management</i>	25
1.3.4 Les nouvelles attributions de la fonction Conformité	26
1.3.4.1 Conformité aux réglementations concernant la protection des données personnelles.....	26
1.3.4.2 Lutte contre la corruption	27
1.4 Détail des 10 missions de la fonction Conformité : de la veille réglementaire au contrôle, en passant par le rôle de conseil	27
1.4.1 Assurer et diffuser la veille réglementaire	28
1.4.2 Mettre en place et diffuser les normes et procédures en matière de conformité..	30
1.4.3 Former et informer sur les risques de non-conformité et les dispositifs à mettre en œuvre.....	30
1.4.4 Assurer un conseil aux collaborateurs pour tout élément lié à la conformité.....	32
1.4.5 Donner un avis écrit sur la conformité des nouveaux produits	32
1.4.6 Réaliser et mettre à jour la cartographie des risques de non-conformité	33
1.4.7 Assurer un rôle de contrôle permanent de la conformité	33
1.4.8 Assurer la maîtrise d'ouvrage des applicatifs liés à la conformité et s'assurer que les nouveaux applicatifs métiers ou leurs modifications restent conformes aux obligations réglementaires.....	34
1.4.9 Mettre en place un dispositif de lutte contre la corruption.....	34
1.4.10 Mettre en œuvre un dispositif d'alerte éthique.....	35

Chapitre 2

La fonction de responsable des contrôles permanents 37

2.1	Définition du contrôle permanent de second niveau et rappels réglementaires	37
2.2	Positionnement de la fonction de coordination des contrôles permanents	38
2.3	Facteurs clés de succès d'un contrôle permanent de second niveau.....	39
2.4	Le contrôle permanent des prestations essentielles ou importantes externalisées.....	40

Chapitre 3

Le responsable LCB-FT Le correspondant/déclarant TRACFIN 49

3.1	Une fonction en forte évolution depuis plus de vingt ans.....	49
3.2	Définition du blanchiment et rôle des établissements en matière préventive.....	50
3.3	Positionnement de la fonction dans l'organisation et compétences requises.....	53
3.4	Périmètre des sujets à couvrir par le responsable LCB-FT	56
3.4.1	Assurer une veille réglementaire sur la LCB-FT	56
3.4.2	Mettre à jour les procédures de lutte anti-blanchiment et les diffuser aux personnes concernées.....	57
3.4.3	Mettre à jour la classification des risques de blanchiment.....	59
3.4.4	Intervenir en second niveau dans les entrées en relation et la révision des dossiers clients	60
3.4.5	Analyser les déclarations suspectes et effectuer les déclarations à TRACFIN	60
3.4.6	Piloter le paramétrage des outils de lutte anti-blanchiment	63
3.4.7	Prévenir le financement du terrorisme et le respect des embargos.....	64
3.4.8	Former les collaborateurs et dirigeants.....	66
3.4.9	Effectuer des <i>reportings</i> à la direction générale et aux régulateurs	67
3.4.10	Contrôle permanent de second niveau du dispositif de LCB-FT	67

Chapitre 4

Le responsable du contrôle des services d'investissement RCSI et RCCI 69

4.1	Définition réglementaire.....	69
4.2	Rôle du RCCI/RCSI sur la déontologie des collaborateurs.....	70
4.3	Rôle du RCCI/RCSI sur l'intégrité des marchés.....	71
4.3.1	Rôle dans la mise à jour des listes d'interdiction et de surveillance.....	71
4.3.2	Rôle du RCCI/RCSI dans la prévention des abus de marché.....	72
4.3.3	Rôle du RCCI/RCSI dans le cadre de la délivrance des cartes professionnelles.....	73
4.4	Rôle du RCCI/RCSI dans les relations avec les clients.....	73
4.4.1	Contrôler la catégorisation des clients	74
4.4.2	Contrôler l'adéquation des produits distribués avec le profil des clients.....	74

4.4.3	Vérifier la gouvernance produits et s'assurer que la documentation fournie au client est claire, adaptée et non trompeuse.....	76
4.5	Rôle du RCSI/RCCI dans la prévention et la gestion des conflits d'intérêts.....	80
4.6	Rôle du RCCI/RCSI dans les autres aspects du respect de la réglementation AMF.....	80
4.6.1	Contrôle de la bonne exécution des ordres.....	80
4.6.2	Contrôles du RCCI.....	82
4.6.3	Élaborer et contrôler les <i>reportings</i> à destination des autorités de supervision.....	82

Chapitre 5

La fonction Risques	87	
5.1	Les types de risques à couvrir dans les Établissements bancaires et financiers.....	87
5.1.1	Définition des risques dans les établissements soumis à l'arrêté du 3 novembre 2014.....	87
5.1.2	Les risques dans le secteur des assurances.....	90
5.1.3	La définition des risques dans les sociétés de gestion d'actifs.....	90
5.2	Rôle de la fonction Risques dans les établissements soumis à l'arrêté du 3 novembre 2014.....	91
5.2.1	Coordonner les systèmes de mesure des risques et résultats.....	91
5.2.2	Coordonner la réalisation de la cartographie globale des risques.....	92
5.2.3	Positionnement de la fonction de gestion des risques et de son responsable.....	93
5.2.4	Gestion des risques de crédit.....	97
5.2.5	Gestion et contrôle des risques actif/passif (ALM).....	98
5.2.6	La fonction de gestion des risques opérationnels.....	99
5.2.7	La gestion des plans d'urgence et de poursuite d'activité.....	100
5.3	La fonction Risques dans l' <i>Asset Management</i>	101
5.3.1	Définition des risques et méthodes de suivi.....	101
5.3.2	Positionnement et périmètre de la fonction Risques dans l' <i>Asset Management</i>	105
	a) Indépendance de la fonction.....	105
	b) Recours à un tiers.....	106
	c) Contenu des missions de la fonction Risques.....	107
5.4	Gestion des risques et actuariat dans l'assurance.....	108
5.4.1	Gestion des risques.....	108
5.4.2	Fonction actuarielle.....	113

Chapitre 6

La fonction de responsable de la sécurité des systèmes d'information (RSSI)	117	
6.1	Une fonction connexe aux fonctions clés.....	117
6.2	La raison d'être du RSSI.....	119

6.3	Le périmètre à couvrir par le RSSI	120
6.3.1	Définition du risque maximum tolérable	120
6.3.2	Mesure de la sécurité technique	120
6.3.3	Évaluation des coûts de la sécurité et élaboration d'un budget sécurité	121
6.3.4	Maîtrise d'ouvrage des mesures de sécurité	121
6.3.5	Analyse des contrats d'assurances	122
6.3.6	Sensibilisation et formation	122
6.4	Positionnement de la fonction	122
6.4.1	Indépendance par rapport aux directions informatiques	122
6.4.2	Liens entre RSSI et responsables des risques opérationnels	123
6.5	Les facteurs clés de succès et les écueils à éviter	123

Chapitre 7

La fonction de contrôle périodique / audit interne 125

7.1	Définitions du contrôle périodique / audit interne	125
7.2	Rattachement de la fonction	129
7.3	Élaboration du plan pluriannuel et du programme annuel d'audit interne	130
7.4	Reporter le résultat des missions	131
7.5	Charte d'audit interne et autres bonnes pratiques	132

Chapitre 8

Articulation des fonctions pour un contrôle efficace 135

8.1	Une organisation mouvante au fil du temps	135
8.2	Les différents types d'organisation des fonctions de contrôle dans les établissements assujettis à l'arrêté du 3 novembre 2014, les sociétés d'assurance et mutuelles et les sociétés de gestion d'actifs	135
8.3	Organisation de ces nombreuses fonctions de contrôle dans les établissements de petite taille	139
8.4	Assurer un <i>reporting</i> global des risques et des contrôles à la Direction générale / aux dirigeants effectifs	141

Chapitre 9

Le rôle des organes de gouvernance dans le contrôle interne et la maîtrise des risques 145

9.1	Une implication des organes de gouvernance souhaitée par les régulateurs	145
9.2	Définition de la compétence et autres critères permettant d'être membres du conseil d'administration ou de surveillance	146
9.3	Rôle de l'organe de surveillance	149

9.4	Les principaux Comités spécialisés du Conseil.....	152
9.4.1	Comité des risques et comité d'audit	152
9.4.2	Comité des rémunérations	154
9.4.3	Le Comité des nominations	156
9.5	Informations à transmettre à l'organe de gouvernance et au comité des risques	157
9.5.1	Pour les établissements assujettis à l'arrêté du 3 novembre 2014	157
9.5.2	Concernant les sociétés d'assurance et les mutuelles	160
9.6	Benchmark international : l'exemple du Maroc	161

Conclusion..... 165

Annexes..... 169

1.	Exemple d'organisation des fonctions de contrôle dans un grand établissement	173
2.	Organisation des fonctions de contrôle dans un établissement de taille moyenne	175
3.	Exemple de cartographie des risques pour l'Asset Management.....	177
4.	Organisation du contrôle interne dans les sociétés d'Asset Management.....	179
5.	Références des principaux textes cités dans l'ouvrage	181
▶	Textes législatifs et réglementaires	181
□	Textes européens.....	181
□	Textes français	181
□	Textes hors Europe.....	182
▶	Texte de référence du chapitre 5 «La fonction Risques»: extrait de l'arrêté du 3 novembre 2014 en matière de suivi du risque de liquidité.....	182
▶	La Soft Law	187
6.	Orientations EBA sur l'évaluation du risque lié aux TIC dans le cadre du processus de contrôle et d'évaluation prudentiels (<i>Supervisory Review and Evaluation process – SREP</i>).....	189

INTRODUCTION

Les fonctions de contrôle dans les établissements bancaires et financiers ont subi une mutation importante, depuis l'émergence des premiers textes de contrôle au début des années 1990 jusqu'aux plus récentes évolutions réglementaires post-crise.

Ces fonctions de contrôle prévues par la réglementation sont rendues nécessaires par le fait qu'un établissement de crédit a l'obligation de pouvoir restituer à tout moment à ses clients les fonds qui lui ont été confiés ; une entreprise d'assurance se doit, quant à elle, de pouvoir répondre aux engagements de ses souscripteurs. Le secteur bancaire et assurantiel est, de ce fait, régulé. Nul ne peut exercer ces activités sans un agrément préalable et doit se conformer aux principes permettant de limiter les risques de faillite dont les conséquences en termes de perte de confiance pour le système tout entier sont majeures.

Dans le domaine des produits financiers comme de celui des marchés, les établissements doivent également se conformer aux pratiques de contrôle permettant la protection des épargnants, comme le bon fonctionnement des marchés, et obtenir un agrément pour exercer.

Dans le cadre de cet agrément, l'organisation des dispositifs et fonctions de contrôle est un point primordial étudié par les autorités compétentes (en France, AMF¹ pour les sociétés de gestion d'actifs et ACPR² pour les établissements de crédit, établissements de paiement, établissements de monnaie électronique, sociétés de financement, entreprises d'investissement, entreprises d'assurance et mutuelles notamment).

C'est la raison pour laquelle ont été progressivement publiées des normes de plus en plus détaillées imposant pour le secteur bancaire et financier des fonctions de contrôle, qui devraient permettre de sécuriser l'ensemble des activités des établissements.

Aussi, le règlement du Comité de la réglementation bancaire de 1990, le CRB n° 90.08, avait-il rendu obligatoire, dans tout établissement de crédit, la fonction de responsable de contrôle interne ainsi que la mise en place de dispositifs adéquats de surveillance.

Ce responsable du contrôle interne était chargé de s'assurer de l'existence et de la bonne application des dispositifs de contrôle interne, avec une ambiguïté qui n'a disparu que lors de la modification du règlement CRBF n° 97.02³ de 2005, lui-même remplacé par l'arrêté du 3 novembre 2014. Cette ambiguïté réside dans le fait que le responsable du contrôle interne était parfois considéré par les directions générales non seulement comme celui qui alerte et vérifie l'adéquation des dispositifs mais aussi comme le responsable de la mise en œuvre des dispositifs de contrôle.

1. Autorité des marchés financiers.

2. Autorité de contrôle prudentiel et de résolution.

3. CRBF : Comité de la réglementation bancaire et financière. Le règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements bancaires et des entreprises d'investissement modifié par les règlements 2001-01 et 2004-02 et par les arrêtés du 31 mars 2005, 17 juin 2005, des 20 février et 2 juillet 2007, du 11 septembre 2008, 14 janvier 2009, 5 mai 2009, 29 octobre 2009, 3 novembre 2009, 19 janvier 2010, 25 août 2010 et du 13 décembre 2010. Ce texte a été abrogé et remplacé par l'arrêté du 3 novembre 2014 relatif au contrôle interne.