Henri-Pierre Maders
Jean-Luc Masselin
Hervé Fratta

TOUT POUR RÉUSSIR DANS **LE MÉTIER DE**

AUDITEUR INTERNE ET CONTRÔLEUR PERMANENT

La place de la fonction dans le dispositif
Les meilleures pratiques et les outils associés
L'exercice du métier au quotidien
Le pilotage des deux fonctions

EYROLLES

SOMMAIRE

Henri-Pierre Maders est diplômé de l'ISG, MBA de l'EUA, titulaire d'un Master PNL et auditeur certifié IAA. Fondateur d'HPM Conseils, société de conseil spécialisée dans les dispositifs de gouvernance des risques et de contrôle interne, il intervient depuis plus de 25 ans en audit et pilotage de projet sur ce thème pour le compte de grandes entreprises et de ministères, en France et à l'étranger. Il est également auteur d'une quinzaine d'ouvrages professionnels sur le sujet. Il est enfin vice-président de SOS Sahel, ONG qui intervient auprès des populations rurales d'une dizaine de pays d'Afrique dans le cadre de projets de sécurité alimentaire.

Jean-Luc Masselin est diplômé de l'ESSEC, expert comptable, auditeur certifié IAA et AMF. Il s'est spécialisé dans l'évaluation et la gestion opérationnelle du contrôle interne de grandes entités. Il a ainsi pratiqué 19 ans durant le commissariat aux comptes de grandes structures des secteurs publics et financiers. En qualité de Contrôleur général de la plus grande banque régionale européenne, il a, pendant 5 ans, rénové la pratique de l'audit interne. Depuis 2007, il est directeur du contrôle interne de la banque Neuflize OBC, filiale française d'ABN AMRO Group. Il est aussi l'auteur de deux ouvrages sur le thème du contrôle interne.

Hervé Fratta est titulaire d'un Magistère Banque Finance et d'un DESS d'Ingénierie financière de l'Université de la Sorbonne. Associé dans le cabinet de conseil en organisation et management A2 Consulting, il intervient depuis plus de 20 ans auprès de banques et institutions financières (organisation et amélioration des processus de contrôle interne, mise en place de dispositifs de pilotage et de maîtrise des risques), de directions financières de grandes entreprises (mise en place de dispositifs de calcul, pilotage et réduction des coûts et optimisation des processus d'arrêté et de synthèse).

LE LIVRE QUI VOUS FAIT **GAGNER 10 ANS D'EXPÉRIENCE !**

Tout pour réussir dans les métiers d'auditeur interne et de contrôleur permanent :

- **Les fondamentaux des deux métiers :** leur rôle dans le dispositif de maîtrise des risques, le cadre légal et réglementaire, les évolutions en cours…
- **Les meilleures pratiques et les outils :** la démarche de conduite d'une mission d'audit interne, les outils communs aux deux métiers…
- **Le quotidien des métiers :** les formations initiales, le positionnement dans l'organigramme, les différents grades, la rémunération…
- **L'évaluation et le suivi d'activité :** les indicateurs de suivi et de performance…

Une signalétique efficace :

EN PRATIQUE	Des conseils et des méthodes à appliquer au quotidien
PAROLE D'EXPERT	Des retours d'expérience de professionnels
	Des focus sur des points précis
	Les idées clés à retenir

Henri-Pierre Maders est un expert reconnu en matière de gestion des risques et de dispositifs de contrôle interne des entreprises et administrations. Jean-Luc Masselin est directeur du contrôle interne de la filiale française d'une grande banque privée et de détail. Hervé Fratta audite et accompagne de grandes entreprises françaises et étrangères dans leurs dispositifs de maîtrise des risques.

www.editions-eyrolles.com

Couverture : Studio Eyrolles / Photo : Shutterstock © Éditions Eyrolles

Les métiers d'auditeur interne et de contrôleur permanent

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05

www.editions-eyrolles.com

Copyright © 2014 Eyrolles.

ISBN : 978-2-212-56050-3

Henri-Pierre Maders
Jean-Luc Masselin
Hervé Fratta

Les métiers d'auditeur interne et de contrôleur permanent

EYROLLES

Du même auteur

Le Métier de chef de projet, H.-P. MADERS, J. LEBLANC, E. CLET et M. GOLDFARB, Éditions Eyrolles, 2013.

Animer une équipe projet avec succès, H.-P. MADERS, Éditions Eyrolles, 2012, ouvrage nominé au prix Qualité & Performance 2013.

Piloter les risques d'un projet, H.-P. MADERS et J.-L. MASSELIN, Les Éditions d'Organisation, 2009.

Piloter un projet d'organisation, H.-P. MADERS, Les Éditions d'Organisation, 2008.

Contrôle interne des risques (livre + CD-ROM), H.-P. MADERS et J.-L. MASSELIN, Les Éditions d'Organisation, 2004, 2007, 2013, Ouvrage nominé au prix Qualité & Performance 2007.

Pratiquer la conduite de projet (livre + CD-ROM), H.-P. MADERS et E. CLET, Les Éditions d'Organisation, 2005.

Comment manager un projet, H.-P. MADERS et E. CLET, Les Éditions d'Organisation, 2004, 2006, 2008.

Manager une équipe projet (livre + CD-ROM), H.-P. MADERS, Les Éditions d'Organisation, 2003.

Conduire une équipe projet (livre + CD-ROM), H.-P. MADERS, 2000, Les Éditions d'Organisation, épuisé, ouvrage finaliste du Prix du livre informatique francophone.

Conduire un projet d'organisation (livre + CD-ROM), H.-P. MADERS, E. GAUTHIER et C. LE GALLAIS, Les Éditions d'Organisation, 1998, 2000, 2002, épuisé.

Conduire un projet dans le tertiaire, H.-P. MADERS et P. LEMAÎTRE, Les Éditions d'Organisation, 1997, 2000, épuisé.

Le Management d'un projet, H.-P. MADERS et E. CLET, Les Éditions d'organisation, coll. « Mémento ÉO », 1995, épuisé.

Assistant : organiser, gérer, faciliter (Livres du maître et de l'élève pour les BTS et IUT), C. GARCIA et H.-P. MADERS, Les Éditions d'Organisation, 1995, épuisé.

Audit opérationnel dans les banques, H.-P. MADERS, Les Éditions d'Organisation, 1994, épuisé.

L'Organisation de l'unité de travail, mémento ÉO, H.-P. MADERS et D. BOIX, Les Éditions d'Organisation, 1992, épuisé.

L'Efficacité du tertiaire par l'analyse de la valeur des processus, 103 fiches outils, P. LEMAÎTRE et H.-P. MADERS, Les Éditions d'Organisation, 1991, épuisé.

Améliorer l'organisation administrative, 100 fiches outils, P. LEMAÎTRE et H.-P. MADERS, Les Éditions d'Organisation, 1989, 1994, épuisé.

Copyright © 2014 Eyrolles.

Table des matières

Partie 3
L'EXERCICE DES MÉTIERS D'AUDITEUR INTERNE ET DE CONTRÔLEUR PERMANENT AU QUOTIDIEN

La faillite de l'Islande

La crise économique mondiale de 2008 a privé des dizaines de millions de personnes de leur épargne, de leur travail et de leur toit.

L'Islande, population : 320 000 habitants ; produit intérieur brut : 13 milliards de dollars ; pertes bancaires : 100 milliards de dollars. L'Islande est une démocratie stable avec un niveau de vie élevé et, hier, encore, un chômage et une dette publique extrêmement bas. « Nous avions toute l'infrastructure d'une société moderne, énergie propre, production alimentaire, pêcheries avec gestion par quota, bon système de santé, d'éducation, air pur, peu de délinquance, un bon environnement familial, on était presque estampillés "fin de l'histoire" » (Gylfi Zoega, professeur d'économie, université d'Islande). Mais, en 2000, le gouvernement lance un vaste plan de dérégulation aux conséquences désastreuses. D'abord pour l'environnement, puis pour l'économie. Il commence par laisser des multinationales comme Alcoa construire d'énormes usines d'aluminium et exploiter les ressources hydro-électriques et géothermal. « Un grand nombre de magnifiques hautes terres, dotées de couleurs spectaculaires, sont géothermiques. Alors, rien n'est sans conséquences » (Andri Magnason, écrivain et réalisateur). À la même époque, le gouvernement privatise les trois premières banques du pays : Islandsbanki, Kaupping et Glitnir. Le résultat : un des plus purs exemples de dérégulation financière. « La finance a pris les commandes et tout mis par terre » (Gylfi Zoega). En l'espace de cinq ans, ces trois banques minuscules, qui n'avaient jamais opéré à l'étranger, empruntent 120 milliards de dollars, dix fois la taille de l'économie islandaise. Les banquiers s'enrichissent entre eux et enrichissent leurs amis. « La bulle a été énorme, le prix des actions a été multiplié par 9, l'immobilier a plus que doublé » (Gylfi Zoega). Cette bulle engendre des individus comme Jon Asgeir Johannesson. Il emprunte des milliards pour acheter des boutiques de luxe à Londres, ainsi qu'un jet privé, un yacht de 40 millions de dollars et un appartement de 25 millions de dollars à Manhattan. « La presse titrait sans arrêt : tel millionnaire a acheté telle société, au Royaume-Uni, en Finlande, en France, etc., au lieu de dire : tel millionnaire a emprunté 1 milliard de dollars pour acheter telle société, et l'argent vient de votre banque » (Andri Magnason). « Ces banques ont créé des fonds monétaires et conseillé à leurs clients d'y transférer leur argent. Une pyramide de Ponzi, c'est gourmand » (Gylfi Zoega). Des cabinets d'audit américains, comme KPMG, contrôlent les banques islandaises et ne voient rien à redire. Les agences de notation américaines encensent l'Islande. « En février 2007, les agences de notation ont donné aux banques la meilleure note possible : AAA » (Sigridur Benediktsdottir, membre du comité d'investigation du Parlement Islandais). L'Islande est citée en exemple. En octobre 2007, par exemple, *Le Figaro* parle du miracle islandais : « Avec un produit intérieur brut de 40 000 euros par habitant, les Islandais jouissent, selon l'ONU, du niveau de vie le plus élevé au monde, juste après les Norvégiens. » « Le chômage est inexistant, la dette minime, et, ces dix dernières années, l'économie s'est accrue de 4,5 % par an en moyenne. » Le Premier ministre de l'époque, M. Geir Haarde, affirme alors : « Notre plus grande fierté, c'est d'avoir amélioré le niveau de vie général de la population. Depuis 1994, le revenu disponible moyen des ménages, après impôts, a augmenté de 75 % ! » « On a même vu nos gouvernants voyager avec les banquiers, pour faire de la com » (Gylfi Zoega). Lors de ses consultations au titre de l'article IV, le FMI note la taille « colossale » du secteur bancaire, « mais sans que cela soit mis en évidence comme facteur important de vulnérabilité à traiter d'urgence ». Bien au contraire, les rapports du FMI restent très optimistes : « Les perspectives à moyen terme de l'Islande restent enviables. Des marchés ouverts et souples, des institutions saines… ont permis à l'Islande de tirer parti des possibilités offertes par la mondialisation. »

Quand les banques islandaises s'effondrent, fin 2008, le chômage triple en 6 mois. « Pas un islandais n'en sort indemne, beaucoup ont perdu leur épargne. L'Autorité de régulation, censée protéger les citoyens, n'a rien fait. » « Prenez deux avocats de l'Autorité qui allaient dans une banque, évoquer un problème donné. En arrivant, ils voyaient 19 4 × 4 garés devant la banque. Ils entraient et avaient dix-neuf avocats face à eux, fins prêts à démonter tout argument. Et s'ils étaient bons, on leur proposait un boulot » (Gylfi Zoega). Un tiers des membres de l'Autorité de régulation sont débauchés par les banques…

Source : film *Inside Job*.

Introduction

Posséder un empire nécessite de confier certaines provinces à des gouverneurs. Mais ces responsables seront-ils à la hauteur ? L'empereur Charlemagne y a pensé et a trouvé une solution : le contrôleur permanent ! Eh oui les *missi dominici*, littéralement « les envoyés du maître », contrôlent les gouverneurs dans les provinces pour le compte de Charlemagne dès 789 avant même qu'il ne devienne empereur. Ils seront confirmés dans leur mission en 802 après son couronnement. La pratique professionnelle contemporaine de l'audit interne est née en 1941 date de fondation de l'Institut international des auditeurs (IIA), qui, depuis cette date, a beaucoup œuvré pour la reconnaissance du statut professionnel de l'auditeur interne par la recherche et le développement d'un programme commun de connaissances, la mise en place de programmes continus de certification professionnelle, l'adoption des standards pour la pratique professionnelle de l'audit interne (normes) et l'établissement d'un code d'éthique de la profession.

Le métier d'auditeur interne est donc une profession normée.

Son développement est lié à la croissance rapide depuis l'après-guerre des grandes organisations du secteur public et privé, comportant, de par leur taille, des problèmes organisationnels de contrôle et de supervision par leurs dirigeants. C'est pour répondre à ce besoin que les évaluations internes et indépendantes se sont développées, visant ainsi à aider les dirigeants à atteindre les objectifs de façon efficace et efficiente et également de protéger les actifs de l'organisation. Avant les années 1950, l'audit interne classique s'est d'abord focalisé sur la fiabilité comptable et la performance financière. Puis, petit à petit, son champ s'est graduellement étendu à des aspects plus opérationnels de l'organisation, l'objectif devenant l'assistance de tous les membres du management dans l'exercice de leur fonction par la fourniture d'analyses, d'évaluations et de recommandations concernant les domaines audités.

Tout métier repose sur un petit nombre de fondamentaux communs à tous ceux qui l'exercent. Il en est ainsi des métiers du contrôle, que sont les métiers d'« auditeur interne » et de « contrôleur permanent ». Ces deux métiers, proches et complémentaires, reposent sur des bases communes, à savoir des personnes possédant non seulement une bonne connaissance des métiers qu'elles contrôlent et des outils et techniques utilisées par la profession, mais également d'indispensables qualités humaines.

Les fondamentaux d'un métier se transmettent traditionnellement par le compagnonnage, entre un maître et un disciple. C'est le cas de ces deux métiers dans lesquels les collaborateurs sont supervisés tout au long de leur carrière (par un supérieur hiérarchique puis par un pair) et passent des grades à l'instar d'autres métiers, grades indépendants de leur ancienneté mais correspondant plutôt à des niveaux de maturité, de compétence et d'expérience démontrés.

Les fondamentaux d'un métier se transmettent également par des ouvrages et des articles de référence, rédigés par des hommes de l'art. C'est ainsi que notre compréhension du métier de l'audit interne et du contrôle permanent repose sur un article paru en 1973 : « Les 10 commandements de l'inspecteur moderne », écrit par Lawrence B. Sawyer, qui, à l'époque, était directeur de l'audit interne dans une grande compagnie de construction aéronautique américaine. C'est pour cette raison que nous ne résistons pas au plaisir de faire figurer cet article dans notre ouvrage, découpé en une dizaine de morceaux, venant tel un refrain rythmer nos propos. C'est pour cette raison que nous souhaitons également dédier cet ouvrage à ce grand professionnel de l'audit qui, avant beaucoup d'autres, avait déjà tout compris de ce métier.

Nous tenons également à remercier les nombreuses personnes auprès desquelles s'est forgée notre expérience, et plus particulièrement et très chaleureusement Louis Pilard, qui nous a permis de faire nos premières armes au milieu des années 1980, à l'époque où il dirigeait de main de maître la Caisse de Crédit agricole mutuel d'Indre-et-Loire, cette « *belle endormie* » comme il l'appelait alors avec affection (voir témoignage, p. XIV).

Cet ouvrage s'adresse à toute personne souhaitant mieux connaître les métiers d'auditeur interne et de contrôleur permanent, le mot « contrôle » devant être compris dans son acceptation américaine : *to control*, à savoir « maîtriser ». Car il ne s'agit pas pour ces deux métiers complémentaires de réaliser des contrôles pour le seul plaisir de faire montre d'autorité et de sanctionner des fautes fondées sur des jugements de valeur, mais bien de mettre en œuvre les dispositifs permettant à une entreprise d'identifier et de mettre sous contrôle les risques qui pourraient, s'ils se produisaient, contrarier la réalisation de ses objectifs.

L'ouvrage se présente sous la forme suivante :

La première partie présente les métiers d'auditeur interne et de contrôleur permanent. Vous y trouverez une description de leur rôle dans le dispositif de maîtrise des risques (DMR) et, plus précisément, les objectifs de la gestion des risques, la description et les principales composantes d'un DMR. Vous y trouverez également les principaux outils informatiques utilisés par les deux métiers. Y figure aussi le panorama des risques à mettre sous contrôle par l'audit interne et le contrôle permanent, à savoir les risques généraux d'une entreprise, des exemples de risques spécifiques de certains secteurs

d'activité, certains domaines telles les ressources humaines ainsi que dans la pratique sportive. Vous y trouverez enfin les informations relatives à la formation, la rémunération et le parcours de carrière de l'auditeur interne et du contrôleur permanent.

La deuxième partie présente l'environnement des métiers d'auditeur interne et de contrôleur permanent. Vous y trouverez une description de leur positionnement possible dans l'organigramme, la description des différents grades des deux métiers et les fonctions avec lesquelles ils entretiennent des relations privilégiées au sein de l'entreprise. Vous y trouverez également les textes encadrant ces deux métiers. Vous y trouverez enfin les types de compétences que les auditeurs internes et contrôleurs permanents doivent posséder ou développer et les critères d'évaluation de la performance des deux métiers.

La troisième partie présente l'activité des deux métiers au quotidien. Vous y trouverez la description des travaux à réaliser dans le cadre du cycle annuel de l'audit interne et du contrôle permanent ainsi que les outils communs aux deux métiers. Vous y trouverez également la démarche de conduite d'une mission d'audit interne ainsi que les outils spécifiques correspondants.

Des témoignages de personnes occupant des postes de haute responsabilité, pratiquant le métier d'auditeur interne ou de contrôleur permanent au quotidien ou concernées par des métiers à risques, ont été recueillis pour illustrer l'importance de ces métiers dans différentes organisations.

Nous vous donnerons aussi plusieurs exemples de situations caractéristiques dans lesquelles un groupe de personnes, voire une seule personne, de par une déréglementation irresponsable permettant la création de produits financiers tellement complexes que peu de personnes les maîtrisent, une supervision absente et/ou bienveillante, un contexte économique compliqué et variable et un comportement sans aucune déontologie ont entraîné une entreprise, voire un pays même, dans une situation catastrophique, avec les conséquences économiques et sociales que l'on sait.

Trois questionnaires vous permettant de tester vos connaissances sur les métiers d'auditeur interne et contrôleur permanent vous sont proposés à la fin de chaque partie.

Un lexique présentant les mots utilisés par les deux métiers vous est présenté en fin d'ouvrage.

TÉMOIGNAGE

Louis Pilard, ancien directeur général de la Caisse de Crédit agricole mutuel d'Indre-et-Loire

Pour le banquier opérationnel, le contrôle est souvent ressenti comme une contrainte, un obstacle à l'action commerciale. L'audit, par essence, met en évidence les dysfonctionnements, les carences, les défaillances et parfois les « malversations ». Il entraîne dans son acception traditionnelle un jugement souvent assorti d'une connotation moralisatrice. Ainsi, trop souvent, le rapport d'audit reste-t-il sous exploité, parce que non intégré dans le management de l'activité.

Pourtant, toute activité induit un risque. Le risque est dans l'action, comme dans l'inaction. Et toute décision est risque. Toute non décision aussi. L'essentiel réside dans notre aptitude à mesurer le risque lié à nos décisions. Le métier de banquier est, en effet, indissociable du risque. Ne pas prendre de risque, quelle qu'en soit la nature, c'est renoncer à être banquier. Tout l'art consiste à analyser le risque, à le prendre sans mettre en péril l'entreprise, et à l'assumer en toute connaissance de cause : c'est cela, maîtriser le risque. Car notre finalité de banquier, c'est assurer le développement de notre activité, de façon rentable, en offrant un service de qualité, et d'entretenir dans le public une image attractive.

Maîtriser le risque, c'est d'abord l'affaire de chaque opérateur, de chaque agent commercial ou technique. C'est au moment où l'opération se traite que le risque doit être mesuré. En tout état de cause, l'audit n'intervient qu'après. S'il n'est pas responsable de la qualité de l'acte, il doit s'assurer que celui-ci se situe dans une zone de risque supportable par l'entreprise bancaire. L'audit ne devrait que confirmer une chose : l'opérateur a agi en professionnel, avec justesse et précision.

Mais chacun sait que la réalité est différente : l'audit détecte des anomalies, des carences. Les opérateurs, les hommes de terrain en redoutent les effets, car nous sommes habitués à nous culpabiliser devant ces défaillances, parce que l'amour propre est atteint, parce que la sanction peut tomber. Or l'anomalie et la défaillance sont source d'enseignement. La fonction contrôle, en les analysant, nous éclaire sur les risques liés au non respect des procédures, sur les conséquences des risques mal maîtrisés. L'audit n'a pas pour fonction de faire peur : maîtriser le risque, ce n'est pas éviter tout risque. C'est l'apprécier avec justesse, c'est intervenir à l'instant précis.

PARTIE 1

PRÉSENTATION DES MÉTIERS D'AUDITEUR INTERNE ET DE CONTRÔLEUR PERMANENT

La ruine de la Barings

Nick Leeson a causé, du fait de ses manipulations boursières, la ruine de la plus prestigieuse banque britannique, la Barings (elle avait même comme client la famille royale d'Angleterre). Employé par la Barings après avoir travaillé avec succès sur différentes missions en Asie en tant qu'agent de banque, il est promu responsable en chef du marché émergent des dérivés à la bourse de Singapour. En tant que tel, il est chargé d'organiser l'ensemble du traitement des transactions des clients de la banque, avec la responsabilité d'assurer lui-même le *back-office* et les transactions sur le marché. Pour le compte de la Barings et des clients de celle-ci, Nick Leeson achète et vend des contrats à terme sur l'indice boursier Nikkei 225, regroupant les 225 plus grandes entreprises japonaises, mais en opérant sur le marché à terme de Singapour où est côté le contrat Nikkeï. La presse britannique a révélé que les supérieurs hiérarchiques de Leeson avaient touché en 1994 des bonus très élevés. L'année 1994 avait vu la banque réaliser une activité très importante sur les marchés des options sur ce même indice Nikkeï. Conforté dans sa propre maîtrise et ayant gagné la confiance de ses chefs, Leeson pariait sur une baisse de la volatilité de l'indice (que l'indice reste stable à la hausse comme à la baisse) qui était alors déjà relativement élevée. Il lance alors l'opération qui fut fatale à Leeson et à la Barings : la vente d'un *straddle*, c'est-à-dire la vente simultanée d'une option d'achat (*call*) et d'une option de vente (*put*) sur l'indice Nikkei. Or la vente de *straddle*, ainsi que la vente d'options en général, a ceci de particulier qu'elle permet des gains limités mais peut engendrer des pertes en théorie illimitées. Elle permet de gagner de l'argent si le prix du sous-jacent (ici le Nikkei) reste plus ou moins stable à la hausse comme à la baisse. Dans ce cas précis, le principal risque était que les marchés s'effondrent brutalement ou présentent une hausse importante. Ainsi, en 1995, il parie sur la hausse des marchés boursiers japonais et achète des dérivés à fort effet de levier, mais le 17 janvier 1995 survient le tremblement de terre de Kobe qui cause la baisse brutale des marchés. Libre de ses mouvements et sans réel contrôle, Nick Leeson va alors commencer à spéculer secrètement avec les fonds des clients pour rattraper les erreurs commises et tenter de compenser les désastreuses performances financières de son agence. Pour des raisons toujours inconnues de toute la Barings, Leeson a acheté pour près de 20 milliards de dollars de contrats à terme sur le Nikkeï, en fait pour tenter de soutenir le marché. L'achat de ces contrats impose à la banque de verser des appels de marge au marché de Singapour. Le quotidien financier japonais *Nikkeï* a révélé que la banque a même été contrainte de lancer des emprunts inhabituels pour payer ces appels de marge. Aucun de ces faits exceptionnels n'a éveillé la méfiance de la hiérarchie de Leeson. L'entreprise sans contrôle doit cependant faire un jour face à ses engagements. C'est ce qui arriva et coûta très cher à la banque et son opérateur.

Source : http://fr.wikipedia.org/wiki/Nick_Leeson
(texte sous Licence Creative Commons CC BY-SA 3.0).

Il est à noter que c'est à peu de choses près, même si les instruments utilisés étaient différents, ce qui arriva à la Caisse d'épargne en octobre 2008 lorsque l'un de ses traders paria sur une baisse de la volatilité, autrement dit un retour à la normale des marchés financiers…

INTRODUCTION

La première partie présente les métiers d'auditeur interne et de contrôleur permanent. Pour développer ce thème, nous nous sommes appuyés tout d'abord sur le référentiel COSO (Committee of Sponsoring Organizations of the Treadway Commission). Nous avons ensuite synthétisé le fruit de notre expérience en dispositifs de contrôle interne acquise dans le cadre de nos missions de conseil dans différents secteurs d'activité, dont les compagnies de transport aériennes, le milieu de la santé et le milieu sportif, ainsi que de l'exercice de la responsabilité des fonctions de directeur de l'audit interne et de directeur du contrôle interne au sein de plusieurs banques. Nous avons également eu recours à l'enquête CBOK et au site de l'APEC pour synthétiser les tendances du marché sur ces deux fonctions. Nous présentons enfin les formations dispensées par l'Institut de l'audit et du contrôle internes (IFACI) et le Conservatoire national des arts et métiers (CNAM).

Les actionnaires, dirigeants et autorités attendent des auditeurs internes et des contrôleurs permanents qu'ils contribuent à une bonne maîtrise des risques au sein des sociétés qui les emploient. Ils constituent ainsi la cheville ouvrière du dispositif de maîtrise des risques (DMR). Dans cette première partie, vous trouverez une description de leur rôle dans le dispositif et, plus précisément, les objectifs de la gestion des risques, la description et les principales composantes d'un dispositif de maîtrise des risques, à savoir :

- la déontologie ;
- la charte du contrôle interne ;
- l'organisation du dispositif de maîtrise des risques ;
- la cartographie des risques ;
- le corpus documentaire ;
- les plans de contrôle ;
- la veille réglementaire ;
- la déclaration des incidents ;
- le suivi des plans d'action ;
- les indicateurs d'activité et de risques ;

- le reporting ;
- le plan de continuité d'activité ;
- le contrôle des prestations essentielles externalisées ;
- le contrôle des filiales ;
- la gestion de crise.

Vous trouverez également les principaux outils informatiques utilisés par les deux métiers.

Vous y trouverez en outre le panorama des risques à mettre sous contrôle par l'audit interne et le contrôle permanent, à savoir les risques généraux d'une entreprise, des exemples de risques spécifiques de certains secteurs d'activité, tels le secteur bancaire, le secteur du transport aérien ou encore le secteur hospitalier, certains domaines telles les ressources humaines ainsi que la pratique sportive.

Vous y trouverez également les informations relatives à la formation, la rémunération et le parcours de carrière de l'auditeur interne et du contrôleur permanent.

Vous y trouverez aussi trois témoignages illustrant nos propos :

- celui de Philippe Vannier, qui évoque la sérénité et la création de valeur ajoutée apportées par l'audit chez Bull, ainsi que son rôle de vivier ;
- celui de Françoise Chassard, qui attire notre attention sur l'importance de la fonction de contrôle interne pour une institution comme la Caisse des dépôts pour concilier les missions de l'entreprise et maîtriser ses risques ;
- celui de Sandrine Murbach, qui décrit l'importance, quand on pratique un sport à risques tel que l'apnée, de bien se connaître et de disposer d'un dispositif de contrôle performant. Sans ce dispositif, la performance n'est pas possible.

Vous y trouverez également les premier et deuxième commandements de Lawrence B. Sawyer : « connaître les objectifs » et « connaître les contrôles ».

Un questionnaire en fin de partie vous permettra de tester vos connaissances.

CHAPITRE 1

Leur rôle dans le dispositif de maîtrise des risques

CE CHAPITRE VOUS PERMETTRA DE :

- connaître l'intérêt de la gestion des risques au sein d'une organisation ;
- connaître les différentes composantes d'un dispositif de maîtrise des risques ;
- connaître les outils utilisés dans le cadre de la gestion des risques.

Selon la définition du référentiel COSO (Committee of Sponsoring Organizations of the Treadway Commission), le management des risques est « un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'entreprise. 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 événements 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 ». Dès lors, avec un processus de management des risques performant, l'impact et la fréquence de la survenance d'un risque peuvent être diminués.

C'est le rôle des *risk managers* qui doivent, pour remplir leur mission d'assurance de l'atteinte des objectifs d'une organisation, aider à la mise en place des bonnes décisions face aux risques. Ils s'appuient pour cela sur les quatre stratégies fondamentales du management des risques :

- la réduction des impacts ou de la probabilité d'apparition ;
- l'acceptation, dans le cas où la mise en œuvre du dispositif de contrôle est plus coûteuse que la survenance du risque ;
- l'évitement, comme la suppression de l'activité dans lequel se situe le risque ;
- le transfert du risque sur un tiers par une assurance appropriée.

1. LES OBJECTIFS DE LA GESTION DES RISQUES

Pour une entreprise, la gestion de ses risques internes et externes est un levier de management qui contribue à :

- Créer et préserver la valeur, les actifs et la réputation : la gestion des risques permet d'identifier et d'analyser les principales menaces et opportunités potentielles. Elle vise à anticiper les risques au lieu de les subir et, ainsi, à préserver la valeur, les actifs et la réputation.
- Sécuriser la prise de décision et les processus pour favoriser l'atteinte des objectifs : la gestion des risques vise à identifier les principaux événements et situations susceptibles d'affecter de manière significative la réalisation des objectifs. La maîtrise de ses risques permet ainsi de favoriser l'atteinte desdits objectifs. La gestion des risques est intégrée aux processus décisionnels et opérationnels. Elle est l'un des outils de pilotage et d'aide à la décision. La gestion des risques permet de donner aux dirigeants une vision objective et globale des menaces et des opportunités potentielles, de prendre des risques mesurés et réfléchis et d'appuyer ainsi leurs décisions quant à l'attribution des ressources humaines et financières.
- Favoriser la cohérence des actions avec les valeurs fondatrices : de nombreux risques sont le reflet d'un manque de cohérence entre les valeurs de la société et les décisions et actions quotidiennes. Ces risques affectent principalement la crédibilité.
- Mobiliser les collaborateurs autour d'une vision commune des principaux risques et les sensibiliser aux risques inhérents à leur activité.

2. LE DISPOSITIF DE MAÎTRISE DES RISQUES

Il appartient à chaque entreprise de mettre en place un dispositif de gestion des risques adapté à ses caractéristiques propres.

Le dispositif de gestion des risques prévoit tout d'abord un cadre organisationnel comprenant :

- une organisation qui définit les rôles et responsabilités des acteurs, établit les procédures et les normes claires et cohérentes du dispositif ;
- une politique de gestion des risques qui formalise les objectifs du dispositif en cohérence avec la culture de la société, le langage commun utilisé, la démarche d'identification, d'analyse et de traitement des risques, et le cas échéant, les limites que la société détermine (tolérance pour le risque) ;
- un système d'information qui permet la diffusion en interne d'informations relatives aux risques.

Le dispositif doit également prévoir un processus de gestion des risques comprenant, au sein de son contexte interne et externe à l'entreprise, trois étapes :

1. L'identification des risques : cette étape permet de recenser et de centraliser les principaux risques menaçant l'atteinte des objectifs. Un risque représente une menace ou une opportunité manquée. Il se caractérise par un événement de risque, une ou plusieurs sources et une ou plusieurs conséquences. L'identification de chaque risque s'inscrit dans une démarche continue.
2. L'analyse des risques : cette étape consiste à examiner les conséquences potentielles des principaux risques (conséquences qui peuvent être notamment financières, humaines, juridiques, ou de réputation) et à apprécier leur possible occurrence. Cette démarche est elle aussi continue.
3. Le traitement des risques : cette étape permet de choisir les actions à conduire, les actions les plus adaptées. Pour maintenir les risques dans des limites acceptables, plusieurs mesures peuvent être envisagées : la réduction, le transfert, la suppression ou l'acceptation d'un risque. Le choix de traitement s'effectue notamment en arbitrant entre les opportunités à saisir et le coût des mesures de traitement du risque, prenant en compte leurs effets possibles sur l'occurrence et/ou les conséquences du risque.

Le dispositif de gestion des risques nécessite un pilotage en continu :

- Il doit faire l'objet d'une surveillance et d'une revue régulière, son suivi permettant l'amélioration continue du dispositif.
- L'objectif est d'identifier et d'analyser les principaux risques, et d'en tirer des enseignements.

Année après année, grâce à une volonté forte de la direction générale de l'entreprise, le dispositif de maîtrise des risques va prendre de l'épaisseur, les pratiques vont rentrer dans les habitudes de management de la hiérarchie et de comportement des collaborateurs.

Chaque année, une évaluation du niveau de maturité du dispositif permettra de faire le point et de décider des orientations futures.

Tableau 1.1 – Les degrés de maturité possibles des différents composants d'un dispositif de maîtrise des risques

Grille de cotation des composants	Maturité du composant				
	Élevée	Suffisante	Perfectible	Faible	Inacceptable
Efficacité du composant	Robuste	Acceptable	Montre des faiblesses	Montre des déficiences	Montre de sérieuses déficiences
Impact du niveau de maturité du composant sur l'assurance d'atteindre les objectifs SORC	Concourt grandement à l'assurance d'atteinte des objectifs	Concourt à l'assurance d'atteinte des objectifs	Peut éventuellement dégrader modérément l'assurance d'atteinte des objectifs	A de fortes chances de dégrader sensiblement l'assurance d'atteinte des objectifs	Dégrade de façon quasi certaine et significativement l'assurance d'atteinte des objectifs
Attention à apporter au composant par les fonctions de contrôle et les métiers	Inutile	Utile	Souhaitable	Nécessaire	Impératif

L'analyse du niveau de maturité de chaque composant consiste à :

- évaluer l'efficacité du composant au regard des bonnes pratiques professionnelles, des obligations réglementaires, de l'organisation de l'entreprise, de l'appétence de l'entreprise pour le risque, de l'analyse des relations entre les différents composants (générant un fonctionnement efficace ou a contrario fastidieux) et de la compréhension du niveau de culture du risque de l'entreprise (se traduisant au quotidien en matière de management, de communication, d'animation…) ;
- apprécier l'impact sur l'assurance d'atteindre les objectifs stratégiques ;
- en déduire un niveau d'attention à apporter par les fonctions de contrôle et les métiers.

3. LES COMPOSANTES DU DISPOSITIF DE MAÎTRISE DES RISQUES

Un dispositif de maîtrise des risques (DMR) est composé d'une quinzaine de composants interconnectés entre eux. Ces relations entre les composants du système donnent ainsi à celui-ci des propriétés supplémentaires.

La performance d'un DMR est le résultat de :

- l'existence de ces composants ;

- le degré de maturité de chacun des composants ;
- le degré de connexion entre les composants, faisant d'un ensemble de composants indépendants un système.

L'auditeur interne et le contrôleur permanent interviennent dans la conception et le déploiement des différents composants au sein de l'entreprise. Ils sont également en charge de certains d'entre eux au quotidien. Ils interviennent également dans le cas du déploiement d'un progiciel de contrôle interne permettant de relier les composants entre eux et d'utiliser des informations communes (référentiels de processus, cartographie des risques…). Ils en sont ensuite utilisateurs et parfois même administrateur.

Nous présentons plus loin dans ce chapitre les principaux progiciels du marché et leurs fonctionnalités.

3.1. La déontologie et l'appétence au risque

La déontologie peut se définir comme un ensemble de droits et devoirs régissant une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public. La plupart des métiers possède une déontologie, portant *a minima* sur le respect de l'engagement donné, de la qualité annoncée, du client. Certains métiers possèdent, en plus, des règles déontologiques spécifiques. C'est le cas des métiers de médecin, avocat, prêtre ou encore banquier, pour lesquels le secret est une condition à respecter. Ne pas respecter un minimum de règles déontologiques, telles le « service fait », c'est tout simplement s'exposer à perdre la confiance de ses clients. La déontologie d'une entreprise renvoie également aux valeurs de ses dirigeants et correspond à la façon dont les choses doivent, selon eux, se passer dans l'entreprise. Elle renvoie enfin à l'environnement culturel dans lequel évolue l'entreprise.

À ce titre, la déontologie présente des différences fortes si l'on pense au droit sur les brevets et la propriété industrielle que certains pays ne reconnaissent pas… La déontologie est le plus souvent implicite, non formalisée et il faut aller la décoder en analysant comment l'entreprise fonctionne au quotidien. Dans les entreprises où celle-ci est primordiale, elle est explicitée dans un ou plusieurs documents bien précis faisant référence, le plus souvent la « charte » et le « code de déontologie ».

La charte tout d'abord constitue le document le plus général et le code de déontologie présente la façon dont l'activité doit se réaliser, ce qu'il est permis de faire, et ce qui ne l'est pas. À ce titre, il témoigne du degré d'appétence au risque du conseil d'administration de l'entreprise. Ce document présente également le dispositif général de surveillance du respect de la déontologie. Dans une banque, ce document précise le type d'opération qu'il n'est pas possible de proposer aux clients telles les opérations de blanchiment des capitaux et de financement du terrorisme. Ce document précise également les conditions de réalisation de certaines opérations, telles celles ayant des impacts sur la valeur du titre d'une entreprise cliente et qui nécessitent la mise en place d'une « muraille de Chine » entre les équipes concernées par l'opération (fusion, acquisition, émission de titres…) et le reste des collaborateurs de la banque.

La charte et le code de déontologie sont le plus souvent rédigés par le directeur du risque, le directeur de l'audit ou le directeur du contrôle permanent, puis validé par la direction générale de l'entreprise, et souvent également par le comité d'audit, composé d'administrateurs de l'entreprise. En effet, la fixation d'orientations aussi essentielles relève naturellement de la gouvernance (les représentants des actionnaires/propriétaires) mais constitue une tâche assez technique et s'accommode bien d'une préparation par les experts.

Code de déontologie d'une banque de gestion de fortune

Le code de déontologie a pour but de définir les attentes de l'établissement bancaire afin de préserver sa réputation, de même que celle de ses filiales tant dans son pays qu'à l'étranger, en établissant des règles de conduite en matière de confidentialité, de conflit d'intérêts et d'éthique professionnelle.

Pour atteindre ce but et afin de conserver la confiance du public et maintenir la qualité du climat de travail, certains principes fondamentaux peuvent guider la conduite des collaborateurs et doivent être respectés dans les activités quotidiennes :

- Agir avec honnêteté et intégrité.
- Se conformer aux lois.
- Traiter les autres avec respect.
- Protéger la confidentialité des renseignements.
- Éviter les conflits d'intérêts.
- Respecter l'organisation.

Le code de conduite présente donc « comment les collaborateurs doivent se comporter au quotidien ».

Code du soldat de l'armée de terre

- Au service de la France, le soldat lui est entièrement dévoué, en tout temps et en tout lieu.
- Il accomplit sa mission, avec la volonté de gagner et de vaincre et si nécessaire au péril de sa vie.
- Maître de sa force, il respecte l'adversaire et veille à épargner les populations.
- Il obéit aux ordres, dans le respect des lois et des conventions internationales.
- Il fait preuve d'initiative et s'adapte en toutes circonstances.
- Soldat professionnel, il entretient ses capacités intellectuelles et physiques et développe sa compétence et sa force morale.
- Membre d'une équipe solidaire et fraternelle, il agit avec honneur, franchise et loyauté.
- Attentif aux autres et déterminé à surmonter les difficultés, il œuvre pour la cohésion et le dynamisme de son unité.
- Il est ouvert sur le monde et la société et en respecte les différences.
- Il s'exprime avec réserve pour ne pas porter atteinte à la neutralité des armées en matière philosophique, politique et religieuse.
- Fier de son engagement, il est toujours partout un ambassadeur de son régiment, de l'Armée de Terre et de la France.

La déontologie se retrouve également dans la convention collective, en ce sens que celle-ci précise notamment les droits et devoirs des employeurs et des salariés, et dans le règlement intérieur, dont les articles sont la traduction opérationnelle de la convention collective. Le règlement intérieur contiendra les dispositions opposables aux employés notamment le dispositif de sanction jugé nécessaire en cas de non-respect des règles d'éthique énoncées.

4. LA CHARTE DU DISPOSITIF DE CONTRÔLE INTERNE

La logique générale du dispositif de contrôle interne est décrite dans un document de référence, la charte du dispositif de contrôle interne. Ce document est rédigé par le responsable du contrôle interne de l'entreprise, qui peut être le directeur de l'audit interne, le directeur du risque ou encore le directeur du contrôle permanent. Ce document est ensuite validé par la direction générale. Il constitue l'une des composantes essentielles du dispositif général. En effet, il explique comment le dispositif fonctionne.

Les politiques sectorielles constituent les décrets d'application de la charte dans les différentes activités.

EN PRATIQUE

Critères de maturité d'une charte du dispositif de contrôle interne

Périmètre	Elle décrit les principes généraux du dispositif de contrôle interne s'appliquant à l'ensemble de l'entreprise. Elle décrit les composantes du dispositif de contrôle interne : ■ couverture exhaustive des activités et des risques ; ■ responsabilité de l'ensemble des acteurs ; ■ définition claire des tâches ; ■ séparation effective des fonctions d'engagement et de contrôle ; ■ délégations formalisées et à jour ; ■ formalisation des normes et procédures, notamment comptables et de traitement de l'information ; ■ systèmes de mesure des risques et des résultats ; ■ systèmes de surveillance et de maîtrise des risques ; ■ systèmes de contrôle, comprenant des contrôles permanents réalisés par les unités opérationnelles ou par des collaborateurs dédiés (1er et 2e niveaux) et des contrôles périodiques (3e niveau : audit interne et groupe, autorités de tutelle).
Mise à jour	Respect du délai d'application des nouvelles dispositions légales et réglementaires. Les modalités de mise en application sont appropriées.
Organisation	Dispositif cohérent et efficace : toutes les composantes sont connectées, les composantes ne se recouvrent pas. Le dispositif respecte les principes énoncés dans la charte.
Pilotage	Le dispositif fonctionne quotidiennement. Le dispositif permet à la gouvernance de prendre des décisions éclairées.
Connaissance du dispositif par les personnels	Ils connaissent la charte et le dispositif de contrôle interne, y compris les personnels entrants. Des formations et informations sont régulièrement réalisées auprès du personnel de l'entreprise.

5. L'ORGANISATION DU DISPOSITIF DE MAÎTRISE DES RISQUES

Le dispositif de maîtrise des risques (DMR) mobilise plusieurs catégories d'acteurs classées en trois lignes de maîtrise.

La direction générale d'une entreprise, en tant que garant de la pérennité de l'entreprise, se doit d'être au cœur du dispositif de maîtrise globale des risques. Afin d'optimiser le dispositif de maîtrise des activités, un nouveau modèle de gestion globale des risques est apparu : les « trois lignes de maîtrise » (*The Three Lines of Defense in Effective Risk Management and Control*, Institute of Internal Auditors, 2013). Ce modèle permet de clarifier le rôle et les responsabilités de chacun (voir figure 1.1, p. 15). Il s'articule autour de trois pôles de maîtrise des risques.

5.1. Première ligne de maîtrise : les métiers

La première ligne de maîtrise des activités est constituée par les managers opérationnels, responsables de l'évaluation et de la diminution des risques dans les processus dont ils ont la charge. Ces actions se composent :

- des contrôles opérationnels réalisés au fil de l'eau par les collaborateurs dans le cadre du traitement des opérations ainsi que des multiples décisions métier prises par la hiérarchie et des comités spécialisés ;
- des contrôles dits « de premier niveaux » composés de tests réalisés par les responsables hiérarchiques sur les travaux exécutés par leurs collaborateurs.

À ce titre, un métier ne peut pas être en charge de contrôles de deuxième niveau car il serait dans ce cas juge et partie.

5.2. Deuxième ligne de maîtrise : les contrôleurs permanents

La deuxième ligne, constituée par les services fonctionnels (ou support) de l'entreprise, a pour objectif de structurer et de coordonner le dispositif de maîtrise de l'activité de l'organisation. Ces actions comprennent :

- l'assistance aux opérationnels dans l'identification et l'évaluation des principaux risques relevant de leur domaine d'expertise ;
- l'élaboration de politiques et de procédures de groupe par domaine d'activité ;
- la contribution à la conception des contrôles les plus pertinents ;
- le développement des meilleures pratiques ;
- le compte rendu du fonctionnement effectif des processus.

À ce titre, les contrôleurs permanents de deuxième niveau ne peuvent être rattachés hiérarchiquement au métier qu'ils contrôlent. Les acteurs de la deuxième ligne de défense ne servent pas les clients, ne réalisent pas de transactions et ne comptabilisent pas d'opérations.

5.3. Troisième ligne de maîtrise : les auditeurs internes

La troisième ligne de maîtrise concerne l'évaluation globale et indépendante du dispositif de maîtrise des risques, effectuée par l'audit interne. Son rôle est de donner aux organes de gouvernance, président, conseil de surveillance selon la forme juridique de la société, l'assurance que la maîtrise des risques est efficace et efficiente.

À ce titre, le contrôle de troisième niveau est le garant ultime du dispositif. Par ses audits, il fait « ce que le président de l'entreprise ferait lui-même s'il en avait le temps et les compétences ».

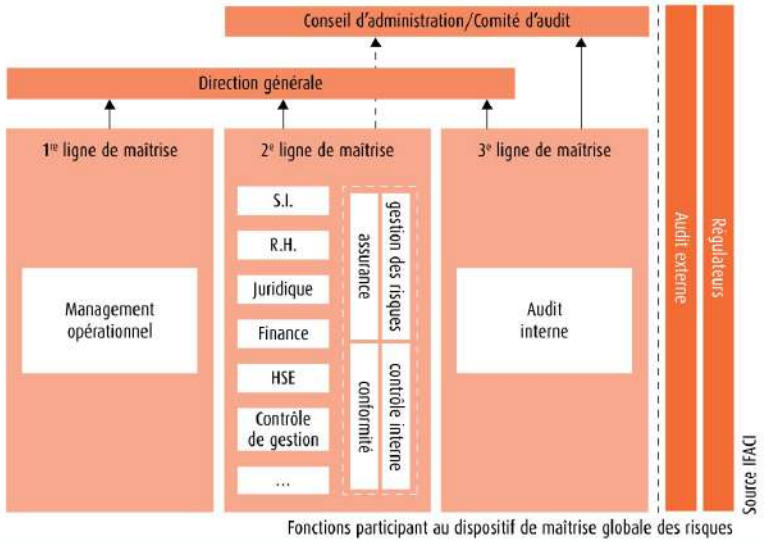
Selon certains utilisateurs, ce modèle permet d'optimiser le temps passé par le management opérationnel, d'une part, et de rendre compréhensible l'organisation pour les dirigeants et la gouvernance de l'entreprise, d'autre part. En fonction de l'activité et des caractéristiques de l'entité, plusieurs schémas sont possibles pour appliquer cette méthode.

EN PRATIQUE

Critères de maturité d'un référentiel des contrôles et des fonctions incompatibles

Périmètre couvert par le principe de séparation des fonctions incompatibles	Les activités des métiers, les fonctions de pilotage et de gouvernance et les fonctions support.
Distinction entre *front, middle* et *back office*	Il existe une dissociation claire entre les tâches de *front office* exécutées par des personnels opérationnels (ex. : instruction d'un dossier de crédit dans le secteur bancaire), celles de *middle offices* exécutées par des spécialistes métier/contrôle permanent de premier niveau réalisés par des contrôleurs permanents spécialisés ou la hiérarchie métier (ex. : analyse risques contradictoires, contrôle de la lettre d'offre avant envoi client, contrôle du contrat avant envoi client, contrôle de la configuration du versement des fonds) et celles de *back office* exécutées par des personnels opérationnels (ex. : enregistrement comptable de l'opération). La séparation des tâches incompatibles est garantie toute l'année même dans le cas d'absence des personnels affectés aux tâches de contrôle.
Inventaire des autorisations de signature	Il existe une liste des personnes autorisées à engager la responsabilité de l'entreprise (ex. : décision d'octroi d'un crédit, accord de passage d'une opération en pertes et profits, accord d'extournes client, accord de recrutement d'une personne, engagement d'une dépense…) avec indication des niveaux d'approbation requis par nature et niveau d'engagement (ex. crédit : délégation chargée d'affaires, délégation directeur des engagements, délégation comité régional d'engagement, délégation comité national d'engagement, délégation comité groupe). Cette liste est revue régulièrement et mise à jour à chaque mobilité des personnes concernées.
Connaissance par les personnels	Les personnels connaissent le principe de la séparation des fonctions incompatibles. Les personnels respectent le principe de séparation.
Connexions	Liens entre la séparation des fonctions incompatibles et le corpus de procédures et les contrôles, la cartographie des risques, le plan de contrôle de 1er niveau.

Figure 1.1 – Le modèle des trois lignes de maîtrise



Fonctions participant au dispositif de maîtrise globale des risques

Les trois lignes de maîtrise sont complétées par d'autres dispositifs organisationnels tels la séparation des fonctions incompatibles. Elles sont également complétées par des dispositifs de protection tels les droits et habilitations.

EN PRATIQUE

Critères de maturité d'un référentiel des droits et habilitations

Périmètre	Processus métier, pilotage et de gouvernance et support.
Gestion des droits et des habilitations	Existence d'une procédure de création des habilitations. Existence d'une procédure de mise à jour des habilitations. Existence de profils types et de modalités garantissant la non-attribution de droits incompatibles.
Règles concernant les profils, les comptes utilisateurs, les mots de passe	Définition adaptée de profil standard. Absence de partage de compte utilisateur. Blocage du compte utilisateur après un nombre donné de connexions. Existence d'un procédé d'authentification/identification des utilisateurs.

.../...

.../...

	Existence de fonctionnalités pour assurer l'administration des utilisateurs. Existence de standards relatifs à la gestion des mots de passe : renouvellement périodique des mots de passe, historisation des mots de passe, contrôle sur la trivialité des mots de passe (longueur, caractères spéciaux), absence de stockage des mots de passe en clair.
Administration du référentiel	Mise à jour régulière des bases habilitations. Historisation des traitements réalisés par un utilisateur. Revue des journaux applicatifs. Revue périodique des habilitations.
Outil utilisé pour le stockage des droits et habilitations	Progiciel du marché plutôt qu'un outil bureautique.
Connexions	Liens entre le référentiel des droits et habilitations et d'autres composantes du dispositif de contrôle interne : référentiel des risques, référentiel des unités et comités.
Connaissance par les personnels de la banque du référentiel des droits et habilitations	Les personnels concernés connaissent les processus inhérents à leur périmètre d'activité. Des actions de sensibilisation sur le thème des processus sont réalisées régulièrement.

6. LA CARTOGRAPHIE DES RISQUES

La cartographie est un outil de pilotage relativement simple, explicite et visuel qui permet de situer les risques, de fixer des objectifs et de contrôler leur évolution. De même, elle est un outil précieux qui n'est pas exclusivement limité à la direction de la maîtrise des risques, mais également à tous ceux qui concourent d'une manière ou d'une autre au processus de management des risques : le comité d'audit, la direction générale, les auditeurs internes et contrôleurs permanents et bien sûr les responsables des risques.

Elle repose sur une taxonomie des risques, véritable dictionnaire des risques possibles en théorie.

EN PRATIQUE

Critères de maturité d'une taxonomie des risques

Périmètre de la taxonomie (liste ordonnée) des risques	La taxonomie présente : ■ les risques opérationnels ; ■ les risques de conformité ; ■ les risques métier (ex. : secteur bancaire) : risques de crédit, de contrepartie, risques de marché, risque de continuité d'activité, risque de réputation.
Composition de la taxonomie des risques	La taxonomie définit chaque risque et présente des exemples caractéristiques correspondant à des incidents avérés à chaque fois que cela est possible.
Niveau de granularité de la taxonomie des risques	La taxonomie présente plusieurs niveaux de risque : risques génériques et risques spécifiques.
Grille de cotation des risques	La taxonomie contient des grilles de cotation des risques : probabilité d'apparition et gravité en cas de survenance.
Administration du référentiel des risques ; règles de mise à jour	Le référentiel est placé sous la responsabilité d'un administrateur. Il existe des règles de mise à jour. Le référentiel est revu annuellement ou ponctuellement à l'occasion de la création d'une nouvelle activité, de la commercialisation d'un nouveau produit ou service, de l'apparition d'un nouveau texte de loi.
Outil utilisé pour le stockage et la publication de la taxonomie des risques	Progiciel du marché plutôt qu'outil bureautique dans la mesure où tous les éléments de la gestion des risques devront y être reliés (pertes, procédures, plan d'actions de réduction des risques…).
Connexions de la composante « Référentiel des risques »	Il existe des liens entre le référentiel des risques et d'autres composantes du dispositif de contrôle interne : référentiel des processus, référentiel des unités et comités…
Connaissance par les personnels de la banque de la taxonomie des risques	Les personnels concernés connaissent la taxonomie des risques. Des actions de sensibilisation sur le thème des risques sont réalisées régulièrement.

La cartographie des risques est le plus souvent réalisée et mise à jour par les fonctions d'audit et de contrôle permanent de l'entreprise.

Les risques figurant dans la cartographie, externes ou internes à l'entreprise, ont tous un impact significatif sur la capacité de l'entreprise à réaliser ses objectifs. À ce titre, ils doivent être mis sous contrôle.

Une cartographie des risques distingue les risques bruts et les risques nets (résiduels), à savoir les risques inhérents à l'entreprise et son activité, d'une part, et les mêmes risques une fois le dispositif de maîtrise des risques en place, d'autre part. Ce DMR sera d'autant plus performant qu'il arrive à réduire les risques bruts à un risque résiduel le plus faible possible.

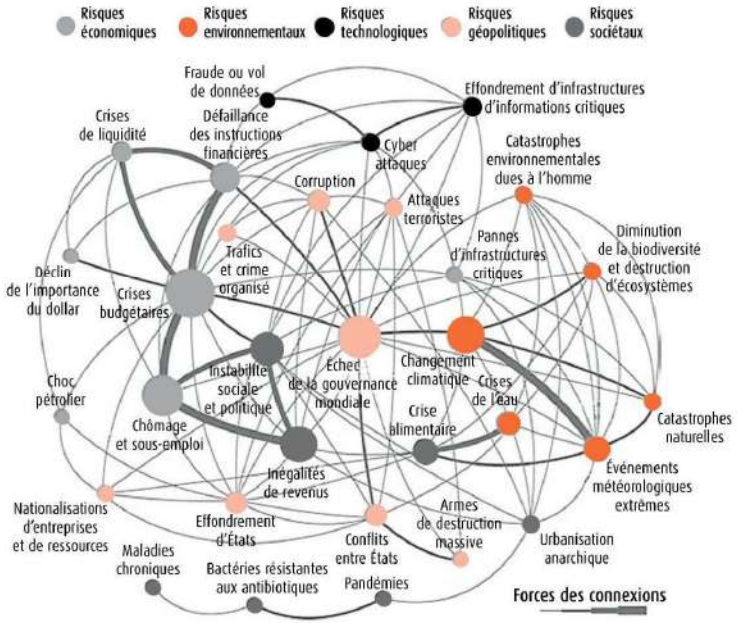
EN PRATIQUE

Critères de maturité d'un dispositif de définition/revue d'une cartographie des risques

Périmètre	Métiers et activités support. Risques opérationnels, risques de conformité, risque d'image, risque de continuité d'activité… unicité de la cartographie, utilisation effective par les organes de direction…
Cotation des risques	Utilisation de grilles de cotation définies dans la taxonomie des risques. Détermination pour chaque risque de sa sévérité brute (calculée par la fréquence d'apparition multipliée par la gravité) et de sa sévérité nette (en regard de l'efficacité du dispositif de maîtrise des risques). Partage par tous les acteurs de la même grille de cotation : métiers, gestionnaires de risques, auditeurs… Grilles cohérentes, le cas échéant, entre niveaux groupe et filiales. Logique cohérente entre la grille de cotation et les choix opérés pour exprimer « l'appétit pour le risque ».
Niveau de granularité des risques	Niveau de granularité adapté.
Administration de la cartographie	La cartographie est placée sous la responsabilité d'un administrateur et de chaque métier. Il existe des règles de mise à jour. La cartographie est revue annuellement ou ponctuellement à l'occasion de la création d'une nouvelle activité, de la commercialisation d'un nouveau produit ou d'un service, de l'apparition d'un nouveau texte de loi.
Outil utilisé pour le stockage et la publication de la cartographie des risques	Progiciel du marché plutôt qu'un outil bureautique.
Connexions	Liens entre la cartographie des risques et d'autres composantes du dispositif de contrôle interne : taxonomie des risques, référentiel des processus, déclaration des incidents avérés, référentiels des unités et des comités.
Connaissance par les personnels	Les personnels concernés connaissent les risques inhérents à leur périmètre d'activité. Des actions de sensibilisation sur le thème des risques sont réalisées régulièrement.

La cartographie des risques concerne tout d'abord les activités habituelles de l'entreprise. Cependant, il serait hasardeux de penser que les risques se limitent à celles-ci. En effet, dans le cas de conduite de projets, l'entreprise est confrontée à de nombreux risques nécessitant également identification et mise sous contrôle. C'est la raison pour laquelle les projets rentrent dans le périmètre de contrôle des fonctions d'audit interne et de contrôle permanent.

Figure 1.2 – Les principaux risques mondiaux et leurs interconnexions



Source : World Economic Forum. Droits réservés

Tout projet rencontre des risques. Ceux-ci peuvent avoir des conséquences en termes d'atteinte de l'objectif et de respect des délais et des moyens mis en œuvre. Maîtriser ces risques suppose de réaliser la cartographie des risques et des facteurs qui peuvent les engendrer. La cartographie permet au chef de projet de synthétiser sa réflexion sur les facteurs de risque du projet et de prendre les mesures préventives permettant d'éviter l'apparition de ces risques ainsi que les mesures curatives permettant d'en limiter les effets.

Nous renvoyons le lecteur qui souhaiterait approfondir le thème de la mise sous contrôle des risques spécifiques des projets à notre ouvrage : *Piloter les risques d'un projet*, Henri-Pierre Maders et Jean-Luc Masselin (Éditions d'Organisation).

Pour chacune des actions à réaliser dans le projet :

- **Identifier les risques possibles** : ce sont souvent les mêmes dans une entreprise ou dans des projets de même nature ; leur probabilité d'apparition : faible, moyenne, forte ; leur gravité sur l'atteinte des objectifs (pourcentage de non-atteinte des objectifs) et le respect des délais (nombre de jours de retard) et des moyens (nombre de jours/homme, budgets…) : faible, moyenne, forte.
- **Inventorier les actions préventives** : elles permettront de limiter la probabilité d'apparition des aléas identifiés.
- **Recenser les actions curatives** : elles permettront de réduire les effets des aléas en cas d'apparition.

Grille de qualification des risques d'un projet informatique

Critères d'évaluation de la criticité des risques du projet

- Criticité faible (1) : ne compromet pas l'atteinte des objectifs du projet en termes de coût, de délai, de qualité ou de fonctionnalités ;
- Criticité moyenne (3) : peut affecter le périmètre du projet, éventuellement nécessiter un avenant ;
- Criticité forte (6) : peut avoir comme conséquence, une perte financière, une insatisfaction du client ou l'arrêt du projet.

Figure 1.3 – Grille de qualification des risques d'un projet informatique

Probabilité forte 6	Risque à suivre 6	Risque à traiter 18	Risque à traiter 36
Probabilité moyenne 3	Risque à surveiller 3	Risque à suivre 9	Risque à traiter 18
Probabilité faible 1	Risque négligeable 1	Risque à surveiller 3	Risque à suivre 6
	Criticité faible 1	Criticité moyenne 3	Criticité forte 6

Critères d'évaluation de la probabilité des risques du projet

- Probabilité faible (1) : il est peu probable que le risque devienne réalité.
- Probabilité moyenne (3) : il existe des signes indiquant que le risque peut devenir réalité.
- Probabilité forte (6) : le risque est certain ou en passe de devenir réalité.

7. LE CORPUS DOCUMENTAIRE

Il est constitué de l'ensemble des procédures et modes opératoires permettant aux collaborateurs de traiter les opérations d'une façon homogène et d'appliquer les mêmes règles de gestion aux mêmes situations. Ainsi, plus l'entreprise est vaste, avec de nombreux employés, des activités variées, des localisations multiples, plus il apparaît clairement utile de déterminer le qui fait quoi, de choisir et de faire connaître les méthodes recommandées, de coordonner et de rendre cohérentes les actions. Le texte reste aujourd'hui le point de référence le plus adapté… et il constitue une référence des plus utiles pour les contrôleurs et auditeurs qui pourront comparer les faits constatés aux comportements attendus. Pour mémoire, c'est le premier document demandé par tout intervenant ou par tout contrôleur externe : juge, enquêteur, commissaire aux comptes, tutelles, superviseurs.

Les fonctions d'audit interne et de contrôle permanent sont généralement des points de passage obligé dans la publication de toute procédure ou mode opératoire. Leur rôle ne consiste pas à rédiger ces documents, cela étant de la responsabilité des métiers, mais de s'assurer de leur qualité de fabrication sous l'angle des fondamentaux d'audit et de contrôle tels que la séparation des fonctions incompatibles, la description des contrôles opérationnels…

Bien souvent, la définition du modèle de rédaction d'une procédure est de la responsabilité des fonctions d'audit interne et/ou de contrôle permanent.

EN PRATIQUE

Critères de maturité d'un corpus documentaire

Périmètre	Les procédures couvrent tous les processus de l'entreprise : management, métier et support.
Modalités de rédaction/validation/codification/publication des procédures	Il existe une méta-procédure (la procédure des procédures). Le format et la codification des procédures sont normalisés. Leur rédaction est homogène : règles de rédaction, style, présentation. Les procédures sont validées par les métiers et le contrôle interne avant publication.
Qualité du contenu des procédures	Les procédures décrivent les rôles, les tâches et les actions à réaliser pour gérer les risques de toutes natures (les « DMR »)… y compris celui de ne pas atteindre un niveau de performance ciblé. Les procédures présentent les risques spécifiques du périmètre concerné, les règles de conformité réglementaires à respecter, les principaux cas de gestion.

.../...

.../...

	Les procédures précisent le qui fait quoi, les rôles et responsabilités et détaillent le schéma délégataire. Les procédures peuvent présenter les schémas comptables.
Mise à jour des procédures	Les procédures sont revues régulièrement et à chaque événement le justifiant (changement organisationnel, évolution réglementaire, incident témoignant d'une inadéquation de la procédure…).
Outil utilisé pour la formalisation, le stockage et la publication des procédures	Mise à disposition : progiciel de publication de type « Google ». Mise en perspectives des actions d'un département dans une chaîne de traitement de « bout en bout » – approche processus : progiciel de type MEGA, ARIS, CASEWISE. Simple documentation : applications bureautiques (Word, Excel, Access, Power Point).
Administration de la base procédures	Un acteur pour tenir les rôles et accéder aux bonnes pratiques : administrateur et correspondants par processus ou activité.
Responsabilité du contenu des procédures	Affectation des procédures à des « propriétaires » métier.
Connexions	Liens entre le corpus de procédures et les contrôles de premier et deuxième niveaux, la cartographie des risques, le référentiel des processus…
Connaissance des procédures par les personnels	Les procédures donnent lieu à des formations régulières. Les procédures sont enrichies des nouveaux cas de gestion dans le cadre d'ateliers d'échanges. Les personnels sont informés des mises à jour concernant les procédures.

8. LES PLANS DE CONTRÔLE

Les plans de contrôle listent les contrôles qui seront réalisés dans l'année à venir par les trois niveaux de maîtrise. Ces plans de contrôle sont définis en fonction des risques et des sinistres survenus lors du dernier exercice. Ils doivent également tenir compte des nouveaux produits et services, ainsi que des modifications des processus de traitement de l'entreprise.

8.1. Contrôles de premier niveau

« Le contrôle interne est l'affaire de tous » est une devise couramment entendue. Elle témoigne du fait que chacun y apporte son concours. Comme dans tout système, le bon fonctionnement de l'ensemble dépend du bon fonctionnement des parties. On observe également que les dysfonctionnements viennent du « grain de sable » dans les rouages (mode de fonctionnement souhaité et « bien » pensé… idéalement documenté dans une

procédure et communiqué). Ces dysfonctionnements peuvent générer des accidents dramatiques, si l'on pense par exemple au transport aérien, à la production d'électricité d'origine nucléaire ou à la banque. C'est pourquoi, dans la plupart des secteurs économiques, une réglementation impose à chaque organisation de mettre en place et de faire vivre un dispositif de maîtrise des risques, dont le fonctionnement est surveillé par l'autorité de tutelle.

Eu égard aux enjeux, à la complexité des processus, à la taille de l'organisation concernée ou tout simplement des responsabilités engagées tant dans l'entreprise qu'au-delà, on impose que cette surveillance laisse une trace documentée, conservée et accessible. Au premier chef, les employés appliquent les procédures et utilisent les formulaires et les systèmes proposés. Les manageurs de terrain y veillent. Il leur est demandé de formaliser un certain nombre de précautions et même de procéder à des tests par sondages documentés pour établir que, dans le réel :

- telle méthode commerciale est bien utilisée en temps opportun (contrôle *a priori* de l'adéquation du produit aux besoins du client) ;
- telle sûreté est bien mise en œuvre (fermeture de la porte de la salle des coffres pour une agence bancaire… pour la petite histoire nous noterons que rien n'est impossible et que dans le cadre d'un test de ce genre il nous est arrivé d'en trouver d'ouvertes…) ;
- les mesures de sécurité restent bien actives dans une usine…

Ce sont les contrôles de premier niveau qui seront à réaliser, selon un calendrier défini à l'avance, par les responsables d'encadrement à partir des opérations traitées par leurs collaborateurs. Par exemple, contrôler un échantillon d'opérations pour s'assurer du respect de la procédure de traitement.

8.2. Contrôles de deuxième niveau

Dans les activités sensibles, il est utile, et souvent requis, qu'un tiers indépendant relevant d'une autre hiérarchie s'assure périodiquement que les équipes de terrain fonctionnent de la « bonne » manière, c'est-à-dire conformément aux procédures, et avec le bon niveau de contrôles de premier niveau à même de garantir ce bon fonctionnement et à même de déclencher les actions de régulation toujours nécessaires dans la pratique (on parle de pilotage du contrôle interne). Une deuxième « ligne de défense » est ainsi constituée de spécialistes soit des processus (équipe de contrôle interne), soit de la réglementation (équipe de conformité), soit de sécurité (équipe du responsable de sécurité des systèmes d'information – RSSI – ou du responsable de la sécurité des personnes et des biens – RSPB), soit d'autres experts de risques. Ils procèdent à des tests indépendants plus ciblés et moins fréquents qui constituent les contrôles de deuxième niveau. Les contrôles de deuxième

niveau seront à réaliser eux aussi selon un calendrier défini à l'avance, par des fonctions de contrôle spécialisées non localisées au sein des métiers mais au sein de structures de contrôle permanent. Par exemple, contrôler que le responsable hiérarchique a bien réalisé les contrôles de premier niveau et que, si des anomalies ont été identifiées, des actions correctives et préventives (formation, adaptation de la procédure…) ont bien été engagées.

8.3. Contrôles de troisième niveau

Quis custodiet custodes ipsos (« Qui gardera les gardiens eux-mêmes ? ») s'interrogeaient les Latins… À l'instar de nos philosophes antiques, il a été jugé pertinent que les pouvoirs donnés aux dirigeants par les propriétaires (actionnaires, associés, porteurs de parts…) soient placés sous surveillance et que dans le cadre de la gouvernance d'entreprise (dispositif de gestion de l'entreprise entre propriétaires et dirigeants), les propriétaires soient dotés de leur corps de contrôle : l'audit interne procédant aux « contrôles de troisième niveau ». Les contrôles de troisième niveau seront à réaliser, selon un calendrier non défini à l'avance ou, en tout cas, non communiqué aux personnes bénéficiaires de ces missions, par une fonction d'audit spécialisée. Le plan de contrôle de troisième niveau est proposé au comité d'audit par le directeur de l'audit interne en fonction de son analyse des risques et en vue de couvrir l'ensemble du périmètre et des préoccupations des actionnaires dans « le plus petit nombre d'exercices possible », comme le demande la réglementation bancaire. Le comité d'audit, lieu d'exercice de la gouvernance rassemblant les représentants des propriétaires et les dirigeants, adapte et approuve le plan d'audit, en suit la réalisation et en exploite les résultats. Il peut être décidé, par exemple, de contrôler la conformité des opérations en cours et d'apprécier les contrôles réalisés par les parties prenantes (les collaborateurs en charge des contrôles opérationnels, les responsables d'encadrement en charge du contrôle des collaborateurs et les fonctions de contrôle de deuxième niveau en charge du contrôle des responsables d'encadrement) et/ou l'efficacité du dispositif de maîtrise des risques.

EN PRATIQUE

Critères de maturité d'un dispositif de contrôle permanent de premier niveau

Périmètre	Risques métiers, le pilotage et les fonctions supports.
Modalités de réalisation	Il existe des fiches de contrôles présentant leur mode opératoire de réalisation et favorisant leur réalisation homogène par les différents contrôleurs. Les contrôles sont précisés dans les procédures.
Cotation des résultats	Il existe des indicateurs permettant d'évaluer le résultat de chaque contrôle. Il existe des normes permettant de porter un jugement sur le résultat de chaque contrôle.
Traçabilité des résultats	Les contrôles réalisés et les éléments contrôlés sont tracés.
Personnes en charge des contrôles	Les contrôles permanents de premier niveau sont réalisés par des contrôleurs permanents localisés dans les métiers ou les responsables d'encadrement. Ils ne peuvent être pris en charge par des contrôleurs de deuxième niveau que par défaut et ponctuellement. Les contrôles respectent la séparation des fonctions incompatibles.
Reporting des résultats	Les incidents sont déclarés, enregistrés et analysés selon les méthodes définies par les responsables de la gestion des risques. Des reportings sont adressés à la fonction de contrôle permanent de deuxième niveau et à la hiérarchie métier.
Plans d'action	Des actions sont engagées dans le cas de résultats de contrôle insatisfaisants.
Mise à jour du plan de contrôle	Le plan de contrôle à réaliser est revu régulièrement (*a minima* annuellement). La survenance d'un événement est de nature à entraîner la revue du plan de contrôle.
Outil utilisé	Progiciel de contrôle interne plutôt qu'une application bureautique.
Connexions	Liens entre les contrôles permanents de premier niveau et les autres composants du dispositif de contrôle interne, notamment le plan de contrôle permanent de deuxième niveau.

Critères de maturité d'un dispositif de contrôle permanent de deuxième niveau

Périmètre	Risques métiers, pilotage et fonctions supports
Modalités de réalisation	Il existe des fiches de contrôles présentant le mode opératoire de réalisation des contrôles. Les contrôles permanents ont deux objectifs : ▪ vérifier que les contrôles permanents de premier niveau sont correctement réalisés ; ▪ constituer des contrôles complémentaires aux contrôles de premier niveau et se fondant sur les résultats de ceux-ci. Le plan de contrôle est revisité *a minima* annuellement (avec résultats des contrôles de premier, deuxième et troisième niveaux, les incidents avérés, les indicateurs de non-conformité, l'évolution des activités et de la réglementation...).

.../...

.../...

Cotation des résultats	Il existe des indicateurs permettant d'évaluer le résultat de chaque contrôle. Il existe des normes permettant de porter un jugement sur le résultat de chaque contrôle.
Traçabilité des résultats	Les contrôles réalisés et les éléments contrôlés sont tracés.
Personnes en charge des contrôles	Les contrôles permanents de deuxième niveau sont réalisés par des contrôleurs permanents de deuxième niveau localisés au sein de la fonction Contrôle permanent.
Reporting des résultats	Des reportings sont adressés aux comités de contrôle interne. Des reportings sont adressés à la hiérarchie métier.
Plans d'action	Des actions sont engagées dans le cas de résultats de contrôle insatisfaisants. Ces actions sont à la charge des métiers, de l'informatique...
Mise à jour du plan de contrôle	Le plan de contrôle à réaliser est revu régulièrement (*a minima* annuellement). La survenance d'un événement est de nature à entraîner la revue du plan de contrôle.
Outil utilisé	Progiciel de contrôle interne plutôt qu'une application bureautique. Requêtes sur bases de données (contrôles à distance).
Connexions	Liens entre les contrôles permanents de deuxième niveau et les autres composants du dispositif de contrôle interne, notamment les plans de contrôle de premier niveau et troisième niveau, la cartographie des risques, le référentiel des processus...

Critères de maturité d'un dispositif de contrôle périodique de troisième niveau

Périmètre	Il couvre les risques métiers, pilotage et fonctions supports. Il prend en compte les plans de contrôle de premier et deuxième niveaux, les rapports de contrôle des autorités de tutelle et du groupe...
Modalités de réalisation	Il existe une démarche et des outils de conduite de mission. Il existe des dossiers permanents.
Révision du programme d'audit	Le programme d'audit est revisité a minima annuellement (et tenant compte de la cartographie des risques, des résultats des contrôles de premier, deuxième et troisième niveaux, des incidents avérés, des indicateurs de non-conformité, de l'évolution des activités, de la réglementation, du contexte économique...).
Cotation des résultats	Il existe des indicateurs permettant d'évaluer le résultat de chaque contrôle. Il existe des normes permettant de porter un jugement sur le résultat de chaque contrôle.
Traçabilité des résultats et des preuves	Les contrôles réalisés et les éléments contrôlés sont tracés.
Personnes en charge des contrôles	Auditeurs internes et externes et inspection générale.

.../...

.../...

Reporting des résultats	Des reportings sont adressés au comité de contrôle interne et à la hiérarchie métier.
Recommandations issues des contrôles	Des recommandations sont formulées dans le cas de résultats de contrôle insatisfaisants. La mise en œuvre de ces recommandations est à la charge des métiers, de l'informatique...
Outil utilisé pour réaliser, tracer et rendre compte des contrôles	Progiciel de contrôle interne plutôt qu'une application bureautique. Requêtes sur bases de données (contrôles à distance). Progiciel d'audit.
Connexions de la composante « Contrôles de troisième niveau »	Il existe des liens entre les contrôles de troisième niveau et les autres composants du dispositif de contrôle interne, notamment les plans de contrôle de premier niveau et deuxième niveau, la cartographie des risques, le référentiel des processus, le suivi des recommandations notamment pour que tous puissent disposer d'une vision consolidée des faiblesses du DMR identifiées et des plans de réduction des risques lancés...

9. LA VEILLE RÉGLEMENTAIRE

Le profil de risques de l'entreprise dépend de ses choix d'activité et d'organisation mais aussi de l'environnement réglementaire. Celui-ci est une forme de DMR de la nation qui va réagir à un risque (dysfonctionnement sectoriel, instabilité, insécurité, atteinte aux personnes ou aux biens, protection du consommateur...) en faisant des choix (interdictions ou limitations), en instaurant du contrôle *a priori* ou *a posteriori* (procédures administratives)... Ne pas être conforme, c'est s'exposer à un risque de sanction et d'image. Les entreprises doivent donc se doter d'un mécanisme d'écoute, d'analyse et d'adaptation leur permettant de procéder à cette adaptation. La complexité, l'intensité, le degré de contrainte croissant de ces réglementations nécessite aujourd'hui dans la plupart des secteurs un dispositif de veille dépassant la simple attention du « bon professionnel ».

Les fonctions d'audit interne et de contrôle permanent ne sont pas toujours en charge de ce dispositif, généralement confié à la direction juridique de l'entreprise. Dans certains secteurs, la direction de la conformité, élément du contrôle permanent, est en charge de cette veille, c'est ainsi un des standards de fait du secteur bancaire. En toutes hypothèses, elles sont naturellement destinataires de toute information devant se traduire par une adaptation du dispositif de contrôle interne de l'entreprise : mise à jour d'une procédure, d'un contrôle opérationnel...

Ce dispositif est extrêmement important pour toute entreprise soumise à une réglementation et/ou une autorité de tutelle ayant le pouvoir de sanction financière, pouvant aller jusqu'au retrait de l'agrément d'exercer le métier en question. C'est le cas de l'Autorité des marchés financiers (AMF) pour tous les « prestataires de services d'investissement » (PSI c'est-à-dire des acteurs intervenant sur les marchés financiers

– « les bourses ») et de l'Autorité de contrôle prudentiel et de résolution (ACPR) pour les banques et pour les compagnies d'assurances.

C'est également le cas également de l'Autorité de la concurrence qui veille à ce que la concurrence s'exerce dans tous les secteurs au bénéfice des consommateurs et qui peut dans ce cadre sanctionner toute entreprise.

Les dix plus fortes amendes infligées par l'Autorité de la concurrence depuis 2000

L'Autorité de la concurrence peut avoir la main lourde : ses amendes peuvent atteindre des centaines de millions d'euros. Ces amendes ont un but « punitif » et « dissuasif » et sont calculées en tenant compte de la gravité des pratiques anticoncurrentielles, des dommages subis par l'économie et de la situation des entreprises.

- 575,4 millions d'euros (16 décembre 2008) : amende record infligée à un cartel de onze entreprises de la sidérurgie, dont trois filiales du géant ArcelorMittal. Cette amende a été par la suite réduite à 73 millions d'euros par la cour d'appel de Paris.
- 534 millions (30 novembre 2005) : le précédent record. Le conseil sanctionne les opérateurs de téléphonie mobile SFR, Bouygues Télécom et Orange pour entente illicite.
- 384,9 millions (20 septembre 2010) : les onze principales banques françaises et la Banque de France sont sanctionnées pour entente sur les coûts de traitement des chèques.
- 367,9 millions (8 décembre 2011) : l'Autorité de la concurrence sanctionne un cartel entre les quatre principaux fabricants de lessives, Unilever, Procter & Gamble, Henkel et Colgate-Palmolive, qui portait sur le prix des lessives et les promotions. Il a été dénoncé par Unilever, qui a par conséquent été totalement exonéré de sanction.
- 242,4 millions (13 mars 2012) : des producteurs français et allemands de farine sont accusés d'ententes illicites. Sept producteurs français membres des groupements France Farine (marque Francine) et Bach Mühle écopent d'une amende de 146,9 millions d'euros pour s'être entendus sur les prix et la production en France de farine destinée à la vente en grande distribution. Un cartel plus large regroupant treize meuniers ou groupements de meunerie français et allemands est par ailleurs condamné à 95,5 millions d'euros d'amende pour avoir limité les importations de farine entre les deux pays entre 2002 et 2008.
- 183,1 millions (13 décembre 2012) : Orange et SFR sont respectivement condamnés à 117,5 et 65,7 millions d'euros d'amende pour pratiques anticoncurrentielles sur le marché de la téléphonie mobile.
- 174,5 millions (19 septembre 2000) : neuf banques, dont le Crédit Agricole, la BNP, la Société Générale et le Crédit Lyonnais, sont punies pour avoir tenté d'empêcher les particuliers de renégocier leurs crédits immobiliers.
- 94,4 millions (2 février 2009) : les sociétés de travail temporaire Adecco, Manpower et VediorBis sont sanctionnées sur le prix de certaines prestations entre mars 2003 et novembre 2004.

.../...

.../...

- 80 millions (7 novembre 2005) : France Télécom est sanctionné pour abus dans l'Internet à haut débit (ADSL).
- 63 millions (9 décembre 2009) : Orange Caraïbe (France Télécom) écope d'une amende pour « avoir freiné abusivement le développement de la concurrence » dans la téléphonie fixe et mobile en Guadeloupe, Martinique et Guyane.

Source : Challenge.fr du 14 mai 2013.

EN PRATIQUE

Critères de maturité d'un dispositif de veille réglementaire (exemple du secteur banque-assurances)

Périmètre	Informations réglementaires (ex. : secteur bancaire) : ■ directives européennes ; ■ directives Banque de France (ex. : CRBF 97-02) ; ■ règlement général de l'AMF ; ■ code des assurances ; Solvency-2 ; ■ autorités bâloises... ■ informations à caractère obligatoire en provenance du groupe.
Politique et modalités pratiques	Il existe un document décrivant les attentes de l'entreprise en matière de veille réglementaire. Il existe des procédures décrivant les modalités de collecte des informations (*push* ou *pull*), la fréquence (fil de l'eau, dates anniversaires) et les moyens (utilisation de sites Web, de plateformes d'échange, abonnement auprès d'organismes spécialisés, d'associations professionnelles types Association française de banque (AFB) ou Office de coordination bancaire et financière (OCBF) pour le secteur bancaire, réception de documents Groupe...), l'historisation et traçabilité des informations, la diffusion auprès des métiers et la décision de prise en compte des impacts dans l'activité (et par là même les produits et services commercialisés, les procédures et notes d'instruction...). Il existe des interlocuteurs désignés (correspondants au sein des métiers, fonctions supports).
Outil utilisé pour le stockage et la publication d'informations	Progiciel du marché plutôt qu'outil bureautique.
Connexions	Liens entre la veille réglementaire et d'autres composantes du dispositif de contrôle interne : taxonomie des risques, référentiel des processus, corpus des procédures...
Connaissance par les personnels de la banque	Les personnels concernés connaissent le dispositif de veille réglementaire. Des actions de sensibilisation sur le thème de la veille réglementaire sont réalisées régulièrement.

10. LA DÉCLARATION DES INCIDENTS

Ce dispositif est très important pour toute entreprise souhaitant progresser dans la qualité de ses prestations. Il permet en effet de s'interroger d'une façon vertueuse sur les incidents, qu'ils aient une incidence financière (perte, amende) ou un impact sur l'image de l'entreprise et sa réputation… En tout état de cause, la réduction du nombre d'incidents ne peut être que bénéfique à l'entreprise, au sens qu'elle réduit la charge de travail des collaborateurs rendue nécessaire par le traitement des incidents et de leurs effets induits : réclamations, dédommagements…

Les fonctions d'audit interne et de contrôle permanent sont destinataires de ces informations. Très souvent, elles administrent le dispositif à l'aide d'un outil de déclaration des incidents décentralisé au sein des métiers.

Ce dispositif se compose de plusieurs sous-systèmes :

- déclaration d'incident ;
- évaluation des impacts de l'incident ;
- action corrective proposée ;
- validation de la déclaration d'incident et de l'action corrective proposée ;
- validation de l'efficacité de l'action réalisée ;
- reporting sur les incidents et les actions vers la hiérarchie et les fonctions de contrôle.

EN PRATIQUE

Critères de maturité d'un dispositif de déclaration des non-conformités et des incidents avérés

Périmètre	Processus métier (prestations visibles des clients), processus de pilotage et processus support.
Processus correspondants	Contrôle des opérations *a priori* aux étapes clés des processus (opérationnels ou contrôleurs permanents de premier niveau) en vue de l'identification de non-conformités. Mémorisation des non-conformités et des pièces justificatives. Déclaration des anomalies. Correction des non-conformités. Identification des causes récurrentes, définition et mise en œuvre des actions préventives. Reporting régulier sur les résultats des contrôles (hiérarchie métier, fonction contrôle permanent, fonction qualité) : taux de conformité.
Administration de la base incidents	Administrateur central et déclarants locaux.

.../...

.../...

Outil utilisé pour la déclaration des incidents	Progiciel du marché plutôt qu'un outil bureautique.
Connexions	Liens entre le dispositif de déclaration des incidents avérés et d'autres composantes du dispositif de contrôle interne : taxonomie des risques, référentiel des processus...
Connaissance par les personnels (ex. : secteur bancaire)	Les personnels concernés connaissent les obligations et modalités pratiques de déclaration des non-conformités et des incidents avérés. Des actions de sensibilisation sont réalisées régulièrement auprès des personnels sur l'identification et la déclaration des non-conformités, le contrôle préventif des opérations, le traitement des causes récurrentes, le reporting...

11. LE SUIVI DES PLANS D'ACTION

Les deux fonctions d'audit interne et de contrôle permanent sont concernées par la mise en place des actions relatives à des incidents ou des carences du dispositif de contrôle interne de l'entreprise.

Elles le sont d'autant plus qu'elles sont souvent à l'initiative de demandes aux métiers de réaliser telle ou telle action, définies dans le cadre de missions d'audit interne ou de contrôle permanent.

EN PRATIQUE

Critères de maturité d'un dispositif de suivi des actions et recommandations

Périmètre	Actions demandées par le contrôle permanent. Recommandations demandées par l'audit interne et les autorités de tutelle.
Processus concernés	Inscription d'une action ou recommandation. Évaluation de la mise en œuvre de l'action ou recommandation. Validation de la mise en œuvre d'une action ou recommandation.
Administration de la base actions et recommandations	Administrateur central et correspondants métier locaux.
Outil utilisé	Progiciel du marché plutôt qu'un outil bureautique.
Reporting	Existence d'un reporting auprès de la hiérarchie métier. Existence d'un reporting auprès des fonctions et comités de contrôle.

.../...

.../...

Connexions	Liens entre le dispositif de suivi des actions et recommandations et d'autres composantes du dispositif de contrôle interne : taxonomie des risques, référentiel des processus...
Connaissance par les personnels (ex. : secteur bancaire)	Les personnels concernés connaissent les obligations et les modalités pratiques de mise en œuvre des actions et des recommandations. Des actions de sensibilisation sur le thème de la mise en œuvre des actions et recommandations sont réalisées régulièrement.

12. LES INDICATEURS D'ACTIVITÉ ET DE RISQUES

Les deux fonctions d'audit interne et de contrôle permanent sont très demandeuses de chiffres. Ceci explique notamment la grande proximité qui existe entre ces deux fonctions et la fonction « contrôle de gestion ».

Les données qui intéressent les deux fonctions d'audit interne et de contrôle permanent sont tout d'abord des données sur les volumes d'activité et les masses financières en jeu. Les autres données sont celles qui concernent les incidents, anomalies, pénalités, amendes… Et c'est souvent la mise en perspective des dernières avec les volumes d'activité qui les rend significatives ou anecdotiques.

Les fonctions « organisation » et « qualité » peuvent également fournir aux fonctions d'audit interne et de contrôle permanent des données précieuses, notamment des normes de qualité, des incidents caractéristiques, des référentiels de processus, des éléments de performance économique, des standards de productivité…

EN PRATIQUE

Critères de maturité d'un dispositif d'indicateurs d'activité et de risques

Périmètre couvert	Les indicateurs mesurent les risques les plus importants de la cartographie des risques. Les indicateurs mesurent les incidents avérés, les non-conformités identifiées...
Pertinence des indicateurs	Les indicateurs sont pertinents au regard des objectifs de mesure recherchés. Les indicateurs sont fiables et faciles à calculer.
Niveau de granularité des indicateurs	Les indicateurs permettent de passer du détail au global et inversement. Chaque niveau hiérarchique dispose des informations de son périmètre de responsabilité et peut ainsi décider d'actions à engager.
Résultat	Il existe des normes permettant de qualifier les résultats à un moment donné ainsi que les tendances historiques.

.../...

.../...

Traçabilité des résultats et des preuves	Les valeurs des indicateurs et les éléments mesurés sont tracés.
Reporting des résultats	Un reporting est réalisé vers les fonctions et instances de contrôle. Un reporting est réalisé vers les métiers.
Pilotage	Les indicateurs sont utilisés par la hiérarchie métier. Les indicateurs sont utilisés par les fonctions et instances de contrôle.
Outil utilisé pour calculer, tracer et rendre compte des résultats	Progiciel de contrôle interne plutôt qu'un outil bureautique.
Connexions	Liens entre les indicateurs de risques et les contrôles de premier et deuxième niveaux, la cartographie des risques, le référentiel des processus...
Connaissance par les personnels des résultats	Les personnels connaissent l'existence des indicateurs. Les personnels sont informés régulièrement sur les résultats.

13. LE REPORTING

Les fonctions d'audit interne et de contrôle permanent sont directement concernées par les reportings hiérarchiques à produire à l'attention de la hiérarchie de l'entreprise et du conseil d'administration d'une part, et à destination des organismes de tutelle d'autre part. Généralement, si ces deux fonctions ne sont pas responsables de la production des données, elles sont responsables de leur collecte, validation, mise en forme et envoi dans les bons formats et aux bonnes dates.

BONNES PRATIQUES

Critères de maturité d'un dispositif de production des reportings réglementaires (exemple secteur bancaire)

Périmètre	États mensuels BDF, rapports annuels commission bancaire...
Contacts réglementaires	Ex.: secteur bancaire. Banque de France, ACPR, AMF...
Personnels concernés	Ex.: secteur bancaire. Existence d'interlocuteurs clés pour chaque instance de tutelle. Existence de correspondants en ce qui concerne la production des reportings réglementaires.

.../...

.../...

Processus concernés par le reporting	Production des données. Production des états réglementaires. Contrôle qualité avant envoi.
Outil utilisé	Application de gestion, application spécifique, progiciel du marché plutôt qu'un outil bureautique. Requêtes sur bases de données.
Connexions	Liens entre les obligations de reporting et l'entretien de contacts réglementaires et d'autres composantes du dispositif de contrôle interne : taxonomie des risques, indicateurs de risques, déclaration des incidents avérés.
Connaissance par les personnels de la banque	Les personnels concernés connaissent les obligations de reporting et les interlocuteurs clés par organe de tutelle. Des actions de sensibilisation sur le thème du reporting réglementaire sont réalisées régulièrement.

14. LE PLAN DE CONTINUITÉ D'ACTIVITÉ

Toute entreprise doit à ses clients une continuité d'activité. C'est également une nécessité imposée par la concurrence et par la simple nécessité financière. Les incidents portent tous, dans des proportions différentes, atteinte à la bonne marche de l'activité. Telle situation nécessite du temps de recherche, de correction, de communication, voire de négociation, avec les clients impliqués. Telle autre pourra avoir des conséquences juridiques, voire judiciaires, qui vont demander du temps de traitement humain voire se traduire par des pénalités et/ou amendes pour l'entreprise. Il est cependant des situations et circonstances «catastrophiques» où une réponse adaptée et exceptionnelle est indispensable.

Cette continuité d'activité peut malheureusement être mise à mal, malgré la bonne volonté de l'entreprise et de ses collaborateurs, par la survenance d'un événement majeur ou d'une accumulation d'événements, rendant cette continuité impossible, pour une durée plus ou moins longue.

Les deux fonctions d'audit interne et de contrôle permanent interviennent en coopération avec les métiers et des experts de tout domaine dans la définition du plan de continuité d'activité, à savoir dans l'inventaire des scénarios plus ou moins compliqués, de nature à contrarier la bonne marche des opérations.

EN PRATIQUE

Critères de maturité d'un plan de continuité d'activité

Périmètre couvert	Existence d'un plan de continuité des activités (PCA). Existence d'un plan de reprise d'activité (PRA).
Processus	Analyse des risques de non-continuité de chaque activité fondée sur une étude d'impacts en matière de durée d'indisponibilité maximale autorisée (DIMA), c'est-à-dire le temps pendant lequel il est possible de se passer des moyens nécessaires à la réalisation des activités et de recourir à des modalités dégradées. Cas des sinistres informatiques : l'étude d'impact porte également sur la perte de données maximale admissible (PDMA) s'évaluant sur les quatre critères suivants : disponibilité, intégrité, confidentialité et preuve (traçabilité).
Test du PCA	Réalisation de tests réguliers (ex. : repli d'une activité sur un site de secours).
Outil utilisé pour le plan de conduite et de reprise d'activités	Progiciel du marché plutôt qu'outil bureautique.
Connexions de la composante « Plan de continuité et de reprise des activités »	Il existe des liens entre le plan de continuité et de reprise des activités et d'autres composantes du dispositif de contrôle interne.
Connaissance par les personnels (ex. : secteur bancaire)	Sensibilisations régulières du personnel au plan de continuité et de reprise des activités.

15. LE CONTRÔLE DES PRESTATIONS ESSENTIELLES EXTERNALISÉES

L'évolution de nos économies vers une spécialisation accrue et les objectifs de professionnalisation et d'économies d'échelle ont conduit de nombreux groupes et sociétés à se « recentrer sur leur cœur d'activité » et, pour continuer à fonctionner, à confier certaines activités ou fonctions à des acteurs spécialisés : calcul de la paie, gestion du courrier, archivage, accueil et sécurité, développement, maintenance, exploitations informatiques… Ces choix ayant souvent vocation à réduire les coûts, les entreprises n'ont pas gardé les spécialistes qu'ils pouvaient avoir embauchés pour assurer ces fonctions et s'en sont remis aux prestataires. Or certains de ces « fournisseurs » ont une telle incidence sur le service rendu par l'entreprise que celle-ci ne peut pas se « désintéresser » des conditions de la réalisation de cette prestation tant au titre de la qualité que de la continuité voire de

la régularité/sécurité, de leurs produits ou de leurs services. Ce sont alors des « prestations essentielles externalisées ». Les prestations essentielles confiées à des sous-traitants rentrent ainsi dans la cartographie des risques de l'entreprise. À ce titre, elles doivent être mises sous contrôle par les deux fonctions d'audit interne et de contrôle permanent.

Dans les banques, les prestations essentielles externalisées (PEE) concernent le traitement des chèques, des effets de commerce, des cartes, l'archivage, l'infogérance informatique…

EN PRATIQUE

Critères de maturité d'un dispositif de contrôle des prestations essentielles externalisées

Périmètre	Les PEE couvrent des prestations participant directement à l'exécution des opérations ou des services : exemple pour une banque : chèques, cartes, conservation des titres… (conformité à la réglementation 97-02, art 37-2 et art 4, r).
Contractualisation avec les fournisseurs de PEE	Les contrats existent. Les contrats sont revus régulièrement et toute modification des termes de la prestation demandée se traduit par un avenant. Les contrats précisent les modalités de continuité d'activité, les modalités de traitement dans le cas de fluctuation des volumes à traiter, les indicateurs qualité, les pénalités en cas de respect du contrat… Les contrats sont validés par les métiers, le département juridique, le contrôle interne… Les contrats sont signés par des personnes habilitées.
Suivi des prestations réalisées	Il existe un reporting fournisseur préalable à chaque facturation. Il existe des réunions qualité régulières. Chaque prestation est contrôlée par un correspondant métier et le contrôle interne. Le personnel concerné a connaissance de la qualité des prestations attendues par les fournisseurs de prestations.
Traitement des non-conformités et des incidents avérés	Le contrat précise les types de non-conformités. Il existe des procédures précisant les modalités opérationnelles de traitement. Les non-conformités donnent lieu à l'application de pénalités.
Contrôle du dispositif de contrôle interne	Les fournisseurs rendent compte régulièrement des prestations réalisées, des problèmes survenus… Il existe des missions de contrôle contradictoires réalisées chez les prestataires selon une fréquence adaptée aux enjeux que représentent les prestations externalisées avec utilisation de référentiels adaptés (ex. : référentiel sécurité chèques). Il existe un suivi des recommandations. Les éléments du dispositif de contrôle interne des fournisseurs sont intégrés dans le rapport annuel sur l'état du contrôle interne de la banque.
Connexions	Liens entre le contrôle des PEE et les contrôles de premier et deuxième niveaux, la cartographie des risques…

16. LE CONTRÔLE DES FILIALES

Les filiales rentrent elles aussi dans la cartographie des risques de l'entreprise. À ce titre, elles doivent être mises sous contrôle par les deux fonctions d'audit interne et de contrôle permanent.

EN PRATIQUE

Critères de maturité d'un dispositif de contrôle des filiales

Périmètre	Les filiales de l'entreprise sont identifiées. Les règles d'inclusion des filiales dans le périmètre des activités à contrôler sont définies et appropriées (pourcentage de capital, participation à la gouvernance).
Dispositif de contrôle interne	Le dispositif de contrôle mis en œuvre par chaque filiale est adapté à ses risques (risques métiers, risques opérationnels, risques réglementaires, risques d'image). Il existe une subsidiarité pour certains thèmes quand une filiale n'a pas les compétences techniques nécessaires (ex. : l'audit informatique). Le dispositif de contrôle interne d'une filiale intègre les modalités de traitement des incidents avérés de la filiale.
Acteurs du contrôle des risques d'une filiale	Il existe des correspondants identifiés au sein de chaque filiale (plan de continuité d'activité, déclaration des incidents avérés, etc.). Il existe des personnes au sein de l'entreprise en charge du suivi des filiales (contrôle interne, métiers).
Séparation des fonctions incompatibles entre maison mère et filiale	Le principe de séparation des fonctions incompatibles est respecté entre maison mère et filiale afin de ne pas avantager une filiale au détriment d'autres (ex. : collaborateur de la banque également administrateur d'une filiale)
Contrôle du dispositif de contrôle interne des filiales	Les filiales rendent compte régulièrement de l'état de leur dispositif de contrôle. Il existe des missions de contrôle contradictoires au sein des filiales selon une fréquence adaptée aux enjeux de chaque filiale. Les contrôles exercés sur place par la maison mère sont réalisés à l'aide de référentiels adaptés plus ou moins détaillés selon l'enjeu. Il existe un suivi des recommandations demandées aux filiales. Les éléments du dispositif de contrôle interne des filiales sont intégrés dans le rapport annuel sur l'état du dispositif de contrôle interne de la banque.
Connexions	Liens entre l'intégration des filiales et les contrôles de premier et deuxième niveaux, la cartographie des risques...

17. LA GESTION DE CRISE

Dans le cas d'une crise grave, il y a nécessité de mise en place d'une cellule de pilotage, et ce afin de coordonner les opérations, la communication interne et externe…

Les deux fonctions d'audit interne et de contrôle permanent sont impliquées dans la gestion des situations de crise, de par leur proximité avec la direction générale, et la confiance élevée que cette dernière a pour elles.

EN PRATIQUE

Critères de maturité d'un dispositif de gestion de crise

Existence	Dispositif et cellule de gestion de crise.
Périmètre couvert	Tout type de crise (réglementaire, juridique, financière, humaine, informatique, image).
Organisation et processus	Correspondant au traitement des différents scénarios de crise possible. Liste des personnes à contacter par nature de crise. Procédures de diagnostic, action, communication, retour d'expérience.
Information du personnel	Connaissance par le personnel des personnes à contacter et des procédures à suivre en cas de crise. Sessions de sensibilisation et de formation sur le thème.

18. LES OUTILS DU DISPOSITIF DE MAÎTRISE DES RISQUES

18.1. L'enquête du CBOK

L'enquête du CBOK a permis de lister l'ensemble des outils et des méthodes utilisés dans le cadre d'un dispositif de maîtrise des risques.

Panorama des outils et méthodes utilisés par l'audit interne

- L'extraction de données.
- Les outils de communication tels les e-mails.
- L'approche par les risques.
- L'échantillonnage statistique.
- Les documents de travail électroniques.

.../...

.../...

- La revue analytique.
- L'auto-évaluation des contrôles.
- Le *benchmarking*.
- Les logiciels de *flow-chart*.
- L'application de cartographie des processus.
- Les techniques d'audit supportées par l'informatique.
- Le tableau de bord.
- Le logiciel de modélisation de processus.
- Les outils de gestion de la qualité.
- L'audit continu en temps réel.
- La technique de gestion qualité.

L'enquête montre que l'approche par les risques est prédominante.

Nos observations montrent que trop peu d'équipes utilisent de façon efficace les logiciels d'audit et de contrôle permettant de suivre d'une façon automatique des valeurs, de mettre en évidence des opérations inhabituelles ou encore de réaliser des sondages sur des populations importantes. Et pourtant, au-delà des bénéfices certains de ces approches sur la qualité/pertinence des analyses, elles y gagneraient en termes d'optimisation des ressources.

18.2. Les outils de eGRC

Il existe un grand nombre de progiciels d'eGRC (Gouvernance Risk Compliance) sur le marché et notre propos n'est pas d'en faire ici une liste exhaustive ou de vanter les mérites de tel ou tel éditeur de progiciel. Par contre, notre propos est de montrer pourquoi ce type d'outil métier est indispensable en matière de dispositif de contrôle interne et de mise sous contrôle des risques. Les deux fonctions d'audit interne et de contrôle permanent ont donc toutes les chances de travailler dans un environnement équipé d'un progiciel d'eGRC ou de participer à son déploiement.

Les progiciels du marché s'adressent à des entreprises de toutes tailles sachant que leurs coûts de paramétrage et de fonctionnement les destinent plutôt à des entreprises de taille importante, avec au minimum une centaine d'utilisateurs, et allant jusqu'à plusieurs dizaines de milliers.

La plupart des progiciels du marché ont été conçus pour répondre à la réglementation américaine (comme « Sarbanes-Oxley ») ou européenne.

Les progiciels du marché sont le plus souvent construits sur une même logique :

- une plateforme contenant des référentiels : entités, processus, risques, procédures, contrôles… ;
- une architecture en *work-flow* permettant à la hiérarchie de valider ;
- des modules interconnectés entre eux permettant de planifier des plans de contrôle, déclarer des incidents, planifier des actions, mémoriser le résultat des contrôles avec ou sans les preuves correspondantes (contrôle de premier niveau, contrôle de deuxième niveau et contrôle de troisième niveau), calculer des résultats, produire des reporting hiérarchiques et à destination des autorités de tutelle ;
- des possibilités d'import et d'export des données vers des tableurs de type Excel ;
- un dispositif d'alerte permettant l'envoi de messages aux utilisateurs directement sur leur messagerie pour les prévenir d'un contrôle à réaliser ou une action à mettre en œuvre.

Nous vous invitons à aller consulter les sites Internet des fournisseurs de logiciels pour approfondir le sujet.

Les principaux outils du marché

- ACL : ACL Audit Exchange.
- BWise.
- Devoteam : RVR Risque, Contrôle, Audit.
- eFront : Front GRC.
- Enablon : Suite Enablon ERM.
- IBM : Open Pages GRC.
- MEGA : MEGA GRC.
- Oracle : Oracle Enterprise, Governance, Risks and Compliance.
- Productiviti : PGP .
- Etc.

18.3. Les outils de contrôle permanent

Ces outils sont connectés aux applications de gestion de l'entreprise et analysent de façon automatique et en continu les flux de données. Leur première mission est l'identification d'informations inhabituelles ou atypiques.

Dans le cas de traitements bancaires, ce type d'outil permet à l'auditeur interne et au contrôleur permanent d'identifier un comportement inhabituel d'un client, par exemple

faire des retraits répétés dans des distributeurs à l'étranger alors que la personne fait habituellement peu de retraits et jamais à l'étranger.

Leur seconde mission est l'identification des opérations ne respectant pas la réglementation ou des règles de gestion internes et qui auraient été réalisées en « forçant » le système, par exemple forcer un niveau d'habilitation pour accorder un crédit à un client par exemple.

Ce type d'outil est donc très utile dans le cadre de la recherche de fraudes internes ou externes, sujet parfois d'actualité dans les missions d'audit interne et de contrôle permanent.

Les principaux outils du marché

- CaseWise ;
- SAP GRC ;
- etc.

18.4. Les outils d'analyse de données

Les deux fonctions d'audit interne et de contrôle permanent sont concernées par de grands volumes de données à « faire parler ». Ces données sont le plus souvent stockées dans des bases de données, voire des entrepôts de données. Il s'agit alors de sélectionner certaines de ces données sur des critères particuliers, ou de sélectionner des échantillons de données au hasard, ou encore de passer toutes les données au peigne fin sur un critère…

Dans le cas de bases de données informatiques, ils utilisent alors des outils de requêtes permettant d'extraire des données selon des protocoles définis.

Ces logiciels permettent de traiter les informations provenant d'un fichier électronique en faisant une copie fidèle de la population à auditer. Le plus « simple » de ces outils est le tableur Excel. Cet outil est très puissant et intéressant mais, en même temps, artisanal et donc source de nombreuses erreurs.

EN PRATIQUE

Vous devez posséder la pratique de la suite Office, ce qui veut dire savoir :

- établir des listes ;
- les trier et les filtrer ;
- organiser un tableau de type base de données et procéder à des analyses sous la forme de tableaux croisés dynamiques ;

- rechercher dans une liste ;
- dénombrer et lister les « lignes » ayant certaines caractéristiques ;
- rapprocher, comparer des listes et pour cela adapter/transformer une liste pour qu'elle puisse être rapprochée (établissement d'une « clé » commune) ;
- idéalement partager, publier, collaborer sur un tableau Excel ;
- faire des macros sous Excel.

La maîtrise du gestionnaire de base de données de Microsoft (Access) est indéniablement une solution plus puissante mais nécessite un apprentissage plus lourd donnant des constructions moins « accessibles » et moins facilement maintenues que les solutions à base d'Excel.

Cela n'est pas suffisant et vous devez également posséder la pratique d'autres outils telles que ceux de modélisation de processus, de requête dans des bases de données ou encore d'outils d'eGRC.

Utilisables par des « non-informaticiens », les outils d'analyse de données possèdent des fonctionnalités d'audit et d'analyse de données prédéfinies comme :

- le contrôle de séquence (rupture et doublon) ;
- l'import/export et extraction de données ;
- la totalisation, la stratification, la classification des champs clés ;
- l'échantillonnage simple ;
- la réalisation de calculs simples et complexes ;
- la possibilité de joindre, fusionner, trier, nettoyer des fichiers.

Les résultats sont quasi immédiats pour des analyses simples et permettent de générer des rapports de qualité et rapides à obtenir. Ce sont des outils puissants qui permettent d'analyser l'exhaustivité d'une population très conséquente. C'est d'ailleurs, avec les analyses répétitives (identiques réalisées dans différentes entités) et récurrentes (identiques à des périodes successives), la principale raison de leur utilisation dans les missions d'audit.

Les principaux outils du marché

- Datawatch : Monarch Report Analytics.
- Business Object.
- QlickView.
- etc.

PAROLE D'EXPERT

Lawrence B. Sawyer, introduction

« Qu'exige donc la pratique de l'inspection moderne ? Je ne songerai pas à vous dire que c'est simple. Ça ne l'est pas, et certains, qui ont d'excellentes références, s'essayent dans ce secteur et n'y parviennent jamais. Oh si ! Ils peuvent faire une inspection ! Mais ils la font "au ras du sol", sans étincelle, sans imagination, sans observer les règles fondamentales. Ce qui m'amène à quelques-uns des "piliers" de l'inspection moderne… Les concepts que l'inspecteur moderne doit emporter avec lui lorsqu'il se rend à son travail… Les combinaisons qui l'aideront à ouvrir les coffres-forts les mieux gardés de l'information. Je les considère comme les dix commandements de l'inspection moderne. Ils ne sont pas particulièrement nouveaux, mais je pense qu'ils sont particulièrement importants. »

TÉMOIGNAGE

Philippe Vannier, président de Bull

L'audit interne est une fonction optimiste et positive qui aide l'entreprise à voir l'avenir avec sérénité. Ce n'est pas Cassandre avec ses prophéties pessimistes et parfois dramatiques.

Au fil des ans chez Bull, l'audit interne qui m'est directement rattaché est devenu un outil de management au service de l'entreprise. Par sa connaissance de l'organisation, sa capacité de discernement et la pertinence de ses diagnostics et propositions, l'audit interne m'a non seulement apporté plus de sérénité mais a aussi été créateur de valeur ajoutée pour Bull. Elle incite à traquer les risques et à améliorer les méthodes de travail. C'est une assurance sur l'efficacité des systèmes de gestion des risques et de contrôle interne.

L'audit interne peut d'autant plus rendre service à l'organisation et nous aider à tenir nos objectifs qu'il appréhende les différents aspects de l'activité. Comme un médecin généraliste, il examine Bull dans tous les domaines : commercial, économique, comptable, fiscal, sécurité, informatique, éthique… La vision juste et objective de ce service de l'entreprise lui a permis d'être considéré par tous chez Bull comme un partenaire qui aide à réaliser des économies, à améliorer l'efficience, à éliminer des dysfonctionnements et à réduire les risques. C'est un poste d'observation privilégié sur tout le groupe.

L'audit interne délivre des messages clairs, précis et factuels afin que chacun puisse saisir l'ampleur exacte du risque et la pertinence des recommandations. Celles-ci sont d'autant mieux acceptées que la fonction est crédible. Sa crédibilité passe, j'en suis convaincu, par une relation forte avec la direction générale. Cette relation aide l'audit interne à faire face aux pressions et aux obstacles qui jalonnent ses missions. Ce soutien l'aide aussi à anticiper les risques, à affirmer ses convictions et sa vision du futur pour pouvoir agir et communiquer rapidement, avec discernement et sans crainte.

Bien entendu, l'audit interne doit faire preuve d'une intégrité absolue et la relation forte avec la direction générale ne doit surtout pas l'empêcher de préserver son indépendance et sa liberté d'expression. C'est à ce titre que l'audit interne fait trimestriellement un compte rendu de ses travaux au comité d'audit du conseil d'administration. Cette réunion se tient avec des administrateurs indépendants et je n'y participe pas. Ces méthodes mises en place sont les garants de la réussite de la mission d'audit interne pour déceler, identifier, comprendre, anticiper et proposer sans contrainte.

En conclusion, l'audit interne est une fonction clé chez Bull. Elle attire diverses compétences de l'entreprise et permet d'acquérir un savoir-faire dans les mécanismes de risque, dans les métiers et dans l'organisation. L'audit interne est un vivier, une plaque tournante, pour des collaborateurs performants qui essaiment ensuite dans l'entreprise pour développer la valeur ajoutée tout en maîtrisant les risques.

CHAPITRE 2

Les risques à « mettre sous contrôle »

CE CHAPITRE VOUS PERMETTRA DE :

- connaître le panorama des risques généraux d'une entreprise ;
- connaître la variété des risques spécifiques de certains secteurs d'activité, de certaines fonctions et activités et même de certaines pratiques sportives.

La direction générale d'une entreprise met en place un dispositif de contrôle interne pour assurer la maîtrise globale des risques et avoir une assurance raisonnable d'atteindre ses objectifs.

Le dispositif de contrôle interne est constitué du contrôle permanent et du contrôle périodique (audit interne/inspection générale/autorité de contrôle), distincts et indépendants l'un de l'autre, tout en étant complémentaires. Le contrôle permanent est le dispositif qui met en œuvre, de façon continue, les actions de maîtrise des risques et de suivi de la réalisation des actions stratégiques. L'audit interne vérifie ponctuellement l'efficacité de celui-ci.

Le dispositif de contrôle permanent s'applique à tous les types de risques encourus par l'entreprise. Il s'appuie pour ce faire sur :

- les opérationnels, premiers responsables des risques générés par les activités dont ils ont la charge ;
- des fonctions de contrôle indépendantes (risques, conformité…) dont la responsabilité première est de superviser la façon dont les risques sont pris et gérés par les opérationnels, en particulier par l'exercice d'un second regard sur certaines décisions.

Si les managers sont responsables de la mise en place de dispositifs de contrôle interne efficaces et de la mise en œuvre au quotidien des procédures, ils sont aidés par la fonction de contrôle permanent. Les perturbations économiques qui ont touché les entreprises depuis 2008 ont modifié la hiérarchie des activités des deux fonctions d'audit interne et de contrôle permanent. Face aux différents scandales financiers de ces dernières années, les deux fonctions d'audit interne et de contrôle permanent ont tendance à étudier de plus près le thème des fraudes internes et externes.

Mais le périmètre de l'audit interne et du contrôle permanent s'est aussi étendu. Leurs missions dépassent désormais le contrôle interne financier. Une part essentielle de cette fonction concerne la gestion des risques opérationnels dont notamment ceux liés aux systèmes d'information qui se sont complexifiés ces dernières années, mais aussi les risques liés aux problématiques de gouvernance. Les audits informatiques permettent d'étudier la fiabilité des logiciels informatiques de gestion, de vérifier la conformité des paramétrages pour s'assurer de l'adéquation des outils à l'interprétation des données et de s'assurer de l'efficacité des procédures de sauvegarde et de protection des données. L'élargissement des missions de l'audit interne et du contrôle permanent ne va pas toujours de pair avec un accroissement de son budget, au contraire, les instabilités économiques de ces dernières années ont conduit à une réduction générale des budgets alloués à l'audit interne.

1. PANORAMA DES RISQUES GÉNÉRAUX D'UNE ENTREPRISE

Toute entreprise est confrontée à de nombreux risques. Certains sont communs à toutes les entreprises, d'autres sont spécifiques à une entreprise, à un moment donné de son histoire et aux métiers et marchés sur lesquels elle est positionnée. Certains sont internes, d'autres sont externes, en fonction de son environnement.

1.1. Les risques relatifs à la gestion interne

Les principaux risques auxquels une entreprise est confrontée dans sa gestion interne sont variés et parfois aussi graves que les risques liés aux activités strictement métier : les risques liés à la fonction personnel (embauche, fixation des salaires, primes, paiement d'heures supplémentaires…), les risques liés aux frais généraux (dérapages, abus, collusion entre acheteurs et fournisseurs…), les risques liés aux immobilisations (utilité, collusion, pertes, vols, destruction, abus de biens sociaux, ventes frauduleuses…), les risques liés aux archives (exhaustivité, destruction…), les risques liés à la comptabilité (compétence du personnel, qualité du système d'information…), les risques liés au contrôle de gestion (performance, champ d'action…) et les risques liés à la sécurité (biens, personnes, valeurs…).

Le contrôle doit porter sur la qualité de la gestion du personnel, sur les frais de fonctionnement, sur les immobilisations, sur la mémorisation des informations, sur le système comptable, sur le contrôle de gestion, sur le système informatique et sur la sécurité des valeurs, des biens et des personnes.

Le personnel

L'audit interne et le contrôle permanent doivent s'assurer que l'entreprise possède un système d'information et de contrôle de gestion permettant d'obtenir une image instantanée et évolutive du personnel (effectif, qualifications, masse salariale, classification, taux de rotation, pyramide des âges).

La productivité doit être étudiée par rapport aux grandes masses du bilan (emplois/effectifs, ressources/effectifs) et par rapport au compte de résultat (charges de personnel/total des charges × 100) ou encore par rapport au chiffre d'affaires (CA/effectifs).

L'entreprise doit posséder un plan de formation répondant aux objectifs stratégiques de la direction générale.

Les embauches de personnel doivent être effectuées par une personne autorisée en fonction d'un besoin justifié. La sélection doit s'opérer à l'aide d'un profil de poste précis et de dossiers de candidature dont les informations sont contrôlées.

La titularisation ne peut intervenir qu'après une période d'essai concluante. Le salaire et les éléments constitutifs doivent figurer dans le dossier et ne peuvent être autorisés que par une personne habilitée. Ces informations doivent être régulièrement vérifiées.

Les heures supplémentaires, les primes et augmentations de salaire ne peuvent de même être autorisées que par une personne habilitée.

Les départs doivent respecter les dispositions juridiques du Code du travail (lettre en cas de démission, établissement d'un solde de tout compte, personne autorisée en cas de licenciement, provisions constituées en cas de litiges).

Les prêts au personnel doivent être soumis au préalable à une personne habilitée, selon des modalités connues par l'ensemble du personnel. Il en va de même pour les avances sur salaire.

1.2. Les risques liés aux frais généraux

L'audit interne et le contrôle permanent doivent être vigilants à tout dérapage des frais généraux ou à tout abus manifeste. Tous les comptes de frais généraux doivent être contrôlés par un contrôle budgétaire. Les dépassements de budget doivent nécessiter une autorisation de la direction générale.

Tout achat de biens et de services doit systématiquement faire l'objet d'une séparation de pouvoirs :

- Autorisation : toute commande doit être signée par une personne habilitée.
- Réalisation : un seuil doit être déterminé au-delà duquel des appels d'offres systématiques doivent être effectués, toute livraison de biens et de services doit être systématiquement comparée au bon de commande et à la facture et les comptes fournisseurs doivent être régulièrement pointés et justifiés.

- Contrôle : les règlements des fournisseurs ne peuvent être réalisés qu'en présence d'un bon à payer signé par une personne habilitée. Le stock économat doit être contrôlé à l'aide d'un inventaire permanent, le stock valorisé, un contrôle physique réalisé régulièrement et une provision pour dépréciation constituée si nécessaire. Les stocks doivent être inclus dans les actifs et les provisions pour dépréciations constatées.

1.3. Les risques liés aux immobilisations

Les projets d'investissement doivent faire l'objet d'études préalables sur leur rentabilité. Les acquisitions doivent recevoir l'autorisation d'une personne habilitée. Pour les investissements importants, un appel d'offres doit être systématiquement réalisé.

Un inventaire permanent doit exister, sous la forme d'un fichier pour l'ensemble des immobilisations, inventaire contrôlé par un inventaire physique régulier permettant d'éliminer les matériels hors d'usage, détériorés ou obsolètes.

Les cessions d'immobilisation doivent être autorisées par une personne habilitée et la comptabilisation des plus ou moins-values doit être correctement effectuée.

1.4. Les risques liés aux archives

La durée de conservation des différentes catégories de documents doit correspondre à la réglementation en vigueur. Par ailleurs, une assurance doit couvrir leur destruction accidentelle.

1.5. Les risques liés à la comptabilité

Le personnel de la fonction comptable doit posséder des compétences en comptabilité générale et analytique. De plus, il doit maîtriser parfaitement la réglementation du secteur d'activité. Des compétences métier sont indispensables car, derrière les comptes et les chiffres, il y a des activités dont la connaissance est nécessaire à leur interprétation et leur contrôle. Enfin, des compétences en fiscalité, en informatique… sont utiles.

Le système informatique doit être en mesure de satisfaire les besoins de la comptabilité : possibilité d'inclure des écritures complémentaires dans les situations provisoires issues du système, état de gestion (tableaux de bord, résultats périodiques, analyses particulières), états réglementaires.

Les contrôles effectués par le service comptabilité sont nombreux, car cette dernière doit s'assurer de la cohérence des chiffres issus d'un ensemble de dispositifs : contrôle quotidien de la journée comptable (exhaustivité de la comptabilisation, rejets recyclés, justifications conservées, anomalies de traitement ou de résultat régularisées),

ouvertures de comptes généraux de la responsabilité de la comptabilité, participation à l'élaboration des chaînes informatiques et justification des comptes.

Un manuel comptable doit définir les principales règles du jeu : les principes comptables appliqués, la structure du plan comptable, la liste des comptes et leur contenu, les règles d'ouverture et de clôture des comptes, la procédure de justification des comptes, les contrôles comptables quotidiens et périodiques à réaliser, les travaux d'inventaire, le calendrier de chaque arrêté comptable et les procédures de consolidation si nécessaire.

1.6. Les risques liés au contrôle de gestion

La fonction contrôle de gestion est l'une des fonctions essentielles de l'entreprise. Elle doit être rattachée à la direction générale et son champ d'action doit être la totalité de l'activité de l'établissement. Un système de contrôle de gestion performant doit évaluer la rentabilité des opérations, des produits, des clients et donc des segments de marché.

1.7. Les risques liés à la sécurité

Les entrées du site doivent être protégées et leurs accès limités aux personnes habilitées. À l'intérieur du site pareillement, certains locaux doivent nécessiter une habilitation particulière : salle informatique, salle des archives du personnel et des dossiers clients…

Il doit exister un plan « incendie ».

1.8. Les risques informatiques

Les principaux risques auxquels une entreprise est confrontée avec son système informatique sont : le risque lié à la concentration de l'information, et donc aux problèmes de destruction, de disparition et de confidentialité, le risque lié au coût des équipements et des logiciels, le risque lié à la complexité des systèmes informatiques, demandant des informaticiens une compétence technique de plus en plus grande, le risque lié au fait que la machine effectue les opérations dans leur totalité (autorisation, réalisation et contrôle) sans traces écrites (pistes d'audit), le risque lié à la vulnérabilité des systèmes (intrusions, virus). À ces risques s'ajoutent ceux liés au manque de connaissances en informatique de la part des contrôleurs et des membres de la direction générale.

Le contrôle doit porter sur les aspects de conception (le *built*) et d'exploitation (le *run*).

L'audit interne et le contrôle permanent doivent évaluer la pertinence du système de contrôle interne : les locaux doivent être d'un accès réservé aux personnes autorisées ; les protections incendie doivent être adéquates et l'assurance doit couvrir les dommages

éventuels (machines, logiciels et données) ; les logiciels de base (applicatifs) et les données doivent être conservés dans des armoires ignifugées ; chaque fichier magnétique doit être identifié avec une étiquette interne et externe avec le nom du fichier et la date de dernière mise à jour ; un double des fichiers doit être conservé dans un endroit distant de la salle de l'ordinateur ; à chaque mise à jour ou modification des fichiers, les duplicatas des fichiers doivent également être mis à jour ; un contrat de back-up doit être passé avec une autre société (cf. le développement du cloud) ; une séparation des tâches doit être instaurée entre les études informatiques (études, conception, réalisation), l'exploitation (production) et la saisie des informations.

De plus, les analystes et programmeurs ne doivent avoir accès, ni à la salle d'ordinateur ni aux programmes en exploitation sauf munis d'une autorisation particulière en cas de panne. Leur accès doit être limité au test des applications en cours de réalisation.

Sauf en cas de panne, aucun programme ne doit être modifié sans demande écrite des utilisateurs validée par une personne autorisée. Après chaque modification, la documentation du programme doit être complétée et mise à jour. Les modifications doivent être tracées.

Les nouvelles applications doivent faire l'objet d'une démarche cohérente en quatre phases successives : étude d'opportunité, conception selon un cahier des charges précis (études), réalisation (développement), mise en œuvre (test et réception utilisateurs) et suivi.

En cas de recours à des sous-traitants, une étude sur leur honorabilité et leur pérennité doit être réalisée. Des appels d'offres systématiques doivent être réalisés.

L'accès au système informatique doit être soumis à une série de limitations, pour éviter les usages abusifs ou frauduleux : accès limités aux heures ouvrables, nécessité d'un mot de passe ou d'un code d'accès régulièrement modifiés, supprimés en cas de départ de la personne, mots de passe et terminaux ne donnant accès qu'à certaines fonctions.

L'audit interne et le contrôle permanent doivent enfin contrôler l'environnement des systèmes informatiques : contrôle des mesures essentielles de sécurité, enquête auprès des utilisateurs (adéquation du système par rapport aux besoins, traitement et restitution de l'ensemble des opérations saisies, fiabilité et exhaustivité des informations produites, pertinence des informations produites, utilité des états informatiques produits, système de sauvegarde des mots de passe et habilitations, etc.).

1.9. Les risques relatifs au management

Les principaux risques auxquels une entreprise peut être confrontée au niveau de son management sont que celui-ci soit inadapté aux niveaux de compétence et de motivation de son personnel.

En effet, le niveau de performance d'un collaborateur dépend en grande partie du style de management que son responsable hiérarchique adopte à son égard. S'il n'y a pas de style de management idéal, il y a des styles plus ou moins adaptés aux situations. L'utilisation par le manager du style approprié dans la bonne situation permet une optimisation des efforts produits par ce dernier et garantit la réussite pour le collaborateur. *A contrario*, l'utilisation d'un style moins approprié entraîne une consommation d'énergie supérieure pour le manager et peut aller à l'encontre de la réussite pour le collaborateur.

Les deux facteurs qui permettent de déterminer le style de management à adopter sont le niveau de compétence et le niveau de motivation du collaborateur. La compétence correspond à la capacité à réaliser une tâche spécifique et la motivation correspond au niveau d'engagement à réaliser une tâche spécifique.

Pour chacun des collaborateurs, l'audit interne et le contrôle permanent repèrent, non pas de façon globale, mais tâche par tâche, les niveaux de compétence et de motivation. En fonction de ceux-ci, ils portent un avis sur le style de management utilisé.

Ce modèle de management est développé plus loin dans l'ouvrage (p. 256).

Nous renvoyons par ailleurs le lecteur souhaitant approfondir les aspects de management à notre ouvrage : *Animer une équipe projet avec succès*, Henri-Pierre Maders, Éditions d'Organisation.

2. EXEMPLES DE RISQUES SPÉCIFIQUES

Les risques auxquels l'audit interne et le contrôle permanent peuvent être confrontés sont de natures diverses. Certains sont spécifiques à un secteur d'activité, et nous prendrons comme illustration les risques spécifiques du secteur bancaire, des compagnies de transport aérien et de l'hôpital et, plus précisément, ceux du bloc opératoire ; d'autres concernent un thème transversal et nous prendrons comme illustration les risques relatifs aux ressources humaines ; d'autres enfin sont spécifiques à une activité et nous prendrons comme illustration les risques relatifs à la pratique sportive.

2.1. Les risques spécifiques du secteur bancaire

Les banques sont confrontées à des risques généraux et à des risques spécifiques aux activités qu'elles proposent à leurs clients. Ces risques concernent les emplois, les ressources, les opérations avec l'étranger, les succursales et agences et les opérations de marché.

L'Autorité de contrôle prudentiel et de résolution (ACPR) regroupe la Commission bancaire et l'Autorité de contrôle des assurances et mutuelles depuis le 9 mars 2010. Elle

assure la sécurité des secteurs bancaires et des assurances : agrément des établissements, supervision de leur activité, inspection sur place environ tous les cinq ans, réglementation et mesures disciplinaires le cas échéant. Cette approche « prudentielle » (favoriser le développement de l'activité mais dans des conditions de sécurité satisfaisantes) n'est pas spécifique à la France, Ainsi, elle supervise le dispositif « Bâle-2 » (évolution européenne de la réglementation bancaire destinée à ajuster plus finement le niveau d'activité autorisé pour une banque à son profil de risques et sa surface financière) notamment :

- la validation des modèles internes et du dispositif (agrément) ;
- le reporting des risques (supervision) ;
- le contrôle des fonds propres (supervision).

L'ACPR supervise également le dispositif de contrôle interne. Ce travail se fait par référence à un texte fondateur, le règlement CRBF 97-02 qui pose les grands principes du contrôle interne :

- l'organisation pour le contrôle permanent et le contrôle périodique ;
- le système de contrôle des opérations et des procédures internes ;
- l'organisation comptable et traitement de l'information ;
- les systèmes de mesure des risques et des résultats ;
- les systèmes de surveillance et de maîtrise des risques ;
- le rôle des organes exécutif et délibérant et du régulateur (ACPR) ;
- la continuité d'activité (obligation de disposer d'un PCA).

Le dispositif évolue régulièrement depuis 1997 :

- En 2005 une réforme structurante avec la séparation entre contrôle permanent et contrôle périodique (identification plus claire des niveaux 2 et du niveau 3).
- Entre 2009 et 2010, huit modifications au texte, portant sur le reporting des incidents significatifs, le suivi des actions de correction, la liquidité, la troisième directive européenne sur la lutte anti-blanchiment, la politique de rémunération, la filière risques.

Ce dispositif tient compte également :

- du règlement général de l'AMF pour les activités de prestataires de services d'investissement des banques (réception et transmission d'ordres de bourse, conseil en investissement, voire gestion sous mandat…) ;
- des réglementations applicables aux filiales à l'étranger et aux activités spécialisées et des usages professionnels les plus reconnus.

Le contrôle interne porte sur tous les aspects d'activité de la société et sur tous les risques. Les services de contrôle permanent sont souvent ciblés sur les risques dits

Copyright © 2014 Eyrolles. © Groupe Eyrolles

opérationnels là où les gestionnaires de risques vont mesurer et surveiller les risques relevant de leur zone d'expertise.

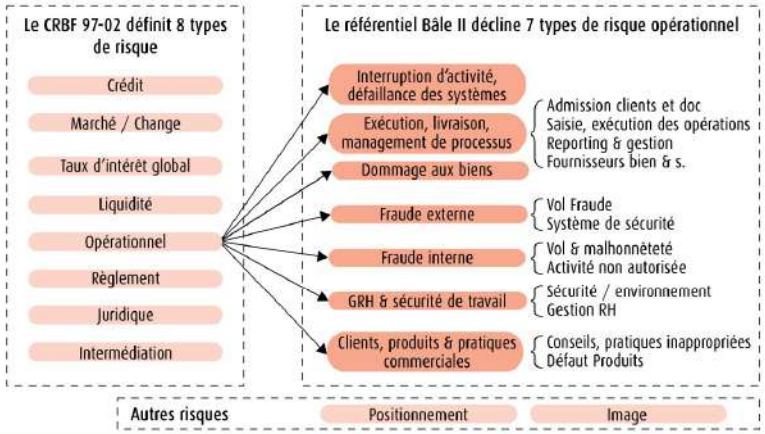
Les autorités européennes bancaires ont bien défini le cadre d'analyse et de surveillance du risque opérationnel.

Le comité de Bâle a défini sept types d'événements de risques :

1. la fraude interne ;
2. la fraude externe ;
3. les pratiques sociales et la sécurité sur le lieu de travail ;
4. les clients, les produits et les pratiques commerciales ;
5. les dommages aux actifs matériels ;
6. l'interruption d'activité et la défaillance de systèmes ;
7. l'exécution, la livraison et la gestion des processus.

Nous renvoyons le lecteur qui souhaiterait approfondir les risques bancaires à notre ouvrage : *Audit opérationnel dans les banques*, Henri-Pierre Maders, Éditions d'Organisation.

Figure 2.1 – Panorama des risques bancaires



2.1.1. Les risques spécifiques concernant les emplois

Le principal risque auquel est confronté un établissement de crédit est le non-remboursement des crédits accordés à ses clients, et ce pour les causes suivantes :

- la défaillance soudaine et non prévisible de certains clients, risque contre lequel il est impossible de se prémunir ;
- une maîtrise des risques insuffisante par une absence de politique générale ;
- une concentration des risques sur quelques clients ou un secteur d'activité ;
- une étude insuffisante des dossiers de crédit ;
- un laxisme dans le système d'autorisation des crédits et dans leur suivi et une faiblesse de la fonction contentieux-recouvrement ;
- une maîtrise administrative insuffisante par une mauvaise organisation, des négligences, notamment dans les prises de garanties et leur suivi, une absence de séparation des tâches, un système informatique défaillant, des applications de conditions non conformes, une protection insuffisante des valeurs et des garanties, des envois en recouvrement tardifs et une faiblesse des systèmes d'information et de contrôle de gestion.

Le contrôle doit porter sur la politique générale, sur la maîtrise des risques ainsi que sur la qualité de l'organisation administrative de l'activité.

La couverture des risques

L'audit interne et le contrôle permanent doivent s'assurer que les fonds propres de la banque sont suffisants pour que la défaillance d'un gros client ne la mette pas en danger.

La division des risques

L'audit interne et le contrôle permanent doivent s'assurer que le portefeuille de la banque est suffisamment diversifié pour que la défaillance d'un client ou d'un groupe de clients, d'un secteur d'activité ou d'une zone géographique ne la mette pas en danger.

La politique générale en matière de crédit

L'audit interne et le contrôle permanent doivent s'assurer que la banque dispose d'une politique générale écrite et d'objectifs précis en matière de crédits, tant en termes de types de clients recherchés que de qualité des risques recherchés.

Le système de délégation

L'audit interne et le contrôle permanent doivent prendre connaissance du système d'autorisations et des procédures de décision de la banque et s'assurer de leur respect : analyse

et présentation des dossiers, prises de garanties, déblocage des crédits, suivi et revue des dossiers.

Par ailleurs, l'audit interne et le contrôle permanent doivent s'assurer que les conditions de taux et de commissions sont clairement définies et appliquées par l'ensemble du personnel de la banque ainsi que par ses dirigeants.

La qualité des dossiers

L'audit interne et le contrôle permanent doivent s'assurer que les dossiers des clients présentent tous les éléments permettant de prendre des décisions d'augmentation, de maintien, de réduction ou de suppression des concours : statuts, pouvoirs, contrats, copie des garanties, analyses financières de la situation du client, informations économiques sur le marché, informations sur les actionnaires et les dirigeants, articles de presse, comptes rendus de visite, mouvements du compte, impayés et note de synthèse lors de l'autorisation de la modification ou du renouvellement du crédit, ainsi que la recommandation motivée de l'auteur.

Une étude des contentieux dans une grande banque française a mis en évidence que plus de la moitié des décisions avaient été prises, non sous la pression d'une contrainte de développement (20 % des cas), ni à la suite d'une erreur dans l'analyse technique (25 % des cas), mais sous l'influence de la relation entre le client et le banquier (55 % des cas).

Étude sur la relation « client-banquier »

Une analyse plus approfondie de l'influence de la relation client-banquier a permis de mettre en évidence dix-sept « syndromes » conduisant à des prises de risques inconsidérées.

- Le syndrome de la pitié : le banquier prend une décision irrationnelle, par ce que le client fait vibrer la corde sensible des sentiments.
- Le syndrome de l'avocat : le banquier se met à la place de son client et estime que son rôle est de le défendre, quitte à oublier les intérêts de la banque.
- Le syndrome des relations extérieures : le banquier prend une décision parce qu'il a confiance, de façon irrationnelle, envers son client qu'il connaît.
- Le syndrome du paon et de l'hôtesse de l'air : le banquier, ne pouvant résister au charme de la cliente, prend une décision irrationnelle.
- Le syndrome de Saint-Tropez : le banquier, impressionné par la poudre aux yeux ou le statut social de son interlocuteur, prend une décision irrationnelle.
- Le syndrome du développement : le banquier cherche à n'importe quel prix à réaliser, voire à dépasser ses objectifs.

.../...

.../...

- Le syndrome de la concurrence : pour ne pas rater une affaire que le client dit faire auprès de la concurrence sauf un accord rapide, le banquier prend la décision.
- Le syndrome du mouton de Panurge : le banquier se laisse influencer par l'annonce vraie ou fausse d'un accord donné par un confrère prestigieux.
- Le syndrome du banquier frileux : pour éviter un dépôt de bilan, de prendre une mauvaise décision, de commettre une erreur...
- Le syndrome de la fuite en avant : le banquier donne un petit coup de pouce de plus à un client afin que ce dernier se rétablisse (peut se terminer en soutien abusif).
- Le syndrome de l'interne du samedi soir : dans un environnement où les défaillances se succèdent, le banquier ne voit plus que des mauvais dossiers, et perd toute référence rationnelle. Il finit, pour faire des affaires, par accepter des dossiers un peu moins mauvais que les autres.
- Le syndrome de l'impuissance : le banquier est tellement engagé qu'il ne peut plus que continuer.
- Le syndrome du balancier : le banquier n'accorde plus de dossier parce que ses risques globaux ont augmenté, puis accorde tous les dossiers parce qu'il est en retard sur ses objectifs (*stop and go*).
- Le syndrome de l'alphabet : le banquier accorde plus de dépassements aux premiers de la liste que vers la fin de celle-ci (effet de série).
- Le syndrome de l'archiviste : le banquier prend ses décisions en se basant sur l'ancienneté de la relation avec le client ou de la qualité du secteur d'activité d'après ses expériences.
- Le syndrome du jugement dernier : le banquier se sent valorisé par la gestion des risques et considère la gestion des risques comme étant l'essentiel de sa fonction : il prend plaisir à mettre ses clients et ses collaborateurs dans l'attente de sa décision.
- Le syndrome de l'ivresse du pouvoir : le banquier a le pouvoir de dire « oui », parfois dans un village dans lequel il habite et est connu.

Le suivi des risques

L'audit interne et le contrôle permanent doivent s'assurer de la qualité du suivi des dossiers de crédit en cours :

- chaque dossier doit être affecté à un responsable ;
- chaque responsable de dossier doit posséder une fiche synthétisant l'ensemble des concours accordés ;
- une surveillance quotidienne des dépassements doit être réalisée ; tout impayé propre à un client ou sur une valeur remise à l'encaissement ou à l'escompte par un client doit être suivi de décisions ;
- les arrêtés de compte mensuels et trimestriels doivent être examinés ;

- les mouvements irréguliers des comptes, les dépassements fréquents, les retraits immédiats après remises et les soldes débiteurs permanents doivent donner lieu à des actions spécifiques ;
- les garanties doivent être suivies régulièrement ;
- les événements susceptibles d'amoindrir leur valeur doivent être identifiés et des garanties de substitution prises si nécessaire ;
- les avis financiers et les articles de presse concernant les clients doivent figurer dans les dossiers client, les dossiers doivent contenir le rapport annuel du client ;
- une revue des prêts doit être réalisée pour tous les clients de la banque au minimum tous les ans, de préférence tous les trois mois.

Le système d'information

L'audit interne et le contrôle permanent doivent évaluer la capacité du système d'information à fournir des informations permettant de mesurer les risques et la rentabilité des crédits :

- la banque doit disposer d'un système de cotation interne mettant en évidence les encours par catégories de risques ;
- la banque doit disposer d'un système de calcul de la rentabilité des crédits, des clients et des segments de clientèle.

Le système informatique

L'audit interne et le contrôle permanent doivent s'assurer que la banque dispose d'un système informatique apte, à partir d'une saisie initiale des caractéristiques de chaque crédit, à réaliser automatiquement toute une série de traitements, à savoir :

- la production des plans d'amortissement et des documents contractuels ;
- la comptabilisation du crédit, des intérêts et des remboursements ;
- la production des statistiques et des états analytiques et synthétiques ;
- le prélèvement automatique des échéances ;
- le calcul et la comptabilisation des intérêts courus permettant la détermination des résultats de la banque ;
- la gestion des encours et la production à la demande ou systématiquement de l'état des encours.

Par ailleurs, le système de contrôle interne doit prévoir une série de sécurités pour interdire la saisie des crédits, de conditions particulières, de prorogations ou de modifications non autorisées.

La séparation des tâches

L'audit interne et le contrôle permanent doivent s'assurer que la banque applique bien une totale séparation des tâches en matière de crédit :

- Autorisation : les crédits doivent être autorisés dans le cadre d'un système de délégation clair et précis. Un dossier adéquat doit être établi.
- Réalisation : la phase de déblocage du crédit doit être placée sous la responsabilité d'une personne ou d'un service dont la tâche est de mettre les fonds à la disposition de l'emprunteur, de comptabiliser et de gérer le crédit. Cette personne ou ce service doit être différent de celui qui a autorisé le crédit. Le contrôleur doit s'assurer que les réalisations sont faites par des personnes ayant une autorisation, que les garanties stipulées dans le contrat sont réelles et que les dossiers sont complets.
- Contrôle : après la réalisation des crédits, ceux-ci doivent être vérifiés par des personnes habilitées, différentes de celles qui les ont traités. Les contrôles doivent porter sur le montant autorisé, les conditions appliquées (taux, commissions et frais), dates de valeur (départ, échéance), échéancier du remboursement du prêt, catégorie de crédit (éligible, non éligible, nature du crédit, durée…), domiciliation pour le remboursement.

Le système comptable

L'audit interne et le contrôle permanent doivent vérifier que le système comptable est apte à satisfaire les besoins de la banque centrale ainsi que les comptes annuels de la banque. Ce système doit en outre permettre une justification permanente des comptes généraux et des comptes auxiliaires. Les principes de comptabilisation doivent être respectés.

La gestion du portefeuille d'escompte

L'audit interne et le contrôle permanent doivent s'assurer que l'ensemble des traitements concernant l'escompte sont sécurisés par le service du Portefeuille :

- Autorisation : à leur arrivée, les effets, accompagnés d'un bordereau de remise à l'escompte, doivent être contrôlés sous l'angle de leur conformité (signature, date, montant, domiciliation, etc.). Le responsable de compte doit ensuite examiner le risque (non-dépassement de la ligne d'escompte, vraisemblance de la remise par rapport à l'activité et à la qualité des tirés, solvabilité du tiré, niveau de concentration par tiré, éventuels « tirages de famille », éventuelles créances fictives, etc.) et décider du paiement total, partiel ou du non-paiement.
- Traitement : les remises sont ensuite saisies informatiquement. Le logiciel de gestion du portefeuille doit permettre le calcul et la perception des agios (intérêts, commissions

et frais), l'édition du bordereau d'escompte, la génération des écritures comptables, la gestion de l'échéancier et de l'inventaire permanent, la gestion des informations utiles aux états réglementaires, le calcul et la comptabilisation des intérêts courus mensuellement, la sortie des effets à l'échéance, la gestion des autorisations d'encours, avec l'édition d'un état d'alerte en cas de dépassement ou d'autorisation échue et la gestion des effets sortis pour acceptation, prorogation ou régularisation.

- Contrôle : les créances saisies doivent être vérifiées *a posteriori* par une personne habilitée, différente de celle qui a exécuté la saisie (conditions appliquées : taux, commissions et frais ; dates de valeur : date de départ et échéances ; catégories de crédit : créances commerciales, crédits exports, crédits de trésorerie, etc. ; domiciliation ; justification des modifications : prorogations, échéances, taux, etc.). Ensuite, le contrôleur s'assurera de la sécurité de conservation des effets et de la réalisation régulière, par la banque, d'un inventaire physique destiné à s'assurer de l'existence des effets. De plus, le contrôleur doit s'assurer que les règles de comptabilisation sont correctes : justification des comptes généraux, classification correcte des créances… Enfin, le contrôleur doit s'assurer que les créances sont encaissées par la banque à bonne date, afin d'éviter toute perte de trésorerie.

La fonction contentieux-recouvrement

L'audit interne et le contrôle permanent doivent s'assurer que la fonction contentieux-recouvrement existe bien dans la banque. Cette fonction doit posséder des procédures spécifiant les relations entre l'exploitation et le contentieux, et plus précisément le moment où le dossier doit être transmis au contentieux.

De plus, la politique de la banque en matière de transferts en créances douteuses doit être claire, de même que la politique en matière de provisions pour créances douteuses et pour risques spécifiques et généraux.

Enfin, régulièrement, les dossiers contentieux doivent être revus pour décider des actions à entreprendre, des provisions à constituer ou à reprendre et de l'annulation des créances et des provisions.

2.1.2. Les risques spécifiques concernant les ressources

Les principaux risques auxquels une banque est confrontée dans son activité de collecte de dépôts de la clientèle sont un risque de liquidité dû à une insuffisance quantitative ou qualitative de ressources rendant la banque dépendante du marché monétaire, ou une mauvaise répartition des dépôts créant une dépendance vis-à-vis des déposants, un coût excessif des ressources ayant des répercussions sur la rentabilité et une gestion administrative et un contrôle interne défaillants entraînant des erreurs, des négligences et des fraudes externes ou internes.

Le contrôle doit porter sur la politique générale, sur la maîtrise des risques ainsi que sur la qualité de l'organisation administrative de l'activité.

La politique en matière de ressources

L'audit interne et le contrôle permanent doivent s'assurer que la banque dispose d'une politique générale concernant les ressources. Cette politique doit se traduire en objectifs permettant l'existence d'une base de dépôts clientèle stable, gage de sécurité et de rentabilité.

La sécurité et la stabilité des dépôts

L'audit interne et le contrôle permanent doivent évaluer le niveau de dépendance de la banque vis-à-vis du marché interbancaire. De plus, ils doivent s'assurer que les ressources ne sont pas trop concentrées sur quelques clients, un segment de marché ou une zone géographique. Enfin, l'auditeur interne et le contrôleur doivent estimer les ressources selon leur durée en évaluant les ressources longues (comptes d'épargne, dépôts à terme, bons de caisse, etc.) rémunérées mais importantes pour la liquidité.

Le système d'information et de contrôle de gestion

L'audit interne et le contrôle permanent doivent évaluer la capacité du système d'information et du contrôle de gestion à fournir la mesure des capitaux moyens des ressources par catégories et par produits, la mesure des coûts par catégories, la mesure de la rentabilité par catégories et la mesure du risque de taux sur les intérêts à payer.

La gestion administrative des comptes

L'audit interne et le contrôle permanent doivent évaluer la rigueur des procédures à différents niveaux :

- Autorisation : à l'ouverture des comptes, les procédures doivent permettre d'éviter les clients non souhaitables, les comptes fictifs et les désagréments et les pertes consécutives, notamment, à la délivrance de chéquiers et de cartes de paiements. Pour ce faire, l'ouverture d'un compte doit être préalablement autorisée par une personne habilitée.
- Réalisation : ensuite, un certain nombre de renseignements doivent être rassemblés et contrôlés : identité, adresse, moralité bancaire, capacité juridique, statuts, pouvoirs, etc., pour les sociétés.
- Contrôle : l'ouverture doit enfin être approuvée par un responsable après examen des documents fournis par le client et de la fiche d'ouverture de compte. L'audit interne et le contrôle permanent doivent évaluer la qualité de la base de données informatique « clients ».

Les ouvertures, les modifications ou les clôtures de compte doivent être effectuées par des personnes habilitées et tout changement doit être contrôlé. Un état informatique listant les mises à jour de la base de données doit être édité régulièrement. L'audit interne et le contrôle permanent doivent s'assurer que chaque client dispose d'un dossier qui contient l'ensemble des documents se rapportant à l'ouverture et à la vie du compte. Ces dossiers doivent être conservés dans un local dont l'accès doit être limité aux personnes habilitées. Les dossiers du personnel doivent être conservés de préférence au service du personnel ou rassemblé dans une agence. L'audit interne et le contrôle permanent doivent porter une attention particulière aux arrêtés de comptes. Ils doivent s'assurer que les intérêts créditeurs et débiteurs concernant les comptes d'épargne et les comptes de dépôt sont bien calculés. Seule une personne habilitée peut effectuer des corrections, des réductions ou des suppressions d'agios, et ce dans des limites qui doivent être précisées et contrôlées.

La communication avec les clients

L'audit interne et le contrôle permanent doivent s'assurer que les courriers à destination des clients sont envoyés par un service indépendant de l'exploitation ou des services de production. Les lettres de réclamation doivent être transmises à la direction de l'audit pour enregistrement et traitement.

La surveillance des comptes à risques

Certaines catégories de comptes présentent des risques particuliers. L'audit interne et le contrôle permanent doivent les analyser systématiquement. Concernant les comptes dormants qui sont des comptes qui n'enregistrent aucun mouvement pendant une durée d'au moins six mois, ils doivent s'assurer que la banque a procédé au blocage du compte, ce qui interdit toute opération.

Par ailleurs, la banque doit disposer d'un état d'alerte signifiant toute opération passée ce délai. Les opérations enregistrées dans les comptes du personnel doivent être examinées régulièrement, et plus précisément ceux des agents présentant un train de vie anormalement élevé, structurellement débiteurs, en place depuis une durée très longue ou ne partant jamais en vacances.

Les opérations effectuées sur les comptes de succession doivent être surveillées comme pour les comptes dormants.

Les comptes de passage, ouverts pour des clients de passage et pour une opération particulière, peuvent servir à des opérations irrégulières, illégales ou frauduleuses. Ces comptes doivent être justifiés régulièrement.

Les ressources à terme

Concernant les ressources à terme, l'audit interne et le contrôle permanent doivent vérifier la qualité et l'application des procédures. Les taux appliqués doivent correspondre à ceux fixés par la direction de la banque. Les taux pratiqués doivent tenir compte du montant et de la durée (plus la somme est importante, plus la durée est longue et plus le taux d'intérêt doit être élevé). L'audit interne et le contrôle permanent doivent vérifier que ce principe est appliqué et que les clients bénéficiant de conditions particulières les ont obtenues de personnes habilitées et contrôlées.

Des dates rétroactives ne doivent en aucun cas être appliquées.

Le stock physique de bons de caisse doit correspondre au stock comptable. La procédure de remboursement des bons anonymes doit permettre d'éviter tout remboursement auprès de porteurs illégitimes ou sur des bons contrefaits.

Les remboursements anticipés doivent comporter des pénalités qui doivent être précisées sur les contrats, de même que les avances consenties sur les remboursements de comptes à terme et de bons de caisse.

Les comptes sur livrets d'épargne

L'audit interne et le contrôle permanent doivent vérifier la concordance entre le solde comptable et les soldes portés sur les livrets.

2.1.3. Les risques spécifiques concernant les opérations avec l'étranger

Les principaux risques auxquels une banque est confrontée dans ses opérations avec l'étranger sont les risques liés aux opérations de crédit, les risques pays, les risques de change, les risques de contrepartie, les risques administratifs et le risque de fraude.

Le contrôle doit porter sur la qualité des procédures et la compétence du personnel, qui doit être apte à maîtriser des procédures complexes dans un contexte très réglementé.

L'audit interne et le contrôle permanent doivent porter leur attention sur cinq types d'opération. Pour chacune d'entre elles, ils doivent s'assurer de la qualité des procédures, de l'existence d'un recueil des signatures autorisées, de la confidentialité des clés télégraphiques, de l'existence d'une parfaite séparation des pouvoirs et du respect de la réglementation.

Transferts et rapatriements

Les transferts et rapatriements s'effectuent par télex, swift, chèque ou ordre de paiement « papier ». L'audit interne et le contrôle permanent doivent s'assurer que les transferts sont autorisés par une personne habilitée, dans le respect de la réglementation des

changes. Les ordres de transfert reçus par les correspondants doivent être authentifiés avant d'être exécutés (clés télégraphiques, recueil des signatures autorisées).

Encaissements documentaires

Les encaissements documentaires sont des transferts accompagnés de documents (factures, titres de transport, assurance, certificat d'origine, etc.).

Le rôle de la banque correspond à un mandat qui consiste à présenter des documents, à les encaisser et à transférer des fonds. L'audit interne et le contrôle permanent doivent s'assurer de la rigueur des procédures et du respect de la réglementation sur les changes.

À l'export, l'exportateur confie ses documents à sa banque. Celle-ci les envoie à son correspondant et, dès réception des fonds, met ceux-ci à la disposition de son client exportateur sous déduction de ses frais et commissions.

À l'import, la banque reçoit de son correspondant la traite accompagnée des documents. Elle avise son client et, dès son accord, règle le correspondant, sous déduction éventuelle de ses frais et de ses commissions.

Crédits documentaires

Les crédits documentaires, opérations complexes comptabilisées en hors-bilan, doivent être traités par un personnel très expérimenté et contrôlé régulièrement par l'audit interne et le contrôle permanent. Un importateur (donneur d'ordre) donne l'ordre à sa banque d'ouvrir un crédit à un fournisseur par le biais de son correspondant étranger (banque notificatrice). Ce crédit est un engagement par signature, par lequel la banque émettrice prend l'engagement de payer (réalisation contre paiement) ou d'accepter de payer (réalisation contre acceptation) la banque notificatrice si celle-ci fournit les documents et respecte les conditions spécifiées dans l'ouverture de crédit documentaire. La banque émettrice ouvrira un crédit par l'intermédiaire de son correspondant (banque notificatrice). La banque notificatrice signera le crédit auprès de son client exportateur ou de la banque de l'exportateur. Elle peut ajouter sa confirmation. La confirmation ajoutée au crédit documentaire engage la banque notificatrice à payer l'exportateur, même en cas de défaillance de la banque émettrice, à la seule condition que les documents stipulés dans les termes de l'ouverture de crédit soient respectés par l'exportateur.

Cautions

Les cautions sont données par la banque sur ordre de ses clients. Elles peuvent concerner les douanes, porter sur l'achèvement de travaux, etc. La banque encaisse en contrepartie des commissions, ce dont doit s'assurer l'audit interne et le contrôle permanent.

Crédits par caisse

Les crédits par caisse, préfinancement export, mobilisation de créances nées sur l'étranger, avances en devises, avances sur marchandises, crédits acheteurs ou fournisseurs sont elles aussi des opérations complexes qui donnent lieu à intérêts et à commissions, ce dont doit s'assurer également l'audit interne et le contrôle permanent.

2.1.4. Les engagements par signature

Le risque principal auquel une banque est confrontée dans ses engagements par signature est de ne pas comptabiliser l'intégralité des opérations impliquant son engagement. Il peut donc s'ensuivre une mauvaise évaluation de la situation réelle de l'établissement quant à l'étendue de ses risques.

Le contrôle doit porter sur l'évaluation de l'ensemble des engagements de la banque.

L'audit interne et le contrôle permanent doivent s'assurer que la banque dispose d'un système de comptabilisation des engagements par signature. Cette comptabilisation doit cerner de façon exhaustive l'ensemble des engagements de la banque. Pareillement, les engagements reçus d'autres établissements doivent être comptabilisés avec le même souci d'exhaustivité.

Les engagements en devises doivent être réévalués conformément aux dispositions réglementaires. Tout engagement par signature doit faire l'objet d'une autorisation préalable.

En cas de contentieux, les provisions correspondantes doivent être constituées. Les procédures doivent s'assurer que l'intégralité des commissions a été perçue.

2.1.5. Les succursales et les agences

Les risques auxquels une banque est confrontée avec ses succursales et ses agences sont les mêmes que pour la banque dans sa globalité, ce n'est que l'échelle qui change. Cependant, certains risques, liés à l'éloignement géographique, sont spécifiques aux succursales, par exemple, la non-application de la politique générale et la mauvaise application des procédures et fourniture au siège d'informations incomplètes ou non fiables.

Le contrôle doit porter sur l'application de la politique générale, sur la maîtrise des risques ainsi que sur la qualité de l'organisation administrative de l'activité.

L'audit interne et le contrôle permanent doivent s'assurer que la politique commerciale de la banque est connue et appliquée correctement. À ce titre, une évaluation doit être faite sur les résultats de la succursale par rapport à son marché local, et par comparaison avec les autres succursales de la banque. L'application des procédures de travail doit être vérifiée, notamment en ce qui concerne le système de délégation, la séparation des fonctions, la conservation des informations et la qualité de l'information fournie aux clients. Un contrôle des existants doit être réalisé en ce qui concerne les espèces, les valeurs et les

moyens de paiement. Les risques concernant le portefeuille de crédits en cours doivent être évalués puis comparés aux informations transmises au siège de la banque.

2.1.6. Les opérations de marché

« Derrière tout employé de banque, il y a un fraudeur en puissance. Et pourquoi les employés de banque fraudent-ils ? À cause des femmes et du jeu. » Cette grande vérité fut pendant longtemps transmise d'inspecteur confirmé à inspecteur stagiaire au sein d'un grand groupe bancaire mutualiste français… et c'est vrai, il arrive que des collaborateurs fraudent, parfois seuls, parfois à plusieurs, et parfois même avec la complicité de clients…

Cependant, avec le développement des technologies de l'information et des corps de contrôle, il est de plus en plus difficile de frauder. Par ailleurs, il est également de plus en plus difficile d'utiliser le produit de son larcin sans éveiller des soupçons.

Par contre, certains collaborateurs de banque peuvent engager leur entreprise dans des opérations risquées en détournant les procédures en place, et, parce qu'ils peuvent faire dans un premier temps de bonnes affaires et faire gagner beaucoup d'argent à leur entreprise, bénéficier de la complicité implicite de leur encadrement. Cela est notamment le cas en ce qui concerne les opérations de marché.

En droit français, la fraude en matière civile ne se démarque guère de la fraude pénale. Il s'agit d'un acte qui a été réalisé en utilisant des moyens déloyaux destinés à surprendre un consentement, à obtenir un avantage matériel ou moral indu ou réalisé avec l'intention d'échapper à l'exécution des lois. Le risque de fraude est généralement assimilé à un risque opérationnel et rentre dans le périmètre de l'audit interne et du contrôle permanent.

Il se répartit selon les catégories bâloises entre :

- La fraude interne : pertes dues à des actes volontaires pour frauder, s'approprier un bien ou contourner une règle légale ou une règle ou une politique de la société (sauf événements discriminatoires) qui impliquent au moins une personne interne à l'entreprise.
- La fraude externe : pertes dues à des actes volontaires pour frauder, s'approprier un bien ou contourner une règle légale par un tiers.

Les causes peuvent provenir de trois facteurs connus également sous le nom de « triangle de la fraude », théorie développée dans les années 1960 par un sociologue américain, Donald Cressey :

- Les pressions externes (provenant de la part des investisseurs, prêteurs…) ou internes (objectifs à atteindre dans un contexte de pression extrême : évolution du cours de bourse, niveau de résultat, de marge…), renforcées par des dispositifs de rémunération, dépendant de la réalisation d'objectifs individuels (recherche de réussite sociale et de reconnaissance, montrer qu'on est le plus fort, appât du gain, goût du jeu…) pour des personnes en position de contourner les contrôles.
- L'opportunité pour frauder (à la moindre réduction des contrôles internes ou de la gestion des risques, des occasions de fraude peuvent apparaître) par défaut de contrôle interne et externe (autorités de contrôle) de façon permanente et également lors de situations souvent non couvertes par les contrôles et très courantes : périodes de changement de système d'information, d'acquisition ou de lancement de nouvelles activités et/ou produits, de carences de personnel…
- Une rationalisation de l'acte par le fraudeur qui lui permet de le rendre acceptable par ses valeurs (un manque de reconnaissance, une promotion manquée…).

Les spécificités de ce type risque

- Certains indicateurs de fraude relevant de la vie personnelle (problèmes de dépendance, pertes financières…), le risque de fraude est parfois difficile à détecter *a priori;* les ressources humaines possèdent à ce titre un rôle important dans la prévention des fraudes.
- Le dispositif de maîtrise des risques de fraude passe par un ensemble de dispositifs (dispositif d'alerte, enquêtes, outils informatiques…).
- Dans un environnement de crise, les trois facteurs du triangle de la fraude (voir tableau 2.1) sont d'autant plus renforcés : les pressions deviennent plus fortes, les opportunités plus nombreuses suite à une réduction des contrôles internes, la rationalisation plus forte en cas de conflits sociaux.

EN PRATIQUE

Bien que les fraudes soient souvent dénoncées par une tierce personne, les mesures de prévention classiques correspondant à des « fondamentaux » en matière de dispositif de contrôle interne doivent permette d'en déjouer le plus grand nombre, même si les fraudeurs ont souvent un temps d'avance et que « l'occasion fait le larron » :

- sensibilisation du personnel au risque de fraude par des formations et la diffusion d'un code de conduite et sanctions immédiates en cas de non-respect des règles ;
- séparation des fonctions (salles de marché : *front office*, *middle office* et *back office* rattachés à des directions différentes) et procédures explicites ;
- rotation du personnel sensible (traders et aussi chefs d'agence, chargés de clientèle, acheteurs, auditeurs…) ;

Copyright © 2014 Eyrolles. © Groupe Eyrolles

- tests à l'embauche des personnes occupant des fonctions sensibles et suivi permanent de leur résultat, comportement, train de vie... ;
- diagnostic régulier des risques de fraude sur la base de scénarios et de séances de *brainstorming* au sein des différentes entités ou fonctions et diagnostic de la couverture correcte des risques et mise en œuvre de mesures complémentaires ;
- mise en œuvre de contrôles informatiques permettant d'analyser les transactions inhabituelles.

Tableau 2.1 – Le « triangle de la fraude »

	Triangle de la fraude		
	Pressions	**Opportunités**	**Rationalisation**
Cas Madoff	Rémunération liée aux performances, pression des investisseurs	Dysfonctionnement du processus de contrôle de la part des autorités de tutelle (SEC)	Volonté d'être reconnu pour ses qualités d'investisseur n'étant pas issu du sérail
Cas Kerviel	Rémunération liée aux performances, pressions pour améliorer le rendement des opérations	Dysfonctionnement dans le processus de contrôle interne et dans la chaîne hiérarchique de contrôle	Volonté d'être reconnu pour ses qualités de trader
Cas Nick Leeson	Obligation de rattraper les erreurs commises et améliorer les performances financières de son agence	Liberté de mouvement sans réel contrôle	Volonté d'être reconnu pour ses qualités de trader

Certains comportements peuvent mettre en péril une banque. D'autres comportements peuvent risquer de provoquer la crise du système bancaire tout entier...

Le *hedge fund* Long Term Capital Management

Long Term Capital Management est un *hedge fund* apparu en 1994 et dont la quasi-faillite en 1998 fit courir un risque majeur au système bancaire international et créa des perturbations importantes sur les marchés financiers. Son fondateur était John Meriwether, célèbre responsable de l'arbitrage, puis de l'ensemble du *trading* de taux d'intérêt pour la banque Salomon Brothers, qu'il avait dû quitter peu après une manipulation de marché trop visible de l'un de ses traders. En fondant LTCM, il souhaitait reformer « l'arbitrage group » de Salomon et répliquer ses stratégies. Il débaucha la quasi-totalité de ses anciennes équipes.

L'objectif principal du fonds consistait à profiter des opportunités d'arbitrage sur les marchés de taux d'intérêt grâce à une approche purement quantitative et mathématique. Deux futurs lauréats du Prix Nobel d'économie (Myron Scholes et Robert Merton), déjà consultants chez Salomon, faisaient partie des associés. Un vice-président en exercice de la banque centrale américaine, David Mullins, démissionna pour venir les rejoindre. La quasi-totalité des grandes banques d'investissements participèrent au tour de table initial et ceux qui avaient d'abord refusé s'empresseront de les rejoindre lorsque les premiers succès du fonds seront avérés. La réputation académique de M. Scholes et R. Merton permit de convaincre les plus réticents. On comptera même la banque centrale d'Italie parmi les investisseurs du fonds. La convergence des marchés obligataires de la future zone euro vers l'union monétaire de janvier 1999 fournit tout d'abord des profits aisés et conséquents à LTCM grâce à des effets de levier très importants. Le fonds cultivait le secret sur ses méthodes et ses positions, mais les traders de LTCM, presque tous passés entre les mains du professeur Robert Merton à l'université, étaient considérés comme des génies des mathématiques financières et leurs modèles semblaient pouvoir les faire gagner à tous les coups.

En 1998, le *hedge fund* fut victime de l'avidité et de la démesure de ses dirigeants. Il disposait alors, à l'insu de tous, de positions tout à fait inouïes, inimaginables pour l'époque, qui représentaient plus de 1 200 milliards de dollars, soit l'équivalent du PIB de la France au début des années 1990. Après la crise asiatique de 1997, LTCM paria sur un retour à la normale des taux obligataires pour la fin 1998, mais la crise asiatique se propagea vers la Russie. À la fin de l'été 1998, le défaut de la Fédération de Russie, lors de la crise financière russe de 1998, provoqua un nouveau choc sur les marchés obligataires qui allaient à l'exact opposé des anticipations de LTCM qui vit, en quelques jours, son capital détruit presque instantanément.

Le 23 septembre 1998, LTCM était au bord de la faillite. Le président de la banque fédérale de New York, William J. McDonough (père du ratio McDonough) réunit les patrons des grandes banques d'affaires de Wall Street et de quelques banques européennes et les obligea à recapitaliser en catastrophe le fonds afin d'éviter ce qu'il percevait comme un risque d'éclatement du système financier international. Exposées au risque de contrepartie, les principales banques d'investissement dont le fonds était client reprirent donc le fonds (à l'exception notable de Bear Stearns, qui refusa de participer au tour de table) pour lui laisser le temps de déboucler ses positions. Pendant plusieurs mois, on assista à des mini-chocs, tel jour sur les marchés obligataires, tel autre jour sur les marchés de changes, à mesure que les positions de LTCM étaient dénouées les unes après les autres. La crise systémique fut évitée, mais les marchés financiers mettront quelques mois avant de retrouver leur calme.

Source : http://fr.wikipedia.org/wiki/Long_Term_Capital_Management
(texte sous Licence Creative Commons CC BY-SA 3.0).

2.2. Les risques spécifiques des compagnies de transport aérien

Les compagnies de transport aérien sont confrontées à des risques généraux et également à des risques spécifiques à leur activité. La liste qui suit en présente les principaux pour une compagnie de transport européenne.

- Caractère saisonnier et caractère cyclique de l'industrie du transport aérien.
- Attentats, menaces d'attentats, instabilité géopolitique, épidémies ou menaces d'épidémies.
- Évolution des réglementations et législations internationales, nationales ou régionales.
- Perte de créneaux horaires ou non-accès à des créneaux horaires.
- Règles de compensation du consommateur.
- Environnement.
- Prix du pétrole.
- Événements naturels entraînant des situations exceptionnelles, intoxication alimentaire, accident aérien.
- Défaut d'un système informatique crucial et risques informatiques.
- Non-respect des règles de concurrence.
- Examen par les autorités de régulation des accords de coopération commerciale entre transporteurs.
- Engagements pris par la compagnie vis-à-vis de la Commission européenne.
- Concurrence des autres transporteurs aériens et des transporteurs ferroviaires.
- Financement.
- Négociation des accords collectifs et conflits sociaux.
- Plans de retraite.
- Utilisation de prestations de tiers.
- Assurance.
- Juridique et procédures judiciaires d'arbitrage.
- Marché : change, taux d'intérêt, carburant, liquidité, financement et placement.

2.3. Les risques médicaux spécifiques au bloc opératoire

Les risques spécifiques au bloc opératoire concernent tout d'abord les personnes qui y passent le plus de temps : chirurgiens, anesthésistes, infirmiers, aides-soignants, brancardiers… et naturellement les patients.

2.3.1. Les risques « patient »

Une opération chirurgicale demande qu'un grand nombre de risques soient mis sous contrôle afin que tout se passe au mieux pour le patient… En effet, même si le risque patient dépend fortement de l'état physiologique de santé du patient en dehors de l'affection motivant l'intervention, il dépend également d'autres facteurs de risques.

Tableau 2.2 – Principaux risques « patient »

Risques à l'arrivée du patient	Contrôle de l'identité et du dossier (ex. : le patient va être opéré du côté droit alors qu'il aurait dû l'être du côté gauche). Transfert sur le plateau mobile de la table d'opération ou sur le brancard et acheminement vers la salle d'opération.
Risques d'induction de l'anesthésie.	Mise en œuvre de l'anesthésie.
Risques relatifs à l'acte opératoire	Contrôle de l'anesthésie. Positionnement opératoire. Préparation cutanée. Drapage : pose des champs. Installation de l'instrumentation et branchement du matériel. Intervention chirurgicale à proprement parler et de ses éventuelles complications : ■ complication grave imputable à l'anesthésie ; ■ chirurgie : évolution des lésions, importance du délabrement tissulaire, localisation, caractère hémorragique de l'intervention et durée (à ce titre, la chirurgie en urgence présente 10 fois plus de mortalité et 3 fois plus d'accidents que la chirurgie réglée) ; ■ infection ; Arrêt de l'anesthésie.
Risques lors de la surveillance postopératoire	Transfert du patient en salle de surveillance postopératoire. Installation : documentation, branchements pour le réveil. Surveillance : réveil, extubation, drains, détresse psychologique. Validation de sortie.

2.3.2. Les risques professionnels

Les personnels intervenant au bloc opératoire sont concernés par des risques de différentes natures : manutentions de charges ou de patients, risques biologiques, chimiques, psychosociaux et sociaux, risques de chute.

Tableau 2.3 – Principaux risque du personnel hospitalier « bloc opératoire »

Risques liés aux manutentions manuelles de charge ou patients	Manutentions de charges lourdes et/ou encombrantes. Manutentions répétitives ou à cadence élevée. Manutentions de patients. Manutentions entraînant des postures contraignantes (dos courbe, charge éloignée du corps...).
Risques biologiques	Par contact avec du sang ou autre liquide biologique Par piqûre/coupure. Par projection.
Risques chimiques	Liés à l'utilisation de produits toxiques (glutaraldehyde, gaz et vapeurs anesthésiques...). Liés à l'utilisation de produits nocifs ou irritants (latex...).
Risques de chute	Sols glissants.
Risques psychologiques et sociaux	Confrontation avec la souffrance et/ou la mort. Risques entre professionnels : agression verbale, harcèlement.

2.3.4. Les risques organisationnels et management

Ils sont également nombreux et de différentes natures et concernent :

- la planification et la programmation ;
- les ressources humaines (répartition du travail, composition des équipes, stress, fatigue, vigilance, habitudes, soumission à l'autorité du chirurgien…) ;
- les matériels (conception de la salle, disponibilité des matériels…) ;
- la communication (procédures, information, langages professionnels, nationalités différentes…).

2.3.5. Les risques environnementaux et techniques

Ils recouvrent la qualité de l'air, la qualité de l'eau, l'alimentation électrique, la sécurité incendie, les gaz à usage médical, les dispositifs médicaux (équipement pour l'anesthésie, table opératoire, bistouri, colonne vidéo, lasers, pompes pour la circulation sanguine extracorporelle, petits dispositifs à usage unique ou réutilisable comme les sondes d'intubation, l'instrumentation chirurgicale…), les déchets et linges.

2.4. Les risques transversaux relatifs aux ressources humaines

En matière de ressources humaines, quelle que soit l'entreprise en question, la liste est longue. En voici quelques-uns.

2.4.1. Les différences culturelles

Citons d'abord les valeurs culturelles du personnel établies selon le modèle de Geert Hofstede (distance hiérarchique, c'est-à-dire degré de soumission à l'autorité ; niveau de besoin de contrôle de l'incertitude ; degré d'individualisme ; degré de différenciation des rôles entre les sexes). Les spécificités culturelles du pays dans lequel est localisée l'entreprise influencent également le rôle de l'auditeur interne et du contrôleur permanent. Elles sont au nombre de quatre :

- La distance hiérarchique : si l'inégalité entre les individus est une constante de l'histoire de l'humanité, il apparaît que, dans certaines cultures, celle-ci soit acceptée, ou plutôt combattue. Lorsque les individus acceptent les inégalités, la culture est alors qualifiée de distance élevée et, dans le cas inverse, de faible.
- Le contrôle de l'incertitude : nous vivons dans l'incertitude de ce qui va arriver et en sommes parfaitement conscients. Ce phénomène créé chez l'homme une anxiété souvent intolérable. Les sociétés à fort besoin de contrôle de l'incertitude disposent d'institutions qui cherchent la stabilité, la sécurité et l'évitement de tout risque. Sur un plan général, on peut dire que l'acceptation de l'incertitude génère un comportement de liberté, alors que son refus, un comportement totalitaire.
- L'individualisme : les hommes n'ont pas la même manière de vivre ensemble selon les peuples. Les sociétés communautaires valorisent le temps passé pour le groupe alors que les sociétés individualistes valorisent le temps passé, chez les individus, pour leur vie personnelle.
- La répartition des rôles entre les sexes : elle n'est pas la même pour tous les peuples. À la base se trouvent des faits biologiques : les femmes portent les enfants, puis les nourrissent. Pour cette raison, elles continuent à les soigner et les élever, vivre et travailler avec eux. Les hommes, quant à eux, dans les cultures primitives, s'occupent généralement de la chasse et de la guerre. De cette structure biologique, découle chez certaines sociétés une structure sociale dans laquelle la femme assure les travaux domestiques, pendant que l'homme s'affaire à des travaux économiques, voire politiques. Dans certaines sociétés, les rôles sont différenciés, et dans d'autres, interchangeables.

2.4.2 Le choc des générations

L'existence de plusieurs générations de collaborateurs dans les entreprises est une source de complexité pour l'exercice des métiers d'auditeur interne et de contrôleur permanent.

Pour les générations précédent les générations X et Y, le niveau de confiance entre le salarié et son employeur sont élevés, bien que les conflits soient permanents. Les salariés sont loyaux (sens du devoir) et les employeurs paternalistes. Le projet de vie

s'apparente au projet professionnel qui est l'élément central. Réussir dans la vie professionnelle est ce qui compte le plus.

Pour les générations X et Y en revanche, le niveau de confiance entre le salarié et son employeur est faible, et ce dernier est moins attaché à l'entreprise qu'à son projet de vie personnel, projet de vie dont la partie professionnelle n'est que l'une des parties, et non plus la partie essentielle. Réussir sa vie devient alors ce qui compte le plus…

Citons enfin la diversité du personnel (âge : plusieurs générations peuvent cohabiter dans l'entreprise ; expérience : des autodidactes peuvent côtoyer des surdiplômés ; origines : milieu social d'origine, religion, zone géographique, ethnique…).

2.4.3. Autres risques RH

- Non-fidélité des collaborateurs (*turnover*).
- Malversation, détournement, abus de bien social…
- Harcèlement sexuel et moral.
- Manque de clarté sur les rôles respectifs et la chaîne de commandement.
- Résistances au changement, au conservatisme.
- Problème de communication.
- Compétence des collaborateurs (connaissances, savoir-faire, comportement).
- Motivation des collaborateurs.
- Rareté de la main-d'œuvre.

2.5. Les risques relatifs à la pratique sportive

L'entraînement sportif intensif n'est pas toujours le meilleur ami de la santé. Athlètes de haut niveau ou joggers du dimanche, les sportifs s'exposent à de nombreux risques, parfois mortels. Claquages, élongations, hernies discales, entorses, usure des articulations, tous ces ennuis de santé sont bien connus des sportifs. Et la liste est longue. Parfois même, l'effort physique peut être fatal : entre 1 000 et 1 500 sportifs décèdent ainsi brutalement chaque année.

Prenons quelques exemples tirés notamment d'une étude de l'INSERM de 2008 :

- La natation génère de fréquentes tendinites de l'épaule (jusqu'à 21 % de l'ensemble des blessures dans certaines études), pouvant conduire des champions et championnes olympiques à arrêter l'activité.
- La pratique du cyclisme est responsable de fréquentes tendinopathies au niveau du genou (13 pour 100 000 kilomètres parcourus).

- La course à pied provoque des syndromes rotuliens, des tendinites du genou et de la cheville et des fractures de fatigue responsables de 8 % à 20 % des blessures selon les études, contre 1 % en moyenne pour les autres sports.
- La plongée subaquatique génère des accidents de décompression et/ou des surpressions pulmonaires (1 cas toutes les 10 000 plongées environ).

En général, les sportifs de haut niveau sont conscients de ces risques et les acceptent pour gagner de l'argent et des médailles. Ceci explique les nombreux cas de dopage mis en lumière (citons le désolant exemple du cycliste Lance Armstrong, porté aux nues pendant des années, suspecté, jurant ses grands dieux qu'il était innocent, puis effectuant son *mea culpa* et jeté aux orties par les mêmes qui l'avaient adoré), tout en sachant qu'ils ne sont que la partie visible de l'iceberg. En effet, le dopage existe dans le sport depuis la création des compétitions sportives, au temps de la Grèce antique…

Le danger existe aussi dans le sport de loisir. La plupart des Français choisissent de faire du sport pour leur bien-être, en croyant que cela va les aider à garder la forme. Mais l'entraînement se termine parfois à l'hôpital. Le risque de crise cardiaque serait par exemple sept fois plus élevé au cours d'une pratique sportive qu'au repos. De quoi adopter le célèbre adage de Winston Churchill à qui un journaliste demandait le secret de sa longévité et à qui il répondit : *No sport* !…

Les risques psychologiques sont enfin présents dans le sport. Une pratique trop intensive peut rendre les sportifs plus anxieux et plus fragiles. Et une pratique trop fréquente peut même conduire à l'addiction, comme l'alcool ou le tabac… Des travaux récents ont estimé à 4 % environ, dans la population sportive générale, la proportion de sujets susceptibles de « glisser » vers l'addiction. Une addiction dépendant du type de sport, du niveau de pratique, de l'environnement sociofamilial sachant que les hommes sont plus concernés par le phénomène d'addiction. Le niveau de pratique, l'environnement sociofamilial ou la recherche de sensations amplifient ou limitent cette vulnérabilité. Les sports les plus concernés sont la course de fond, le marathon et le body-building, plutôt pratiqué par les hommes.

PAROLE D'EXPERT

Lawrence B. Sawyer, premier commandement : connaître les objectifs

« Connaître la mission, le but, la "raison d'être". De quelque façon qu'on le dise et quelle que soit la langue que l'on emploie, la première étape, pour l'inspecteur moderne, consiste à connaître l'objectif de la société, du secteur, du département, de l'activité ou de la fonction qu'il contrôle. Je ne veux pas dire par là les rapports publiés sur les fonctions et les responsabilités, ce ne sont souvent guère plus que des déclarations avantageuses, de l'étalage, de l'esbroufe, des boniments de vendeur, je veux dire le véritable objectif. L'objectif du service "Comptabilité fournisseurs" n'est pas uniquement d'effectuer des paiements à des fournisseurs. Cela n'est que l'objectif apparent. L'objectif réel est beaucoup plus large, s'il consiste à remplir la mission que le président de la société a à l'esprit. Je vois l'objectif du service "Comptabilité fournisseurs" comme le fait d'autoriser les paiements aux créanciers lorsqu'ils sont dus, pour ce qui a été réellement effectué ou livré, tout en veillant à conserver le maximum de trésorerie. Comment peut-on comparer cela à "effectuer des paiements à des fournisseurs". Eh bien, selon les véritables objectifs, l'inspecteur verra le service "Comptabilité fournisseurs" sous un jour différent. Il pourrait alors se demander pourquoi les opérations à payer nécessitent chacune une facture spécifique de la part des fournisseurs en ce qui concerne des opérations de routine. Est-ce que le "paiement de ce qui est dû" ne nécessite pas seulement la preuve de l'accord, un ordre d'achat par exemple, et la preuve de la réception effective des services et des produits ? Cela évite d'avoir à faire le rapprochement entre trois documents et n'en nécessite que deux. Actuellement, de nombreuses sociétés procèdent ainsi. De même, du point de vue de l'objectif consistant à ne payer que ce qui est dû, l'inspecteur cherchera à savoir si tout ce qui est réglé est réellement dû. De nombreux paiements ne sont pas justifiés par la réception de mémorandums, parce qu'ils peuvent couvrir des services. Ces paiements nécessitent l'autorisation de la Direction. L'inspecteur cherchera à savoir comment celui qui donne les autorisations de règlement s'assure que le service a bien été rendu avant d'approuver la facture, ou si ce dernier signe uniquement pour la forme, sans vraiment savoir ce qu'il autorise. En ce qui concerne le paiement de ce qui est dû, l'inspecteur voudra savoir selon quel processus on s'assure que les paiements seront effectués à temps pour bénéficier des remises, mais pas trop tôt pour que la trésorerie n'en soit pas affectée. En ce qui concerne la conservation des fonds, l'inspecteur voudra savoir si le personnel du service "Comptabilité fournisseurs" refuse les ordres de change qui augmentent le prix des ordres d'achat sans autorisation à haut niveau. Et si la règle en matière d'achat ne prévoit pas d'autorisation à un niveau suffisamment élevé, la Direction du service "Comptabilité fournisseurs" devra transmettre l'affaire à un dirigeant de la société pour que le problème soit traité. Il voudra savoir ce que le service "Comptabilité fournisseurs" fait en ce qui concerne le paiement du matériel reçu bien avant qu'il soit nécessaire. Qui contrôle les réceptions ? Qui les approuve ? Sur quelles bases ? Lorsque l'on connaît les véritables objectifs, l'inspection peut, d'une simple vérification de documents, devenir de l'inspection moderne. »

TÉMOIGNAGE

Françoise Chassard, responsable risques et conformité, Caisse des dépôts

Le contrôle permanent, ou contrôle interne, est une fonction encore méconnue au sein des entreprises. Mise en place par la direction générale, cette fonction a pour objectif de fournir une assurance raisonnable quant à la réalisation et à l'optimisation des opérations, la fiabilité des informations financières et la conformité aux lois et aux réglementations en vigueur.

En termes d'organisation, à la Caisse des dépôts, le contrôle permanent du groupe est rattaché directement à la direction générale et s'appuie sur un réseau dédié. En effet, la fonction est déployée dans l'ensemble des directions opérationnelles et des filiales à travers un réseau des responsables risques. Pour assurer leur mission, les responsables risques sont des acteurs hiérarchiquement indépendants des activités opérationnelles. Ils ont en charge de relayer la stratégie groupe en matière de réduction des risques opérationnels et de superviser la conformité de l'activité au sein de leur entité. Les bénéfices attendus se situent sur plusieurs plans : sur le plan réglementaire tout d'abord, mais aussi sur le plan économique et financier par la réduction des pertes liées aux risques opérationnels grâce à la mise en place de contrôles, et enfin sur le plan de l'organisation, en améliorant la qualité des processus de décision et en développant la vigilance des collaborateurs. La démarche se structure autour des principaux outils à disposition qui sont la cartographie des risques opérationnels par processus, la collecte des incidents dans une base informatique et la mise en place d'un plan de contrôle. Le dispositif doit s'intégrer dans l'environnement et être évolutif pour pouvoir prendre en compte facilement les nouveaux risques.

La fonction de contrôleur des risques permet, pour les collaborateurs qui l'exercent, d'avoir une vision d'ensemble des activités et offre de nombreuses opportunités d'évolution en termes de mobilité à la fois de par l'appartenance à un véritable réseau risque déployé à l'échelle du groupe et de par la connaissance approfondie des métiers développée dans le cadre de leur mission. Enfin, soulignons que les facteurs clés de succès incontournables pour diffuser la culture risques dans l'entreprise sont l'impulsion du management et l'implication des collaborateurs à travers notamment des actions de sensibilisation, parce qu'une meilleure maîtrise des risques c'est l'affaire de tous !

CHAPITRE 3

La formation, la rémunération et le parcours de carrière

CE CHAPITRE VOUS PERMETTRA DE :

- connaître la formation initiale recommandée pour se préparer aux deux fonctions ;
- connaître le panorama des formations permanentes existantes ;
- connaître les secteurs d'activité qui recrutent ;
- connaître les niveaux de rémunération actuelle des deux fonctions ;
- connaître les perspectives de carrière.

Nous l'avons dit à plusieurs reprises, les métiers d'auditeur interne et de contrôleur permanent sont des métiers réglementés nécessitant une solide formation initiale et de la formation permanente régulière.

Parce que ces deux métiers sont complexes, ils permettent des niveaux de rémunération intéressants dès l'embauche, souvent plus élevés que des rémunérations de jeune cadre d'autres spécialités.

Enfin, parce qu'ils permettent de s'intéresser à différentes problématiques, à différents domaines ou métiers… de l'entreprise, en relation avec de nombreuses personnes d'un niveau hiérarchique souvent élevé, ces deux métiers permettent des parcours de carrière intéressants, soit en premier emploi, soit au cours d'un parcours de carrière, soit en fin de carrière.

1. LA FORMATION INITIALE

La formation initiale des auditeurs internes et des contrôleurs permanents est variée, à l'instar de la grande variété des missions possibles et des secteurs d'activité concernés.

1.1. Le point de vue de l'Apec

D'après l'Apec, les formations initiales les plus appropriées pour exercer la fonction d'auditeur interne sont variées mais cependant d'au moins Bac + 5 :

- Les écoles de commerce : master spécialisé AICG (audit interne et contrôle de gestion) de l'ESC Toulouse, ISC Paris spécialisation Audit et Contrôle…
- Les masters spécialisés en audit-contrôle : master 2 Comptabilité Contrôle Audit de l'IAE de Bordeaux, MBA Audit et contrôle de gestion de l'ESG…
- Les instituts d'études politiques ayant une section économique et financière.
- Les écoles d'ingénieur.

Nos observations personnelles montrent que ce sont les diplômés des écoles de commerce et d'ingénieur dites « de rang 1 », qui sont les plus recherchés.

1.2. Le point du site Internet Letudiant.fr

D'après le site Internet Letudiant. fr, la formation initiale de l'auditeur interne est la suivante : diplôme d'école supérieure de commerce ou formation à l'université (master professionnel en comptabilité, contrôle de gestion) complété le plus souvent par un diplôme comptable, ce qui correspond à un Bac + 5 à 8.

Nos observations montrent que les grands cabinets d'audit permettent souvent aux auditeurs internes de suivre dans le cadre de leur formation professionnelle un diplôme d'expertise comptable, ce qui est très rarement proposé en entreprise.

1.3. L'enquête du CBOK

D'après l'enquête mondiale du CBOK (Common Body of Knowledge) réalisée par la Fondation de la recherche de l'IIA en 2010, l'âge des auditeurs est compris entre 25 et 66 ans et plus. En France, il est à noter qu'un tiers à moins de 35 ans.

D'après la même étude, la profession est plutôt masculine. En France, 60 % des auditeurs sont des hommes.

D'après la même étude encore, le niveau de formation initiale des auditeurs est très élevé en France avec plus de 80 % d'un niveau minimum « master » soit le double qu'aux États Unis, pays qui donne pourtant généralement le « La »… Les domaines de formation initiale étant surtout la comptabilité aux États-Unis mais pas en France où les formations initiales sont plus diversifiées : finance et comptabilité bien sûr, mais également économie, droit, administration des entreprises, informatique…

Nos observations montrent par ailleurs que :
- Si la profession à tendance à se rajeunir, les postes de responsabilité restent occupés par des personnes de l'âge de leurs parents, ce qui n'est pas sans poser quelques étincelles relatives aux différences de génération.
- La profession se féminise au regard d'autres fonctions partenaires de l'audit interne et du contrôle permanent tels le contrôle de gestion, l'organisation ou encore les ressources humaines.
- La réussite dans le métier de l'audit interne et du contrôle permanent ne peut se passer de solides bases en comptabilité.

2. LA FORMATION PERMANENTE

Les formations possibles sont très variées et dépendent de la formation d'origine des auditeurs internes et contrôleurs permanents, des exigences des autorités de tutelle (diplôme de l'AMF pour les banquiers par exemple), des métiers exercés par l'entreprise, de la diversité des risques identifiés dans la cartographie des risques de l'entreprise et des souhaits des personnes concernées.

Nos observations montrent que l'audit interne et le contrôle permanent sont des métiers qui font une grande place à la formation permanente et que cela convient bien à des personnes disposant de cette prédisposition d'esprit. Pour les autres, cette obligation peut être vécue comme une contrainte non reposante...

2.1. Les formations comptables

Elles constituent le socle de formation des auditeurs internes et contrôleurs permanents et sont donc impératives pour toute personne souhaitant faire carrière.

2.1.1. Le diplôme de comptabilité et de gestion (DCG) et le diplôme de gestion et de comptabilité (DGC)

L'objectif de la formation est d'acquérir une formation dans les disciplines fondamentales des métiers de la comptabilité.

Le diplôme permet une insertion professionnelle à un niveau d'encadrement intermédiaire en entreprise ou en cabinet ou la poursuite d'études (notamment vers le DSCG/DSGC).

C'est un diplôme de niveau Bac + 3. L'admission se fait avec le Bac. La durée moyenne des études à temps plein est de 3 ans pouvant être réduite en cas de dispense d'épreuves ou de validations des acquis.

La formation se fait par exemple au Conservatoire des arts et métiers (CNAM) à distance, en apprentissage, en formation initiale ou en formation continue. Le diplôme s'obtient également par validation des acquis professionnels (VAE).

Sont autorisés à suivre cette préparation les candidats ayant l'un des diplômes suivants :

- le baccalauréat ;
- un titre ou un diplôme admis en dispense du baccalauréat en vue d'une inscription dans les universités ;
- un titre ou un diplôme étranger permettant l'accès à l'enseignement supérieur dans le pays de délivrance ;
- deux unités d'enseignement (UE) du Conservatoire national des arts et métiers ;
- les diplômes homologués niveaux I, II, III ou IV figurant sur l'arrêté du 17 juin 1980 modifié ;
- les diplômes enregistrés aux niveaux I et II du RNCP (Répertoire national des certifications professionnelles) ;
- l'accès dérogatoire par la validation des acquis professionnels au vu des études, des formations et de l'expérience professionnelle ou personnelle.

2.1.2. Le diplôme supérieur de comptabilité et de gestion (DSCG) et le diplôme supérieur de gestion et de comptabilité (DSGC)

L'objectif de la formation est d'approfondir les matières du DCG et/ou DGC et se préparer aux métiers de la comptabilité, du contrôle de gestion, de l'audit et de la finance.

Les titulaires du DSCG/DSGC ont vocation à poursuivre leur carrière :

- dans les cabinets d'expertise comptable et/ou de commissariat aux comptes comme collaborateurs ou stagiaires et futurs associés ;
- dans des postes de responsabilité dans les directions comptables et financières, de contrôle de gestion et d'audit interne des organisations privées ou publiques ;
- dans des cabinets de consultants.

C'est un diplôme d'État de niveau Bac + 5 (le DSCG confère le grade de master). L'admission se fait à Bac + 3 de la filière. La durée moyenne des études à temps plein est de 2 ans pouvant être réduite en cas de dispense d'épreuves ou de validations des acquis.

La formation se fait par exemple au Conservatoire des arts et métiers (CNAM) à distance, en apprentissage, en formation initiale ou en formation continue. Le diplôme s'obtient également par validation des acquis professionnels (VAE).

Peuvent s'inscrire au DSCG/DSGC, les titulaires d'un des diplômes suivants :

- DGC ou DCG ou de tout titre ou diplôme admis en dispense du DCG (par arrêté ministériel) ;
- DECF de l'État ;
- responsable comptable du CNAM (exclusivement pour le DSGC Intec) ;
- master Comptabilité Contrôle Audit (CCA) ou tout autre master délivré en France ou dans un autre État membre de l'Espace européen de l'enseignement supérieur ;
- accès dérogatoire par la VAP85 au vu des études, formations et expérience professionnelle ou personnelle.

Les unités d'enseignement constituant le diplôme

- La gestion juridique, fiscale et sociale.
- La finance.
- Le management et contrôle de gestion.
- La comptabilité et l'audit.
- Le management des systèmes d'information.
- L'économie.
- Les relations professionnelles.

Sont déclarés admis au DSGC, les candidats qui remplissent les trois conditions suivantes : être titulaire du DCG ou du DGC (ou d'un titre ou diplôme admis en dispense) ou d'un master ou d'un diplôme conférant le grade de master ou obtenu dans un autre État membre de l'Espace européen de l'enseignement supérieur ou avoir présenté un dossier VAE ; avoir obtenu l'ensemble des sept UE le composant par dispense, par VAE ou par l'examen (note au moins égale à 6/20) et une moyenne pondérée d'au moins 10/20 aux UE passées à l'examen de l'État.

2.1.3. Le diplôme d'expertise comptable (DEC)

C'est un diplôme d'excellence reconnu sur le plan international qui s'acquiert après un stage de trois ans en cabinet d'expertise comptable.

Ce diplôme permet l'inscription à l'ordre des experts-comptables et/ou à la compagnie des commissaires aux comptes pour l'exercice libéral ou salarié de ces métiers. Ce diplôme donne accès, en outre, à des fonctions de direction dans les services comptables et financiers de grandes entreprises privées et publiques.

Les deux UE se préparent pendant une année universitaire complète (deux semestres). La durée normale de la préparation (parallèlement à une activité professionnelle) est d'un an.

La formation se fait par exemple au Conservatoire des arts et métiers (CNAM) en formation initiale.

L'inscription est exclusivement réservée aux experts-comptables stagiaires ou anciens stagiaires (l'attestation de fin de stage est à fournir pour s'inscrire à l'examen d'État). Aucune possibilité de dispenses ou de validation des acquis de l'expérience à ce jour.

Le certificat d'aptitude aux fonctions de commissaire aux comptes (CAF/CAC)

L'objectif de cette formation est d'obtenir son inscription sur la liste des commissaires aux comptes publiée chaque année par la Compagnie nationale des commissaires aux comptes (CNCC) pour l'exercice de la profession.

La durée normale de la préparation est de deux ans (chaque classe se prépare normalement en un an). Une année de préparation porte sur les disciplines comptables et de gestion et une autre sur les disciplines juridiques.

La formation se fait par exemple au Conservatoire des arts et métiers (CNAM) : formation en ligne uniquement.

EN PRATIQUE

Les conditions d'inscription au certificat d'aptitude aux fonctions de commissaire aux comptes (CAF CAC)

Selon l'article R. 822-2 du Code de commerce modifié par le décret n° 2013-192, sont admis à se présenter au CAF CAC sous réserve de justifier de la délivrance de l'attestation de fin de stage : les titulaires d'un diplôme national de master ou d'un titre ou d'un diplôme conférant le grade de master délivré en France ou d'un diplôme obtenu dans un État étranger et jugé de niveau comparable au diplôme national de master par le garde des Sceaux, ministre de la Justice, et qui ont subi avec succès les épreuves du certificat préparatoire aux fonctions de commissaire aux comptes ou sont titulaires du diplôme d'études comptables supérieures (DECS) régi par le décret n° 81-537 du 12 mai 1981 ou du diplôme d'études supérieures comptables et financières (DESCF) ou ont validé au moins quatre des sept épreuves obligatoires du diplôme supérieur de comptabilité et de gestion (DSCG). Ou sont titulaires de diplômes jugés d'un niveau équivalent à

ceux du point 2 par le garde des Sceaux, ministre de la Justice. Peuvent également être admises à présenter les épreuves du CAF CAC les personnes qui sont dispensées du stage professionnel et les personnes qui ont exercé pendant une durée de quinze ans au moins une activité publique ou privée leur ayant permis d'acquérir dans les domaines financier, comptable et juridique intéressant les sociétés commerciales, une expérience jugée suffisante par le garde des Sceaux, ministre de la Justice.

Les conditions d'admission au certificat préparatoire aux fonctions de commissaire aux comptes sont les suivantes : selon l'article A. 822-1 du Code de commerce modifié par le décret n° 2013-192, sont admis à se présenter au certificat préparatoire aux fonctions de commissaire aux comptes les titulaires d'un diplôme national de master ou d'un titre ou d'un diplôme conférant le grade de master délivré en France ou d'un diplôme obtenu dans un État étranger et jugé de niveau comparable au diplôme national de master par le garde des Sceaux, ministre de la justice ; et qui ne remplissent pas les conditions d'inscription au CAF CAC.

L'inscription au certificat d'aptitude aux fonctions de commissaire aux comptes

Les dossiers de candidature sont à déposer au siège de la compagnie régionale des commissaires aux comptes de son domicile entre le 1er et le 30 juin.

Un stage professionnel d'une durée de trois ans doit être accompli chez une personne physique ou une société inscrite sur la liste des commissaires aux comptes mentionnée à l'article R. 822-1 du Code de commerce. Le stage professionnel régulièrement accompli donne lieu à la délivrance d'une attestation de fin de stage.

L'inscription au certificat préparatoire aux fonctions de commissaire aux comptes : les dossiers de candidature sont à déposer au siège de la compagnie régionale des commissaires aux comptes de son domicile entre le 1er et le 30 janvier.

Les épreuves du certificat d'aptitude aux fonctions de commissaire aux comptes et du certificat préparatoire aux fonctions de commissaire aux comptes ont lieu une fois par an. La date et le lieu des épreuves sont notifiés aux candidats par la CNCC.

Les chiffres clés du commissariat aux comptes en France :
- **19 303** : c'est le nombre de professionnels en 2011 au service des entreprises et entités sur l'ensemble du territoire national.
- **200 000** : c'est le nombre de mandats exercés chaque année en France par les commissaires aux comptes ;
- **2,23 milliards d'euros** : c'est le chiffre d'affaires réalisé en 2010 par la profession.
- **45 % du produit intérieur brut (PIB)** est contrôlé par l'audit légal.
- **17,8 % de femmes.**

Les certifications professionnelles

Plusieurs certifications professionnelles sont appropriées aux métiers d'auditeur. Les certifications professionnelles de l'IAA, dispensées en France par l'IFACI, et qui s'adressent en priorité aux auditeurs. Notons la certification professionnelle d'auditeur interne (CPAI), la certification d'auditeur interne (CIA), la certification en auto-évaluation des contrôles (CCSA), la certification en audit des services financiers (CFSA), la certification en audit des organisations publiques (CGAP) ou encore la Certification in Risk Management Assurance (CRMA).

Le contenu de ces formations est très complet et nous ne saurions trop conseiller aux auditeurs internes et contrôleurs permanents de les suivre en parallèle à l'exercice de leur métier.

La certification professionnelle d'auditeur interne (CPAI)

Inscrite au Répertoire national des certifications professionnelles (RNCP), la CPAI atteste que l'auditeur détient les compétences indispensables à la conduite d'une mission d'audit interne en conformité avec les meilleures pratiques professionnelles internationales.

La CPAI, évalue la capacité de l'auditeur à exercer son métier selon les meilleures pratiques professionnelles.

Elle atteste de son aptitude à évaluer la capacité de son organisation à atteindre ses objectifs et à faire des propositions pour la renforcer :

- Concevoir le programme de sa mission d'audit interne conformément aux attentes des clients.
- Préparer sa mission d'audit à partir des objectifs et des risques du domaine audité et des contrôles qui devaient être mis en place pour les maîtriser.
- Hiérarchiser les risques du domaine audité, concevoir et planifier son programme de travail en se concentrant sur les risques les plus significatifs.
- Collecter des informations fiables sur la conception des contrôles, sur leur fonctionnement et sur leur capacité à maîtriser les risques.
- Communiquer pendant et après la mission d'audit avec l'ensemble des parties prenantes.
- Élaborer des recommandations à valeur ajoutée en tenant compte des causes des éventuels dysfonctionnements observés.

La certification d'auditeur interne (CIA)

La CIA est la seule certification en audit interne de portée mondiale. Elle est délivrée par l'IIA (Institute of Internal Auditors) depuis 1972. L'IFACI assure la promotion de l'examen en langue française pour le monde entier.

Contenu du CIA

- Directives obligatoires de l'IIA (définition ; code d'éthique ; normes internationales).
- Contrôle interne et risques (typologie des contrôles ; techniques de management du contrôle interne ; utilisation des référentiels de contrôle interne ; référentiel de contrôle interne alternatif ; vocabulaire et concepts relatifs aux risques ; sensibilisation au risque de fraude).
- Outils et techniques pour mener une mission d'audit (collecte des données ; analyse des données et interprétation ; restitution des données ; documentation/papiers de travail ; cartographie du processus).
- Évaluation de la qualité d'une preuve ;
- Gestion de la fonction d'audit interne (rôle stratégique de l'audit interne ; rôle opérationnel de la fonction de l'audit interne ; établissement d'un plan d'audit basé sur les risques).
- Gestion des missions d'audit interne (planification des missions d'audit ; supervision de la mission ; communication des résultats de la mission ; suivi des résultats de la mission).
- Risques de fraude et contrôles (risques de fraude courants relatifs au périmètre de la mission ; prise en compte du risque de fraude au cours de la mission ; besoin d'investigation ; revue de processus pour prévention de la fraude ; détection de la fraude ; sensibilisation au risque de fraude ; techniques d'interrogation et d'investigation ; investigation légale).
- Gouvernance (principes de gouvernance corporate et organisationnelles ; sauvegarde environnementale et sociale ; responsabilité sociale corporate).
- Management des risques (technique de management des risques ; utilisation des référentiels de risques).
- Structure organisationnelle et processus opérationnels (impact des différentes structures d'organisation ; schémas typiques des cycles opérationnels ; analyse des processus d'activités ; techniques et concepts de gestions des stocks ; transfert de fonds électronique/échange de données informatisées ; cycle de vie de développement de l'activité ; le référentiel ISO ; les processus de sous-traitance).
- Communication (communication ; relation avec les actionnaires).
- Aptitudes à diriger (management de la stratégie ; comportements organisationnels ; compétences managériales ; gestion des conflits ; gestion de projet/gestion du changement).
- Continuité d'activité et continuité informatique (sécurité ; développement des applications ; infrastructure des systèmes ; continuité d'activité).
- Gestion financière (comptabilité et finance ; compatibilité de gestion).
- Environnement économique mondial (environnement financier et économique ; environnement culturel et politique ; concepts généraux juridiques et économiques ; impact de la législation et de la réglementation). La Certification in Risk Management Assurance (CRMA)

La CIA permet de certifier l'aptitude des auditeurs internes à fournir aux comités d'audit et aux directions générales des conseils et des évaluations sur l'efficacité des dispositifs de gestion des risques et de gouvernance de leurs organisations.

2.2. Les formations relationnelles et comportementales

Elles permettent de mieux comprendre comment fonctionne un interlocuteur et ainsi faciliter la communication, notamment lors des entretiens de collecte d'information, de compréhension des situations, de recherche d'idées de changement… Elles permettent également d'appréhender plus facilement la mise en œuvre des changements en adaptant les façons de faire aux personnes.

Elles permettent pareillement de prendre du recul sur son propre comportement et ainsi de mieux se connaître, ce qui est nécessaire pour mieux s'apprécier, condition nécessaire pour mieux apprécier les autres…

La plus connue des techniques de communication est la programmation neurolinguistique qui, depuis le début des années 1990, est devenue un standard. Les organismes de formation proposant des cursus de formation sont légion et proposent généralement des formations fondées sur trois niveaux : « praticien », « master » et « enseignant ». Le niveau « master » est nécessaire et suffisant pour l'exercice des deux métiers. Ce niveau demande néanmoins plusieurs années de formation en alternance… se déroulant souvent le week-end et le soir…

3. LE RECRUTEMENT

Les grandes entreprises recrutent beaucoup de jeunes auditeurs internes et de contrôleurs permanents, et utilisent pour cela les filières classiques que sont les associations d'anciens élèves et les cabinets de recrutement.

Par ailleurs, les cabinets d'audit sont un vivier dans lequel les grandes entreprises puisent avec avidité…

3.1. Le point de vue de l'Apec

D'après l'Apec, les profils les plus demandés pour les postes d'auditeurs internes sont les diplômés BAC + 5 possédant en plus une bonne vision des métiers de l'entreprise. On note un élargissement des profils recrutés pour ce poste. Le recrutement est donc plutôt orienté vers les jeunes diplômés fraîchement sortis d'école et qui vont suivre un parcours dans l'entreprise, dans un premier temps au sein de la direction de l'audit puis vers une direction opérationnelle ou une autre fonction support. Les jeunes diplômés peuvent exercer la fonction d'auditeur junior dans une entreprise de taille importante.

Les entreprises recrutent souvent d'anciens auditeurs externes ayant 2 à 5 ans d'expérience. Un responsable de l'audit interne aura une dizaine d'années d'expérience en direction financière et/ou en conseil en organisation. Les entreprises recrutent de plus

en plus de cadres ayant une diversité d'expériences professionnelles : en ressources humaines, gestion du risque, finance… ce qui leur permet d'avoir une meilleure appréhension des différentes activités de l'entreprise.

Les postes précédents les plus recherchés pour intégrer un service d'audit interne sont « auditeur externe » et « contrôleur de gestion ».

Employeurs possibles pour les deux fonctions d'audit interne et de contrôle permanent :

- Les grandes entreprises industrielles.
- Les groupes cotés tous secteurs.
- Les banques et assurances.
- L'administration centrale et territoriale.

Les fonctions d'audit interne et de contrôle permanent semblent avoir de grandes ressemblances. En revanche, c'est la typologie des risques de chaque secteur d'activité auxquels l'auditeur interne et le contrôleur permanent auront à faire face qui est très différente…

3.2. L'enquête du CBOK

D'après cette enquête, les organisations qui recrutent de jeunes auditeurs internes et des contrôleurs permanents sont plutôt les entreprises cotées et les administrations publiques, les entreprises non cotées et les associations et ONG venant loin derrière.

Nos observations montrent que ce sont effectivement les grandes organisations qui ont les moyens et/ou l'obligation de se doter de dispositifs de maîtrise des risques et de dispositifs de contrôle interne. Il n'est donc pas étonnant que ce soit celles-ci qui recrutent le plus. Dans les PME-PMI, le coût de ces fonctions est souvent jugé dissuasif et la valeur ajoutée non reconnue. Cependant, il existe dans les PME-PMI des fonctions qui contribuent au contrôle, telles les fonctions relatives à l'assurance qualité ou au contrôle de gestion.

Les mesures incitatives pour favoriser un recrutement par rapport à d'autres fonctions ne sont pas très originales : le véhicule de société et l'augmentation de salaire restent les mesures préférées devant les indemnités de transport, les stock-options (très rares en France), la prime d'embauche et la prise en charge des dépenses de réinstallation.

Recrutement d'un directeur de l'audit interne

Il se fait par :

- mobilité interne (27 %) ;
- réseaux professionnels (24 %) ;
- filières d'audit externe (19 %) ;
- filières universitaires (11 %) ;
- cabinets de recrutement (9 %).

D'après nos observations, le recrutement se fait plutôt en interne quand le dispositif de maîtrise des risques et de contrôle interne est à un bon niveau de maturité. En revanche, si cela n'est pas le cas, le recrutement externe à l'aide du réseau est nécessaire et peut même être incité par les aurorités de tutelle.

4. LES NIVEAUX DE RÉMUNÉRATION

Les niveaux de rémunération, comme nous l'avons signalé précédemment, sont souvent de bonne tenue, notamment au sein des grandes entreprises internationales demandant, il est vrai, en retour, une grande disponibilité horaire et géographique, sans oublier une très bonne pratique parlée et écrite de l'anglais, voire d'une ou deux autres langues.

4.1. Le point de vue de l'Apec

L'Apec a fait le point sur les taux de rémunération de la fonction d'auditeur.

Rémunérations concernant la fonction d'auditeur :

- Jeune diplômé : entre 30 et 40 K€.
- Jeune cadre (2 à 5 ans d'expérience) : entre 40 et 50 K€.
- Cadre confirmé : entre 50 et 80 K€ et plus pour le responsable de l'audit interne.

4.2. Le point de vue du site Internet Letudiant.fr

D'après le site Internet Letudiant. fr, le salaire de l'auditeur interne débutant brut moyen mensuel est de 2 300 euros (2014).

Nos observations montrent que les niveaux de rémunération peuvent être élevés au

regard du niveau d'expérience et de maturité des personnes. En début de carrière, le salaire d'embauche est très fortement corrélé au diplôme d'origine, les écoles de rang 1 plus un MBA à l'étranger garantissant une prime à l'embauche. Par contre, après quelques années, les différences de salaires ont tendance à se lisser en fonction des niveaux de performance des personnes, même si la formation d'origine, en France, suit la carrière de la personne du début à la fin…

5. LES PERSPECTIVES DE CARRIÈRE

En matière de perspectives de carrière, il est clair que la fonction fait appel à des personnes de différents niveaux de compétences et d'expérience.

C'est la raison pour laquelle on peut passer par l'audit interne et le contrôle permanent :

- en premier emploi, ou quasi premier emploi, si l'on est passé par une ou deux années en cabinet d'audit ;
- en milieu de carrière pour occuper une fonction de chef de mission, spécialiste d'un métier, d'un pays… ;
- en fin de carrière pour occuper le poste de directeur de l'audit et/ou de directeur du contrôle permanent, postes dont il est difficile de « sortir », à moins d'aller dans une autre entreprise.

5.1. Le point de vue de l'Apec

Concernant les perspectives de carrière, voici, selon l'Apec, les possibilités qui s'offrent à un auditeur interne.

Fonctions qu'il est possible d'occuper après une fonction d'auditeur interne

- Responsable de l'audit interne.
- Superviseur, chef de mission au sein de la direction de l'audit interne.
- Directeur opérationnel d'un centre de profit.
- Consultant en organisation.
- Administrateur des systèmes d'information.
- *Risk manager*.
- Directeur du contrôle interne.

5.2. L'enquête du CBOK

D'après cette enquête, l'ancienneté des équipes est plus récente en France qu'aux États-Unis, avec 50 % des fonctions créées il y a moins de dix ans dans les grandes entreprises.

Quant à l'âge des personnes occupant la fonction, il semblerait qu'il soit plutôt élevé en ce qui concerne les fonctions de direction avec plus de 80 % des personnes occupant la fonction depuis plus de six ans.

5.3. Nos observations

Nos observations montrent que la création des fonctions d'audit interne et de contrôle permanent est corrélée aux obligations des autorités de tutelle de chaque secteur d'activité. À ce titre, le constat est que c'est l'obligation qui créé le besoin dans un premier temps et qu'il faut des années et de nombreuses victoires d'étape pour acculturer une entreprise au contrôle… Il est rassurant de constater que, dans des entreprises que nous connaissons bien, telles celles du secteur bancaire, la culture du contrôle s'est développée en vingt ans d'une façon significative et qu'elle commence à faire partie intégrante du travail des collaborateurs (contrôles opérationnels et contrôle de premier niveau décrits dans les procédures).

Nos observations montrent également que les fonctions de directeur de l'audit interne et directeur du contrôle permanent supposent une grande connaissance de l'entreprise, de ses métiers, de ses personnels, ainsi que la confiance des dirigeants et du comité d'audit. Tout cela prend du temps… Par ailleurs, quand on occupe une telle fonction, on a accès à des informations parfois très confidentielles. Tout ceci fait qu'il est difficile d'occuper une autre fonction interne au sein de l'entreprise et qu'il n'est pas étonnant que ces fonctions soient occupées par des personnes dont c'est le dernier poste.

PAROLE D'EXPERT

Lawrence B. Sawyer, deuxième commandement : connaître les contrôles

« L'exploitation d'une société repose sur trois activités de base : la planification, l'organisation et le contrôle. Le contrôle est le domaine spécifique de préoccupation de l'inspecteur. Dans ce domaine, il peut fournir le meilleur travail, s'il connaît les règles. Et il existe certaines règles de contrôle avec lesquelles l'inspecteur doit se familiariser totalement. Lorsqu'il inspecte une organisation, il doit rechercher certains contrôles administratifs de base. Et il le fera dans le cadre des objectifs. Les contrôles ne sont pas effectués dans le vide, ils sont effectués pour vérifier que certains objectifs sont atteints. Je ne dispose pas d'assez de temps pour énumérer les nombreux contrôles qui devraient être appliqués dans le cadre de la marche des affaires d'une société, mais, pour vous donner une idée, j'en citerai quelques-uns :

- La direction devrait fixer des normes pour son personnel.
- La direction devrait instruire son personnel de ces normes.
- La direction devrait juger son personnel par rapport à ces normes.
- Toute fonction devrait avoir un budget et un programme et le personnel doit en rendre compte.
- Il faudrait vérifier en priorité les derniers travaux réalisés.
- Les travaux en suspens devraient être évalués et les retards mis en évidence.
- Le directeur devrait savoir ce que fait chacun des membres de son personnel.
- Le directeur devrait informer son personnel des exigences et des méthodes des services "en amont" et "en aval", et ce pour chaque service.
- De temps en temps, le directeur ou ses contrôleurs devraient procéder à des tests de vérification des opérations afin de voir si les procédures en vigueur sont réellement suivies.
- Toute organisation devrait disposer, en ce qui concerne ses activités, d'un organe central de contrôle (journal, registre ou document de contrôle) permettant de garder la trace de tous les travaux ou de toutes les activités de l'organisation.
- Toute organisation devrait disposer d'un système à "rétroaction" permettant de signaler les résultats non conformes aux normes.
- Les travaux devraient être évalués à des moments précis et non pas une fois les projets réalisés.

Il existe encore bien d'autres contrôles, et pour chacun d'entre eux, l'inspecteur moderne doit avoir une bonne connaissance. En fait, on peut résumer le concept de contrôle administratif dans son ensemble par une formule de neuf mots : surveillance constante, retours en arrière et… pas de surprise !

Montrez-moi un directeur qui suit de près tout travail en cours et toute activité, qui dispose d'un système à rétroaction lui indiquant, non seulement le moment où les choses ont commencé à mal aller, mais aussi celui où elles pourraient mal aller, un directeur qui a établi un réseau d'information lui évitant d'être surpris par l'imprévu… Montrez-moi un tel directeur et je vous montrerai un homme qui fera probablement faire les choses à temps, conformément aux spécifications et aux instructions, et ce, à un coût raisonnable. »

TÉMOIGNAGE

Sandrine Murbach, présidente de ABB & A, championne de France d'apnée dynamique 2013 et 2014, championne de France d'apnée 2014

Je pratique, depuis mon plus jeune âge, différents sports à risques. Cependant, l'apnée est celui dans lequel la connaissance du risque et sa gestion sont des éléments cruciaux.

Quelle que soit la discipline pratiquée en compétition, statique, dynamique ou profondeur, l'objectif est toujours d'atteindre sa propre limite, tenir le plus longtemps possible, nager le plus loin ou le plus profond possible… Si la limite est dépassée, la sanction est radicale, c'est la syncope. Et le risque, si les conditions de sécurité ne sont pas remplies, c'est la noyade.

Deux points sont donc déterminants dans la gestion de ce risque :

- Mettre en place un dispositif de sécurité pour prévenir les accidents et intervenir le cas échéant : surveillance avec contrôle de la lucidité de l'athlète mais surtout des apnéistes (ou plongeurs) de sécurité ; la règle numéro 1 de l'apnée, en loisir, à l'entraînement et d'autant plus en compétition c'est « jamais d'apnées seul ».
- Se connaître parfaitement, connaître ses limites, physiques et mentales et avoir une capacité à être à l'écoute de soi en permanence, pour savoir exactement où l'on en est, détecter ce qui est inhabituel, l'évaluer, l'intégrer dans sa performance pour la gérer au mieux.

En compétition en piscine par exemple, pour les épreuves d'apnée dynamique (parcours de la plus grande distance possible en apnée), la sécurité est assurée par deux nageurs en surface qui nous suivent tout au long de notre performance. Au moindre signe de défaillance, ils interviennent. La présence de ces deux anges gardiens au-dessus de nos têtes et à nos côtés à la sortie de l'eau nous sécurise, il nous reste « juste » à nous concentrer pour sortir le meilleur de nous-même.

Sans ce dispositif de sécurité, sans cette garantie que le risque est maîtrisé, sans la sérénité inhérente, impossible de réaliser une performance maximale.

L'apnée est un sport complet et complexe : il est physique, technique et mental. Il impose, pour approcher ses limites sans jamais les dépasser, de se connaître parfaitement. Les capacités d'écoute de soi que l'on développe, de perception des sensations internes et externes, d'évaluation du niveau d'effort, de fatigue, de contrôle du corps et du mental, sont un formidable atout dans la vie sportive, mais aussi dans la vie personnelle et professionnelle.

Aussi à l'aise dans l'eau que nous puissions l'être, n'oublions jamais que les défaillances existent, tout comme les imprévus et les accidents : « Savoir pour prévoir, afin de pouvoir », disait Auguste Comte.

En résumé

Cette première partie a présenté les métiers d'auditeur interne et de contrôleur permanent et plus précisément :

- une description de leur rôle dans le dispositif de maîtrise des risques (DMR) d'une entreprise ;
- les objectifs de la gestion des risques, les principales composantes d'un DMR, les principaux outils informatiques utilisés par les deux métiers ;
- le panorama des risques à mettre sous contrôle par l'audit interne et le contrôle permanent, à savoir les risques généraux d'une entreprise, ainsi que des exemples de risques spécifiques à certains secteurs d'activité, tels le secteur bancaire, le secteur du transport aérien ou encore le secteur hospitalier, certains domaines tel les ressources humaines ainsi que dans la pratique sportive ;
- les informations relatives à la formation, la rémunération et le parcours de carrière de l'auditeur interne et du contrôleur permanent ;
- trois témoignages illustrant nos propos :
  - Philippe Vannier a évoqué la sérénité et la création de valeur ajoutée apportées par l'audit chez Bull, ainsi que son rôle de vivier,
  - Françoise Chassard a attiré notre attention sur l'importance de la fonction de contrôle interne pour une institution comme la Caisse des dépôts, afin de concilier les missions de l'entreprise et maîtriser ses risques,
  - Sandrine Murbach a décrit l'importance, quand on pratique un sport à risques tel que l'apnée, de bien se connaître et de disposer d'un dispositif de contrôle performant. Sans ce dispositif, la performance n'est pas possible ;
- les premier et deuxième commandements de Lawrence B. Sawyer : « connaître les objectifs » et « connaître les contrôles ».

Le questionnaire qui termine cette première partie va maintenant vous permettre de tester vos connaissances…

TEST DE CONNAISSANCE

Ce questionnaire a pour objectif de vous aider à faire le point sur vos connaissances des métiers de l'audit interne et du contrôle permanent.

Pour ce faire :

- répondez aux questions ci-après en choisissant pour chacune d'entre elles : « je pense » ou « je ne pense pas » ;
- à chaque fois que vous avez répondu : « je ne pense pas », à une question, relisez le passage du livre indiqué.

Questions

1. Le management des risques vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.

   (Réponse : chapitre 1, introduction, p. 5.)

2. Le dispositif doit également prévoir un processus de gestion des risques comprenant, au sein de son contexte interne et externe à l'entreprise, trois étapes : l'identification des risques, l'analyse des risques et le traitement des risques.

   (Réponse : chapitre 1, le dispositif de maîtrise des risques, p. 7.)

3. L'analyse du niveau de maturité de chaque composant du dispositif de maîtrise des risques consiste à évaluer l'efficacité de celui-ci au regard des bonnes pratiques professionnelles, des obligations réglementaires, de l'organisation de l'entreprise, de l'appétence de l'entreprise pour le risque et de l'analyse des relations entre les différents composants.

   (Réponse : chapitre 1, le dispositif de maîtrise des risques, p. 8.)

4. Le code de déontologie constitue la première composante du dispositif de maîtrise des risques d'une entreprise.

   (Réponse : chapitre 1, la déontologie et l'appétence au risque, p. 9.)

5. Le dispositif de maîtrise des risques est composé de trois lignes de maîtrise : les managers opérationnels, les contrôleurs permanents et les auditeurs internes.

   (Réponse : chapitre 1, l'organisation du dispositif de maîtrise des risques, p. 12.)

6. La cartographie des risques repose sur une taxonomie des risques, véritable dictionnaire des risques possibles en théorie.

   Un grand projet peut disposer de sa propre cartographie des risques.

   (Réponse : chapitre 1, la cartographie des risques, p. 16.)

7. Les contrôles de premier niveau seront à réaliser, selon un calendrier défini à l'avance, par les responsables d'encadrement à partir des opérations traitées par leurs collaborateurs.

   (Réponse : chapitre 1, les plans de contrôle, p. 22.)

8. Les deux fonctions d'audit interne et de contrôle permanent interviennent en coopération avec les métiers et des experts de tout domaine dans la définition du plan de continuité d'activité, à savoir dans l'inventaire des scénarios plus ou moins compliqués, de nature à contrarier la bonne marche des opérations.

   (Réponse : chapitre 1, le plan de continuité d'activité, p. 34.)

9. Les outils de contrôle permanent sont connectés aux applications de gestion de l'entreprise et analysent de façon automatique et en continu les flux de données. Leur première mission est l'identification d'informations inhabituelles ou atypiques.

   (Réponse : chapitre 1, les outils du contrôle permanent, p. 40.)

10. L'audit interne et le contrôle permanent doivent s'assurer que l'entreprise possède un système d'information et de contrôle de gestion permettant d'obtenir une image instantanée et évolutive du personnel.

    L'accès au système informatique doit être soumis à une série de limitations, pour éviter les usages abusifs ou frauduleux : accès limités aux heures ouvrables, nécessité d'un mot de passe ou d'un code d'accès régulièrement modifié, supprimé en cas de départ de la personne, mots de passe et terminaux ne donnant accès qu'à certaines fonctions.

    Pour chacun des collaborateurs, l'audit interne et le contrôle permanent repèrent, non pas de façon globale, mais tâche par tâche, les niveaux de compétence et de motivation. En fonction de ceux-ci, ils portent un avis sur le style de management utilisé.

    (Réponse : chapitre 2, les risques relatifs à la gestion interne, p. 46.)

TEST DE CONNAISSANCE
Copyright © 2014 Eyrolles.

11. Le comité de Bâle a défini sept types d'événements de risques :
    - fraude interne ;
    - fraude externe ;
    - pratiques sociales et sécurité sur le lieu de travail ;
    - clients, produits et pratiques commerciales ;
    - dommages aux actifs matériels ;
    - interruption d'activité et défaillance de systèmes ;
    - exécution, livraison et gestion des processus.

    (Réponse : chapitre 2, les risques spécifiques du secteur bancaire, p. 51.)

12. Les formations comptables constituent le socle de formation des auditeurs internes et contrôleurs permanents et sont donc impératives pour toute personne souhaitant faire carrière.

    (Réponse : chapitre 3, la formation permanente, p. 79.)

13. Le CIA est la seule certification en audit interne de portée mondiale. Elle est délivrée par l'IIA (The Institute of Internal Auditors) depuis 1972.

    (Réponse : chapitre 3, les certifications professionnelles, p. 84.)

14. Les formations relationnelles et comportementales permettent à l'auditeur interne et au contrôleur permanent de mieux comprendre comment fonctionne un interlocuteur et ainsi de faciliter la communication, notamment lors des entretiens de collecte d'information, de compréhension des situations, de recherche d'idées de changement… Elles permettent également d'appréhender plus facilement la mise en œuvre des changements en adaptant les façons de faire aux personnes.

    (Réponse : chapitre 3, les formations relationnelles et comportementales, p. 86.)

15. Les grandes entreprises recrutent beaucoup de jeunes auditeurs internes et contrôleurs permanents, et utilisent pour cela les filières classiques que sont les associations d'anciens élèves et les cabinets de recrutement.

    (Réponse : chapitre 3 – Le recrutement, p. 86)

PARTIE 2 L'ENVIRONNEMENT DES MÉTIERS D'AUDITEUR INTERNE ET DE CONTRÔLEUR PERMANENT

Copyright © 2014 Eyrolles.

L'arnaqueur de Wall Street

Le financier philanthrope, ami du gotha new-yorkais, n'était en fait qu'un vulgaire escroc. Partout dans le monde, ses victimes se réveillent groggy. Le scandale de trop pour la planète Finance. C'est un scénario digne d'*Il était une fois en Amérique*, le chef-d'œuvre crépusculaire de Sergio Leone. L'histoire d'un gamin juif du Queens parti de pas grand-chose et devenu en quelques décennies l'une des figures les plus éminentes de la haute société new-yorkaise. Avant de tout perdre en une poignée d'heures : arrêté le 11 décembre, Bernard Madoff (70 ans), ex-PDG du Nasdaq, patron de la très respectée Madoff Investment Securities, spécialisée dans la gestion de fortune, a admis être l'auteur de ce que certains ont déjà baptisé « la fraude du siècle ». C'est près de 50 milliards de dollars que Madoff, qui comptait parmi ses clients investisseurs quelques-unes des plus grandes banques du monde, a reconnu avoir détournés, à la barbe de régulateurs mystifiés. Une parabole en forme de résumé des travers d'une planète financière qui n'en finit plus d'étaler ses turpitudes. Et se demande quelle drôle de tuile lui est encore tombée sur la tête… L'escroquerie échafaudée par Madoff, connue sous le nom de « pyramide de Ponzi », était d'une simplicité biblique. Elle consistait à payer les rendements de ses investisseurs – de 10 % à 13 % chaque année, avec une régularité métronomique – grâce aux apports de nouveaux clients. Une technique efficace en régime de croisière, mais beaucoup plus dangereuse par gros temps. Et carrément intenable en période de tsunami financier. Depuis plusieurs mois, banques et *hedge funds*, au bord de l'asphyxie, rapatrient une grande partie des capitaux qu'ils ont placés les uns chez les autres. Résultat : les fonds les plus faibles ou les moins bien gérés – c'est déjà le cas de près d'un tiers des *hedge funds* – disparaissent. Quant aux escrocs, ils n'ont plus aucun moyen de masquer la vraie nature de leur activité. L'incontestable talent de Bernard Madoff est là tout entier. Mieux que personne il sait vendre à ses clients un bien intangible, mais ô combien précieux : la confiance. Et son tableau de chasse est aussi hétéroclite qu'impressionnant. Car on trouve de tout chez Madoff. Des *hedge funds*, par exemple, dont certains étaient même entièrement investis chez lui, comme le Fairfield Sentry Fund qui a perdu plus de 7 milliards de dollars, des associations caritatives : la fondation Wunderkinder de Steven Spielberg ou la fondation Élie Wiesel pour l'humanité. Également saignées, de grandes fortunes privées : le prince saoudien Al-Waleed, qui aurait reconnu avoir perdu 4 milliards de dollars, ou Saul Katz, codétenteur du mythique club de base-ball des New York Mets. Sans compter les partenaires de golf de « Bernie », dont beaucoup, de Long Island à Palm Beach, en passant par Boston, sont désormais complètement ruinés. Et, bien sûr, des banques. L'étrange M. Madoff, qui se refusait à donner des informations sur son *business model*, avait pourtant de quoi éveiller les soupçons. Un concurrent, Harry Markopolos, avait même, dès 1999, dénoncé les pratiques de Madoff au gendarme américain des marchés, la SEC. « Madoff Securities est le plus gros schéma de Ponzi du monde », précisait-il alors. À quatre reprises, en 1992, 2001, 2005 et 2007, la SEC a mené des enquêtes, qui n'ont jamais débouché sur quoi que ce soit. La faillite de l'organisme de contrôle se passe de commentaires. De quoi conforter tous ceux, de plus en plus nombreux, qui jugent que l'inertie des régulateurs est l'une des principales causes de la crise. « Compter sur le système financier pour s'autoréguler, c'est comme compter sur un héroïnomane pour refuser la seringue qui lui est tendue », estime un gérant de fonds. Encore une leçon durement apprise, pour les professionnels de Wall Street, qui finissent l'année essorés par les catastrophes en série. Quand ils n'ont pas purement et simplement perdu leur emploi…

Source : lexpansion.lexpress.fr, 16/12/2008, Benjamin Masse-Stamberger (http://lexpansion.lexpress.fr/actualite-economique/madoff-l-arnaqueur-de-wall-street_726756.html

INTRODUCTION

La deuxième partie présente l'environnement des métiers d'auditeur interne et de contrôleur permanent. Pour développer ce thème, nous nous sommes tout d'abord appuyés sur l'Institut de l'audit et du contrôle internes (IFACI). En effet, en raison de son rôle de représentant en France de l'IAA, l'IFACI diffuse en langue française les normes et bonnes pratiques professionnelles, constituant à ce titre la référence. Nous nous sommes également appuyés sur des informations en provenance de l'Association pour l'emploi des cadres (APEC), notamment pour tout ce qui concerne les secteurs qui recrutent et leurs conditions salariales. Avec 39 000 entreprises servies, l'APEC peut être considérée comme un excellent baromètre. Nous avons également consulté le site internet Letudiant.fr pour connaître les informations adressées aux étudiants, et celles qui manquent, notamment en matière de parcours professionnel. Nous avons enfin consulté l'Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque. Cet organisme publie régulièrement des études sur les métiers dans le secteur bancaire, gros pourvoyeur d'emploi sur les deux métiers qui nous intéressent.

Vous y trouverez une description de leur positionnement possible dans l'organigramme et la description des différents grades des deux métiers :

- directeur de l'audit interne ;
- chef de mission ;
- auditeur et assistant ;
- directeur du contrôle permanent ;
- contrôleur permanent.

Vous y trouverez les fonctions avec lesquelles ils entretiennent des relations privilégiées au sein de l'entreprise :

- contrôle de gestion ;
- contrôle comptable ;
- gestionnaires de risques ;

- qualité ;
- organisation ;
- directions métier.

Vous y trouverez également les textes encadrant les deux métiers, tels le code de conduite de l'IAA.

Vous y trouverez les critères d'évaluation de la performance des deux métiers :

- évaluation des résultats collectifs ;
- évaluation des compétences individuelles.

Vous y trouverez également quatre témoignages illustrant nos propos :

- Alain Ledemay pose la question de la rentabilité des deux fonctions dont la mise en œuvre à été rendue obligatoire chez Galian par la réglementation. Par ailleurs, il apporte un éclairage sur la complémentarité des deux fonctions.

- Christophe Estivin montre en quoi l'intervention de l'audit dans les missions de due diligence réalisées par In Extenson, Finance & Transition pour le compte de ses clients, est déterminante dans le prix de cession d'une entreprise.

- Bernard Pédamon montre en quoi une démarche organisée de gestion des risques au sein d'Air France KLM, basée sur une cartographie et se traduisant par des actions à entreprendre face à des risques identifiés, notamment au décollage et à l'atterrissage, est de nature à sécuriser les vols.

- Jean-Baptiste Parnaudeau montre en quoi l'audit, métier passionnant, est, chez SITA Recyclage, un partenaire de la direction générale et également de toute l'entreprise et de la ligne managériale de gestion des risques.

Vous y trouverez aussi les troisième, quatrième, cinquième et sixième commandements de Lawrence B. Sawyer : « connaître les nomes », « connaître la population », « connaître les faits » et « connaître les causes ».

Un questionnaire en fin de partie vous permettra de tester vos connaissances.

CHAPITRE 4

Les missions

Les missions des auditeurs internes et des contrôleurs permanents répondent à ce qui a été développé plus en amont dans l'ouvrage, et plus précisément aux rôles des trois lignes de maîtrise. Rappelons que les métiers constituent la première ligne de maîtrise, le contrôle permanent la deuxième et l'audit interne la troisième.

CE CHAPITRE VOUS PERMETTRA DE :

- connaître l'étendue et la complémentarité des missions de l'audit interne et du contrôle permanent ;
- connaître le détail des fonctions selon les grades.

1. LES MISSIONS DE LA DIRECTION DE L'AUDIT INTERNE

1.1. Le point de vue de l'IFACI

D'après l'IFACI, l'audit interne est « une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise et en faisant des propositions pour renforcer leur efficacité ».

En adéquation avec les missions fixées par la réglementation et la direction générale et en complément avec les autres fonctions concernées par la maîtrise des risques (intervenant dans le cadre du contrôle permanent) – direction conformité et déontologie, direction des risques opérationnels, direction de la sécurité… –, la direction de l'audit interne, dans le cadre du contrôle périodique :

- évalue et fait progresser le dispositif de contrôle interne (contrôles au premier degré, second degré…) ;
- réalise des audits de domaines et de systèmes, de filiales… ;
- réalise des missions ponctuelles ;

Un programme annuel est défini pour répondre au plus près aux risques de l'entreprise. Ce programme représente 50 % à 75 % de la charge de travail prévisionnelle des auditeurs.

1.2. Le directeur de l'audit interne

Rattaché directement au président ou au directeur général de l'entreprise, le directeur de l'audit interne :

- propose la politique de contrôle ;
- rédige le programme d'audit et les lettres de mission ;
- affecte les missions ;
- suit la réalisation du programme d'audit ;
- apprécie ses collaborateurs ;
- en développe la compétence ;
- définit les méthodes de travail ;
- valide les missions conduites dans sa direction ;
- présente les rapports à la direction générale ;
- intervient personnellement sur des missions d'audit stratégiques ou sur des dossiers « brûlants ».

Il est nommé pour une durée de 5 à 7 ans, parfois plus.

1.3. Le chef de mission

Rattachés au directeur de l'audit interne, les chefs de mission :

- pilotent les missions qui leur sont confiées ;
- affectent les travaux aux auditeurs (inspecteurs ou contrôleurs) ;
- suivent l'avancement des travaux ;
- interviennent de façon importante dans les phases de préparation des missions et de rédaction des rapports de mission ;
- valident les travaux réalisés par les auditeurs ;
- interviennent directement sur des missions ponctuelles.

Ils sont nommés pour une durée de 3 à 5 ans

Nos observations montrent qu'il est rare qu'un chef de mission devienne directeur de l'audit interne. De même, il est rare également qu'un chef de mission devienne directeur des contrôles permanents.

1.4. Les auditeurs internes et assistants

Les auditeurs internes sont rattachés à un chef de mission pendant la durée d'une mission. Les auditeurs (inspecteurs ou contrôleurs) réalisent les travaux qui leur sont confiés et sont nommés pour une durée de 3 à 5 ans. Ils peuvent devenir chef de mission ; ils sont parfois spécialisés par métier ou technique (informatique, comptabilité…).

Les assistants :

- sont rattachés au directeur de l'audit ;
- tiennent à jour les dossiers permanents ;
- réalisent certains contrôles à distance ;
- s'occupent des travaux administratifs de la direction ;
- sont nommés pour une durée de 5 à 7 ans.

1.5. Le point de vue de l'Apec

D'après l'Apec, l'audit interne a pour mission d'aider l'entreprise à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques et de contrôle interne, son organisation, et en faisant des propositions pour renforcer son efficacité.

Les missions principales de l'audit interne

- Respecter et rendre efficace les systèmes de contrôle interne et de gestion des risques.
- Recenser les risques et les procédures de contrôle du groupe.
- Contrôler la pertinence et l'application de ces procédures par la réalisation d'audits.
- Élaborer des recommandations pour en améliorer l'efficacité.
- Évaluer l'efficacité du contrôle interne nécessaire à l'établissement des comptes de l'entreprise et à la performance opérationnelle en accord avec les obligations légales et les exigences des actionnaires.

Tableau 4.1 – L'audit selon l'APEC

Définition du plan d'audit	▪ Analyser les structures financières et les schémas organisationnels de l'entreprise ainsi que les données externes pour identifier et évaluer les risques financiers comptables et organisationnels. ▪ Établir le plan annuel d'audit et les orientations stratégiques de l'audit des filiales.
Réalisation des missions d'audit	▪ Préparer la mission par la définition précise de l'objectif et du programme de travail correspondant. ▪ Intervenir dans le site ou les départements concernés par le biais de différentes méthodes : observation, dialogue avec les collaborateurs concernés sur leurs méthodes et leurs travaux quotidiens, tests. ▪ Établir des constats sur les méthodes utilisées, la formalisation des procédures et leurs conséquences sur la maîtrise des risques. Le cas échéant concevoir des actions correctrices. ▪ Identifier et préconiser des pistes d'améliorations afin d'optimiser les process. ▪ Valider ces constats et actions avec le responsable du site audité. ▪ Rédiger le rapport de synthèse de la mission.

Ponctuellement, les auditeurs internes peuvent, en dehors de leurs missions d'audit, accompagner les opérationnels dans la mise en place de nouvelles procédures. Ils peuvent notamment animer des formations à de nouveaux outils de gestion, assurer le transfert de compétence de la culture du contrôle interne ou opérer une mission d'évaluation des organisations internes pour en optimiser le fonctionnement. Les auditeurs internes peuvent aussi mener des audits juridiques. Ces missions consistent à faire la revue de tous les contrats de l'entreprise signés et en cours vis-à-vis des fournisseurs, prestataires de services, à évaluer l'engagement financier correspondant et à évaluer les risques juridiques éventuels pour non-conformité des obligations.

1.6. Le point de vue du site Internet Letudiant.fr

D'après le site Internet Letudiant.fr, contrairement à l'auditeur externe qui est rattaché à un cabinet d'audit, l'auditeur interne est salarié de l'entreprise, le plus souvent dans un grand groupe. Ce qui ne l'empêche pas de se déplacer régulièrement, comme son confrère, pour auditer les différents sites de la société : usines, succursales, boutiques, etc. Maillon indispensable d'une gestion rigoureuse, il analyse le fonctionnement des activités de l'entreprise à partir de données écrites et d'entretiens avec les salariés. Il peut ainsi détecter des anomalies dans le respect des procédures ou des faiblesses dans les méthodes de travail. Enfin, il rédige un rapport dans lequel il émet ses recommandations.

FICHE MÉTIER
Inspection générale – Audit interne

Inspection générale

- Évaluer le dispositif de contrôle permanent mis en place par l'organisation.
- Piloter des missions de contrôle thématiques et d'évaluation de contrôle interne afin de contribuer au meilleur fonctionnement de l'entreprise à travers ses analyses et ses rapports.

Audit interne

- Assurer un service d'audit interne indépendant et de qualité à toutes les entités de l'entreprise.
- Assurer un contrôle périodique.
- Auditer l'ensemble des filiales, métiers ou fonctions sur la base d'un plan d'audit pluriannuel.

Exemple : les missions d'un auditeur interne, banque

Au sein de l'inspection générale, rattaché au chef de mission, l'auditeur interne participe à des travaux d'audit sur l'ensemble du périmètre de l'entreprise, tant en France qu'à l'étranger.

- Il est l'une des parties prenantes dans la préparation des missions, les interviews, la réalisation et l'exploitation de tests, la rédaction des synthèses et des rapports.
- Il présente oralement ses conclusions aux audités et à leur hiérarchie.
- Il assure un suivi permanent des risques au sein des différents secteurs. Pour cette raison, il est en relation avec les contrôleurs internes.

Figure 4.1 – Fiche de fonction d'auditeur interne, banque commerciale

Filières risques et finances	Métier : Auditeur	Rôle : Spécialiste
Rattachement hiérarchique : Manager de manager ou Manager Opérationnel		
FINALITÉS :		
Dans le cadre des orientations définies par le N + 1 :		
– Participer au contrôle de la qualité des systèmes de contrôle interne de l'entreprise dans les domaines présentant des risques importants et nécessitant une expertise particulière		
MISSIONS/SAVOIRS FAIRE/ACTIVITÉS PRINCIPALES :		
Réaliser les missions d'audit et élaborer des recommandations :		
– Préparer le déroulement des missions et les planifier		
– Mettre en œuvre le programme de vérification dans le respect du planning et réaliser et/ou superviser la conduite des missions		
– Rédiger et valider les recommandations des rapports de missions et assurer leur transmission		
– Assurer le suivi de la mise en place des recommandations		

.../...

.../...

Garantir la réalisation de missions d'audit dans le cadre du plan d'action défini :
– S'assurer du respect des délais de réalisation des missions d'audit
– Analyser les écarts et les expliquer
– Apporter des correctifs et arbitrer en cours d'exercice
Veiller à la coordination, la qualité et la pertinence des missions de contrôle :
– Identifier les risques dans le cadre des différents domaines d'activités de l'entreprise et les quantifier
– Veiller sur leur évolution
– Participer à l'élaboration du plan de mission pluriannuel
– Veiller à l'application de la politique de l'entreprise
Organiser, planifier et piloter l'activité le cas échéant :
– Définir les contributions individuelles des collaborateurs dédiés dans le cadre de la mission d'audit
– Planifier et coordonner leur mise en œuvre
– Analyser les résultats et décider des actions correctrices

Source : Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque.

1.7. Le point de vue de l'Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque

L'Observatoire a défini les principales missions de l'audit.

Missions de l'audit interne

- Contrôler sur place et sur pièce les procédures internes.
- S'assurer que les risques et la sécurité des opérations bancaires sont maîtrisés.
- Contrôler le dispositif de contrôle interne afin de vérifier sa fiabilité et sa pertinence.
- Évaluer l'efficacité des outils de gestion et de contrôle notamment et de l'entité auditée.
- Établir un diagnostic avec une formalisation des axes d'amélioration/recommandations.
- Réaliser un suivi de la mise en œuvre des recommandations par l'entité auditée.

.../...

.../...

- Définir un plan d'audit annuel en prenant en compte les exigences réglementaires, le suivi des recommandations, la cartographie des risques et les demandes des organes exécutifs et délibérants.
- Contrôler l'efficacité du dispositif de contrôle interne et de gestion des risques de la banque.
- Réaliser des contrôles périodiques sur place et sur pièces afin d'évaluer la sincérité des documents et des procédures mises en place.
- Mesurer la fiabilité et l'intégrité des informations financières communiquées.
- Apprécier le respect des réglementations et des lois en vigueur de la part des collaborateurs de la banque.
- Assurer le suivi de la mise en œuvre effective des recommandations validées.

2. LES MISSIONS DE LA DIRECTION DU CONTRÔLE PERMANENT

La direction du contrôle permanent est en charge du contrôle du bon fonctionnement de l'entreprise au quotidien. Pour ce faire, elle met en œuvre et anime un dispositif composé de différentes briques complémentaires (cf. la partie 3 de l'ouvrage qui présente les composantes du dispositif de maîtrise des risques).

Composition du dispositif

- Un référentiel des risques.
- Une composante de contrôle de premier niveau à destination des responsables d'encadrement métiers.
- Une composante de contrôle de deuxième niveau réalisé par des contrôleurs spécialisés localisés dans différents lieux géographiques de l'entreprise.
- Une composante de déclaration des incidents opérationnels à destination de référents localisés au sein des services et en charge desdites déclarations.
- Une composante d'indicateurs d'activité et de risques.
- Une composante de gestion des plans d'actions demandés aux métiers et répondant à des faiblesses identifiées dans le cadre des contrôles de deuxième niveau réalisés.
- Une composante d'information et de formation à destination des collaborateurs de l'entreprise permettant ainsi leur acculturation aux risques.
- Une composante de reporting vers la hiérarchie de l'entreprise et les autorités de tutelle.

2.1. Le directeur du contrôle permanent

Personne expérimentée et très au fait des métiers et des risques sous-jacents de l'entreprise, il a trois natures de responsabilité :

- Animation : il est responsable hiérarchique d'une équipe de contrôleurs centralisée et également répartis au sein des métiers. Dans ce cas, il n'est pas leur responsable hiérarchique mais les anime dans le cadre de l'animation de la filière contrôle.
- Gestion : il gère des budgets mis à sa disposition pour remplir ses objectifs (budgets d'étude, de consulting, de formation…).
- Organisation : il organise le dispositif de contrôle permanent de l'entreprise et, notamment, le dote d'outils permettant une couverture appropriée des risques et des contraintes réglementaires.

2.2. Le contrôleur permanent

2.1.1. Le point de vue de l'Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque

L'Observatoire a défini les missions principales du contrôle permanent.

Missions du contrôle permanent

- Identifier et assurer la veille sur le périmètre de contrôle.
- Réaliser une cartographie des risques de non-conformité afin d'identifier les dispositifs de maîtrise des risques et les plans d'action à mettre en place.
- Transposer les dispositions réglementaires liées à la conformité dans les outils et les procédures internes de la banque.
- Mettre en œuvre un plan de contrôle spécifique aux risques opérationnels ou métiers s'ils ne sont pas couverts par un gestionnaire de risque spécifique.
- Réaliser des missions de contrôles.
- Collecter des incidents liés aux risques qu'il contrôle.
- Organiser des formations à l'attention des salariés afin de les sensibiliser aux problématiques du moment, telles que la protection de la clientèle, la lutte contre le blanchiment…
- Organiser et coordonner des reportings, des outils de suivi et de prévention du dispositif de maîtrise des risques.
- Couvrir un périmètre spécifique équivalent à une ligne métier.
- Mettre en œuvre le plan de contrôle défini par le responsable de contrôle interne (mission de contrôle permanent). Mettre en œuvre des contrôles sur les étapes risquées des processus.

.../...

.../...

- Suivre les contrôles mis en place et des procédures de traitement des opérations bancaires *via* un système de remontée d'alertes avec des indicateurs tels que le taux d'erreur, les délais, etc.
- Analyser, évaluer l'exposition aux risques et la proposition des plans d'amélioration.
- Vérifier que la banque est conforme aux lois, règlements et normes professionnelles.
- Garantir la qualité et le niveau de sécurité des systèmes d'information.

2.2.2. Le point de vue de l'IFACI

D'après l'IFACI, le contrôleur permanent « métier », rattaché à une direction support ou une direction métier, a pour fonction « d'accompagner et conseiller les lignes opérationnelles et fonctionnelles concernées par la mise en œuvre d'un dispositif de contrôle interne cohérent avec les orientations définies au niveau du groupe ».

Concrètement, ses tâches sont de concevoir, accompagner, évaluer et rendre compte :

- Concevoir : identifier des activités de contrôle spécifiques à son domaine de responsabilité en s'assurant de leur pertinence avec le responsable du contrôle interne.
- Accompagner : apporter un appui méthodologique aux entités relevant de son domaine de responsabilité et proposer des axes d'amélioration pour un usage managérial du contrôle interne. Assister les entités lors de leur exercice d'auto-évaluation.
- Évaluer : mettre en œuvre le référentiel de contrôle interne et les plans de contrôle définis par le responsable du contrôle interne. Tester la conception et la mise en œuvre des activités de contrôle par les entités relevant de son domaine de responsabilité. Actualiser la cartographie des risques, le plan de tests, les outils et les procédures sur son périmètre de responsabilité.
- Rendre compte : informer les instances dirigeantes relevant de son périmètre de responsabilité. Participer aux instances locales de coordination avec les autres fonctions dédiées à l'amélioration de la performance et à la maîtrise des risques (qualité, sécurité, gestionnaires des risques). Participer au réseau de contrôle interne notamment en assurant la remontée d'informations fiables et en temps utile ainsi que le partage des bonnes pratiques.

Le poids des activités de conception, accompagnement, évaluation et reporting pourra varier en fonction du secteur d'activité, de l'organisation, du niveau de maturité du dispositif de contrôle interne, de l'effectif et de l'organisation de la « filière contrôle interne », de la nature des relations avec le responsable du contrôle interne.

Fiche métier
Conformité

- Réaliser des missions de contrôle permanent du risque de non-conformité en toute indépendance (avec les métiers opérationnels, les autres mesures des risques, l'inspection).
- Piloter la veille réglementaire et juridique en collaboration avec les métiers concernés afin d'en assurer la déclinaison opérationnelle.
- Coordonner les plans de contrôle nécessaires pour veiller aux risques de non-conformité.

Source : Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque.

Fiche de fonction
Contrôleur de la conformité (banque commerciale)

Sa mission consiste à assurer la réalisation des contrôles de conformité et d'application des procédures. Ses missions principales sont les suivantes :

- Réaliser des contrôles visant à s'assurer de la maîtrise des risques de non-conformité.
- Réaliser des contrôles visant à s'assurer du respect des procédures opérationnelles.
- Produire des livrables tels que des comptes rendus des contrôles, des contributions aux différents reportings.
- Réaliser le suivi de la mise en œuvre des procédures correctrices.
- Proposer des contrôles récurrents (automatisés) suite à la réalisation de contrôles.

Source : Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque.

Fiche de fonction
Compliance officer (banque commerciale)

La direction de la conformité s'assure que la banque suit l'ensemble des lois et règlements qui régissent son activité et déploie alors des actions *a priori* (procédures, conseils, formations) et *a posteriori* (contrôles de second niveau). Au sein de la direction de la conformité, le *compliance officer* intervient en tant que contrôleur interne sur un périmètre dédié.

À ce titre, ses principales missions sont les suivantes :

- Conseiller et assister les opérationnels dans la mise en œuvre des dispositions réglementaires.
- Assurer le suivi des activités.

.../...

.../...

- Rédiger les procédures/normes de déontologie sur le périmètre des entités couvertes.
- Assurer la veille réglementaire et technologique des périmètres couverts.
- Participer à l'élaboration et à la mise en œuvre de formations des opérationnels.
- Contribuer à l'émission d'avis de conformité sur les nouveaux produits.
- Réaliser des contrôles de conformité sur l'ensemble du périmètre couvert.

Source : Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque.

PAROLE D'EXPERT

Lawrence B. Sawyer, troisième commandement : connaître les normes

« Le travail dans les services, le contrôle effectif de contrôle et de vérification des opérations, est essentiellement un travail de mesure. Et mesurer implique une norme par rapport à laquelle mesurer. Cela implique également des unités de mesure. On mesure la vitesse d'un coureur de 100 mètres avec un chronomètre : les secondes et les mètres, ce sont les unités de mesure. Mais les unités de mesure ne signifient rien sans normes. Nous savons que 10 secondes, c'est un assez joli temps pour 100 mètres. Ce n'est pas un record, mais c'est assez bon. Nous savons que 9,3 secondes, c'est magnifique. À l'aide de ces informations, on pourra exprimer une opinion en connaissance de cause la prochaine fois qu'un coureur sera chronométré. En ce qui concerne l'inspection, l'inspecteur découvrira qu'il a perdu beaucoup de temps et d'efforts s'il n'a pas fixé (ou conclu un accord sur) des normes avant de commencer les tests. Si, par exemple, il contrôle la précision des plans d'ingénierie, il voudra se mettre d'accord avec l'ingénieur en chef quant au nombre ou au pourcentage de rejet des plans considérés comme "normaux". Ensuite, lorsqu'il effectuera ses tests, il saura si les normes ont été ou non respectées. Il existe des normes pratiquement à chaque stade de l'effort humain. Elles peuvent être fixées par une moyenne arithmétique. Elles peuvent être fixées par directive de la direction, par contrat, par cahier des charges, par décret, par ordonnance gouvernementale, par des méthodes comptables généralement acceptées, par une bonne expérience des affaires ou d'après une table de multiplication... Mais quelle que soit la façon dont ces normes auront été fixées, l'inspecteur devra les comprendre avant de procéder à ses tests. Il est rare qu'un inspecteur puisse effectuer des tests et affirmer intuitivement, et avec certitude, que les résultats sont bons ou mauvais, sans les avoir confrontés à une norme. Et l'inspection moderne, qui touche à des domaines extérieurs à la comptabilité, pose des problèmes particuliers. Ainsi, la règle "connaître les normes" s'applique tout particulièrement dans ce cas. Et le fait même que l'inspecteur comprenne la nécessité de déterminer les normes avant d'effectuer des tests lui donne, dès le début, une légère avance sur les autres. »

TÉMOIGNAGE

Alain Ledemay, directeur général, Galian

Les exigences de l'autorité de contrôle – l'ACPR pour les sociétés de financement telles que Galian – n'ont cessé d'augmenter au cours de ces dernières années. Audit interne et contrôle permanent sont désormais des impératifs qui, indépendamment de leur mise en œuvre opérationnelle, posent la question des bénéfices pour l'entreprise.

Aussi, face aux coûts associés à ces fonctions, quels sont les retours attendus pour les établissements assujettis ?

Ils sont en fait multiples. La preuve en est si tangible, qu'après avoir mis en place ces fonctions, on n'imaginerait plus s'en passer ! Audit interne et contrôle permanent deviennent au fil du temps, lorsqu'ils jouent efficacement leur rôle, des acteurs à part entière de la stratégie de l'entreprise.

Ainsi, l'audit interne par un plan pluriannuel adapté, couvre les risques structurels de l'entreprise. Interlocuteur privilégié du président, il répond par ailleurs aux exigences de surveillance du comité d'audit et du conseil d'administration. Ses interventions régulières devant ces organes de surveillance garantissent pédagogie et information indépendantes qui favorisent une appréhension concrète des risques et du fonctionnement de l'entreprise.

Le contrôle permanent qui cartographie les risques gérés par les équipes, s'assure que les contrôles prévus dans les filières concernées sont efficaces et que les éventuels dysfonctionnements relevés ne sont pas de nature à mettre l'entreprise en difficulté. Il participe également à l'information régulière de la gouvernance.

On voit dès lors la complémentarité de ces deux piliers du système de contrôle interne, l'audit interne portant de façon périodique et approfondie son regard sur telle ou telle zone sensible, le contrôle permanent scannant de façon continue les risques dispersés au sein de l'entreprise. Ces deux niveaux d'analyse permettent une surveillance et une mesure efficace des risques.

Deux points d'attention sont pris en compte chez Galian pour garantir cette efficacité : l'audit interne doit assurer le suivi rigoureux de ses recommandations et le contrôle permanent veiller à ce que son radar soit toujours positionné au bon niveau, de façon à se concentrer en permanence sur les risques réels, lesquels évoluent avec les activités de l'entreprise.

CHAPITRE 5

Les interlocuteurs

Comme n'importe quel collaborateur de l'entreprise, l'auditeur interne et le contrôleur permanent ont une hiérarchie… Par ailleurs, la bonne réalisation de leurs missions sous-entend l'entretien de relations de proximité avec certaines fonctions.

CE CHAPITRE VOUS PERMETTRA DE :

- connaître les interlocuteurs des deux fonctions ;
- connaître leur hiérarchie au sein de l'entreprise ;
- connaître leurs fonctions partenaires au sein de l'entreprise et en dehors de celle-ci.

1. LA HIÉRARCHIE

L'auditeur interne et le contrôleur permanent font partie d'une ligne hiérarchique :

- assistant → auditeur junior → auditeur senior → responsable de mission → directeur de mission → directeur de l'audit interne ;
- assistant → contrôleur junior → contrôleur senior → responsable de domaine de contrôle → directeur du contrôleur permanent.

Ces deux directions sont par ailleurs rattachées à une fonction d'état-major au plus haut niveau de l'entreprise. Quel que soit son rattachement, ce qui est important est que ces deux fonctions puissent fonctionner en toute indépendance.

1.1. Le point de vue de l'Apec

Le rattachement fonctionnel de l'audit interne et du contrôleur permanent est habituellement :

- la présidence de la société ;
- la direction générale ;
- la direction financière.

La nature des missions varie selon le rattachement hiérarchique : lorsque l'audit interne dépend de la direction générale, les missions sont plus variées, moins centrées sur l'analyse des comptes et des flux financiers. Lorsque le rattachement hiérarchique est la direction financière, les missions sont centrées sur l'audit de sécurité des flux financiers des filiales ou des analyses de rentabilité.

Environnement de travail et les interlocuteurs de l'audit interne :

- Les directions opérationnelles de centres de profit.
- La direction des systèmes d'information.
- Tous les services concernés par les audits réalisés.
- Le comité d'audit.
- La direction des risques ou du contrôle interne.

1.2. L'enquête du CBOK

D'après cette enquête, la direction de l'audit interne est principalement rattachée à la direction générale dans une proportion de deux tiers, plus rarement au comité d'audit ou au directeur financier.

Nos observations montrent que le rattachement des deux fonctions est de plus en plus souvent à la direction générale, et que cette tendance est à l'augmentation, alors qu'il y a quelques années, ce n'était pas le cas. Si l'on regarde dix à vingt ans en arrière, la fonction de contrôle permanent n'existait pas et la fonction d'audit interne, essentiellement centrée sur le respect de la conformité comptable, était rattachée au directeur financier ou au secrétaire général.

2. LES FONCTIONS PARTENAIRES

À l'intérieur de l'entreprise, l'auditeur interne et le contrôleur permanent entretiennent des relations avec des fonctions spécialisées : le contrôle de gestion, le contrôle comptable, les gestionnaires de risques, la qualité, l'organisation informatique…, et également avec les métiers en charge des contrôles opérationnels et de premier niveau.

À l'extérieur de l'entreprise, l'auditeur interne et le contrôleur permanent entretiennent des relations avec les autorités de tutelle et le commissaire aux comptes.

2.1. La fonction « contrôle de gestion »

Le contrôle de gestion assure la synthèse, l'analyse et le suivi du reporting de gestion d'une activité et formule des recommandations.

Principales missions

- Analyser les écarts entre le prévisionnel et le réalisé (rapprochements entre le résultat estimé et le résultat comptable définitif).
- Préparer le budget et les *business plans*.
- Constituer l'information analytique adaptée à chaque niveau de reporting.
- Rédiger les rapports de gestion (budget, point à mi-année, rapport annuel), les notes de synthèse et les présenter.
- Réaliser des analyses ponctuelles à la demande des opérationnels.
- Contribuer à l'amélioration des outils de synthèse.

La fonction fournit donc à l'audit interne et au contrôle permanent des données chiffrées, des alertes, des analyses…

2.2. Le contrôle comptable

Le contrôleur comptable est en charge :

- de produire, d'analyser, d'assurer des corrections éventuelles et de valider les résultats comptables dans le cadre des arrêtés mensuels et trimestriels ;
- d'effectuer les rapprochements entre les résultats économiques et les résultats comptables.
- d'identifier et de justifier de façon détaillée les écarts de méthode ;
- d'effectuer le rapprochement entre les comptes rendus de stocks et les encours comptables ;
- d'identifier et de justifier de façon détaillée les écarts et de procéder aux régularisations ;
- de participer aux projets du pôle et d'être force de proposition pour faire évoluer les outils et les processus.

La fonction fournit à l'audit interne et au contrôle permanent l'assurance que la comptabilité est bien tenue.

2.3. Les gestionnaires de risques

Ils sont en charge du contrôle de deuxième niveau de certains risques tels les risques de sécurité, les risques concernant l'environnement…

Fiche de fonction
Analyste risques de crédit (banque commerciale)

L'analyste risques de crédit contribue à l'ensemble des travaux d'analyse crédit pour un secteur d'activité (aéronautique, immobilier, télécoms, pétrole, etc.).

Ses principales missions consistent à produire dans des délais courts des analyses de crédit et des recommandations sur les nouvelles demandes des métiers et/ou sur les revues de transactions.

À ce titre :

- Il effectue des analyses économiques et financières des contreparties de son secteur, puis expose et argumente ses recommandations en comité.
- Il analyse et valide les financements et les transactions de marchés consentis en évaluant les risques encourus par la banque et il apporte des recommandations pertinentes. Il assure le monitoring et le suivi des transactions dans les systèmes.
- Il participe aux développements méthodologiques internes d'évaluation du risque. Il propose des notations et garantit la mise à jour annuelle des notations et engagements de son secteur.

2.4. La fonction « qualité »

La fonction fournit à l'audit interne et au contrôle permanent des données sur les incidents, les anomalies, les réclamations clientèles…

2.5. La fonction « organisation – informatique »

La fonction fournit à l'audit interne et au contrôle permanent des données sur la structure, les processus, le système d'information…

2.6. Les directions métier de l'entreprise

Elles sont les correspondants de l'audit interne et du contrôle permanent en matière de mise en œuvre des plans de contrôle de premier niveau.

2.7. Les interlocuteurs externes des deux métiers

Ils correspondent aux autorités de tutelle à qui l'audit interne et le contrôle permanent rendent des comptes et aux commissaires aux comptes.

PAROLE D'EXPERT

Lawrence B. Sawyer, quatrième commandement : connaître la « population »

« "Population" est un terme souvent employé dans l'échantillonnage statistique. Cela correspond à l'ensemble des points ou des questions sur lesquels l'inspecteur aura à exprimer une opinion. Et le concept s'applique à toutes les tâches de l'inspecteur, dans le cadre ou non, de l'échantillonnage statistique. L'inspecteur devra déterminer s'il s'occupera uniquement des opérations en cours ou des opérations réalisées durant toute une année ou durant tout un exercice. Lorsqu'il cherche simplement à apprécier le système de contrôle interne actuel, ce qui s'est produit auparavant a moins d'importance que ce qui se passe au moment même. Si, pour la période qui l'intéresse, les opérations sont variées, il devra déterminer, auparavant, le type des opérations dont il s'occupera et ne pas porter son attention sur les autres. Il devra savoir qu'il ne pourra exprimer d'opinion que sur la population, ou partie de celle-ci, qu'il aura vérifiée. Il ne pourra exprimer d'opinion sur ce qu'il n'a pas vérifié. S'il essayait, des faits ultérieurs pourraient le mettre dans l'embarras. Ainsi, déterminer et définir de façon précise ce qui constitue sa population doit être l'un des principes importants de l'inspecteur moderne. Ce principe est implicitement contenu dans le but de l'inspection. Cela permet à l'inspecteur de dire à son lecteur ou à sa direction : "Voilà ce que j'ai fait et sur quoi je peux exprimer une opinion, et voilà ce que je n'ai pas fait et sur quoi je ne peux pas exprimer une opinion." Lors de l'inspection des bilans, l'inspecteur commence normalement ses vérifications à l'aide du solde du grand livre. Ce solde représente un total. C'est un nombre réconfortant à avoir. Tout ce que l'inspecteur vérifiera ou analysera est compris dans cet unique chiffre. De petits nombres épars ne pourront surgir une fois le travail terminé. L'inspecteur moderne qui s'occupe d'opérations non financières devra également rechercher ce total. Il devra pouvoir fixer, pour sa population, des limites ou des paramètres. Il devra connaître exactement ce dont il s'occupe. Pour l'inspection des approvisionnements par exemple, il devra savoir combien d'ordres d'achat ont été établis et à combien ils s'élèvent. Pour une inspection des plans d'ingénierie, il voudra savoir combien de plans ont été mis en circulation le mois écoulé ou l'année précédente, et combien de modifications ont été apportées aux plans au cours de la même période. Pour une inspection de l'équipement, il voudra savoir de combien d'éléments l'équipement se compose, ce qu'ils coûtent, quelle pourrait être leur valeur actuelle et où se trouvent les dossiers centraux. Etc. Pour une inspection, lorsque l'inspecteur connaît sa population, ses perspectives deviennent plus nettes, et le champ d'application de l'inspection devient plus facilement apparent. »

TÉMOIGNAGE

Christophe Estivin, associé, président, In Extenso Finance & Transmission

La principale activité, d'In Extenso Finance & Transmission concerne la cession d'entreprise.

Le rôle des auditeurs est essentiel et très particulier à ce moment de la vie d'une entreprise.

Aucune cession ne peut se traiter sans *due diligence* adaptée aux caractéristiques de l'entreprise, de son métier et de ses hommes.

Les conclusions des auditeurs sont très souvent déterminantes pour fixer le prix définitif, les éventuels compléments de prix, les garanties liées au crédit vendeur et/ou à la GAP (garantie d'actif et de passif). Elles sont aussi indispensables pour prendre la décision finale : acheter ou pas.

Les qualités principales attendues des auditeurs sont les suivantes :

- diplomatie et capacité d'adaptation à des cas et des personnalités très variés ;
- curiosité, habileté pour mener à bien les investigations appropriées ;
- sang-froid et rigueur pour une mission régulièrement menée dans des délais très courts et sous la pression.

L'objectif des auditeurs est double : découvrir et conseiller.

Les enjeux financiers peuvent rapidement être très importants au regard du prix de cession de l'entreprise et ceci dans la durée.

Sur des valeurs de cession d'entreprise entre 1 et 20 millions d'euros, il arrive que les conclusions de l'audit portent sur la moitié de la valeur de cession.

Pour les dossiers de TPE/PME que nous traitons, les audits comptables, juridiques et financiers sont généralement suffisants. Il n'est pas nécessaire de pousser vers d'autres investigations sur les plans technique et scientifique. Le repreneur et, éventuellement, ses directeurs et managers, détiennent l'expertise de la filière métier concernée.

Les qualités requises évoquées précédemment peuvent faire la différence. Une analyse mal maîtrisée des éléments comptables et financiers peut entraîner pour l'acheteur des conséquences financières tout à fait désastreuses.

En conclusion pour être compétitif dans son marché, il y a nécessité de bien acheter avec des conditions d'achats performantes. Les *due deals* permettent ainsi de préserver une valeur d'achat performante et donc une meilleure compétitivité de l'entreprise sur son marché.

Les *due diligence* sont une forme tout à fait aboutie du rôle d'aide à la décision stratégique des auditeurs.

CHAPITRE 6

Les textes encadrant la pratique

Les textes encadrant la pratique de l'audit interne et du contrôle permanent sont de deux natures, réglementaire et professionnelle. En effet, les fonctions d'auditeur interne et de contrôleur permanent sont soumises à une éthique et des pratiques décrites et validées par une association professionnelle internationale.

CE CHAPITRE VOUS PERMETTRA DE :

- connaître la réglementation spécifique aux deux métiers ;
- connaître les textes professionnels régissant l'exercice de la profession.

1. LES TEXTES RÉGLEMENTAIRES

À noter qu'il n'existe pas de texte de portée générale. La mise en place d'un dispositif de gestion des risques et la mise sous contrôle des activités sont considérées comme « une saine pratique » recommandée pour tous et d'autant plus importante que l'entreprise est grande, géographiquement étendue, diverse notamment en termes d'activités… S'il y va de la sécurité des personnes ou de la stabilité économique ou de l'intérêt général, alors le « contrôle » devient une obligation réglementaire.

Ainsi, les textes réglementaires correspondent-ils à la réglementation en vigueur dans certains secteurs. Par exemple :

- Dans le secteur bancaire, supervisé par l'ACPR, la réglementation du contrôle interne est détaillée dans le « Règlement CRBF 97_02 » prévoyant dans son article 6 le métier de contrôleur interne (6a) et celui d'auditeur interne (6b). Le reste du texte détaille sa mission, ses moyens, ses obligations.
- Dans le secteur des services d'investissement, supervisé par l'AMF, la réglementation du contrôle interne est contenue dans le « Règlement général de l'AMF » qui prévoit une responsabilité personnelle du « Responsable de la conformité et du contrôle interne » (RCCI à l'article R313 du RGAMF). Le texte prévoit explicitement ce que doit contrôler le RCCI (contrôleur interne) sous sa responsabilité.

- Dans l'Armée, le commissaire est un officier en charge de la gestion et du contrôle du fonctionnement de l'unité. Dans l'Armée de l'air, il y a plus de trente ans, « l'Instruction 30500 » prévoyait que le commissaire de l'Air a notamment pour mission d'assurer des contrôles internes qu'il documente dans le Registre des actes administratifs (RAA).
- Avec les réformes successives, les différentes administrations (secteur médical, municipalités…) se dotent de dispositifs de contrôle comptable puis de contrôle interne, de contrôleurs interne et enfin de dispositifs de gestion des risques.

Le développement du métier d'auditeur interne va de pair avec le développement de la réglementation de la « gouvernance » dont le but est d'obtenir des « propriétaires » une gestion plus proactive de leur responsabilité. L'auditeur interne est le moyen, pour la gouvernance, d'exercer avec efficacité et professionnalisme sa vigilance.

Le développement du métier de contrôleur interne va lui de pair avec le développement de la réglementation en matière de prévention des risques.

2. LES TEXTES PROFESSIONNELS

Ils concernent l'exercice des métiers d'auditeur interne et de contrôleur permanent quel que soit le secteur d'activité. Ils portent sur les aspects déontologiques et les modalités pratiques d'exercice. Au niveau international, le code de conduite est défini par l'IIA, dont le représentant en France est l'IFACI.

2.1. Le code de conduite de l'IIA

Compte tenu de la confiance placée en l'audit interne pour donner une assurance objective sur les processus de gouvernement d'entreprise, de management des risques et de contrôle, il était nécessaire que la profession se dote d'un code de déontologie allant au-delà de la définition de l'audit interne et incluant deux composantes essentielles :

- Des principes fondamentaux pertinents pour la profession et pour la pratique de l'audit interne.
- Des règles de conduite décrivant les normes de comportement attendues des auditeurs internes. Ces règles sont une aide à la mise en œuvre pratique des principes fondamentaux et ont pour but de guider la conduite éthique des auditeurs internes.

2.2. Les quatre principes fondamentaux

Il est attendu des auditeurs internes qu'ils respectent et appliquent les principes fondamentaux suivants.

Principe 1 : l'intégrité

L'intégrité des auditeurs internes est à la base de la confiance et de la crédibilité accordées à leur jugement. À ce titre, les auditeurs internes :

- doivent accomplir leur mission avec honnêteté, diligence et responsabilité ;
- doivent respecter la loi et faire les révélations requises par les lois et les règles de la profession ;
- ne doivent pas sciemment prendre part à des activités illégales ou s'engager dans des actes déshonorants pour la profession d'audit interne ou leur organisation ;
- doivent respecter et contribuer aux objectifs éthiques et légitimes de leur organisation.

Principe 2 : l'objectivité

Les auditeurs internes montrent le plus haut degré d'objectivité professionnelle en collectant, évaluant et communiquant les informations relatives à l'activité ou au processus examiné. Les auditeurs internes évaluent de manière équitable tous les éléments pertinents et ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui. À ce titre, les auditeurs internes :

- ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de leur organisation ;
- ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel ;
- doivent révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées.

Principe 3 : la confidentialité

Les auditeurs internes respectent la valeur et la propriété des informations qu'ils reçoivent ; ils ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale professionnelle ne les oblige à le faire. À ce titre, les auditeurs internes :

- doivent utiliser avec prudence et protéger les informations recueillies dans le cadre de leurs activités ;
- ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel ou d'une manière qui contreviendrait aux dispositions légales ou porterait préjudice aux objectifs éthiques et légitimes de leur organisation.

Principe 4 : la compétence

Les auditeurs internes utilisent et appliquent les connaissances, les savoir-faire et les expériences requis pour la réalisation de leurs travaux. À ce titre, les auditeurs internes :

- ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires ;
- doivent réaliser leurs travaux d'audit interne dans le respect des normes internationales pour la pratique professionnelle de l'audit interne ;
- doivent toujours s'efforcer d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

PAROLE D'EXPERT

Lawrence B. Sawyer, cinquième commandement : connaître les faits

« Un fait est l'une des choses les plus insaisissables du monde. Il faut du travail, du *know-how*, de l'expérience et de la ténacité pour le découvrir, le saisir et le fixer. Un fait est difficile à prouver. Cependant, l'inspection moderne, malgré les domaines ésotériques où elle pourra se trouver, doit toujours établir ses conclusions sur une fondation solide de faits indiscutables. Un fait est un phénomène réel ou une condition qui existe, quelque chose qui s'est réellement produit, une réalité absolue distincte d'une simple supposition ou d'une opinion. Et avant que l'inspecteur puisse prononcer ces mots sans équivoque : "J'ai trouvé", il doit être sûr qu'il a réellement "trouvé" et qu'il n'est pas simplement en train de faire des suppositions ou de tirer des conclusions hâtives. Le "ouï-dire" n'aura aucune valeur. Il devra pouvoir dire : "Je sais parce que j'ai vu, parce que j'ai vérifié, parce que j'ai contrôlé." Plus d'un inspecteur se laisse induire en erreur par l'évidence du "ouï-dire". Par exemple, quelqu'un en qui il a confiance lui dit ce qu'il pense être un fait. L'inspecteur n'a pas vérifié lui-même le fait. Pourtant, il est possible qu'il admette ce qu'on lui aura dit et le rapporte comme un fait. Mais ce n'est pas un fait. C'est ce que quelqu'un d'autre pense être un fait. L'inspecteur pourra dire, en toute confiance : "Dupont m'a dit que les expéditions ont été retardées de vingt jours en moyenne." C'est un fait, non, pas que les expéditions ont été retardées, mais que Dupont a prononcé la phrase (si, dans la réalité, Dupont a réellement prononcé ces paroles et que l'inspecteur les a soigneusement notées). Les retards présumés dans les expéditions font partie du "ouï-dire". Et l'inspecteur ne peut pas, n'oserait pas, ne doit pas donner une opinion sur quelque chose qu'il n'a pas vu lui-même. Cela m'amène à un problème analogue : prenons le cas d'une personne parfaitement digne de confiance, occupant un poste à un niveau élevé, disant à l'inspecteur : "À mon avis, ces opérations sont traitées d'une façon tout à fait appropriée, vous n'avez pas besoin de vérifier." L'inspecteur qui accepte cette affirmation, et rapporte, qu'à son avis, ces opérations sont effectuées d'une façon appropriée, n'assume pas ses responsabilités. Les dirigeants d'une entreprise désirent, attendent, et sont en droit d'obtenir l'opinion de l'inspecteur, pas de quelqu'un d'autre. L'opinion de l'inspecteur ne peut avoir de substitut. Elle ne peut faire l'objet d'une délégation, c'est une conclusion professionnelle basée sur d'avantage que "simplement des faits". Elle est fondée sur une aptitude solide à analyser les faits, sur une objectivité totale, et sur une formation professionnelle. Elle repose sur l'expérience de nombreuses autres inspections dans lesquelles des conditions semblables ont pu être observées, lorsque ces conditions et la façon dont elles ont été résolues constituent des précédents pour les conclusions de l'inspecteur et lui permettent de renforcer son opinion. Dans la société, personne d'autre n'a cette expérience précise et personne d'autre ne dispose donc de la base nécessaire à une opinion d'inspecteur. La direction d'une entreprise "achète" beaucoup de choses lorsqu'elle achète l'opinion d'un inspecteur. Et l'opinion de quelqu'un d'autre, puisse-t-il être haut placé, ne conviendra pas, tout simplement. Si l'inspecteur n'apprécie pas ou ne peut apprécier les faits lui-même, ou par l'intermédiaire de subordonnés dont il peut vérifier le travail, il n'a pas le droit d'exprimer une opinion sur ces faits. L'inspecteur doit savoir que toute sa réputation repose sur un seul principe simple : s'il dit quelque chose, c'est que c'est vrai. Il peut le prouver et le soutenir parce que ses conclusions s'appuient sur des faits solides, irréfutables. »

TÉMOIGNAGE

Bernard Pédamon, commandant de bord Boeing-777, administrateur Air France KLM de 2004 à 2014

La gestion des risques est au cœur du métier d'une compagnie aérienne. Elle comprend trois étapes essentielles : l'identification des dangers, l'évaluation des risques associés à ces dangers et enfin le contrôle de ces risques, à savoir la détermination de l'acceptabilité du risque. Elle aboutit à la définition des trois grands principes de sécurité des opérations aériennes : maîtriser, récupérer et atténuer, avec comme but de rendre les opérations de la compagnie aérienne « résistantes » aux erreurs humaines comme aux défaillances techniques. Ainsi dans le cadre d'un audit en ligne réalisé à Air France auprès des pilotes en 2011, portant sur l'analyse des dangers, l'approche « Threat and Error Management » (TEM) a été développée afin d'identifier les menaces auxquelles les équipages sont confrontés et les erreurs qu'ils sont susceptibles de commettre tout au long de leur mission. Les menaces sont des événements prévisibles ou imprévisibles qui nécessitent une action immédiate de la part des pilotes si l'une d'elles venait à se réaliser. C'est l'action de l'équipage et la conséquence sur le vol en matière de sécurité qui fait l'objet de toutes les attentions. Lorsque la menace est prévisible, l'équipage doit l'anticiper ; si elle ne l'est pas, il doit la reconnaître quand elle survient et, dans tous les cas, adopter l'action la plus appropriée afin de la contenir le mieux possible. Dans la pratique, les pilotes à chaque phase de vol, mais plus particulièrement au décollage et à l'atterrissage, identifient les menaces du jour et précisent les stratégies qu'ils adopteront si l'une de ces menaces survenait. À l'occasion d'un décollage avec des orages à proximité de l'aéroport, les pilotes brancheront leurs radars pour les éviter une fois en vol et réviseront la procédure à mettre en œuvre en cas de cisaillement de vent (changement brutal de la direction du vent) pendant la course au décollage afin d'agir conformément aux procédures en vigueur en pareil cas. C'est finalement une approche très similaire à celle des entreprises quand elles abordent la question des risques, formalisée dans une cartographie, sachant que, dans le cas d'un équipage en ligne, l'élément majeur de différenciation est le facteur temps.

CHAPITRE 7

L'évaluation des performances

L'évaluation de la performance d'une direction de l'audit interne, d'une direction du contrôle permanent, d'un auditeur ou d'un contrôleur n'est pas chose facile.

CE CHAPITRE VOUS PERMETTRA DE :

- connaître les indicateurs d'évaluation des deux fonctions ;
- connaître les questions permettant l'auto-évaluation d'une direction de l'audit interne ;
- connaître les modalités de certification d'une direction de l'audit interne.

Leur performance doit-elle être jugée « bonne » parce que :

- l'entreprise n'a pas eu de pénalité financière suite à une mission d'audit de son autorité de tutelle par opposition à celles épinglées par l'Autorité de la concurrence ?
- l'entreprise a une bonne réputation durablement et n'est victime d'aucun incident visible de ses clients par opposition, par exemple, à Toyota en 2014 obligé de rappeler 2 millions de véhicules, pour un défaut caché de type « air bag » ?
- les missions d'audit interne et les contrôles permanents ne décèlent pas d'erreur, d'anomalies, de détournements, etc. ?

L'enquête du CBOK a déterminé un certain nombre de critères d'évaluation essentiels.

Critères d'évaluation des performances de l'audit interne

- Délai d'élaboration des rapports d'audit (délai entre l'achèvement des travaux sur site et l'émission du rapport final).
- Recommandations acceptées/mises en œuvre.
- Nombre de missions d'assurance ou de conseil demandées par la direction.
- Durée de la mission d'audit entre la réunion d'ouverture et la diffusion du projet de rapport.
- Confiance des auditeurs externes sur les travaux de l'audit interne.

.../...

.../...

- Taux de réalisation de plan d'audit.
- Nombre de constats d'audit importants.
- Taux de couverture du périmètre.
- Temps passé/temps prévu.
- Enquêtes auprès de clients/de personnes auditées.
- Résolution rapide des défaillances constatées par l'audit.
- Assurance donnée sur le management des risques/le contrôle interne.
- Requêtes/commentaires de conseil, du comité d'audit et/ou de la direction générale.
- Absence de problèmes réglementaires ou de réputation et de dysfonctionnements graves.
- Tableaux de performance (*balanced scorecard*).
- Économies/coûts évités et améliorations grâce à la mise en œuvre des recommandations.

D'après Richard F. Chambers, Charles B. Eldridge et Paula Park, sept qualités personnelles maximisent l'impact des directeurs de l'audit interne et du contrôle permanent les plus performants :

1. un sens aigu de l'activité de l'organisation ;
2. de réelles qualités de communicant ;
3. une intégrité parfaite ;
4. une déontologie sans faille ;
5. une expérience variée ;
6. une excellente connaissance des risques de l'entreprise ;
7. un courage inébranlable.

Tableau 7.1 – Grille de compétences du contrôleur permanent (banque de gestion de fortune)

Niveau 1	Niveau 2	Niveau 3	Niveau 4
Connaissance du vocabulaire, de la réglementation, des procédures et des niveaux de contrôle.	Capacité à utiliser les techniques d'audit au domaine audité.	Capacité à choisir, adapter et mettre en œuvre les techniques d'audit au domaine audité.	Capacité à mettre en œuvre des techniques novatrices pour garantir la pertinence et l'exhaustivité de l'audit.

Les activités et responsabilités clés du contrôleur permanent

- Assurer le contrôle de second niveau pour les domaines confiés en réalisant les contrôles nécessaires selon un plan de contrôle prédéfini ou amélioré, voire défini, par lui.
- Maîtriser les procédures des domaines confiés et s'assurer de leur clarté, de leur pertinence et de leur diffusion. Gérer leur validation (création/mise à jour). Participer à l'analyse des risques liés aux produits et services (notamment opérationnels), à la validation de la pertinence des contrôles de 1er niveau et de leur reprise dans les procédures.
- Assurer la définition et l'optimisation des contrôles de second niveau à réaliser, l'actualisation annuelle du plan de contrôle. Assurer sa présentation au responsable opérationnel du domaine.
- Préparer et conduire les missions de contrôle. Réaliser ou faire réaliser les contrôles nécessaires. S'assurer de l'application des procédures et notamment de la réalisation des contrôles de premier niveau, en respectant les normes de documentation fixées.
- Développer une compréhension et contribuer à l'évaluation du process de bout en bout.
- Préparer les restitutions dans le cadre du reporting du contrôle interne et participer à ces restitutions avec les métiers.
- Contribuer à la rédaction des rapports réglementaires.
- Suivre la correction des erreurs ou anomalies identifiées lors des vérifications. Faire remonter les problèmes graves, non résolus ou excessivement récurrents. Formuler toute recommandation pour sécuriser/optimiser les processus. Suivre et faciliter la mise en œuvre des recommandations de l'audit et du contrôle et en assurer le reporting. Maintenir une connaissance des problèmes opérationnels des domaines et contribuer à leur prise en compte.
- Tenir à jour la documentation du domaine : description, chiffres clés, risques, contrôles de premier et second niveaux. Tenir à jour des indicateurs d'activité, de risques et d'incidents utiles à la cartographie des risques, au ciblage des contrôles et à la mesure des bénéfices des contrôles.
- Coordonner et contrôler l'activité des contrôleurs juniors dans le cadre des missions. Contribuer à la réalisation de leurs objectifs.

Tableau 7.2 – Grille d'évaluation des performances d'un contrôleur permanent (banque commerciale)

Objectifs	Description de l'objectif	Importance relative	Critères de réalisation
Objectif 1	Résultats	15 %	■ Résultat net du groupe : *x* millions d'euros (5 %). ■ Développement des actifs sous gestion : *x* millions d'euros (5 %). ■ RSE : (5 %). ■ Baisse de 5 % de la consommation de papier. ■ Diminution de 2 % des émissions de CO_2. ■ Participation à la formation RSE (*e-learning*).
Objectif 2	Performance collective	10 %	Collectif : ■ Provision pour dépréciation des crédits. ■ Pertes opérationnelles. ■ Mise en place des solutions retenues pour les risques et les contrôles.
Objectif 3	Performance individuelle	40 %	■ Piloter le plan de contrôle assigné au quotidien. ■ Développer la relation avec les responsables de service contrôlés (comprendre l'activité, les enjeux, les projets en cours, les méthodes de travail). ■ Atteindre les objectifs pour les indicateurs du contrôle (Plan/contrôle/procédures/recommandations) au niveau de seuils à préciser au sein de la direction. ■ Réaliser des contrôles pertinents, fiables, bien documentés et discutés avec les services. ■ Remplir les objectifs du Groupe en termes de fréquence des contrôles les plus importants. ■ Finaliser l'ajustement des plans de contrôle, en ligne avec les résultats de la campagne annuelle de revue des risques et des contrôles, les liens entre contrôles de niveau 1 et 2 dans le respect du cadre réglementaire. ■ Adopter l'outil d'eGRC et contribuer à son adoption par les services.
Objectif 4	Transversalité & Synergies	10 %	■ Améliorer le lien entre mise à jour des procédures, analyses de risques et mise à jour des plans de contrôle. ■ S'affirmer comme un référent du domaine contrôlé apte à décrire la situation telle qu'elle est sur le terrain et à comprendre les enjeux de performance des services pour faire des suggestions utiles.

.../...

.../...

Objectifs	Description de l'objectif	Importance relative	Critères de réalisation
Objectif 5	Compliance, Audit et Risques	15 %	■ Pas de note « faible » ou pire, pas de recommandation « haut risque » > 1 mois, pas de recommandation émise ou reçue > 6 mois. ■ Plans d'action finalisés dans les délais. Campagne de revue annuelle des plans de contrôle finalisée selon le planning groupe. Procédures mises à jour dans les délais fixés en ligne avec les contingences éventuelles du projet d'optimisation des processus. ■ Plan de premier niveau en place dans chaque département des risques, avec résultats des contrôles et actions correctives traçables. ■ Procédures revues dans les délais
Objectif 6	Développement Personnel	10 %	Élément propre à chaque collaborateur destiné à développer ses compétences, son employabilité et à favoriser son évolution de carrière.

Les indicateurs de suivi des performances de la direction de l'audit interne et de la direction du contrôle permanent portent sur les résultats de l'activité et également sur des aspects plus financiers.

On distingue ainsi des indicateurs de résultat collectifs, de gestion, de management, de climat social et d'acculturation de l'entreprise au contrôle interne.

1. LES DIFFÉRENTS THÈMES À ÉVALUER

D'une façon habituelle, il est d'usage d'évaluer les thèmes suivants :

- le plan d'audit et la planification ;
- la gestion et le suivi des missions ;
- l'archivage des dossiers ;
- la formation des auditeurs ;
- l'acculturation de l'entreprise au contrôle interne.

L'ÉVALUATION DU PLAN D'AUDIT ET DE LA PLANIFICATION

Pour mesurer l'adéquation des missions réalisée au regard de la cartographie des risques de l'entité :

- Périmètres des domaines sensibles audités = Nombre de domaines sensibles audités/Nombre total de domaines audités × 100 (fréquence annuelle).

Pour mesurer la proportion des activités d'audit interne réalisées par rapport à celles prévues à la planification initiale actée par la direction générale :

- Respect de la planification initiale (en nombre de missions) = Nombre de missions réalisées/Nombre de missions du plan d'audit × 100 (fréquence trimestrielle).
- Respect de la planification initiale (en nombre de semaines terrain) = Nombre de semaines/homme réalisées/Nombre de semaines/homme du plan d'audit × 100 (fréquence trimestrielle).

Pour mesurer le temps consacré aux activités d'audit interne par rapport à l'ensemble des activités de l'unité :

- Temps consacré aux travaux d'audit interne = Nombre de jours/homme réalisés/Nombre total de jours/homme travaillés net (Nombre de jours brut – Congés, formation, maladie et jours fériés) × 100 (fréquence annuelle).

Pour disposer d'une visibilité sur le nombre de missions d'assurance sur le total des missions de l'audit :

- Taux de mission d'assurance = Nombre de jours/homme de missions d'assurance réalisés/Nombre de jours/homme d'audit réalisés × 100 (fréquence annuelle).

Pour s'assurer de la rotation des équipes de l'audit :

- Taux d'utilisation des auditeurs par branche = Nombre de semaines/homme terrain sur un secteur/Nombre total de semaines/homme terrain par l'auditeur × 100 (fréquence trimestrielle).

L'ÉVALUATION DE LA GESTION ET DU SUIVI DES MISSIONS

Pour s'assurer que les personnes auditées sont averties dans les délais de la mission d'audit :

- Taux de conformité à la lettre de mission = Nombre de lettres de mission conformes/Nombre total de lettres de missions × 100 (fréquence trimestrielle).

Pour s'assurer de la qualité de la préparation de la mission :

- Taux de conformité de la préparation = Nombre de semaines/homme de préparation conformes aux prévisions/Nombre total de semaines/homme de préparation × 100 (fréquence trimestrielle).

Pour s'assurer de la correcte documentation des dossiers de travail :

- Taux de documentation des tests = Nombre de dossiers de travail documentés/Nombre total de dossiers de travail × 100 (fréquence trimestrielle).

Pour s'assurer du respect du délai de diffusion du projet de rapport mentionné aux personnes auditées à la fin de la réunion de clôture :

- Taux de conformité du délai de diffusion du projet de rapport = Nombre de projets de rapport envoyés dans les délais/Nombre total de projets de rapport envoyés × 100 (fréquence trimestrielle).

Pour s'assurer du respect du délai de diffusion du rapport final mentionné aux personnes auditées à la fin de la réunion de clôture :

- Taux de conformité du délai de diffusion de rapports finaux = Nombre de rapports finaux envoyés dans les délais/Nombre total de rapports finaux envoyés × 100 (fréquence trimestrielle).

Pour mesurer la valeur ajoutée de l'audit :

- Taux de recommandations acceptées par les personnes auditées = Nombre de recommandations acceptées/Nombre total de recommandations émises × 100 (fréquence trimestrielle).

Pour déterminer le niveau de mise en application des recommandations figurant sur les rapports de mission :

- Taux de recommandations totalement ou en partie mises en œuvre = Nombre de recommandations mises en œuvre en totalité ou en partie/Nombre total de recommandations émises × 100 (fréquence trimestrielle).

Pour mesurer les économies monétaires réalisées, récurrentes ou non, liées à un gain de productivité, à une réduction ou abandon d'une activité :

- Bénéfices monétaires potentiels relatifs aux recommandations = Somme des économies identifiées lors de la réallocation des ressources nécessaires à la réalisation de l'activité concernée/Budget total de l'unité d'audit interne × 100 (fréquence annuelle).

LES INDICATEURS D'ÉVALUATION

L'ÉVALUATION DE L'ARCHIVAGE DES DOSSIERS

Pour s'assurer du classement correct des documents en fin de mission :

- Taux d'archivage des dossiers de travail : nombre de dossiers correctement archivés/nombre total de dossiers × 100 (fréquence trimestrielle).

Pour s'assurer de la destruction des documents de travail, papier ou électroniques de la mission :

- Taux de destruction des dossiers de travail : nombre de dossiers de travail détruits/nombre total de dossiers de travail × 100 (fréquence trimestrielle).

Pour s'assurer de la destruction des dossiers de mission :

- Taux de destruction des dossiers de mission : nombre de dossiers de mission détruits/nombre total de dossiers de mission × 100 (fréquence trimestrielle).

L'ÉVALUATION DE LA FORMATION DES AUDITEURS

Pour s'assurer de la formation continue des auditeurs :

- Nombre total d'heures de formation = Nombre d'heures/homme de formation suivies par les auditeurs (fréquence trimestrielle).
- Taux de participations aux formations demandées = Nombre de formations suivies/Nombre de formations demandées × 100 (fréquence trimestrielle).

L'ÉVALUATION DE L'ACCULTURATION DE L'ENTREPRISE AU CONTRÔLE INTERNE

Pour mesurer la proximité de l'audit interne vis-à-vis de ses parties prenantes :

- Nombre de réunions d'information auprès de la direction générale (fréquence trimestrielle).
- Nombre de réunions d'information auprès du management de l'entreprise (fréquence trimestrielle).
- Nombre de réunions d'information auprès des responsables d'encadrement en charge de la réalisation des contrôles de premier niveau (fréquence trimestrielle).

Pour mesurer les formations réalisées par l'audit interne au bénéfice des parties prenantes :

- Nombre de jours/homme de formation à la direction générale (fréquence trimestrielle).
- Nombre de jours/homme de formation au management de l'entreprise (fréquence trimestrielle).
- Nombre de jours/homme de formation aux responsables d'encadrement en charge de la réalisation des contrôles de premier niveau (fréquence trimestrielle).

2. LES QUESTIONNAIRES D'ÉVALUATION

L'évaluation de la fonction d'audit interne peut être réalisée au travers de questionnaires portant sur différents thèmes et adressés aux différentes parties prenantes : le comité d'audit composé d'administrateurs, la direction générale et les responsables des grandes fonctions et le cabinet d'audit externe. Il est également possible à l'audit interne de faire sa propre introspection à l'aide de questions clés portant sur l'adéquation de ses finalités, indépendance, compétences, résultats… au regard de l'entité.

Les axes d'évaluation peuvent être multiples :

- La mesure de l'atteinte des objectifs de la fonction. Les grilles d'évaluation de l'auditeur interne et du contrôleur interne seront légèrement différentes :
  - pour l'auditeur interne, son apport à la gouvernance sera l'axe testé : prise en compte des attentes du comité d'audit, définition du plan d'audit, mise en œuvre du plan et restitution des résultats ;
  - pour le contrôleur interne, sa capacité à déterminer, conduire et rendre compte d'un plan de contrôle permettant de tenir à jour un tableau de bord du contrôle interne sera l'axe testé.
- La mesure de la qualité perçue par les tiers : un questionnaire de satisfaction peut être établi et soumis aux acteurs interagissant avec nos professionnels (auditeurs et contrôleurs) :
  - compréhension de la mission, des moyens et résultats des interventions ;
  - appréciation des méthodes et restitution ;
  - avis sur la pertinence et l'efficacité ;
  - évaluation de la capacité à s'adapter, à écouter et à réaliser un apport constructif.
- La mesure de la technique employée. C'est probablement le point où les questionnaires seront les plus proches ; les démarches et techniques de ciblage, d'entretien, de test, de conclusion, d'échange et de suivi étant relativement voisins entre les deux métiers, comme en témoigne cet ouvrage.

GUIDE D'ÉVALUATION DES AUDITEURS INTERNES (INSPIRÉE DES TRAVAUX DU AUDIT COMMITTEE INSTITUTE, KPMG)

Questions à l'attention des membres du comité d'audit

Questions sur la compréhension

- L'audit interne démontre-t-il qu'il :
  - reconnaît son devoir d'information direct envers le conseil et le comité d'audit ?
  - comprend parfaitement les responsabilités et le fonctionnement du comité d'audit ?
  - comprend les attentes du comité d'audit et de son président ?
  - comprend l'activité et les risques y afférent ?
- L'audit interne a-t-il toujours une vision réaliste et opérationnelle de l'activité ?

Questions sur la charte et la structure

- La charte de l'audit interne définit-elle :
  - les missions et responsabilités ?
  - les normes de travail ?
  - l'organisation et le processus d'audit ?
  - la référence aux principes, codes, normes en vigueur dans le groupe ?
- La charte de l'audit interne a-t-elle été révisée au cours des deux dernières années ?
- La charte répond-elle aux besoins actuels de l'entité ? À ses besoins futurs ?
- La charte de l'audit interne peut-elle être consultée par tous les membres de l'entité ?
- La structure de l'audit interne facilite-t-elle :
  - une cohérence en termes de qualité des services fournis à l'entité ?
  - la compréhension des problématiques opérationnelles de l'entité ?
  - l'apport d'une valeur ajoutée pour l'entité ?

Questions sur la compétence et l'expérience

- La structure et la composition de l'équipe d'audit interne sont-elles en adéquation avec les recommandations de l'IFACI ?
- Au regard du travail réalisé au cours des douze derniers mois, l'audit interne semble-t-il disposer du personnel adéquat, ayant les compétences nécessaires dans divers domaines spécialisés, tels que l'informatique et la trésorerie ?

- L'équipe d'audit interne bénéficie-t-elle d'un programme de formation continue adéquat ?
- Estimez-vous que l'audit interne soit réellement indépendant par rapport aux activités qu'il doit contrôler ?
- Estimez-vous que le comité d'audit a confiance dans l'audit interne ?

Questions sur la communication

- L'audit interne a-t-il assisté à toutes les réunions du comité d'audit auxquelles il devait assister ?
- L'audit interne a-t-il fait en sorte de pouvoir être consulté hors des réunions du comité d'audit ?
- L'audit interne est-il réceptif concernant les demandes émanant du comité d'audit, et notamment les demandes de contrôles ?
- L'audit interne est-il franc vis-à-vis du comité ?
- L'audit interne traite-t-il correctement les questions délicates ou controversées ?
- L'audit interne s'assure-t-il que le président du comité d'audit est parfaitement mis au courant des conclusions ou des développements significatifs avant la tenue des réunions du comité d'audit ?
- La préparation des réunions du comité d'audit est-elle correctement réalisée par l'audit interne ?
- Les rapports et les comptes rendus de l'audit interne présentés au comité d'audit sont-ils pertinents et précis ?
- L'audit interne a-t-il émis des rapports de façon suffisamment régulière ?
- L'audit interne informe-t-il rapidement le comité d'audit des problématiques significatives et, notamment, concernant des projets spécifiques, tels que les enquêtes sur des fraudes éventuelles ?
- L'audit interne informe-t-il rapidement le comité d'audit de tout changement important apporté au plan d'audit interne ?
- L'audit interne a-t-il la capacité de suivre les problématiques en suspens ?
- L'audit interne a-t-il informé le comité de la manière dont il atteignait un niveau d'assurance raisonnable ?
- L'audit interne partage-t-il ses connaissances de manière proactive avec toute l'entreprise ?

Copyright © 2014 Eyrolles.
GUIDE D'ÉVALUATION DES AUDITEURS INTERNES

Questions sur la performance

- Le plan d'audit est-il exhaustif ?
- La couverture des zones à risque élevé est-elle satisfaisante ?
- Le plan d'audit interne initial a-t-il laissé des points significatifs non couverts ?
- D'après les rapports remis au comité, était-il évident que l'audit interne :
  - avait réalisé les travaux prévus dans le plan ?
  - avait respecté le calendrier convenu au préalable ?
- Existe-t-il une coordination efficace entre les travaux de l'audit interne et ceux de l'audit externe ?
- Des indicateurs de réussite sont-ils utilisés pour évaluer les performances de l'audit interne ?
- L'audit interne offre-t-il des perspectives d'évolution de carrière adéquates à ses équipes ?
- Existe-t-il des systèmes de gratification fondés sur les performances pour motiver les équipes d'audit interne ?
- Considérez-vous que l'audit interne a apporté une valeur ajoutée à l'entité ?
- De manière générale, évaluez-vous comme bonnes les performances de l'audit interne ?

Questions à l'attention des responsables des principales branches d'activité et du directeur financier

Questions sur la planification

- La charte de l'audit interne peut-elle être consultée par tous les membres de l'entité ?
- Les auditeurs internes ont-ils suffisamment planifié et agi en coordination avec les départements concernés préalablement à chaque phase de l'audit ?
- L'audit interne a-t-il discuté avec vous de son approche et des principales zones d'audit identifiées ?
- Avez-vous identifié des zones d'audit critiques qui n'ont pas été examinées par l'équipe d'audit interne ?

Questions sur les compétences et le niveau d'expérience

- Considérez-vous que l'équipe d'audit interne dispose d'une expérience professionnelle, de compétences en matière de gestion de projets, de qualités relationnelles et

d'une ancienneté suffisantes pour pouvoir s'acquitter de manière efficace de ses fonctions ?

- Considérez-vous que l'équipe d'audit interne dispose de connaissances suffisantes dans les domaines de spécialité (tels que l'informatique, la trésorerie) pour pouvoir remplir de manière efficace ses fonctions ?
- Les responsables de l'équipe d'audit interne ont-ils fait preuve d'une bonne connaissance des problématiques les plus significatives pour vous ?
- Les membres de l'équipe d'audit interne ont-ils fait preuve d'indépendance dans toutes leurs délibérations ?
- Pensez-vous que les membres de l'équipe d'audit interne sont indépendants vis-à-vis des activités qu'ils contrôlent ?
- Les membres de l'équipe d'audit interne ont-ils été suffisamment supervisés ?

Questions sur le programme de travail

- Une coopération efficace a-t-elle été établie entre les auditeurs internes et votre département afin d'éviter des perturbations au sein de votre entité ?
- Existe-t-il un processus formel permettant d'assurer que l'audit interne vous tenait informé de l'avancement de l'audit ?
- L'audit interne a-t-il identifié rapidement et vous a-t-il informé sans délai des problématiques critiques et de tout retard ?
- L'audit interne a-t-il proposé des solutions aux problématiques identifiées ?
- Ces recommandations étaient-elles réalistes, solides, et ont-elles été exposées clairement et en temps utile ?
- Comment l'audit interne a-t-il répondu aux besoins de l'entité et, notamment, aux demandes de contrôles spécifiques ?
- Les rapports de l'audit interne étaient-ils :
  - pertinents, clairs et constructifs ?
  - suffisamment détaillés pour permettre à la direction d'agir efficacement ?
  - émis dans les délais prévus ?
- Les conclusions de l'audit interne ont-elles été discutées avec vous avant leur présentation au comité d'audit ?
- L'audit interne a-t-il effectué un suivi des recommandations qu'il avait formulées, afin de voir si elles avaient été appliquées ?
- Existe-t-il de sérieux désaccords entre vous et l'audit interne n'ayant pu être réglés ?

Copyright © 2014 Eyrolles.
GUIDE D'ÉVALUATION DES AUDITEURS INTERNES

Question sur la performance globale

- Considérez-vous que l'audit interne a apporté une valeur ajoutée à votre entité ?

Questions à l'attention de l'auditeur externe de la société mère et des filiales

Question sur la mission

- Compte tenu de votre connaissance des bonnes pratiques applicables à l'audit interne et au secteur d'activité, considérez-vous que le niveau de qualité des missions actuelles de l'audit interne reste élevé ?

Questions sur les compétences et l'expérience

- Considérez-vous que l'équipe d'audit interne dispose d'une expérience professionnelle, de compétences techniques, de qualités relationnelles et d'une ancienneté suffisantes pour pouvoir s'acquitter de manière efficace de ses missions ?
- Le niveau de connaissance des responsables de l'équipe d'audit interne concernant l'entité, son activité et les risques en jeu sont-elles suffisantes ?
- L'expérience de l'équipe d'audit interne dans les domaines de spécialité clés, par rapport aux connaissances nécessaires pour s'acquitter correctement de ses missions et responsabilités, est-elle suffisante dans les domaines suivants : informatique ? trésorerie ? comptabilité ? fiscalité ? achats ?
- Compte tenu de vos relations avec les membres de l'équipe d'audit interne et de votre connaissance des bonnes pratiques applicables à l'audit interne et au secteur d'activité, considérez-vous que l'audit interne dispose des ressources suffisantes pour s'acquitter de ses missions ?
- Les ressources de l'audit interne sont-elles suffisantes pour réaliser correctement les services définis dans son plan d'audit interne, dans les délais précisés ?
- La structure et la composition de l'équipe d'audit interne facilitent-elles la compréhension des problématiques opérationnelles de l'entité ?
- La structure et la composition de l'équipe de l'audit interne sont-elles en adéquation avec les recommandations de l'IFACI ?
- Selon vous, la méthodologie utilisée par l'audit interne est-elle solide et reflète-t-elle les tendances récentes en matière d'audit interne ?

Questions sur le programme de travail

- L'audit interne et externe échangent-ils régulièrement sur l'évaluation des risques ?

- L'audit interne et externe ont-ils échangé régulièrement sur l'avancement des travaux par rapport au plan d'audit ?
- Avez-vous reçu des copies de tous les rapports émis par l'audit interne ?
- Les copies des rapports d'audit interne ont-elles été reçues de façon régulière ?
- Les rapports de l'audit interne sont-ils d'un niveau comparable à ceux d'autres entités ?
- À votre connaissance, existe-t-il des zones de risques ou des problématiques que l'audit interne semble ne pas avoir couverts ?

Questions à l'attention du responsable de l'audit interne (auto-évaluation).

Questions sur la compréhension

- Les responsabilités et le fonctionnement du comité d'audit sont-ils efficaces ?
- L'activité de l'entité répond-elle aux standards de la profession ?
- Les risques majeurs auxquels l'entité est confrontée sont-ils tous pris en compte dans les missions d'audit ?
- Le système de contrôle de l'entité est-il adapté ?

Question sur la charte et la structure

- La charte de l'audit interne définit-elle de façon suffisamment détaillée :
  - les missions et responsabilités ?
  - les normes de travail ?
  - l'organisation et le processus d'audit ?
  - la référence aux principes, codes et normes en vigueur dans le groupe ?
- L'étendue actuelle des missions de l'audit interne répond-elle aux besoins actuels de l'entité ?
- À ses besoins futurs ?
- La structure de l'audit interne doit-elle s'améliorer en termes :
  - d'objectivité ?
  - de compréhension des problématiques opérationnelles de l'entité ?
  - de capacité à répondre aux problématiques opérationnelles de l'entité ?

Questions sur les compétences et l'expérience

- La structure et la composition des équipes d'audit interne sont-elles en adéquation avec les recommandations de l'IFACI ?
- La composition et les compétences de l'équipe d'audit interne sont-elles adaptées ?
- Le degré d'indépendance des équipes d'audit interne est-il satisfaisant par rapport aux activités qu'elles doivent contrôler ?

Questions sur la communication

- L'audit interne est-il réactif concernant des demandes émanant du comité d'audit et, notamment, des demandes de contrôles spécifiques ?
- L'audit interne agit-il de façon franche vis-à-vis du comité ?
- L'audit interne traite-t-il de façon appropriée les problématiques critiques ou controversées ?
- Au cours des douze derniers mois, le président du comité d'audit a-t-il été parfaitement mis au courant des conclusions et des développements significatifs avant la tenue des réunions du comité d'audit ?
- Le processus d'audit interne visant à contrôler la résolution de problématiques en cours est-il efficace ?

Questions sur la performance

- L'audit interne apporte-t-il de la valeur ajoutée à l'entité ?
- Les performances de l'audit interne sont-elles bonnes ?

3. LA CERTIFICATION DE LA DIRECTION DE L'AUDIT INTERNE

L'évaluation du niveau de performance d'une direction de l'audit interne peut se faire dans le cadre d'une certification de celle-ci au regard de bonnes pratiques professionnelles. Cette certification permet de garantir un niveau de performance et de légitimité à la fonction, tout en la plaçant dans une logique de progrès continu.

Officiellement reconnue et promue par l'Institut international de l'audit interne (IIA) et la Confédération européenne des instituts d'audit interne (ECIIA), la certification est recherchée par les instances de direction pour l'assurance donnée sur la fonction d'audit interne, composante clé du dispositif de contrôle interne de leur organisation.

La certification donne donc l'assurance raisonnable que la direction de l'audit interne se focalise sur les bonnes priorités métier et risques, optimise la qualité de ses activités, et répond aux préoccupations des instances dirigeantes.

Plus concrètement, l'intérêt de la certification est de :

- donner l'assurance aux parties prenantes de l'entreprise sur le professionnalisme avec lequel sont évalués les processus de gestion des risques et de contrôle interne ;
- affirmer la capacité de l'audit interne à éclairer la décision managériale dans les domaines à forts enjeux, et à accompagner les projets innovants de l'organisation ;
- conforter la stature et la visibilité de l'audit interne au sein de l'organisation, par une reconnaissance de sa valeur reconnue par un organisme indépendant ;
- pérenniser, perfectionner et homogénéiser l'organisation et les pratiques ;
- fédérer les auditeurs autour d'un projet dynamique et exigeant, permettant d'attirer, de former et retenir les meilleurs professionnels.

En France, la certification peut être obtenue depuis 2005 par l'IFACI jouant dans ce cas le rôle d'évaluateur externe. Cette certification repose sur le Référentiel professionnel de l'audit interne (RPAI), lui-même issu de normes internationales d'audit interne, composé de trente exigences générales classées en trois catégories : moyens, prestations et pilotage.

La certification confirme donc qu'un département d'audit interne se concentre bien sur les enjeux de son organisation et répond aux cinq préoccupations fondamentales des instances dirigeantes :

- Sécurité : a pris les dispositions nécessaires pour vérifier que les processus de management des risques et de contrôle interne sont bien maîtrisés, dans le cadre des moyens financiers accordés.
- Économie : est mis en œuvre sur la base de ressources technologiques et humaines en nombre et qualité adéquats, avec un coût financier maîtrisé.

- Efficience : assure le meilleur rapport entre la qualité de ses prestations et les ressources humaines et technologiques employées.
- Efficacité : délivre des résultats et apporte de la valeur conformément aux objectifs établis en concertation avec les instances dirigeantes.
- Pertinence : oriente ses objectifs vers la maîtrise des risques majeurs menaçant l'atteinte des objectifs principaux de l'organisation.

QUESTIONNAIRE SUR L'INTÉRÊT DE LA CERTIFICATION À DESTINATION DU MANAGEMENT D'UNE DIRECTION DE L'AUDIT INTERNE

Secteur :

Ancienneté :

Différents postes occupés à l'audit :

- Quel est, selon vous, l'objectif, l'intérêt de la certification d'un service d'audit interne ?
- Avez-vous participé à une mission de certification ? Si oui combien de fois ?
- Quelles impressions en tirez-vous ?/Quelle perception en avez-vous ?
- Suite aux différents audits de certification, avez-vous constaté des évolutions dans le département d'audit ? Si oui sur quels points ?
- Que voyez-vous aujourd'hui comme points forts de la démarche de certification ?
- Quels sont selon vous les points faibles de cette démarche, les freins éventuels (disponibilité, intérêt de la démarche, coût…) ?
- Quels sont, selon vous, les apports/la valeur ajoutée de la certification ?
- Comment est perçue la certification par les parties prenantes de l'audit, notamment les audités ? Pensez-vous que la certification leur apporte un plus ? Si oui lequel ?
- La certification a-t-elle modifié votre manière de travailler ? De percevoir votre métier ?
- Selon vous, l'audit groupe doit-il continuer à se certifier, indépendamment de ce que dictent les normes ?

Tableau 7.3 – Résultat d'une enquête interne sur les apports d'une certification de la direction d'audit interne

Apports	Pour la DG et le comité d'audit	Pour la direction de l'audit interne	Pour les métiers audités
Apports internes			
Aiguillon		X	
Amélioration des méthodes de travail		X	
Diffusion des bonnes pratiques de la profession		X	
Mobilisation des équipes		X	

.../...

QUESTIONNAIRE SUR LA CERTIFICATION

.../...

Apports externes			
Communication		X	
Conformité aux normes d'audit interne		X	
Conformité à la qualité de la direction de l'audit interne	X		
Confort dans la conduite des missions d'audit			X
Crédibilité de la direction de l'audit interne	X		X

PAROLE D'EXPERT

Lawrence B. Sawyer, sixième commandement : connaître les causes

« Les problèmes abondent dans les affaires. Toute déficience importante que l'inspecteur découvre au cours de son inspection présente un problème nécessitant une solution. L'inspecteur de la vieille école le désigne du doigt et dit : "Réglez-le." L'inspecteur moderne décrit une situation et suggère une solution. Mais, avant de résoudre un problème, il faut en connaître les causes. Une bande adhésive ne guérira pas une blessure profonde et infectée. Elle ne fera que la dissimuler. Dans les affaires, de nombreux problèmes se présentent comme un défaut de surface. Il faut approfondir pour trouver ce qui se cache en dessous et ce qui provoque vraiment la difficulté. Aussi, lorsque l'inspecteur détermine, d'après ses tests et observations, qu'il existe un problème, problème nécessitant une solution, la direction attend de lui qu'il en recherche la cause. Aucun problème important ne peut être résolu définitivement si les causes ne sont pas trouvées. Comment l'inspecteur moderne recherche-t-il les causes ? Il sait que chaque problème n'a qu'une seule cause réelle, c'est-à-dire un événement ou association d'événements qui produira toujours le résultat indésirable. Comme dans une expérience de laboratoire, chaque fois que certains éléments seront combinés, il en résultera certains effets. Il sait également que chaque problème signifie que l'on s'est écarté d'une norme ou d'un résultat prévus. Il s'en suit donc que la cause d'un problème doit être attribuée à quelque changement. Pour rechercher ce changement, l'inspecteur moderne :

- identifiera le problème avec précision ;
- le décrira en termes de temps et d'étendue ;
- isolera le changement précis ayant provoqué l'écart de la norme.

Il sait que lorsqu'il décrit une situation à la direction, la première question est habituellement : "Pourquoi cela est-il arrivé ?" Et la direction s'attend à ce que l'inspecteur lui donne une réponse, la cause qui a créé la situation. »

TÉMOIGNAGE

Jean-Baptiste Parnaudeau, responsable du contrôle interne de SITA Recyclage (Suez Environnement)

Le métier de contrôleur interne, souvent méconnu des étudiants et du monde universitaire, est particulièrement exigeant et captivant. En effet, au carrefour du juridique, du financier et de l'opérationnel, le contrôleur interne est un véritable partenaire de la direction générale dans sa maîtrise de l'activité, et il trouve toute sa place dans la ligne managériale de gestion des risques. C'est tout du moins ainsi qu'il est vécu dans les activités de recyclage de SITA, filiale de Suez Environnement.

La difficulté du métier, qui fait aussi son côté passionnant, tient à la manière de présenter le contrôle interne et de le mettre concrètement en application : le contrôleur interne doit trouver un équilibre entre l'aspect « compliance », ou réglementaire (nécessaire), et l'aspect « conseil », qui va permettre d'intégrer le contrôle interne dans les gènes de l'entreprise et faire en sorte que le contrôle interne soit « auto-portant ». Ce dosage change en fonction de la culture préexistante dans l'entreprise ou les filiales, et rend primordial un accompagnement du changement. C'est particulièrement vrai lors de croissances externes, et de l'intégration de petites structures (PME, start-up...) : les exigences du contrôle interne se heurtent alors souvent à deux barrières : celle d'une hypercentralisation, où tous les pouvoirs sont concentrés dans les mêmes mains, ou, à l'inverse, celle de la confiance « illimitée » faite aux salariés. Comportements humains, mais incompatibles avec une maîtrise raisonnable de son activité.

La complémentarité du contrôle interne avec les commissaires aux comptes et avec les fonctions d'audit interne est très forte. Ces deux organes de contrôle ponctuels vont pouvoir se reposer sur le dispositif de contrôle interne, si celui-ci est jugé adéquat à l'issue de la revue et des tests faits. Le contrôle interne y trouve également son compte, car l'évaluation faite par les CACs et l'audit interne va lui donner un retour et un regard externe sur son travail, à la fois sur l'adéquation des contrôles aux risques qu'ils entendent maîtriser et sur le travail des personnes en charge de faire les contrôles.

Au quotidien, un contrôleur interne doit donc montrer des capacités d'écoute, de prise de recul, d'intégrité et de rigueur dans son jugement, ainsi que des qualités de communication vers tous les collaborateurs de la société, de l'opérateur de tri jusqu'au conseil d'administration. Mais il doit avant tout faire preuve de bon sens et de tact.

En résumé

Cette deuxième partie a présenté l'environnement des métiers d'auditeur interne et de contrôleur permanent et plus précisément :

- une description de leur positionnement possible dans l'organigramme, la description des différents grades des deux métiers ;
- les fonctions avec lesquelles ils entretiennent des relations privilégiées au sein de l'entreprise :
  - contrôle de gestion,
  - contrôle comptable,
  - gestionnaires de risques,
  - qualité,
  - organisations,
  - directions métier ;
- les fonctions avec lesquelles ils entretiennent des relations privilégiées à l'extérieur de l'entreprise :
  - autorités de tutelle,
  - commissaires aux comptes ;
- les textes encadrants les deux métiers, tels le « code de conduite » de l'IAA mettant en avant quatre principes de comportement fondamentaux :
  - l'intégrité,
  - l'objectivité,
  - la confidentialité,
  - la compétence ;
- les critères d'évaluation de la performance des deux métiers :
  - plan d'audit et planification,
  - gestion et suivi des missions,

  - archivage des dossiers,
  - formation,
  - acculturation de l'entreprise au contrôle interne ;
- la certification de la direction de l'audit interne ;
- quatre témoignages illustrant nos propos :
  - Alain Ledemay a posé la question de la rentabilité des deux fonctions dont la mise en œuvre à été rendue obligatoire chez Galian par la réglementation. Par ailleurs, il a apporté un éclairage sur la complémentarité des deux fonctions,
  - Christophe Estivin a montré en quoi l'intervention de l'audit dans les missions de due diligence réalisées par In Extenson, Finance & Transition pour le compte de ses clients, est déterminante dans le prix de cession d'une entreprise,
  - Bernard Pedamon a montré en quoi une démarche organisée de gestion des risques au sein d'Air France KLM, basée sur une cartographie et se traduisant par des actions à entreprendre face à des risques identifiés, notamment au décollage et à l'atterrissage, est de nature à sécuriser les vols,
  - Jean-Baptiste Parnaudeau a montré en quoi l'audit, métier passionnant, est, chez SITA Recyclage, un partenaire de la direction générale et également de toute l'entreprise et de la ligne managériale de gestion des risques ;
- les troisième, quatrième, cinquième et sixième commandements de Lawrence B. Sawyer : « connaître les nomes », « connaître la population », « connaître les faits » et « connaître les causes ».

Le questionnaire qui termine cette deuxième partie va maintenant vous permettre de tester vos connaissances…

TEST DE CONNAISSANCE

Ce questionnaire a pour objectif de vous aider à faire le point sur vos connaissances des métiers de l'audit interne et du contrôle permanent et plus précisément sur l'environnement des métiers d'auditeur interne et de contrôleur permanent.

Pour ce faire :

- répondez aux questions ci-après en choisissant pour chacune d'entre elles : « je pense » ou « je ne pense pas » ;
- à chaque fois que vous avez répondu : « je ne pense pas », à une question, relisez le passage du livre indiqué.

Questions

1. D'après l'IFACI, l'audit interne est « une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise et en faisant des propositions pour renforcer leur efficacité ».

   (Réponse : chapitre 4, les missions de la direction de l'audit interne, p. 101.)

2. D'après l'IFACI, le contrôleur permanent « métier », rattaché à une direction support ou à une direction métier, a pour fonction « d'accompagner et conseiller les lignes opérationnelles et fonctionnelles concernées par la mise en œuvre d'un dispositif de contrôle interne cohérent avec les orientations définies au niveau du groupe ».

   (Réponse : chapitre 4, le contrôleur permanent, p. 109.)

3. À l'intérieur de l'entreprise, l'auditeur interne et le contrôleur permanent entretiennent des relations avec des fonctions spécialisées : le contrôle de gestion, le contrôle comptable, les gestionnaires de risques, la qualité, l'organisation informatique… et également avec les métiers en charge des contrôles opérationnels et de premier niveau.

   (Réponse : chapitre 5, les fonctions partenaires, p. 114.)

TEST DE CONNAISSANCE

4. Les quatre principes fondamentaux du code de conduite de l'IIA s'appliquant aux auditeurs internes et contrôleurs permanents sont l'intégrité, l'objectivité, la confidentialité et la compétence.

   (Réponse : chapitre 7, le code de conduite de l'IIA, p. 120.)

5. Les indicateurs de suivi des performances de la direction de l'audit interne et de la direction du contrôle permanent portent sur l'évaluation du plan d'audit et de la planification, l'évaluation de la gestion et du suivi des missions, l'évaluation de l'archivage des dossiers, l'évaluation de la formation des auditeurs et l'évaluation de l'acculturation de l'entreprise au contrôle interne.

   (Réponse : chapitre 7, les différents thèmes à évaluation, p. 129.)

6. L'évaluation de la fonction d'audit interne peut être réalisée au travers de questionnaires portant sur différents thèmes et adressés aux différentes parties prenantes : le comité d'audit composé d'administrateurs, la direction générale et les responsables des grandes fonctions et le cabinet d'audit externe.

   (Réponse : chapitre 7, les questionnaires d'évaluation, p. 133.)

7. La certification donne donc l'assurance raisonnable que la direction de l'audit interne se focalise sur les bonnes priorités métier et risques, optimise la qualité de ses activités, et répond aux préoccupations des instances dirigeantes.

   (Réponse : chapitre 7, la certification de la direction de l'audit interne, p. 141.)

PARTIE 3 L'EXERCICE DES MÉTIERS D'AUDITEUR INTERNE ET DE CONTRÔLEUR PERMANENT AU QUOTIDIEN

Copyright © 2014 Eyrolles.

La perte record de la Société Générale

Jérôme Kerviel entre en août 2000 à la Société générale au sein de la division banque d'investissement et de financement (SG CIB) dans son siège social à La Défense. Il travaille d'abord au *middle office* et au *back office*, avant de passer en 2005, au *front office*. Il est alors en charge de l'arbitrage sur des contrats à terme portant sur des indices boursiers. Le 24 janvier 2008, à l'occasion de la publication des résultats de son exercice 2007, la direction de la Société Générale organise une conférence de presse afin de dévoiler l'affaire dont elle se dit victime. D'après Daniel Bouton, P.-D.G. de la banque, un opérateur de marché, faisant partie de ses effectifs, aurait exposé la banque à un risque de marché alors que ce n'était pas dans ses attributions. Il aurait accumulé des positions acheteuses sur les contrats à terme portant sur indice et dissimulé ces opérations faites sur le marché en introduisant dans le système informatique de la Société Générale des opérations inverses fictives les compensant. Le trader aurait pris des positions plutôt heureuses en 2007, réussissant à masquer l'importance et le risque des positions qu'il avait prises grâce à sa très bonne connaissance des procédures de contrôle interne, connaissances qu'il aurait acquises lors de ses quelques années passées au *middle office*. Il n'y aurait eu, selon les dirigeants de la banque, aucun enrichissement personnel. Selon la banque, il aurait reconnu lors de l'enquête interne de la Société Générale au moment de la découverte de ses malversations, avoir effectué les opérations litigieuses et les avoir masquées. Lorsque les positions secrètes ont été découvertes le 18 janvier 2008, la perte latente enregistrée était assez faible au vu des montants engagés, mais la Société générale a estimé que cela l'exposait à des risques considérables. Le P.-D.G. de la banque, Daniel Bouton a ainsi déclaré que « si une guerre avait éclaté lundi ou si les marchés avaient chuté de 30 %, la Société Générale (GLE) risquait le pire avec une telle exposition ». La banque a donc préféré déboucler dans le secret les positions au plus vite en vendant pour 60 milliards d'euros d'options du lundi au mercredi suivant, mais jouant alors de malchance avec la chute des places financières, elle enregistre une moins-value nette record de 4,9 milliards d'euros (sur un bénéfice annuel 2007 estimé préalablement à 7 milliards d'euros). La Société Générale a procédé au débouclage de ses positions en respectant les seuils de volume maximum recommandés par les autorités financières. Pour pouvoir atteindre une telle perte, les montants engagés étaient de l'ordre de 50 milliards d'euros concentré sur des *futures* à fort effet de levier portant sur les indices Eurostoxx, DAX et Footsie. Le trader a été condamné une première fois le 5 octobre 2010 pour abus de confiance, faux, usage de faux et introduction frauduleuse de données dans un système automatisé par le tribunal correctionnel de Paris et a fait appel de la décision. Le 24 octobre 2012, la cour d'appel de Paris, confirmant le jugement de première instance, condamne Jérôme Kerviel à une peine de cinq ans de prison dont deux ans assortis du sursis. La juridiction le condamne par ailleurs à rembourser en totalité le préjudice subi par la Société Générale, partie civile, qui s'élève à un peu plus de 4,91 milliards d'euros. Le 19 mars 2014, la Cour de cassation confirme la condamnation de Jérôme Kerviel à la prison mais annule les dommages et intérêts de 4,9 milliards d'euros. Depuis le 18 mai 2014, il purge sa peine de trois ans de prison…

Source : http://fr.wikipedia.org/wiki/Jérome_Kerviel (texte sous Licence Creative Commons CC BY-SA 3.0)*Source : L'Express*, 16 décembre 2008.

INTRODUCTION

La troisième partie présente l'activité des deux métiers au quotidien. Pour développer ce thème, nous nous sommes appuyés tout d'abord sur la démarche et les outils que nous utilisons dans notre pratique quotidienne, outils également utilisés par de nombreuses équipes d'auditeurs internes et de contrôleurs permanents. La plupart de ces outils sont anonymes ; d'autres en revanche, ont une origine identifiée : le diagramme de Pareto, le management situationnel, la méthode AMDEC, la pyramide des besoins ou la carte des forces. Pour les compétences relationnelles et comportementales, nous avons trouvé nos sources auprès de l'APEC, du site Letudiant.fr, de l'Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque et de l'enquête du CBOK.
Vous y trouverez la description des travaux à réaliser dans le cadre du cycle annuel de l'audit interne et du contrôle permanent tels que :

- le programme d'audit et le plan de contrôle permanent ;
- le rapport annuel sur l'état du dispositif de contrôle interne.

Vous y trouverez également les outils communs aux deux métiers :

- la cartographie des risques ;
- la méthode AMDEC ;
- les fondamentaux de contrôle ;
- les procédures ;
- l'analyse fonctionnelle ;
- le tableau des risques ;
- les indicateurs de tendance centrale ;
- la carte de contrôle ;
- le relevé de non-conformité ;
- les sondages ;
- l'hexamètre de Quintilien ;
- les questions écrites ;
- les vérifications ;

- les rapprochements ;
- les questionnaires de contrôle interne ;
- les auto-évaluations ;
- la narration ;
- l'organigramme fonctionnel ;
- la grille d'analyse des fonctions incompatibles ;
- le diagramme de circulation ;
- les contrôles ;
- la grille « gravité/probabilité » ;
- la feuille de révélation et d'analyse de problème ;
- le test de cheminement ;
- le diagramme de Pareto ;
- le *benchmarking* ;
- le *brainstorming* ;
- le plan d'action ;
- la carte des forces ;
- l'analyse SWOT.

Vous y trouverez aussi les types de compétences que les auditeurs internes et contrôleurs permanents doivent posséder ou développer telles :

- la pratique de la communication verbale et non verbale ;
- les techniques de communication telles la PNL ;
- l'écoute active ;
- les techniques d'entretien ;
- la conduite de réunion ;
- la présentation orale ;
- les règles de rédaction (critères de lisibilité) ;
- les règles d'élaboration de « transparents » ;
- l'art du plan avec des méthodes telles « ESPRIT » ou « Minto » ;

- la compréhension de la répartition des rôles au sein d'une équipe ;
- les types de besoins recherchés par une personne ;
- le management situationnel.

Vous y trouverez également la démarche de conduite d'une mission d'audit interne :

- la préparation de la mission (choix de l'équipe, étude préliminaire, prise de connaissance, entretien avec le management de l'entité auditée, préparation du programme de travail) ;
- la réalisation des travaux terrain (réunion d'ouverture, tests d'audit, formalisation des constats et présentation, réunion de clôture de phase de vérification) ;
- la conclusion et restitution (réunion de restitution, réunion de validation).

Vous y trouverez également les outils spécifiques correspondants :

- la lettre de mission ;
- les papiers de travail ;
- les dossiers permanents et le dossier de mission ;
- la note d'orientation ;
- la feuille de couverture ;
- le projet de rapport d'audit ;
- les standards de qualification ;
- les termes de hiérarchisation ;
- les expressions de recommandation ;
- le rapport final.

Vous y trouverez également cinq témoignages illustrant nos propos :

- Manon Mourier des Gayets montre en quoi l'audit interne et les commissaires aux comptes permettent de donner aux contributeurs la garantie d'une gestion rigoureuse et transparente des fonds collectés par l'ONG SOS Sahel International France ;
- Éric Guilhou montre l'importance de disposer d'un référentiel de contrôle interne dans une entreprise de service telle Socotec, notamment dans un contexte de changements permanents ;

- Patrick Georgelin montre quant à lui que le contrôle interne ne se limite pas aux organisations de taille importante mais concerne également les PME-PMI et suppose d'être confié à une personne de toute confiance ;
- Olivier Faujour insiste sur les profils et qualités que les auditeurs internes doivent posséder pour être en mesure de contribuer pleinement au développement d'une entreprise internationale telle que Yoplait ;
- Xavier Tremblay présente l'exercice des métiers d'expert comptable et de commissaire aux comptes tels que normés par la Compagnie nationale des commissaires aux comptes.

Vous y trouverez aussi les septième, huitième, neuvième et dixième commandements de Lawrence B. Sawyer : « connaître l'effet », « connaître les personnes », « savoir communiquer et à quel moment » et « connaître les méthodes modernes ».

Un questionnaire en fin de partie vous permettra de tester vos connaissances.

CHAPITRE 8

Le cycle annuel du contrôle

CE CHAPITRE VOUS PERMETTRA DE :

- connaître le cycle annuel du contrôle au sein d'une entreprise :
  - débutant par le programme d'audit pour la fonction d'audit interne et plan de contrôle pour la fonction de contrôle permanent ;
  - et se terminant par le rapport annuel sur l'état du dispositif de contrôle interne.

L'audit interne et le contrôle permanent interviennent selon plusieurs cycles. Le cycle annuel est présenté dans cette partie. Il démarre avec la détermination des contrôles qui seront réalisés dans l'année à venir sous la forme d'un programme d'audit (niveau 3) et d'un plan de contrôle permanent (niveau 2). Le cycle annuel se termine avec la rédaction d'un bilan des missions d'audit et des contrôles permanents réalisés dans l'année sous la forme d'un document faisant en quelque sorte l'état des lieux des contrôles face aux risques identifiés. Ces deux « livrables » sont parfaitement complémentaires. Mieux, ils se nourrissent l'un de l'autre et constituent, rappelons-le, avec les contrôles opérationnels et les contrôles de niveau 1 (hiérarchiques) le dispositif de maîtrise.

On peut parler de « cycle » dans les activités de nos deux métiers, pour les raisons suivantes :

- Pour l'auditeur interne, sa mission est de « couvrir dans le plus petit nombre d'exercices possibles l'ensemble du périmètre d'audit » (réglementation bancaire). Pour une activité et une organisation données, une entreprise a ainsi un nombre fini « d'objets d'audit » (Unités opérationnelles, systèmes d'information ; thématiques, prestataires…). Chacun de ces objets d'audit a une priorité, en fonction de son importance pour l'entreprise et des risques qu'il porte. Sur la base de l'inventaire priorisé des objets d'audit, l'audit interne prépare un plan d'audit pluriannuel soumis à la gouvernance. Reste à mettre en œuvre et rendre compte de ce plan. La gouvernance dispose ainsi d'un diagnostic professionnel périodiquement (au rythme du cycle du plan d'audit) mis à jour.

- Pour le contrôleur interne, la cartographie des risques et des processus de l'entreprise, son domaine d'intervention, joue un rôle assez similaire. Ce périmètre doit être surveillé et une information doit aboutir aux niveaux de responsabilité adéquats de l'entreprise. Il y a ici aussi une notion de cycle, la surveillance permanente s'appuyant sur des cycles de contrôles couvrant au fur et à mesure le périmètre. Il y a une autre notion de cycle à laquelle le contrôleur interne contribue : celle de la gestion et la maintenance du dispositif de contrôle interne de l'entreprise. Ainsi, une analyse est faite conduisant à la conception et à la mise en place d'un dispositif de maitrise des risques (DMR) qui est alors mis en œuvre (et fait l'objet des contrôles et rapports du contrôleur interne). À l'issue de l'exercice, les acteurs de risques, du contrôle et les métiers opérationnels se retrouvent et font le bilan et l'actualisation de ce dispositif pour l'adapter et l'améliorer ; et le cycle recommence alors.

LE PROGRAMME D'AUDIT ET LE PLAN DE CONTRÔLE

Élaboré au quatrième trimestre de l'année $n-1$ à partir de la cartographie des risques, des sinistres constatés au cours de l'année, des modifications de l'organisation ou des prestations et produits commercialisés par l'entreprise, des recommandations émises par les corps de contrôle internes et externes, validé par la direction générale de l'entreprise, le programme d'audit et le plan de contrôle présentent les contrôles qui seront réalisés dans l'année. Le programme d'audit présente les contrôles de troisième niveau dits « périodiques » qui seront réalisés sous la forme de missions d'audit par l'audit interne dans l'année. Il comporte : la liste des missions d'audit qui seront réalisées dans l'année, leur objectif, leur période de réalisation. Chaque mission inscrite au programme d'audit sera reprise et détaillée dans une lettre de mission.

EN PRATIQUE

Gardez ce document confidentiel.

Intégrez ce programme annuel dans un programme à 3 ans incluant l'intégralité des domaines à auditer selon des fréquences appropriées.

Évitez, afin de couvrir collectivement le périmètre le plus vaste, d'auditer systématiquement les domaines dans lesquels sont réalisés des contrôles permanents.

Le plan de contrôle présente les contrôles de deuxième niveau dits « permanents » qui seront réalisés sur place ou à distance selon une périodicité déterminée par les équipes du contrôle permanent. À la différence des missions d'audit interne, ces contrôles sont permanents au sens « régulièrement réalisés » selon une périodicité fonction de la gravité du risque. Ils peuvent à ce titre se dérouler une fois par an, semestre, trimestre, mois, voire semaine ou jour. Ils consistent en grande partie à contrôler la bonne exécution des contrôles de niveau 1 par les responsables d'encadrement. Les contrôles relatifs au plan de contrôle permanent ne donnent pas lieu à la rédaction de lettres de mission.

EN PRATIQUE

Présentez ce document aux contrôleurs de premier niveau (au sein des métiers) et à leur management.

Adaptez la fréquence de contrôle au risque à couvrir. Rien ne sert d'adopter une fréquence très élevée pour un risque de faible impact ; une fréquence annuelle est parfois suffisante.

LE RAPPORT ANNUEL SUR L'ÉTAT DU DISPOSITIF DE CONTRÔLE INTERNE

Élaboré une fois par an en début d'année pour l'année $n-1$, le rapport sur l'état du dispositif de contrôle interne présente la situation du dispositif de contrôle interne au regard de la cartographie des risques de l'entreprise en intégrant les changements intervenus dans le dispositif.

Le rapport présente :

- la cartographie des risques (évolution des risques, inventaire des risques nouveaux…) ;
- les contrôles au premier degré, second degré et troisième degré : changement d'acteurs, d'outils, de fréquence…) ;
- le dispositif documentaire (modifications de procédures, règles de gestion, schémas comptables) ;
- les moyens mis à la disposition de la fonction (rappel des budgets de fonctionnement, des effectifs et des outils) ;
- les missions d'audit qui ont été réalisées dans l'année (principales faiblesses identifiées et recommandations faites) ;
- les actions de renforcement du dispositif de contrôle interne en cours de réalisation ; ce rapport sur l'état du dispositif de contrôle est adressé au président du conseil d'administration de l'entreprise, aux autorités de tutelle et aux commissaires aux comptes.

EN PRATIQUE

Utilisez ce document pour montrer les progrès réalisés dans l'année.

Illustrez ce document de données chiffrées : indicateurs d'activité et indicateurs de risques.

Réservez la primeur du document au directeur général, puis au président, aux commissaires aux comptes et enfin au conseil d'administration.

PAROLE D'EXPERT

Lawrence B. Sawyer, septième commandement : connaître l'effet

« La critique la plus sérieuse portée contre l'inspecteur de la vieille école est sa prédilection pour mettre en vedette des erreurs mineures. Sa tendance à "chercher la petite bête", sa joie d'afficher des écarts peu importants de la règle comme preuve de son "œil de lynx". Les hommes de loi ont une expression pour cela : *De minimis non curat lex* (« La Loi ne s'occupe pas des affaires insignifiantes »). L'inspecteur moderne cherche fortement à éviter cette tendance à « monter les vétilles en épingle ». À cette fin, il se demande, lorsqu'il a découvert une "entorse" aux règles : "Quel en est le résultat ?" Si le résultat est défavorable, important et permanent, il est alors certain que ce problème doit être signalé, c'est-à-dire porté à l'attention de la personne qui régularisera la situation indésirable et à l'attention de la personne qui s'assurera que celle-ci a été régularisée. L'inspecteur s'inquiétera du résultat possible d'une situation mal contrôlée, ainsi que du résultat réel. L'inspecteur moderne est le gardien des contrôles de la société. Si un contrôle essentiel fait défaut, c'est-à-dire un contrôle dont l'absence pourrait permettre à des erreurs graves de se produire, il doit "hisser le drapeau rouge", qu'il découvre ou non que la faiblesse des contrôles a occasionné des opérations fausses. Une voiture fonçant à 100 *miles* à l'heure dans une rue à grande circulation d'une ville mérite une citation, qu'elle ait provoqué un accident ou non. Mais, et c'est tout aussi important, lorsque l'inspecteur recherchera les effets, il verra sous son vrai jour l'erreur qu'il a décelée. Il sera en mesure de séparer le "pou" des "monstres". Il sera en mesure de porter les yeux sur les mêmes horizons que ceux qui retiennent l'attention de la direction générale. Pour chaque découverte qu'il fait, il se demandera : "À qui cela nuit-il ? À quel point leurs intérêts sont-ils lésés ?" Si les réponses sont : "personne" et "pas beaucoup", la découverte reste alors dans ses papiers de travail, et peut faire l'objet d'une discussion aux niveaux appropriés, mais ne mérite pas de place dans le rapport d'inspection. »

TÉMOIGNAGE

Manon Mourier des Gayets, responsable financière SOS SAHEL International France

En France, dès lors qu'une association bénéficie d'un montant annuel de subventions publiques et/ou reçoit des dons ouvrant droit à un avantage fiscal pour un montant annuel supérieur à 153 K€, elle est soumise à l'obligation légale d'établir des comptes annuels et de nommer un commissaire aux comptes (audit légal). Aussi, les partenaires financiers institutionnels accompagnent généralement leurs financements d'une obligation de réaliser un ou plusieurs audits financiers externes (audits contractuels) au cours de la vie du projet qu'ils soutiennent. Au-delà de l'obligation légale, l'audit externe, qui ponctue la vie des associations et des projets qu'elles portent, constitue une véritable opportunité pour leur activité. En effet, il permet, en externe, de renforcer la confiance des donateurs et des partenaires financiers et en interne, de créer une dynamique d'amélioration continue des processus de gestion.

SOS Sahel International France est une association reconnue d'utilité publique dont les ressources sont principalement issues de subventions publiques, de mécénat et de produits de la générosité du public. La nature de ces ressources rend particulièrement essentiel pour l'association de pouvoir rendre des comptes et donner à ses contributeurs la garantie d'une gestion rigoureuse et transparente des fonds collectés. À ce titre, la mission du commissaire aux comptes constitue un élément clé car il certifie à travers un rapport publié annuellement, que les comptes sont sincères, conformes aux règles et principes comptables applicables et qu'ils donnent une image financière fidèle de l'activité de l'association et de son patrimoine.

Le rapport du commissaire aux comptes est également un outil indispensable au service de la gouvernance de l'association puisqu'il lui permet de prendre des décisions en s'appuyant sur des données fiables. Dans le cadre de sa mission d'audit légal, le commissaire aux comptes peut également être amené à constater des points d'amélioration nécessaires dans le système de contrôle interne de l'association et émettre ainsi des recommandations. Cette alerte permet à la gouvernance de prendre conscience des risques auxquels l'association peut être confrontée et en conséquence de mettre en place des solutions (nouveaux outils de contrôles) pour assurer un contrôle optimal.

Enfin, dans un secteur en constante évolution et dans lequel de nombreuses réglementations très spécifiques s'appliquent, le commissaire aux comptes est un partenaire précieux car il se tient constamment informé des évolutions du cadre légal et réglementaire et peut ainsi alerter et accompagner l'association dans une mise à jour de ses procédures internes. La mise en place du nouveau compte d'emploi des ressources (CER) désormais annexé aux comptes annuels des associations faisant appel à la générosité du public en est un très bon exemple.

La mission du commissaire aux comptes, comme celle d'auditeurs dans le cadre d'audits financiers contractuels sur des projets, permet donc à l'association de pérenniser ses activités et de les développer en faveur de ses bénéficiaires.

CHAPITRE 9

Les outils techniques

CE CHAPITRE VOUS PERMETTRA DE :

- connaître l'éventail des outils techniques utilisés par les deux fonctions.

Nous l'avons déjà dit en amont dans l'ouvrage, les métiers d'auditeur interne et de contrôleur permanent sont très proches et complémentaires puisque, rappelons-le, un dispositif de contrôle interne efficace est constitué de trois lignes de maîtrise (appelées également les 3 lignes de défense) :

- La première ligne de défense est composée des collaborateurs réalisant des contrôles opérationnels dans le cadre du traitement des opérations et de l'encadrement réalisant des contrôles sur échantillon dits de « premier niveau ».
- La deuxième ligne de défense est composée des contrôleurs permanents en charge de contrôles à fréquence régulière, et notamment de s'assurer que les contrôles de premier niveau sont réalisés.
- La troisième ligne de défense est composée des auditeurs internes en charge de l'évaluation périodique de l'efficacité du dispositif de contrôle interne de l'entreprise.

C'est pourquoi l'audit interne et le contrôle permanent partagent l'utilisation d'un grand nombre d'outils.

1. L'ENQUÊTE DU CBOK

L'enquête du CBOK a mis au jour un certain nombre de compétences techniques et professionnelles.

Compétences techniques des professionnels de l'audit interne

- La vision prospective.
- La gestion de la qualité totale.
- L'aptitude à négocier.
- La connaissance de l'approche qualité et des normes ISO.
- Le tableau de performance (*balanced scorecard*).
- Les techniques et outils de GRC (*governance risk and compliance*).
- Les compétences opérationnelles et de management.
- La gestion de projet.
- La résolution de problèmes techniques.
- La compréhension de l'activité.
- Les techniques d'analyse des risques et d'évaluation des contrôles.
- Les compétences juridiques/sensibilité à la fraude.
- Les *business processus analysis*.
- L'analyse financière.
- L'identification des types de contrôle (préventifs, correctifs).
- L'utilisation de l'information.
- Les techniques et outils de collecte et d'analyse de données.
- L'échantillonnage statistique.

Nos observations montrent que les compétences techniques sont indispensables mais ne suffisent pas sans les qualités relationnelles et comportementales.

De plus, l'enquête montre que l'auditeur interne doit posséder des savoir-faire complémentaires.

Savoir-faire de l'auditeur

- Compréhension des systèmes d'information.
- Compétences dans le domaine comptable.
- Connaissance de langues étrangères.
- Capacité d'identification et de résolution des problèmes.
- Communication écrite et orale.
- Aptitude à l'organisation.
- Capacité à faire de la veille (sectorielle, réglementaire, professionnelle).
- Capacité à conduire le changement.
- Techniques de formation.
- Capacité à promouvoir la valeur de l'audit interne au sein de l'organisation.
- Capacité de résolution des conflits.

2. NOS OBSERVATIONS

Nos observations montrent que les savoir-faire comportementaux, encore une fois, font la différence entre deux professionnels. Par ailleurs, la seule pratique de l'anglais en plus de sa langue maternelle n'est plus suffisante. Une seconde langue, telle l'espagnol, le chinois, le japonais, le russe…, est autant d'atout. Et, avec la pratique des langues étrangères, la compréhension des cultures est nécessaire dans les groupes internationaux. En effet, la façon de conduire les missions, de rédiger les rapports et de conduire le changement diffère d'une culture à l'autre. Nous renvoyons le lecteur à notre publication *Animer une équipe projet avec efficacité*, H.-P. Maders (Éditions Eyrolles) pour approfondir cet aspect.

LA CARTOGRAPHIE DES RISQUES

La cartographie des risques constitue la liste des risques impactant un métier, une activité, un processus, une prestation… Les objectifs de la cartographie des risques permettent à l'auditeur interne ou au contrôleur permanent d'orienter leur énergie sur les enjeux de l'entreprise.

La cartographie des risques identifie les risques bruts inhérents au métier ainsi que les autres types de risques : risques opérationnels, réglementaires, d'image… et présente également les risques résiduels.

Protocole pour utiliser une cartographie des risques

- Partir d'un périmètre défini : métier, activité, processus, prestation…
- Identifier les risques bruts en partant de listes types (ex. : liste des sept catégories de risques bâlois pour les risques opérationnels pour une banque).
- Compléter l'analyse par la prise en compte des sinistres recensés.
- Évaluer pour chaque risque brut identifié sa probabilité d'apparition et sa gravité ainsi que son impact réglementaire et d'image.
- Passer du risque brut au risque net en intégrant l'environnement organisationnel (séparation des fonctions, plan de continuité d'activité, compétences des personnels…), la qualité du corpus de procédures et des contrôles de niveaux 1 et 2, l'existence d'indicateurs de risques…

EN PRATIQUE

Revisitez la cartographie des risques *a minima* tous les ans.

Utilisez des taxonomies de risques standard pour éviter de passer à côté de risques possibles.

LA FICHE DE RISQUE

La fiche de risque constitue la carte d'identité d'un risque. Elle synthétise en effet ses principales caractéristiques, à savoir :

- Famille d'appartenance : le risque doit faire partie d'une des familles retenue dans le cadre de la cartographie des risques. Par exemple : risque stratégique, risque commercial, risque RH, risque financier, risque fiscal, risque déontologique, risque opérationnel, etc.
- Numéro de référence : il permet de connecter le risque en question notamment avec :
  - La cartographie des risques ;
  - Le référentiel des processus ;
  - Les déclarations d'incidents et les plans d'action correspondants ;
  - Les indicateurs de risques et les reportings.
- Intitulé : il doit être suffisamment précis pour être « parlant » en tant que tel.
- Description : situations caractéristiques.
- Propriétaire : personne en charge de la définition et mise en œuvre des contrôles et actions permettant sa maîtrise.
- Responsable de la documentation : personne en charge de documenter le risque, et notamment le mode opératoire de réalisation des contrôles correspondants (Cf. Fiche de contrôle présentée plus loin dans l'ouvrage).
- Types d'impacts du risque : financier, juridique, réputation, social, réglementaire, continuité d'activité.
- Causes explicatives de la survenance du risque.
- Position face au risque : décision du propriétaire du risque à l'égard de celui-ci.
- Evaluation de l'exposition pour l'année N-1 : fréquence d'apparition du risque et impact financier constaté.
- Plan d'action : description des actions, responsables et échéances permettant de mieux maîtriser le risque en question.

EN PRATIQUE

Partez des risques retenus dans la cartographie des risques.

Revisitez les fiches annuellement afin de mettre en jour a minima les parties « Position face au risque », « Évaluation de l'exposition pour l'année N-1 » et « Plan d'action ».

Figure 9.1 – Fiche de risque (exemple secteur bancaire)

Fiche de risque				
Famille de risque	Risques commerciaux	**N° de référence du risque**	FRR/05/07	
Intitulé du risque	Dossier client particulier incomplet			
Description du risque	Risque de perte financière relative à la fermeture d'un compte client présentant un découvert non autorisé et pour lequel il n'est pas possible d'effectuer un recouvrement Pénalité de l'Autorité de contrôle prudentiel et de résolution (ACPR) en cas de mission de contrôle pour cause de mauvaise connaissance des clients			
Propriétaire du risque	M. ..., Directeur commercial			
Responsable documentation	M. ..., Adjoint au Directeur commercial			

Types d'impact du risque				
	Financier	X	**Réputation**	
	Juridique	X	**Réglementaire**	X
	Social		**Continuité d'activité**	

Causes explicatives de la survenance du risque
Méconnaissance de la procédure d'entrée en relation par les personnels de Front Office
Mauvaise segmentation du client réalisée par le Front Office
Personnes apparentées au client déjà clients de la banque

Position face au risque		**Évaluation de l'exposition 2014**	
Acceptation		**Fréquence d'apparition du risque**	*150 dossiers d'entrée en relation présentaient au moins une anomalie (soit 75 % des dossiers)*
Evitement			
Contrôle	X	**Impact financier**	*Pertes financières relatives aux fermetures de comptes de clients débiteurs (sans autorisation de découvert formelle) pour lesquels le dossier n'était pas à jour sans recouvrement possible : 200 000 €* *Pertes financières sur un dossier de prêt non remboursé et pour lequel la caution n'a pas pu être mise en œuvre pour cause d'absence de document à jour : 150 000 €*
Assurance			

Planc d'action 2015	**Description des actions**	**Responsable**	**Échéance**
1	*Revue de la procédure d'entrée en relation*	*Animation commerciale* *Contrôle interne*	*Premier semestre*
2	*Formation des personnels de Front Office sur la procédure d'entrée en relation, la segmentation clientèle et les obligations réglementaires KYC (Know Your Customer - connaître ses clients)*	*Animation commerciale* *Formation*	*Second semestre*
3	*Revue du portefeuille des crédits afin de s'assurer de l'état des cautions*	*Contrôle interne*	*Premier trimestre*
4			
5			

LA MÉTHODE AMDEC

La méthode AMDEC (appelée couramment l'AMDEC) a été développée en 1949 par l'armée américaine (référence militaire MIL-P-1629 : *Procédures pour l'analyse des modes de défaillance, de leurs effets et leurs criticités* publiée le 9 novembre 1949). Depuis 1988, avec les normes ISO 9000 et QS 9000, les fournisseurs automobiles doivent utiliser la planification qualité du procédé (APQP), incluant l'outil AMDEC et développant des plans de contrôle.

C'est une technique multidisciplinaire d'analyse de risque utilisée pour déterminer les modes de défaillance potentiels d'un procédé ou d'un produit (la sévérité de leurs effets et la probabilité d'occurrence) et les causes et mécanismes associés avec chaque mode de défaillance (l'habileté à les détecter). Elle permet de prioriser les interventions d'amélioration continue (réduire les risques les plus grands, élaborer des plans d'action et allouer les ressources de façon rationnelle) et de formaliser la documentation.

L'intérêt de l'AMDEC est pour l'auditeur interne ou le contrôleur permanent de déterminer les points faibles d'un système et y apporter des remèdes, préciser les moyens de se prémunir contre certaines défaillances, étudier les conséquences de défaillances vis-à-vis des différents composants, classer les défaillances selon certains critères, fournir une optimisation du plan de contrôle, une aide éclairée à l'élaboration de plans d'intervention. Elle aide à « pré-voir » pour ne pas être obligé de « re-voir ».

Premier critère : occurrence (O)

L'occurrence caractérise la probabilité ou fréquence d'apparition de la cause qui entraînera la défaillance. On passe de la note « 1 » pour une probabilité très faible à la note « 10 » pour une probabilité très forte. Il revient de déterminer la grille de notation qui dépend de la taille des séries, de la vitesse du processus de fabrication…

Tableau 9.1 – Grille de degrés d'occurrence (exemple)

Valeur	Critères	Taux possible
1	Défaillance presque impossible	Presque jamais
2	Très basse, défaillance très isolée	Une fois par période de 2 ans
3	Basse, défaillance isolée	Une fois par an
4	Modérée, occasionnelle	Une fois par semestre
5		Une fois par trimestre
6		Une fois par mois

.../...

OUTILS TECHNIQUES

.../...

Valeur	Critères	Taux possible
7	Haute, nombreuses défaillances	Une fois par semaine
8		Une fois par jour
9	Très haute, défaillance presqu'inévitable	Une fois par quart de travail
10		Plus d'une fois par quart de travail

Deuxième critère : probabilité de non-détection (D)

La probabilité de non-détection caractérise la probabilité que la défaillance ne soit pas détectée avant son arrivée chez le client (ou le risque de laisser passer un produit défectueux). On passe de la note « 10 » pour une probabilité très forte de laisser passer un produit défectueux à « 1 » pour une probabilité très faible.

Tableau 9.2 – Grille de degrés de probabilité de non-détection (exemple)

Valeur	Critères
1	Signe avant-coureur de la défaillance que l'opérateur pourra éviter par une action préventive ou alerte automatique d'incident.
2	
3	Il existe un signe avant-coureur de la défaillance mais il y a un risque que ce signe ne soit pas perçu par l'opérateur.
4	
5	Le signe avant-coureur de la défaillance n'est pas facilement décelable.
6	
7	Il n'existe aucun signe avant-coureur de la défaillance mis à part l'inspection finale du produit.
8	
9	Il n'existe aucun signe avant-coureur de la défaillance avant l'utilisation du produit par le client.
10	

Troisième critère : gravité (G)

La gravité caractérise la gravité de l'effet de la défaillance pour le client. On passe de la note « 1 » pour une gravité faible (insignifiante pour le client) à « 10 » pour une gravité très forte (risque de mort d'homme par exemple).

Tableau 9.3 – Grille de degrés de gravité (exemple)

Valeur	Critères
1	Défaillance mineure ne provoquant qu'un arrêt de production faible (< 1 heure) et aucune dégradation notable.
2	
3	Défaillance moyenne nécessitant une remise en état ou une petite réparation et provoquant un arrêt de production de 1 à 8 heures.
4	
5	Défaillance critique nécessitant un changement du matériel défectueux et provoquant un arrêt de production de 8 à 48 heures.
6	
7	Défaillance très critique nécessitant une grande intervention et provoquant un arrêt de production de 2 à 7 jours.
8	
9	Défaillance catastrophique impliquant des problèmes de sécurité et/ou une production non conforme et provoquant un arrêt de production supérieur à 7 jours.
10	

Criticité (C)

Cet indicateur caractérise l'importance de la défaillance. La criticité synthétise les trois paramètres précédents :

▸ Criticité = Occurrence × Probabilité de non-détection × Gravité

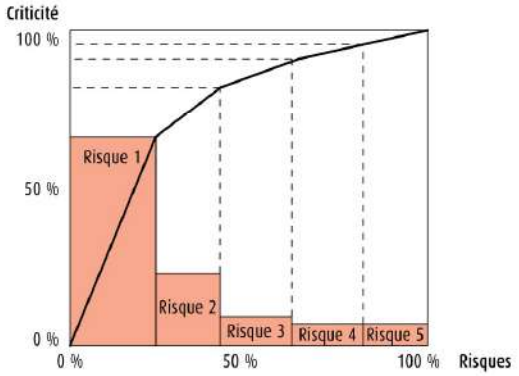
Si chaque facteur est noté de 1 à 10, la criticité de chaque défaillance peut varier de 1 (1 × 1 × 1) à 1 000 (10 × 10 × 10).

La mesure de la criticité permet de hiérarchiser les défaillances potentielles. La réalisation d'un diagramme de Pareto permet de visualiser ce classement. Ce type d'outil permet de mettre en évidence la règle de Pareto à savoir que, généralement :

- 20 % des risques identifiés représentent souvent 80 % des défaillances constatées ;
- 30 % des risques identifiés représentent souvent 15 % des défaillances constatées ;
- 50 % des risques identifiés ne représentent souvent que 5 % des défaillances constatées.

OUTILS TECHNIQUES

Figure 9.2 – Classement des risques en fonction de leur criticité relative



Comme il serait trop coûteux de traiter simultanément toutes les causes de défaillance, on peut fixer un seuil au-dessus duquel on mettra en œuvre des actions correctives. Le seuil courant est 100 mais certains clients peuvent en imposer un autre. (Par exemple, le seuil imposé par la société PSA à ses sous-traitants est de 36.)

LES FONDAMENTAUX DE CONTRÔLE

Les fondamentaux de contrôle correspondent à des pistes d'investigation possibles pour l'auditeur interne ou le contrôleur permanent. Leur objectif est de constituer pour les auditeurs internes et contrôleurs permanents une check-list d'investigation transversale à tous les domaines.

Les fondamentaux de contrôle consistent à passer en revue les fondamentaux qui se retrouvent dans la plupart des missions :

- la politique générale et les normes de performance ;
- la séparation des fonctions incompatibles (autorisation, exécution, validation) ;
- la réalité des informations ;
- l'exhaustivité des traitements ;
- les pistes d'audit ;
- les limites (habilitations, délégations, autorisations, profils informatiques) ;
- l'enregistrement des informations entrant et sortant du système ;
- la mémorisation des pièces utilisées dans le système ;
- les manuels de procédures précisant les risques relatifs à la procédure, le traitement des opérations, les règles de gestion, les règles d'enregistrement comptable, les contrôles opérationnels et de premier degré…

EN PRATIQUE

Partez des informations utilisées dans les traitements : celles-ci entrent dans le système ou sont créées à l'intérieur de celui-ci. Au sein du système, elles peuvent être transformées ou non, stockées ou détruites. À la sortie du système, elles présentent une valeur ajoutée.

Si cela n'est pas le cas, posez-vous la question de l'utilité du système…

Les fondamentaux du domaine comptable

Dans le cadre d'un domaine comptable, les auditeurs internes et contrôleurs permanents réalisent des tests afin de s'assurer que celle-ci est juste et sincère :

- Exhaustivité : assurance qu'aucune écriture comptable n'est oubliée.
- Réalité : assurance que les écritures comptables correspondent bien à des événements réels.
- Unicité : assurance que les écritures ne sont pas passées en double.

OUTILS TECHNIQUES

- Propriété : assurance que les écritures comptables concernent bien l'entreprise.
- Évaluation : assurance que les opérations sont enregistrées pour le bon montant.
- Comptabilisation : assurance que les événements de gestion se traduisent par des comptabilisations sur les comptes correspondants.
- Césure : assurance que les opérations sont enregistrées sur le bon exercice comptable.

Les fondamentaux d'un système d'information

Le système d'information fait partie du champ d'investigation de l'audit interne et du contrôle permanent.

La sécurité des systèmes d'information repose sur quatre facteurs qui s'appliquent aux flux, aux traitements et aux données.

La disponibilité (aptitude des systèmes à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances) est le premier aspect que l'auditeur interne et le contrôleur permanent doivent vérifier.

Tableau 9.4 – Grille de cotation de la disponibilité d'un système

Niveau 0	Une indisponibilité ne provoque aucune perturbation notable et la reprise de l'activité est aisée (la durée maximum d'indisponibilité tolérable est typiquement de plusieurs jours).
Niveau 1	Une indisponibilité est considérée comme un incident mineur et la reprise de l'activité est réalisée sans forte perturbation (la durée maximale d'indisponibilité tolérable est comprise entre 2 et quelques jours).
Niveau 2	Une indisponibilité est supportable mais la reprise de l'activité peut demander des efforts importants (la durée maximum d'indisponibilité tolérable est typiquement de 1 à 2 jours).
Niveau 3	Une indisponibilité provoque une forte perturbation et la reprise de l'activité peut demander des efforts importants (la durée d'indisponibilité tolérable est de l'ordre de quelques heures).
Niveau 4	Les conséquences d'une indisponibilité sont difficilement mesurables et l'activité globale est très fortement perturbée (la durée d'indisponibilité tolérable est de l'ordre de 30 minutes à une heure).

L'auditeur interne et le contrôleur permanent doivent, dans le même ordre d'idée, également vérifier le niveau de disponibilité horaire.

Tableau 9.5 – Grille de cotation de la disponibilité horaire d'un système

Niveau 1	Disponibilité pendant les heures de bureau (du fuseau horaire du site de l'exploitant). Les utilisateurs sont donc localisés géographiquement et aucun traitement de nuit n'est effectué.
Niveau 2	Disponibilité 24 heures sur 24 les jours ouvrés. Les utilisateurs sont localisés dans le monde entier et/ou l'application effectue des traitements de nuit.
Niveau 3	Disponibilité 24 heures sur 24 et 7 jours sur 7. Les utilisateurs sont localisés dans le monde entier et/ou l'application effectue des traitements de nuit y compris le samedi, le dimanche et les jours fériés.

Le deuxième aspect que l'auditeur interne et le contrôleur permanent doivent vérifier est l'impact du projet sur l'intégrité du système d'information (propriété qui assure que des informations sont identiques en deux points dans le temps et dans l'espace).

Tableau 9.6 – Grille de cotation de l'intégrité d'un système

Niveau 0	La perte d'intégrité des données ne risque pas de causer une gêne notable dans l'activité à court terme et à long terme.
Niveau 1	La perte d'intégrité de l'application ou de l'une des données est susceptible de provoquer un incident mineur, sans forte perturbation ;
Niveau 2	La perte d'intégrité de l'application ou de l'une des données est susceptible de provoquer des perturbations gênantes.
Niveau 3	La perte d'intégrité de l'application ou de l'une des données est susceptible de provoquer de fortes perturbations globales mais délimitées et acceptables.
Niveau 4	La perte d'intégrité de l'application ou de l'une des données est susceptible d'engendrer des dommages très importants difficilement mesurables et acceptables.

Le troisième aspect que l'auditeur interne et le contrôleur permanent doivent vérifier est l'impact du projet sur la confidentialité des données du système d'information (propriété qui assure la tenue secrète des informations avec accès aux seules personnes autorisées).

Tableau 9.7 – Grille de cotation de la confidentialité des données d'un système

Niveau 0	Information publique.
Niveau 1	Information interne à l'entreprise.
Niveau 2	Information à diffusion restreinte au sein de l'entreprise.
Niveau 3	Information secrète au sein de l'entreprise.

OUTILS TECHNIQUES

Enfin, le quatrième aspect que l'auditeur interne et le contrôleur permanent doivent vérifier est l'impact du projet sur le système d'information en matière de contrôle et preuve (faculté de vérifier le bon déroulement d'une fonction et non répudiation : impossibilité de nier avoir reçu ou émis un message).

Tableau 9.8 – Grille de cotation d'un système d'information en matière de preuve et contrôle

Niveau 0	Aucun historique n'a besoin d'être mis en œuvre.
Niveau 1	Seuls les événements concernant l'utilisation de l'application ont besoin d'être exploités.
Niveau 2	L'opération réalisée doit être enregistrée et conservée avec un minimum d'information.
Niveau 3	L'opération réalisée doit être enregistrée et conservée, ainsi que l'identification de l'utilisateur à l'origine de ces informations.
Niveau 4	Le détail de l'opération réalisée doit être enregistré et conservé. De plus, l'identification des utilisateurs ayant réalisé l'opération doit être garantie et utilisée comme preuve.

LES PROCÉDURES

Les procédures font partie du référentiel documentaire de l'entreprise. L'objectif des procédures est de constituer le référentiel de réalisation du travail : modes opératoires, contrôles au premier degré à effectuer par la hiérarchie, schémas comptables, règles de gestion… Elles constituent pour l'auditeur interne et le contrôleur permanent une source importante d'information sur « comment doivent être réalisés les traitements ».

Les procédures ont les caractéristiques suivantes :

- Elles doivent présenter la façon de traiter les opérations (cas habituels et atypiques) en renvoyant en annexes les tables de paramètres, les éléments de réglementation et les imprimés.
- Elles doivent être compréhensibles et mémorisables. Pour cela, elles doivent présenter les caractéristiques suivantes : référencement logique ; date de mise à jour ; titre « parlant » ; texte et schémas ; vocabulaire connu des utilisateurs ; phrases courtes, une seule instruction par phrase.
- Le classement des procédures peut être : chronologique, alphabétique, numérique, thématique ou géographique.

EN PRATIQUE

Veillez à définir pour le corpus de procédures une « procédure des procédures » présentant comment doit être rédigée toute procédure.

Corrélez les procédures avec le référentiel des processus, le référentiel des risques et les plans de contrôle.

Un bon dispositif de diffusion des procédures est un intranet utilisant des mots-clés.

OUTILS TECHNIQUES

L'ANALYSE FONCTIONNELLE

L'analyse fonctionnelle est un outil utilisé dans la démarche de l'analyse de la valeur. Cet outil est utile à l'auditeur interne ou au contrôleur permanent pour comprendre les fonctions d'un domaine, d'un système, d'une procédure, d'un produit… Les objectifs de l'analyse fonctionnelle sont de comprendre les fonctions (à quoi sert l'entité, le processus, la fonction… audité) et, ainsi, d'identifier, d'imaginer, de comprendre les risques associés à chacune de ces fonctions.

Protocole pour utiliser l'analyse fonctionnelle

- Identifier les fonctions : fonction principale, fonctions secondaires, fonctions d'estime, fonctions de contrainte interne (imposées par l'entreprise à elle-même), fonctions de contrainte externe (imposées à l'entreprise par l'environnement : la réglementation, la déontologie du secteur...) ;
- Auditer le dispositif de contrôle interne permettant d'avoir une assurance raisonnable d'atteinte des objectifs de chacune de ces fonctions.

▶ EXEMPLE

Le couteau suisse
Fonction principale : couper (c'est avant tout un couteau).
Fonctions secondaires : plein d'autres choses…
Fonction d'estime : Victorinox sinon rien, bien entendu !
Fonction de contrainte interne : il doit présenter une croix suisse.
Fonction de contrainte externe : pour la gamme « enfant », la lame n'est pas très tranchante et est arrondie.

▶ EXEMPLE

Procédure de traitement des courriers client dans une entreprise
Fonction principale : apporter une réponse aux questions des clients.
Fonctions secondaires : faire des offres commerciales aux clients ; donner de l'information générale sur l'entreprise…
Fonction d'estime : valoriser les clients par la qualité du signataire de la lettre de réponse.
Fonction de contrainte interne : informer le service qualité de l'entreprise des courriers reçus et des réponses réalisées.
Fonction de contrainte externe : conserver une trace des courriers et des réponses.

EN PRATIQUE

Utilisez cet outil quand vous découvrez un nouveau domaine : posez-vous la question de son utilité, du niveau de performance qu'il doit atteindre (seuil minimum, seuil maximum) et des risques qui pourraient en contrarier la réalisation.

Ne négligez pas la fonction d'estime. C'est elle que les consommateurs achètent quand ils payent cher un produit de luxe !... Et le fait que le produit soit cher fait partie de son attrait... vis-à-vis des autres !

LE TABLEAU DES RISQUES

La phase d'analyse des risques s'effectue au siège ou sur le terrain, essentiellement par des entretiens permettant à l'auditeur interne ou au contrôleur permanent de comprendre l'organisation et le fonctionnement de l'entité auditée. Le tableau définitif des risques conclut la phase d'analyse des risques et a pour objectif de faire un état des lieux estimatif des forces et des faiblesses réelles ou potentielles de l'entité ou du domaine audité afin d'orienter les travaux détaillés. Conditionnant le reste de l'intervention, cette phase de prise de connaissance et d'analyse des risques, dont dépendront la nature et le dosage des contrôles effectués ultérieurement, fait l'objet d'une réflexion approfondie par tous les membres de l'équipe et les risques sont matérialisés dans le « tableau des risques ».

Protocole pour établir un tableau des risques

- Découper l'activité en tâches élémentaires.
- Indiquer en face de chacune des tâches quel est son objectif (à quoi sert-elle ?).
- En face de chaque tâche et des objectifs assignés, estimer les risques encourus (que peut-il se passer si les objectifs ne sont pas réalisés, si la tâche est mal faite ou non faite ?).
- Évaluer sommairement le risque (en termes d'impact produit et de probabilité de survenance) attaché à la tâche (fort, moyen ou faible).
- Rappeler en face de chacun des risques quel est le dispositif ou quels sont les dispositifs de contrôle interne que l'on devrait trouver pour faire échec au risque identifié.
- Indiquer si le dispositif identifié comme important existe (oui) ou n'existe pas (non).

OUTILS TECHNIQUES

EN PRATIQUE

Utilisez le tableau des risques quand il n'existe pas une cartographie des risques au sein de l'entreprise, ou que le domaine contrôlé ne fait pas partie du périmètre de la cartographie.

Construisez-le alors avec les personnes de l'entité considérée.

LES INDICATEURS DE TENDANCE CENTRALE

La moyenne, la médiane, le mode, l'étendue et l'écart type sont des valeurs qui permettent à l'auditeur interne ou au contrôleur permanent de caractériser une distribution de résultats autour d'une valeur centrale. Leur objectif est de caractériser une distribution de données à un instant donné. Cela constitue une image de la situation.

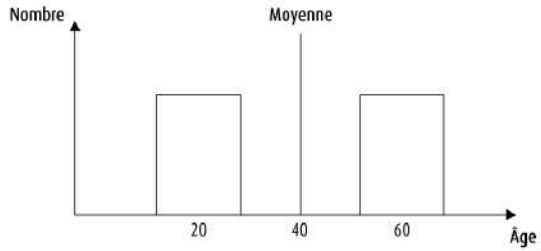
La moyenne de la distribution

La moyenne d'une distribution se calcule par l'addition des résultats puis leur division par le nombre d'éléments de la distribution. Simple à calculer, elle est la plus utilisée. Cependant, elle n'est pas toujours représentative de la population.

▶ EXEMPLE

Une population est composée à 50 % de personnes âgées de 20 ans et à 50 % de personnes âgées de 60 ans.
Sa moyenne arithmétique, égale à 40 ans, n'est pas représentative de la population.

Figure 9.3 – La moyenne arithmétique d'une distribution



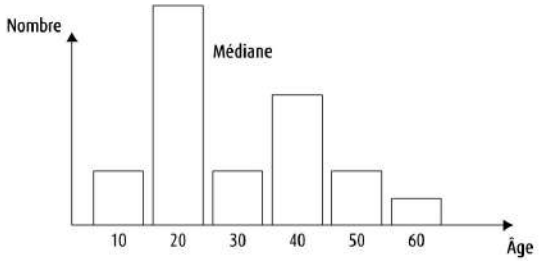
La médiane de la distribution

La médiane d'une distribution en est la valeur centrale, car il y a autant de valeurs inférieures à celle-ci que de valeurs supérieures. Simple à déterminer, elle n'est pas toujours représentative de la distribution.

▶ EXEMPLE

Une population est composée de 10 % de personnes âgées de 10 ans, 40 % de 20 ans, 10 % de 30 ans, 25 % de 40 ans, 10 % de 50 ans et 5 % de 60 ans.
Sa médiane, égale à 25 ans, n'est pas représentative de la distribution.

Figure 9.4 – La médiane d'une distribution



Le mode de la distribution

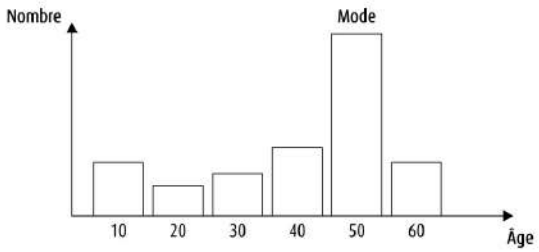
Le mode d'une distribution en est sa valeur la plus représentée.

▶ EXEMPLE

Une population est composée de 15 % de personnes de 10 ans, 10 % de 20 ans, 13 % de 30 ans, 17 % de 40 ans, 35 % de 50 ans et 10 % de 60 ans.
Son mode, 50 ans, n'est pas représentatif de la distribution.

OUTILS TECHNIQUES

Figure 9.5 – Le mode d'une distribution



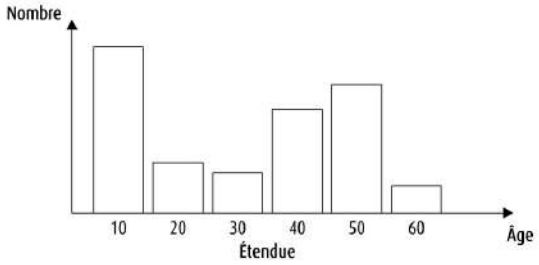
L'étendue de la distribution

L'étendue d'une distribution est égale à l'écart qui sépare la plus petite de la plus grande de ses valeurs. Plus l'étendue est importante et plus la distribution est composée d'éléments de valeurs très différentes.

▶ EXEMPLE

Une distribution est composée de personnes d'âges différents compris entre 10 et 60 ans.
Son étendue est donc égale à 50 ans.

Figure 9.6 – L'étendue d'une distribution



L'écart type de la distribution

L'écart type est utilisé pour caractériser une distribution homogène (moyenne = médiane = mode). Il permet de déterminer la dispersion de cette distribution autour de sa moyenne.

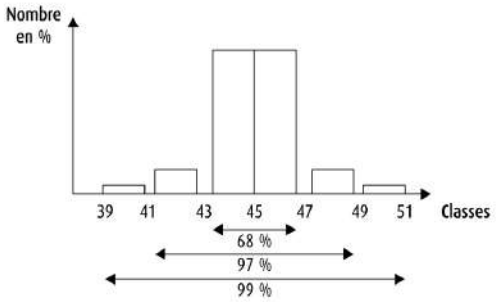
L'écart type se calcule par une formule mathématique, ou s'évalue par une table statistique à l'aide de l'étendue de la distribution. La distribution a la dispersion suivante: 68,26 % de la population est comprise entre la moyenne et +/– 1 écart type, 95,44 % entre la moyenne et +/– 2 écarts types, 99,73 % entre la moyenne et +/– 3 écarts types, 99,999 % entre la moyenne et +/– 4 écarts types et 99,99999 % entre la moyenne et +/– 5 écarts types.

Exemple

La fréquentation d'une agence est variable selon les jours. L'observation de 20 journées prises au hasard donne une fréquentation allant de 40 à 50 clients.
La moyenne arithmétique donne 45 clients.
La dispersion étant égale à 10, nous pouvons calculer avec une table statistique que l'écart type de cette population est égal à 2,68 arrondis à 3 (étendue multipliée par le facteur de multiplication correspondant à la taille de l'échantillon).
Nous pouvons en déduire que :

- 68 % des jours, soit 170 jours sur 250 jours d'ouverture, la fréquentation de l'agence sera comprise entre 42 (45 – 3) et 48 clients (45 + 3). D'une manière plus fine, elle sera comprise entre 42 et 45 clients 65 jours et entre 45 et 48 clients 65 jours.
- 97 % des jours, soit 243 jours, la fréquentation de l'agence sera comprise entre 39 (45 – 6) et 51 clients (45 + 6). D'une manière plus fine, elle sera comprise entre 39 et 42 clients 36,5 jours et entre 48 et 51 clients 36,5 jours.
- 99 % des jours, soit 248 jours, la fréquentation de l'agence sera comprise entre 36 (45 – 9) et 54 clients (45 + 9). D'une manière plus fine, elle sera comprise entre 36 et 39 clients 2,5 jours et entre 51 et 54 clients 2,5 jours.

Figure 9.7 – L'écart-type d'une distribution



EN PRATIQUE

N'oubliez pas que la moyenne arithmétique « est le pire des mensonges ». N'oubliez pas également qu'une analyse de dispersion n'a de sens que si elle s'adresse à une population homogène composée d'un nombre suffisamment élevé d'éléments.

Tableau 9.9 – Table de détermination de l'écart type en fonction de l'étendue de la distribution

Échantillon	Facteur de multiplication
2	0,886
3	0,591
4	0,486
5	0,430
6	0,395
7	0,370
8	0,351
9	0,337
10	0,325
11	0,315
12	0,307
13	0,300
14	0,294
15	0,288
20	0,268
50	0,222
100	0,199
200	0,182
300	0,174
400	0,168
500	0,165
600	0,162
700	0,159
800	0,157
900	0,156
1000	0,154

LA CARTE DE CONTRÔLE

La carte de contrôle permet à l'auditeur interne ou au contrôleur permanent de formaliser les résultats d'observations faits sur un critère de performance, comme un pourcentage de défaut, un nombre de jours, un pourcentage de respect des délais… dans la durée, à la différence de la distribution, qui elle donne une image à un instant donné. La carte de contrôle présente donc un historique et permet de constater les éventuelles évolutions.

Protocole pour utiliser une carte de contrôle

- Identifier le critère à observer.
- Déterminer les seuils de tolérance acceptables :
  - Le seuil minimal : niveau de performance qui dessert la prestation (un délai très court peut être jugé trop court, et peut faire considérer une prestation comme étant quelque peu bâclée, même si cela n'en est rien).
  - Le seuil maximal acceptable : niveau de performance qui, lui aussi, dessert la prestation (un délai très long peut être considéré pareillement trop long et peut faire considérer une prestation comme étant peu performante, même si cela n'en est rien).
- Effectuer par sondage des observations sur une durée suffisante (elle va dépendre de la quantité d'opérations, de dossiers, d'objets… à étudier).
- Calculer :
  - la moyenne des résultats pour chaque journée ;
  - la moyenne des résultats pour la période considérée ;
  - l'étendue des résultats pour chaque journée ;
  - la moyenne des étendues pour la période considérée.
- Reporter ces informations dans une carte de contrôle en mettant en évidence l'évolution des résultats ainsi que leur répartition en proportion.
- Repérer les résultats non compris entre les deux seuils de tolérance.
- Réaliser une réunion de résolution de problème afin de comprendre les causes des performances et d'engager les actions les plus adaptées.

OUTILS TECHNIQUES

EN PRATIQUE

Utilisez cet outil, très graphique, quand vous vous adressez à des personnes auditées peu expérimentées dans l'art des statistiques.

Utilisez-le sur une période de temps significative, afin de mettre en avant d'éventuelles tendances de début ou de fin de période, de hausse ou de baisse constante, ou encore de lisser tout épiphénomène.

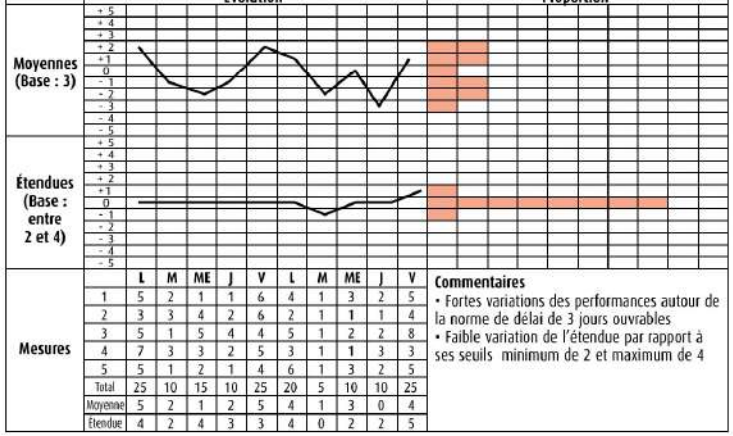
Figure 9.8 – Carte de contrôle qualité d'un processus

Banque de Bel air – Carte de contrôle qualité

Projet : Reengineering du processus de traitement des courriers clients | **Date :** 03/12/2014

Thème : Évaluation des délais de traitement d'un échantillon de 100 lettres sur les 15 premiers jours du mois de novembre 2014 (Norme : 3 jours ouvrables)

Analyste : M. Antoine, Organisateur



	L	M	ME	J	V	L	M	ME	J	V
1	5	2	1	1	6	4	1	3	2	5
2	3	3	4	2	6	2	1	1	1	4
3	5	1	5	4	4	5	1	2	2	8
4	7	3	3	2	5	3	1	1	3	3
5	5	1	2	1	4	6	1	3	2	5
Total	25	10	15	10	25	20	5	10	10	25
Moyenne	5	2	1	2	5	4	1	3	0	4
Étendue	4	2	4	3	3	4	0	2	2	5

Commentaires
- Fortes variations des performances autour de la norme de délai de 3 jours ouvrables
- Faible variation de l'étendue par rapport à ses seuils minimum de 2 et maximum de 4

LE RELEVÉ DE NON-CONFORMITÉ

Cette fiche ou relevé de non-conformité permet à l'auditeur interne ou au contrôleur permanent d'établir le suivi formel ou la traçabilité d'une non-conformité (réelle ou potentielle) au sein d'une activité jusqu'à son éradication ou sa prévention (résultat attendu). Elle donne lieu de la part de leur émetteur à la mise en œuvre d'une demande d'action corrective ou préventive auprès de la personne ou du groupe de personnes compétent.

Protocole pour réaliser des relevés de non-conformité

- Centraliser les fiches auprès du responsable qualité afin de permettre la constitution d'une bibliothèque servant de base de référence, d'échange et d'expérience.
- Réaliser une communication et un feed-back réguliers (en particulier sur les réussites) auprès des acteurs pour promouvoir l'utilisation de cette fiche.
- Réaliser une communication générale, pour une utilisation efficace et par le plus grand nombre, des relevés de non-conformité (raison d'être, objectif, modalités d'utilisation) auprès de l'organisation.
- Faire en sorte que chaque collaborateur soit capable de l'utiliser pour établir le constat formel d'une non-conformité réelle ou potentielle. Cette fiche concerne les non-conformités internes (dysfonctionnement sur un processus interne, erreurs, doublons, etc.) et externes (réclamations client, non-qualité d'une prestation). Chaque fiche ne traite que d'une seule non-conformité.
- Faire valider les fiches par le supérieur hiérarchique qui les adresse au destinataire concerné et compétent pour traitement.
- Faire gérer par chaque service la séquence des fiches ainsi émises (code service + n° de chrono).
- Transmettre cette fiche en copie au responsable qualité. Ce dernier a pour rôle de centraliser, de mettre à jour et de suivre (relance) les fiches de non-conformité ainsi enregistrées et les actions correctives ou préventives correspondantes mises en œuvre. Il apporte également un feed-back sur l'évolution du traitement de la non-conformité et son résultat au service(s) concerné(s).

Tableau 9.10 – Informations à faire figurer sur la fiche de relevé

Service	Service dont dépend l'émetteur.
Nom	Émetteur de la fiche.
Destinataire	Service ou personne compétent pour le traitement de la non-conformité.

.../...

OUTILS TECHNIQUES

.../...

Visa	Émetteur et responsable hiérarchique.
Date	Émission de la fiche.
Non-conformité identifiée	Définition en termes d'exigence non respectée ou manquante.
Causes, origines et conséquences	Le cas échéant enjeu financier.
Action(s) corrective(s) ou préventive(s) envisagée(s) et plan d'action associé	Action et plan d'action précisant qui ? quoi ? quand ?
Validation du résultat	Clôture du traitement de la non-conformité.

EN PRATIQUE

Utilisez cet outil, très employé également par les spécialistes de la qualité, pour suivre la qualité d'un système en fonctionnement, par exemple dans le cadre du déploiement d'une nouvelle organisation.

Utilisez cet outil pour faire le point objectivement sur les performances du nouveau système.

LES SONDAGES

Le sondage, effectué sur une partie de la population, permet à l'auditeur interne ou au contrôleur permanent de déterminer une caractéristique particulière qu'il est possible d'extrapoler au niveau de la population tout entière. L'objectif d'un sondage est de caractériser une population très importante par l'analyse d'une partie de celle-ci (L'opinion des Français est ainsi souvent évaluée avec des échantillons de moins d'un millier de personnes.) L'utilisation des sondages statistiques est requise pour obtenir une information et rechercher les causes d'un phénomène après avoir mesuré son ampleur. Ils s'imposent dès lors qu'une population à auditer est trop nombreuse, lorsque l'on veut mieux répartir son temps en fonction de l'importance relative du sujet traité ou lorsque l'on veut étendre le champ de l'audit sans prendre plus de temps. Les sondages peuvent être « statistiques » *ou « discrétionnaires » (au jugement de* l'auditeur interne ou du contrôleur permanent). Ils doivent toujours être réalisés avec rigueur et respecter certains principes. Pour ne pas avoir à vérifier la totalité d'une « population » (exemple : factures reçues), l'auditeur interne ou le contrôleur permanent sélectionne et examine un échantillon aléatoire et utilise les résultats obtenus pour se forger une opinion. L'objectif peut être la recherche d'un dysfonctionnement ou une meilleure connaissance du fonctionnement (caractérisation de la présence d'un attribut…).

Dans le cas d'un sondage statistique, le résultat observé sur l'échantillon peut *être extrapolé à l'ensemble de la population considérée. La technique statistique employée est assez simple mais en l'absence d'informatique adaptée*, sa mise en œuvre et l'interprétation des résultats s'avèrent souvent délicates pour des non-spécialistes.

EN PRATIQUE

Il n'est pas nécessaire d'être un expert des statistiques pour les utiliser. Cependant, vous devez intégrer que l'étude d'une partie de la population n'est pas l'étude de la population entière et que le résultat ne donne pas une certitude mais une estimation plus ou moins précise qui se mesure avec deux indicateurs :

- Le degré de confiance du résultat : il représente le pourcentage de chance que le résultat soit exact. Un degré de confiance de 95 % se traduit par le fait d'avoir 95 chances sur 100 pour que le résultat trouvé soit exact, et 5 chances sur 100 pour qu'il soit inexact.
- La précision du résultat : elle représente l'intervalle dans lequel est compris le résultat identifié. Une précision de +/– 2 pour un résultat identifié de 80 donne un résultat compris entre 78 et 82.

Utilisez des tableaux statistiques afin d'éviter des calculs fastidieux.

OUTILS TECHNIQUES
Copyright © 2014 Eyrolles.

Protocole de réalisation d'un sondage sur une population dénombrée

- Déterminer le degré de confiance souhaité pour le résultat.
- Déterminer la précision souhaitée pour le résultat.
- Déterminer la taille de l'échantillon à observer à l'aide d'une table statistique.
- Sélectionner l'échantillon physique à l'aide d'une table de nombres au hasard ou par division de la population par la taille de l'échantillon.
- Réaliser l'observation.
- Analyser le résultat.

▶ EXEMPLE

Objectif du sondage : déterminer, sur une population de 5 000 dossiers de crédit, dans quelle proportion les garanties ont été prises.

- Détermination du degré de confiance du résultat : 99 %.
- Détermination de la précision du résultat : +/– 2.
- Détermination de la taille de l'échantillon à l'aide de la table : 306 dossiers.
- Sélection de l'échantillon physique à l'aide d'une table de nombres au hasard : le 10e dossier, le 38e dossier, le 56e dossier, le 95e dossier, le 112e dossier, etc.

Tableau 9.11 – Extrait d'une table de nombres au hasard pour déterminer l'échantillon physique d'une population dénombrée (nombres compris entre 1 et 60)

10	55	27	59	24	54	18	09	50	08	26	14
28	52	03	54	39	05	31	23	12	26	57	08
18	53	42	18	44	50	04	54	34	25	28	47
39	50	01	05	23	15	39	32	54	09	09	59
17	30	50	43	36	32	23	14	20	42	50	44
27	43	20	21	07	31	13	11	08	53	25	53
41	01	30	26	28	56	54	11	15	55	02	06
48	23	34	36	13	46	04	16	21	29	58	47

Tableau 9.12 – Table de détermination de la taille de l'échantillon pour une population dénombrée (degré de confiance : 99 % et précision : +/– 1 % et +/– 2 %)

Taille de la population	+ / – 1 %	+ / – 2 %
2500	856	288
2600	867	289
2700	878	291
2800	888	292
2900	898	293
3000	907	294
3100	916	295
3200	925	295
3300	933	296
3400	941	297
3500	948	298
3600	955	299
3700	962	299
3800	969	300
3900	975	300
4000	981	301
4100	987	302
4200	993	302
4300	999	303
4400	1004	303
4500	1009	304
4600	1014	304
4700	1019	304
4800	1023	305
4900	1028	305
5000	1032	306
5500	1052	307
6000	1069	309
6500	1084	310
7000	1097	311
7500	1108	312
8000	1118	313
8500	1128	313
9000	1136	314
9500	1144	315
10000	1151	315
10500	1157	316
11000	1162	316
11500	1168	316
12000	1173	317

OUTILS TECHNIQUES
Copyright © 2014 Eyrolles.

Protocole de réalisation d'un sondage sur une population non dénombrée

- Estimer le temps disponible pour effectuer le sondage.
- Déterminer la taille de l'échantillon à observer en fonction de ce qui nous semble nécessaire et suffisant.
- Sélectionner l'échantillon physique à l'aide d'une table de nombres au hasard.
- Réaliser l'observation.
- Analyser le résultat et déterminer le degré de confiance et la précision du résultat à l'aide d'une table statistique.

Dans la table de précision d'un sondage, les colonnes vont de 5 % à 50 %. Quand un résultat est égal à 60 % par exemple, la précision est obtenue en additionnant le résultat de 50 % et celui de 10 %.

Exemple

Objectif du sondage : déterminer, sur une population de commerciaux, la proportion de temps passé à des activités commerciales

- Détermination de la taille de l'échantillon : 50 observations.
- Sélection de l'échantillon physique à l'aide d'une table de nombres au hasard : 9 h 00 ; 9 h 10 ; 9 h 38 ; 9 h 56 ; 10 h 35 ; 10 h 52 ; etc.
- Réalisation de l'observation : 50 % du temps est passé à des activités commerciales.
- Détermination du degré de confiance de la précision du résultat : nous avons 99 % de chances que le temps passé à des activités commerciales soit compris entre 32 % et 68 % du temps.

Tableau 9.13 – Table de précision d'un sondage pour une population dénombrée (degré de confiance : 99 %)

NB	5 %	10 %	15 %	20 %	25 %	30 %	35 %	40 %	45 %	50 %
10	0-50	0-54	1-60	1-65	2-69	4-74	6-77	8-81	10-84	13-87
20	0-32	1-39	2-45	4-51	6-56	8-61	11-66	15-70	18-74	22-78
30	0-25	1-32	3-38	5-44	8-50	11-55	15-60	19-65	22-69	26-74
40	0-21	2-28	4-35	7-41	10-46	13-51	17-57	21-61	25-66	29-71
50	0-19	2-26	5-32	8-38	11-44	15-49	19-54	23-59	27-64	32-68
60	1-17	3-24	5-30	9-36	12-42	16-47	20-52	24-57	29-62	33-67

.../...

.../...

NB	5 %	10 %	15 %	20 %	25 %	30 %	35 %	40 %	45 %	50 %
70	1-16	3-23	6-29	9-35	13-40	17-46	21-51	25-56	30-61	34-66
80	1-15	3-22	6-28	10-34	14-39	18-45	22-50	26-55	31-60	35-65
90	1-14	4-21	7-27	10-33	14-38	18-44	23-49	27-54	32-59	36-64
100	1-14	4-20	7-26	11-32	15-38	19-43	23-48	28-53	32-58	37-63
150	2-12	5-18	8-24	12-30	16-35	21-41	25-46	30-51	35-56	39-61
200	2-10	5-17	9-23	13-28	18-34	22-39	27-44	31-49	36-54	41-59
500	3-8	7-14	11-20	16-25	20-30	25-36	30-41	34-46	39-51	44-56
1000	3-7	8-13	12-18	17-23	22-29	26-34	31-39	36-44	41-49	46-54
2000	4-6	8-12	13-17	18-22	23-28	27-33	32-38	37-43	42-48	47-53

▶ Exemple

Procédures de contrôle d'une expédition d'objets rentrant dans le cadre d'une prospection et bénéficiant par là même de conditions tarifaires spéciales – Entreprise de distribution de courriers et colis

Contrôle des objets

Prélever deux à trois objets par prospection dans des contenants différents.
Contrôler le contenu. Contrôler les caractéristiques physiques des objets (dimension, poids) et vérifier le respect des règles de présentation.

Contrôle du tarif

Vérifier si le tarif utilisé correspond à la catégorie, au poids unitaire et au seuil tarifaire.
Appliquer la règle du déclassement figurant dans la plaquette tarifaire lorsque les conditions de tri ne sont pas respectées.

Contrôle des quantités et des tris

Peser les objets avec leurs contenants en trois lots distincts en dénombrant le nombre de contenants par lot: objets en contenants directs; objets en contenants en liasse directe; objets en contenants de liasses à trier;
Déterminer le nombre de contenants, de liasses et d'objets à contrôler à partir de la table d'échantillonnage en tenant compte de l'importance de chaque lot.
Effectuer ensuite les vérifications suivantes sur les contenants, liasses et objets à contrôler: vérification des seuils de confection (les seuils de confection figurent dans la plaquette tarifaire); vérification de la signalétique; recherche des fausses directions et vérifications (dans les contenants à trier notamment) de la formation maximale de liasses et de contenants directs.
Déduire le nombre d'objets à partir du poids moyen des objets et après déduction du poids des contenants (la quantité ne doit pas être validée lorsqu'il y a une divergence de plus de 3 % entre le poids net total constaté et le poids total déclaré sur les bordereaux).

OUTILS TECHNIQUES

À partir du poids total de chaque lot, calculer si le taux de 40 % de contenants directs et de contenants en liasses directes est bien atteint sur l'ensemble de l'expédition (si non, appliquer la règle du déclassement tarifaire sur l'ensemble de l'expédition).

Information au déposant

Le déposant doit être informé le plus rapidement possible de toute anomalie constatée sur son dépôt.
Le dépôt doit être refusé lorsque, dans l'échantillon contrôlé, le pourcentage de fausses directions ou le pourcentage des autres anomalies est supérieur à 10 %.
Par exemple, un dépôt de 30 000 objets composé de 170 sacs et de 1 020 liasses (sur la base de 6 liasses par sac):

- Nombre de sacs à contrôler (sans les ouvrir): 32.
- Nombre de liasses à contrôler (sans les ouvrir): 80.
- Nombre d'objets à contrôler: 295.

L'HEXAMÈTRE DE QUINTILIEN

L'hexamètre de Quintilien est un outil constitué d'une check-list de questions types permettant à l'auditeur interne ou au contrôleur permanent de guider l'analyse exhaustive d'une situation dont il prend connaissance ou tout au moins dont il n'est pas familier.

Il permet de :

- décrire une situation à l'aide de questions commençant par : qui ? quoi ? où ? quand ? comment ?
- chiffrer à l'aide de questions commençant par : combien ? (volumes, durées, euros…).
- prendre du recul sur cette situation à l'aide de questions commençant par : pourquoi ? (recherche des causes explicatives) et pour quoi ? (recherche des finalités).

Protocole d'utilisation de l'hexamètre de Quintilien

- Identifier quelles personnes interviennent dans la situation ? pour faire quoi ? à quel endroit ? à quel moment ? de quelle façon ?
- Chiffrer : combien de fois ? quel volume ? combien de temps ?
- Se demander : pourquoi ? pour quoi ?
- Contrôler la qualité des informations collectées :
  - exactitude (fiabilité, validité, traçabilité) ;
  - clarté (degré de compréhension, signification évidente sans effort d'interprétation) ;
  - précision (sans ambiguïté, d'un sens identique pour tous, reproduction fidèle du réel ne laissant aucune place à l'interprétation) ;
  - approprié (en rapport avec le problème, adéquat, important, intéressant, pertinent).
- Prendre du recul : pour quelles raisons ? pour quelles finalités ?

Exemple de questions d'investigation

Quoi ? L'opération est-elle utile ? L'opération est-elle indispensable ? Que se passerait-il si l'on décidait de ne plus la réaliser ? L'opération est-elle la conséquence d'une autre opération ? Si cela est le cas, laquelle ? L'opération peut-elle prendre une forme plus simple ? Si oui, laquelle ?

Qui ? La personne qui exécute le travail est-elle la plus indiquée ? Le poste de travail dans la filière est-il le plus indiqué pour effectuer ce travail ? L'unité est-elle la plus indiquée pour effectuer ce travail ? Pourquoi est-ce cette personne qui effectue cette tâche ? Est-ce la personne qui convient le mieux ? Si non, quelles compétences sont nécessaires pour occuper ce poste ? Qui serait en mesure de l'effectuer au moins aussi bien ?

OUTILS TECHNIQUES

Où ? Pourquoi cette tâche est-elle réalisée en ce lieu ? Est-ce l'endroit qui convient le mieux ? Peut-on réduire ou faciliter les déplacements en modifiant l'emplacement du poste, de l'unité ? L'ambiance du poste est-elle bonne ? L'aménagement du poste est-il bon ? Les matières, informations, dossiers, outils, matériels sont-ils positionnés correctement ?

Quand ? Pourquoi cette tâche est-elle réalisée à ce moment ? pour ce délai ? Est-ce le moment qui convient le mieux ? Est-ce la durée qui convient le mieux ? Quelles autres conditions conviendraient au moins aussi bien ? Le travail qui incombe à ce poste est-il bien placé dans le cycle général de traitement ? Peut-il être effectué au même moment qu'une autre tâche ?

Comment ? Pourquoi agir de cette façon ? Est-ce la meilleure façon de s'y prendre ? Existe-t-il un procédé, moyen, méthode plus efficace ? Si oui lequel ? L'équipement du poste de travail en matériels, machines… est-il suffisant ? Quels moyens supplémentaires faudrait-il ?

Combien ? Quel est le volume d'activité (nombre de dossiers, bordereaux, pièces…) ? Ce volume est-il linéaire ou présente-t-il des fluctuations ? Combien de personnes sont-elles impliquées dans la tâche ? Quel espace est nécessaire pour réaliser cette activité ? Quel en est le temps habituel de réalisation ?

Pourquoi ? Quelle est la cause de ce travail ? À quel besoin répond-il ? Si on n'effectuait pas ce travail, que se passerait-il ?

Pour quoi ? Quel est le but ou l'objectif de ce travail, de cette tâche ? Dans quelle mesure, cela explique-t-il ce qui est fait, qui en est chargé, où cela est fait, quand cela est fait et comment cela est fait ?

EN PRATIQUE

Commencez par collecter les informations globales avant de procéder à des analyses plus approfondies.

Faites des zooms ponctuels uniquement sur les points nécessaires.

Utilisez cet outil quand vous arrivez dans un nouveau domaine ou une nouvelle entité et que vous n'en avez aucune connaissance.

La question du « combien » est souvent complexe ; pour y répondre, utilisez des techniques d'estimation, telle celle des estimations pondérées, pour obtenir facilement des estimations assez fiables des volumes ou des durées de la part des personnes interviewées.

LES QUESTIONS ÉCRITES

Les questions écrites doivent être concises et précises. Elles permettent à l'auditeur interne et au contrôleur permanent de préparer l'entretien et également de disposer d'un temps de réflexion qui pourrait contribuer à améliorer la qualité des réponses.

EN PRATIQUE

Préparez avec soin les questions écrites car elles donnent à l'avance aux intéressés une image de votre niveau de connaissance du domaine et également de votre expérience du métier de l'audit et du contrôle internes.

Attention au « copier-coller » entre les missions.

LES VÉRIFICATIONS

Les vérifications sont extrêmement diverses : l'auditeur interne et le contrôleur permanent doivent vérifier toute l'information mise à leur disposition et toute observation effectuée. Les plus importantes sont les vérifications arithmétiques, la vérification de l'existence de documents, la recherche d'indices…

EN PRATIQUE

En matière d'audit interne et de contrôle permanent, vous devez toujours avoir la preuve de ce que vous annoncez, sous peine de perdre toute crédibilité.

Cherchez des contre-exemples. Dans bien des cas, la production d'un seul contre-exemple permet d'apporter la preuve qu'il existe des anomalies.

OUTILS TECHNIQUES

LES RAPPROCHEMENTS

Les rapprochements constituent une technique permettant à l'auditeur interne ou au contrôleur permanent une validation des informations provenant de deux sources différentes.

EN PRATIQUE

Rapprochez les documents concernant les fonctions incompatibles telles que « bon de commande », « bon de livraison », « facture » et « écriture comptable ».

Rapprochez les visas de l'état des délégations.

On rapprochera par exemple une écriture comptable correspondant au règlement d'une facture à son corollaire dans la comptabilité du fournisseur concerné.

EN PRATIQUE

La confirmation par des tiers

La confirmation par des tiers est une pratique classique de l'audit externe dans le cadre de la certification des comptes. Elle peut être utilisée par l'auditeur interne et le contrôleur permanent comme moyen de validation des constats et des observations. Cet outil est requis, par exemple, pour vérifier les biens déposés chez les tiers ou pour les questions relatives aux immobilisations (le tiers étant la conservation des hypothèques et le cadastre).

LES QUESTIONNAIRES DE CONTRÔLE INTERNE

Le questionnaire de contrôle interne (QCI) est une grille d'analyse qui permet à l'auditeur interne ou au contrôleur permanent de porter un diagnostic sur le dispositif de contrôle interne d'une entité auditée ou contrôlée et d'en apprécier le niveau effectif. Il comprend un ensemble de questions qui n'admettent, pour l'essentiel, que les réponses «oui» ou «non» qui servent à recenser les moyens en place pour atteindre les objectifs du contrôle interne. Par principe, les réponses négatives désignent les faiblesses du dispositif de contrôle interne alors que les réponses positives désignent les points forts théoriques; l'auditeur interne et le contrôleur permanent évaluent ensuite l'impact des «non» et vérifient la réalité des «oui».

Utilisé pendant la phase de préparation, le QCI est un moyen d'analyse des risques et sert de base à l'élaboration du programme de travail.

Protocole d'utilisation des questionnaires de contrôle interne

- Constituer le QCI en s'inspirant de listes de questions types trouvées dans des ouvrages professionnels, élaborées mission après mission par l'équipe d'audit interne ou de contrôle permanent ou élaborées spécifiquement pour la mission.
- Effectuer la vérification (dans le QCI, une réponse «oui» à une question indique une force apparente, une réponse «non» une faiblesse apparente).

EN PRATIQUE

Vérifiez chaque force et chaque faiblesse sur le terrain. En effet, à ce stade de l'analyse critique, il est dangereux de conclure trop vite: une force peut n'être qu'apparente, et une faiblesse peut être compensée par une force située ailleurs, voire à l'extérieur du domaine audité.

Ouvrez une FRAP pour chaque faiblesse identifiée.

Vérifiez sur le terrain: partez d'un événement déclencheur, suivez son traitement (un dossier, une facture, une note de frais... par exemple).

Prenez un échantillon d'informations (dossiers client, factures, bons de commande...), introduisez une anomalie dans le traitement et observez ce qui se passe: les opérateurs la détectent-ils? Comment la corrigent-ils? Dans quel délai?

OUTILS TECHNIQUES

LES AUTO-ÉVALUATIONS

Les auto-évaluations de contrôle interne très utilisées par l'auditeur interne ou le contrôleur permanent sont des techniques anciennes proches d'un QCI dont les questions s'adressent directement au management qui doit répondre aux questions portant sur les contrôles clés des activités de son périmètre de responsabilité.

Les vérifications de l'audit interne et du contrôle permanent consistent à demander si les auto-évaluations sont pratiquées par la structure auditée ou contrôlée. Dans le cas positif, l'auditeur interne ou le contrôleur permanent s'assure de la matérialisation de cette opération et par la suite de valider la qualité effective des auto-évaluations, qui ne bénéficient pas, par construction, de l'indépendance souhaitable.

L'auto-évaluation constitue un outil de base de la panoplie de l'auditeur interne et du contrôleur permanent. Il n'est pas obligatoire par nature mais pratiquement incontournable à un moment ou un autre dans une mission d'audit ou de contrôle. En l'absence de pratique d'auto-évaluation par la structure auditée ou contrôlée, l'auditeur interne ou le contrôleur permanent peut adresser, en temps utile, préalablement à la mission, un QCI qu'il demandera à la personne auditée ou contrôlée de bien vouloir renseigner et qui servira de préparation à l'entretien.

EN PRATIQUE

Utilisez l'auto-évaluation pour développer la confiance avec les personnes contrôlées. À ce titre, cette méthode peut renforcer la confiance réciproque ou, au contraire, la diminuer.

Utilisez des ateliers d'auto-évaluation pour réaliser rapidement un diagnostic partagé.

L'OBSERVATION PHYSIQUE

L'observation physique, avant d'être un outil, est une qualité de l'auditeur interne et du contrôleur permanent : un bon auditeur interne ainsi qu'un bon contrôleur permanent observe en permanence, partout et à tout moment, il exerce ainsi sa vigilance et son sens critique. Il peut ainsi apprendre, déceler des indices de contradiction, relever des manquements, etc. Il lui reste ensuite à exploiter cette mine d'informations collectées. L'observation en tant qu'outil est un test. C'est un complément indispensable à l'analyse descriptive opérationnelle. Elle sert par exemple à vérifier le respect de certaines consignes et les conditions de réalisation de certains contrôles au-delà de leur matérialisation. L'observation doit être consignée sous forme de papier de travail. Une observation faite à deux a plus de force que celle d'une personne isolée mais n'est pas indispensable. D'une façon générale (hormis la fraude), il est recommandé d'indiquer sur le moment aux acteurs du dysfonctionnement – ou à l'un de leur responsable présent – l'observation faite et en obtenir la confirmation. L'observation doit être utilisée chaque fois que possible. En effet, elle n'est pas consommatrice de temps et permet souvent de contribuer au principe du double contrôle.

EN PRATIQUE

Utilisez l'observation dans l'étude de processus en partant de l'événement déclencheur du processus et en suivant son déroulement jusqu'à son dénouement.

Identifiez ce qui déclenche le fonctionnement du processus (« les entrées ») ainsi que le résultat du processus (« les sorties »).

OUTILS TECHNIQUES

LA NARRATION

La narration est un outil utilisé par l'auditeur interne ou le contrôleur permanent pour permettre à la personne auditée ou contrôlée de décrire un cadre général et à l'auditeur interne ou au contrôleur permanent de rapporter les observations et les vérifications effectuées. C'est une technique qu'il faut utiliser avec prudence et qui doit reposer sur l'habilité à prendre des notes et l'aptitude à les transcrire et à les interpréter. Enfin, on distingue la narration de la personne auditée de celle de l'auditeur interne ou du contrôleur permanent. Ce dernier doit structurer ses phrases décrivant une observation physique, un constat, les conclusions d'un test… afin de faciliter la lecture par des tiers.

EN PRATIQUE

Utilisez cette pratique par défaut dans une entité ou la culture orale est la norme.

Demandez au narrateur de prouver ses dires avec des preuves factuelles et objectives.

Soyez attentifs aux signes de communication non verbale envoyés, parfois à son insu, par le narrateur.

L'ORGANIGRAMME FONCTIONNEL

L'organigramme fonctionnel est construit par l'auditeur interne ou le contrôleur permanent à chaque fois qu'il le juge nécessaire, pour mieux comprendre l'organigramme hiérarchique. Il permet d'enrichir les connaissances obtenues à partir de l'addition de l'organigramme hiérarchique et des fiches de poste. L'auditeur interne ou le contrôleur permanent le construit à partir d'informations recueillies par observation, interview, narration… en principe en tout début de mission ou au début de la phase de réalisation. Cet organigramme a comme caractéristique que les mots figurant dans les cases ne sont pas des noms de personnes (organigrammes hiérarchiques) mais des verbes désignant les fonctions.

EN PRATIQUE

Sachez lire derrière l'organigramme hiérarchique : derrière lui se trouve l'organigramme fonctionnel et, derrière l'organigramme fonctionnel, les personnes, avec leurs affinités, vécu, ambition…

Vous devez également comprendre comment fonctionnent les entités entre elles, quelles en sont les relations non hiérarchiques, non indiquées dans l'organigramme, mais plutôt client-fournisseur dans le cadre des processus ou encore, également, des habitudes et des affinités entre les personnes en faisant partie.

LA GRILLE D'ANALYSE DES FONCTIONS INCOMPATIBLES

La grille d'analyse des fonctions incompatibles permet à l'auditeur interne ou au contrôleur permanent d'analyser l'organisation du travail sous l'angle de la sécurité. Ces fonctions sont toujours les mêmes : autorisation de la réalisation de l'opération, contrôle de la réalité de réalisation de l'opération, accord de règlement de l'opération et règlement de l'opération.

Exemple – Fonctions incompatibles d'un processus achat

Acteur 1 : passation de la commande.
Acteur 2 : validation de la commande (personne habilitée, budget autorisé).
Acteur 3 : réception la commande (NB : la personne ne doit pas savoir ce qu'elle doit réceptionner mais noter ce qu'elle a réceptionné).
Acteur 4 : validation de la réception (comparaison de la réception avec la commande).
Acteur 5 : validation du règlement à faire (comparaison de la facture avec le bon de réception).
Acteur 6 : établissement du règlement fournisseur (au regard du bon de réception).
Acteur 7 : validation du règlement fournisseur (comparaison du règlement avec le règlement à faire).
Acteur 8 : comptabilisation de l'opération.

EN PRATIQUE

N'oubliez pas qu'il existe des fonctions incompatibles dans tous les processus de l'entreprise, qu'ils soient internes ou connectés avec l'extérieur.

Et qu'il vous est donc possible de faire une matrice théorique des fonctions incompatibles.

OUTILS TECHNIQUES

LE DIAGRAMME DE CIRCULATION

Le diagramme de circulation (*flow-chart*) est une représentation schématique et symbolique d'un processus qui permet à l'auditeur interne ou au contrôleur permanent de faire apparaître très clairement :

- les tâches effectuées, leur chronologie et les différents acteurs qui y participent ;
- les documents qui les transcrivent, leur nombre d'exemplaires, leur distribution et leur classement ;
- les contrôles associés aux différentes tâches.

Présenté le plus clairement possible et de façon normative, il est constitué sur la base d'entretiens, d'étude de documents, de tests de cheminement. Il est utilisé pour documenter les processus lorsque cette documentation n'existe pas ou dont la conception est inadaptée au besoin de compréhension et d'analyse de l'audit interne ou du contrôle permanent.

Comment utiliser le diagramme de circulation ?

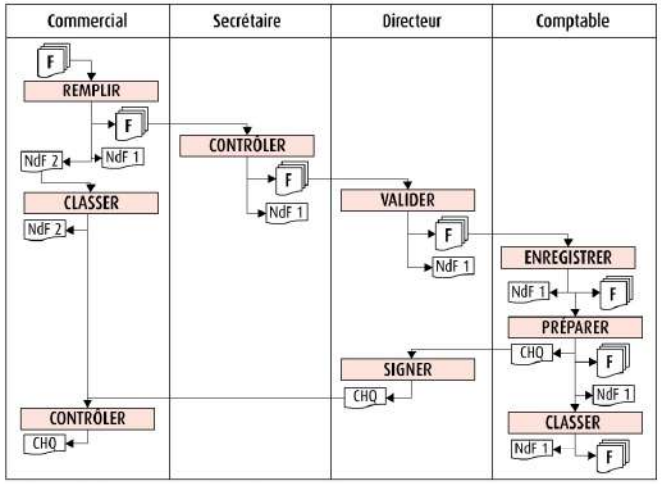
Protocole de modélisation d'un processus

- Identifier les différents acteurs concernés.
- Identifier les différents supports d'information échangés, en différenciant les supports d'information permanents (utilisables plusieurs fois) et les supports d'information non permanents (utilisables une seule fois).
- Identifier les différents traitements réalisés en différenciant ceux effectués par une personne, par une machine ou par une personne à l'aide d'une machine.
- Faire figurer ces informations dans un tableau présentant les canaux de circulation des informations.

Protocole d'analyse critique d'un processus

- S'interroger sur la capacité du processus à répondre à ses finalités (fonctions principales, secondaires, d'estime et de contraintes).
- Évaluer les performances économiques du processus (valeur des traitements : transformation, contrôle, déplacement, recherche, classement et attentes).
- Évaluer les performances sociales du processus (intérêt du travail, degrés d'autonomie et de responsabilisation des personnes concernées…).
- Évaluer la sécurisation du processus (séparation des fonctions d'autorisation, de réalisation et de validation, exhaustivité des traitements, réalité des informations, enregistrements des entrées et des sorties, mémorisation des pièces, comptabilisation des opérations et de leur contrepartie comptable…) ; existence de contrôles opérationnels et de contrôles de premier niveau.

Figure 9.9 – Diagramme de circulation d'un processus de remboursement des notes de frais d'un commercial



F = facture ; NdF = note de frais ; CHQ = chèque

EN PRATIQUE

Soyez attentif : un processus est comme une canalisation d'eau... Attention au débit, aux fuites et aux bouchons !

Vous pouvez utiliser des symboles de représentation graphique afin de visualiser les traitements et les supports d'information utilisés. Si cela est le cas, utilisez une légende !

OUTILS TECHNIQUES

LES CONTRÔLES

Les contrôles font partie intégrante du dispositif de maîtrise des risques. Les objectifs des contrôles sont de contribuer à maîtriser les risques d'un domaine, activité et/ou processus et de responsabiliser les différents acteurs.

Tableau 9.14 – Différents niveaux des contrôles

Le contrôle opérationnel – les collaborateurs	■ Correspond à une instruction figurant au sein d'une procédure. ■ Est réalisé au fil de l'eau dans le cadre du traitement des opérations.
Le contrôle de premier niveau – les responsables hiérarchiques	■ Correspond à un contrôle permanent de la responsabilité d'une direction métier. ■ Est réalisé régulièrement sur la base d'un échantillon d'opérations. ■ Peut se matérialiser sous la forme d'autocontrôle, de contrôle « à 4 yeux » ou de contrôle hiérarchique. ■ Peut être décrit dans les procédures de travail. ■ Donne lieu à une formalisation, à la production d'indicateurs de risques, à la formalisation d'un reporting hiérarchique et à la mise en œuvre d'actions correctrices.
Le contrôle de deuxième niveau – les contrôleurs permanents	■ Correspond à un contrôle permanent de la responsabilité d'une entité spécialisée sans responsabilité opérationnelle. ■ Est réalisé *a posteriori* à distance ou sur place, à fréquence régulière ou ponctuelle par des contrôleurs spécialisés. ■ Inclut l'évaluation du contrôle de premier niveau. ■ Donne lieu à une formalisation, la production d'indicateurs de risques, à la formalisation d'un reporting hiérarchique et l'émission de plans d'action.
Le contrôle de troisième niveau – les auditeurs internes	■ Correspond à un contrôle périodique de la responsabilité d'une entité spécialisée rattachée au plus haut niveau de l'entreprise ou externes (autorités de tutelle, Cour des comptes). ■ Est réalisé *a posteriori* sur place par des auditeurs spécialisés. ■ Peut se baser sur les contrôles de premier et deuxième niveaux. ■ Donne lieu à une formalisation, la production d'indicateurs de risques, à la formalisation d'un reporting hiérarchique et l'émission de recommandations.

Auditeurs internes de troisième niveau et contrôleurs permanents de deuxième niveau, vous ne devez jamais être en charge du contrôle de premier niveau pour le compte des métiers que vous contrôlez sous peine de les déresponsabiliser.

Figure 9.10 – Fiche de contrôle (exemple bancaire)

Fiche de contrôle				
Nature du contrôle	Préventif		N° de référence du contrôle	FDC/05/071
	Détectif	X		
Famille de risque	Risques commerciaux		N° de référence du risque	FRR/05/07
Type de contrôle	Contrôle de niveau 1	X	Contrôle de niveau 2	
Intitulé du contrôle	Contrôle de la complétude des dossiers client à l'entrée en relation			
Propriétaire du contrôle	M. ..., Directeur commercial			
Responsable documentation	M. ..., Adjoint au Directeur commercial			

Description du contrôle				
Degrés de priorité	Obligatoire	X	Recommandé	
Contôleur	Contrôleurs de niveau 1 rattachés aux entités de middle office de la banque au sein de chaque groupe géographique			
Type	Manuel	X	Automatique (SI)	
Mode opératoire	Pour toute demande d'entrée en relation: vérifier, en fonction de la segmentation du client et à l'aide de la check-list des pièces obligatoires et recommandées, la présence desdites pièces dans le dossier du client Dans le cas d'une pièce manquante, et s'il s'agit d'une pièce bloquante, bloquer le processus d'entrée en relation dans l'application « Ouverture de compte » (et donc la fourniture d'instruments de paiement) et demander au Front Office du groupe commercial concerné de faire les diligences nécessaires auprès du client			
Fréquence	Au fil de l'eau	X	Quotidien	
	Hebdomadaire		Mensuel	
	Trimestriel		Semestriel	
	Annuel		Ponctuel	
Résultat du contrôle	Date dernier contrôle	*18/04/13*		
	Contrôleur	*M. ..., contrôleur de premier niveau, Middle Office du Groupe Provence Côte d'Azur*		
	Sources utilisées	*Dossier du client OPQ*		
	Constats	*Absence de copie du justificatif de domicile*		
	Actions décidées	*Demande de la pièce au Front office du Groupe Provence Côte d'Azur*		

OUTILS TECHNIQUES

▶ Exemple

Critères de contrôles retenus dans une banque française pour identifier d'éventuelles fraudes fiscales et se traduisant par des contrôles opérationnels et des plans de contrôle de niveau 1, 2 et 3

- Utilisation d'une société écran (activité non cohérente avec l'objet social; siège social dans un État ou un territoire n'ayant pas conclu de convention fiscale avec la France; siège social à l'adresse privée d'un des bénéficiaires de l'opération suspecte; siège social à l'adresse d'un domiciliataire).
- Société présentant des changements statutaires fréquents non justifiés par la situation économique de l'entreprise.
- Interposition de personnes physiques n'intervenant qu'en apparence – « homme de paille » (pour le compte de la société; pour le compte de particuliers).
- Opérations financières incohérentes ou suspectes (au regard des activités habituelles de l'entreprise) dans des secteurs sensibles aux fraudes à la TVA (informatique, téléphonie, matériel électronique, électroménager, hi-fi, vidéo).
- Progression forte et inexpliquée de sommes créditées (sur une courte période; sur un compte nouvellement créé ou juste là peu actif).
- Constatation d'anomalies dans les factures ou bons de commande présentés comme justification d'opérations financières (absence de numéro de SIREN; absence de numéro d'immatriculation au RCS; absence de numéro de TVA; absence de numéro de facture; absence d'adresse; absence de date).
- Comptes avec solde souvent proche de zéro (dits « comptes de passage »; transit de multiples opérations tant au crédit qu'au débit).
- Comptes professionnels (retraits fréquents d'espèces; dépôts fréquents d'espèces; absence de justification au regard de la nature ou du niveau de l'activité).
- Multiplicité des comptes, d'interlocuteurs, de sociétés, de sociétaires (difficulté d'identifier des bénéficiaires effectifs; mécanismes de gestion et d'administration paraissant peu transparents).
- Opérations financières internationales (absence de cause juridique ou économique apparente; en provenance ou à destination d'un pays/territoire jugé sensible en termes de lutte contre le blanchiment et le financement du terrorisme).
- Refus ou impossibilité de produire des pièces justificatives par le client (provenance des fonds; moyens de paiements).
- Aller-retour vers l'étranger (transferts de fonds vers l'étranger puis rapatriement sous forme de prêt).
- Organisation d'insolvabilité (vente rapide d'actifs à des personnes physiques ou morales liées; vente rapide à des conditions traduisant un déséquilibre manifeste et injustifié).
- Résidents français utilisant régulièrement des comptes de sociétés étrangères.
- Dépôts par un particulier de fonds sans rapport avec son activité ou sa situation patrimoniale connue.
- Transaction immobilière à un prix manifestement sous-évalué.

LA GRILLE « GRAVITÉ/PROBABILITÉ »

La grille de contrôle est un outil qui peut permettre à l'auditeur interne ou au contrôleur permanent de déterminer les modalités de contrôle les plus adaptées à une situation. L'objectif de la grille « gravité/probabilité » est de déterminer les contrôles à mettre en place pour sécuriser un domaine ou un processus.

Protocole d'utilisation de la grille « gravité/probabilité »

- Pour chaque risque identifié, s'interroger sur le type de contrôle à mettre en place en fonction de deux critères discriminants en matière de risque : la gravité du risque et la probabilité d'apparition du risque.
- En fonction de ces deux critères, mettre en place un contrôle exhaustif, un contrôle par sondage (échantillon), global ou par exception ou, au contraire, ne pas mettre en place de contrôle.

Figure 9.11 – La grille de contrôle

<table>
<tr><td colspan="2"></td><td colspan="3">Probabilité d'apparition</td></tr>
<tr><td colspan="2"></td><td>+</td><td>+/-</td><td>-</td></tr>
<tr><td rowspan="3">Gravité</td><td>+</td><td>Contrôle exhaustif</td><td></td><td></td></tr>
<tr><td>+/-</td><td colspan="2">Contrôle par exception, par sondage ou global</td></tr>
<tr><td>-</td><td colspan="3">Pas de contrôle</td></tr>
</table>

EN PRATIQUE

Adaptez les modalités de réalisation des contrôles en fonction des risques.

Faites attention aux coûts de réalisation des contrôles, et également aux impacts d'une absence totale de contrôle pour cause de coût…

OUTILS TECHNIQUES

L'ARBRE DES CAUSES

L'arbre des causes permet à l'auditeur interne ou au contrôleur permanent de découvrir les causes réelles qui expliquent une situation.

Protocole d'utilisation de l'arbre des causes

- Prendre une feuille de papier de préférence d'un format A3.
- Indiquer au centre de la page le problème pour lequel on cherche à inventorier les causes explicatives possibles.
- Rechercher les causes possibles de niveau 1 en se posant la question « pourquoi ? » et en essayant d'y répondre par des phrases commençant par « parce que… ».
- Rechercher ensuite les causes de niveau 2 en repartant de chaque cause de niveau 1, puis…
- Arrêter l'inventaire quand les mêmes causes reviennent plusieurs fois ou que celles-ci correspondent à des critères, des croyances ou des éléments de culture forts.
- Vérifier sur le terrain la réalité de chaque cause identifiée et le poids relatif de chaque cause identifiée.

▶ EXEMPLE : POSE D'UNE PROTHÈSE DE GENOU À UN PATIENT

L'une des erreurs médicales la plus fréquente consiste à réaliser une opération du mauvais côté. Par exemple, le patient arrive pour le remplacement d'une prothèse du genou gauche déjà appareillé et se voit poser une prothèse du genou droit qui n'en avait pas besoin… Dans ce type de situation malheureusement non rare, et qui peut concerner un rein, un poumon, un œil…, les causes sont multiples.

Figure 9.12 – Arbre des causes

EN PRATIQUE

On ne voit que ce que l'on a appris à voir : utilisez donc la check-list « QQOQCCP » ou la règle des « 5 M » (main-d'œuvre, méthodes, milieu, matières et machines) pour ouvrir le spectre du possible et valider l'inventaire.

Constituez un groupe de personnes variées afin de ne pas voir qu'une ou deux familles de causes et passer à côté des autres.

Utilisez un diagramme en arête de poisson (diagramme d'Ishikawa) pour représenter graphiquement le résultat de la phase de vérification terrain.

OUTILS TECHNIQUES

LA FEUILLE DE RÉVÉLATION ET D'ANALYSE DE PROBLÈME

La feuille de révélation et d'analyse de problème (FRAP) est le papier de travail synthétique qu'utilise l'auditeur interne ou le contrôleur permanent pour présenter et documenter chaque « révélation ». Une « révélation » correspond le plus souvent à un dysfonctionnement ou une anomalie observée et méritant la mise en œuvre d'une action d'amélioration.

La FRAP permet :

- de structurer la pensée de l'auditeur interne ou du contrôleur permanent pour formuler l'observation, en peser l'incidence et proposer une amélioration ;
- de favoriser la communication avec la personne auditée ou contrôlée (acceptation, réflexion en commun, pérennité de la formulation…) ;
- de professionnaliser la matérialisation des constats (forme homogène, contenu harmonisé) ;
- de contribuer à la préparation et à la tenue de la réunion de clôture ;
- d'accélérer et harmoniser la production des rapports ;
- de faciliter la réunion de validation ;
- d'améliorer les performances ;
- de traiter des dysfonctionnements, des anomalies, des problèmes ;
- de favoriser le travail en groupe avec les collaborateurs concernés par la situation ;
- d'orienter la réflexion vers une recherche d'améliorations plutôt qu'une recherche des coupables.

Protocole d'utilisation de la FRAP

- Renseigner les fiches d'une façon unitaire (chaque situation ou résultat insatisfaisant doit donner lieu à l'ouverture d'une fiche) :
  - Identification d'une situation ou d'un résultat non conforme au niveau de performance souhaitable ou normal ; inscription de ce fait dans la partie « Faits observés » (attention, les situations évoquées doivent être factuelles et de préférence chiffrées).
  - Évaluation de la conséquence de cette situation ou de ce fait en termes de qualité de service, de coût, de climat social et de sécurité ; inscription de ces conséquences dans la partie « Conséquences réelles/éventuelles ».

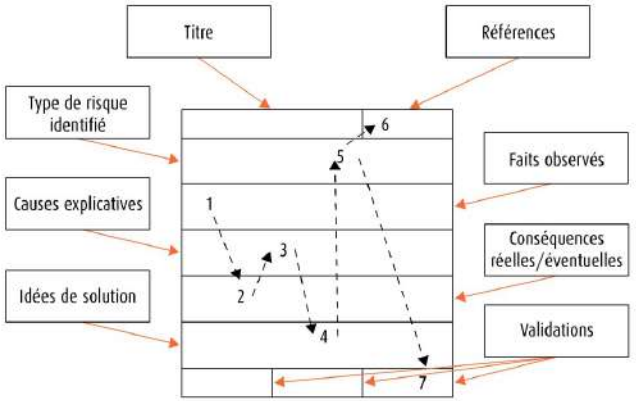
.../...

.../...

– Identification des causes explicatives de cette situation ou de ce résultat ; inscription de ces causes dans la partie « Causes explicatives » ; une fiche présentant un fait, des conséquences réelles et des causes explicatives doit être conservée car elle met en évidence une faiblesse. Si ce n'est pas le cas, le fait ne doit pas être conservé. Recherche d'idées d'amélioration ou de solutions permettant d'améliorer la situation ou le résultat. Inscription de ces idées de solution dans la partie « Idées de solution ».

- Indiquer dans le cartouche supérieur la famille d'appartenance de la faiblesse.
- Classer les fiches par groupes homogènes.
- Hiérarchiser les fiches entre elles.

Figure 9.13 – La feuille d'analyse et de révélation de problème



EN PRATIQUE

Utilisez les FRAP au fil de l'eau pendant la phase de travail terrain.

Ne cherchez pas à rendre les FRAP homogènes : acceptez le principe que certains mettent en évidence un gros dysfonctionnement et d'autres un incident mineur... N'oubliez pas que le contenu des FRAP doit être justifié par des preuves à joindre en annexe.

Respectez l'ordre de rédaction de la fiche (1 → 2 → 3 → 4 → 5 → 6 → 7) car cela est plus simple.

OUTILS TECHNIQUES

LE TEST DE CHEMINEMENT OU LA PISTE D'AUDIT

Le test de cheminement, parfois appelé « piste d'audit » est une méthode de test très utilisée par l'auditeur interne et le contrôleur permanent. Elle permet de remonter à la source en passant par toutes les phases intermédiaires. Le test de cheminement ne concerne qu'une seule opération à la fois et permet à l'auditeur interne ou au contrôleur permanent de contrôler, pour l'opération choisie, tous les stades intermédiaires, leurs justificatifs et justifications.

C'est un outil efficace pour s'assurer de la correcte compréhension du processus et pour matérialiser l'existence des dispositifs de contrôle interne tout au long du processus. Cependant, la démarche suivie ne garantit pas que toute opération en entrée du processus suive le même chemin. Il faut que l'opération soit de même nature et présente les mêmes caractéristiques. Ainsi un montant, une période ou un bénéficiaire différent peuvent conduire à un tout autre traitement.

EN PRATIQUE

Choisissez un événement déclencheur caractéristique du cycle que vous souhaitez contrôler : cycle « achat », cycle « commande client », cycle « recrutement ».

Photocopiez tous les supports d'information utilisés dans le cycle et collez-les sur un *brown paper* accroché au mur.

LE DIAGRAMME DE VILFREDO PARETO

Le diagramme de Pareto, ou loi des « 20/80 », attribuée à l'économiste vénitien Vilfredo Pareto, est un outil permettant à l'auditeur interne ou au contrôleur permanent de focaliser son attention sur les enjeux. Il permet en effet de mettre en évidence des enjeux financiers (zones présentant une forte concentration de profits ou de risques), de se centrer sur l'essentiel et d'éviter ainsi de se perdre dans les détails.

Protocole d'utilisation du diagramme de Pareto

- Déterminer un champ homogène d'utilisation de la loi de Pareto.
- Quantifier « ce qui passe dans les tuyaux ».
- Repérer les enjeux.
- S'interroger sur les enjeux en question au regard du dispositif de contrôle interne.

EN PRATIQUE

La règle des 20-80 (appelés également méthode ABC) ne tombe que rarement exactement sur ces deux valeurs qui doivent être considérées comme des valeurs indicatives.

N'oubliez pas qu'il existe plusieurs natures d'enjeux possibles : en volume, en euros, en durée...

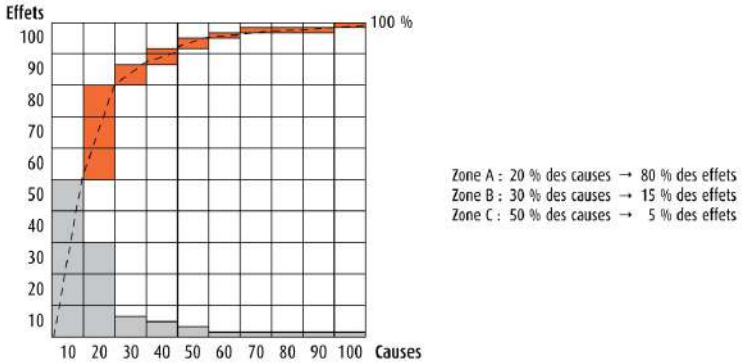
Exemple – Agence bancaire, clientèle de particuliers

Si on considère le produit net bancaire d'une agence bancaire (son chiffre d'affaires), on constate que tous ses clients ne contribuent pas à hauteur égale. L'étude réalisée dans le réseau commercial d'une banque de particuliers présente sur l'ensemble du territoire français a montré en effet que :

- 20 % des clients représentent 80 % du PNB (il est donc rentable de les rencontrer dans le cadre de rendez-vous à leur domicile) ;
- 30 % des clients représentent 15 % du PNB (il est donc préférable de les recevoir à l'agence au guichet ou en rendez-vous) ;
- 50 % des clients représentent 5 % du PNB (il est donc préférable de communiquer avec eux par courrier, téléphone, e-mail...).

OUTILS TECHNIQUES

Figure 9.14 – La règle des 20-80



LE *BENCHMARKING*

Le *benchmarking* est un outil inspiré du principe des analogies. Il consiste à observer ce qui marche bien ailleurs et de s'en inspirer pour imaginer une solution originale et appropriée à la situation. À ce titre, il constitue, pour l'auditeur interne et le contrôleur permanent, un procédé simple et efficace pour trouver des solutions réellement innovantes.

Protocole de réalisation d'un *benchmarking*

- Identifier des entités réputées performantes dans le domaine considéré. Celles-ci peuvent l'être parce que :
  - elles atteignent un très haut niveau de performance dans un domaine particulier, comme la ponctualité ou le niveau de service par exemple ;
  - elles ne rencontrent jamais les problèmes que rencontrent leurs concurrents directs ;
  - elles ont une grande capacité à traiter les problèmes qu'elles rencontrent ;
  - elles ont, de notoriété publique, cette image, même si cela n'est pas vrai !
- Repérer, dans ces entités, les convictions et les principes organisationnels qui expliquent ce niveau de performance.
  Ces convictions peuvent être par exemple : « L'intérêt du client passe avant l'intérêt de l'entreprise » ; « Le personnel de l'entreprise est notre bien le plus précieux » ; « Nous avons une responsabilité au niveau de la collectivité »...
  Ces principes organisationnels peuvent être la polyvalence du personnel, voire la rotation interne périodique ; le fait que chaque client ait un interlocuteur unique ; l'utilisation d'une technologie spécifique : Internet, smartphone, tablette, carte sans contact...
- S'inspirer de ces principes afin de concevoir et de déployer sur mesure la solution qui permettra à l'entreprise d'atteindre ce niveau de performance.

EN PRATIQUE

N'hésitez pas à vous inspirer de ce qui marche ailleurs, même si cela est contraire à ce que vous avez appris à l'école.

Méfiez-vous, une solution organisationnelle n'est jamais transférable telle qu'elle, copier simplement ne suffit pas et peut parfois même s'avérer une très mauvaise idée !...

OUTILS TECHNIQUES

LE *BRAINSTORMING*

Le *brainstorming* est une démarche favorisant la production d'idées par un groupe de personnes. Il permet à l'auditeur interne et au contrôleur permanent de générer des idées originales pouvant déboucher sur des « innovations de rupture ».

Protocole de réalisation d'un *brainstorming*

- Constituer un groupe de créativité composé de cinq à douze personnes.
- Installer les membres du groupe dans une salle propice à la créativité.
- Distribuer à chaque personne un feutre et un paquet de cartes leur permettant d'inscrire leurs idées à leur rythme, sans goulot d'étranglement.
- Expliquer le thème de la recherche et préciser les règles de fonctionnement.
- Inviter les personnes à produire leurs idées et à les coller sur un grand tableau prévu à cet effet (il est possible d'utiliser des post-it) afin que l'ensemble des participants ait en permanence une vue de l'ensemble des idées émises.
- Veiller pendant toute la phase de production d'idées à ce que les personnes ne se censurent pas elles-mêmes et ne critiquent pas les idées des autres participants.
- Quand les participants n'ont plus d'idées, reprendre chaque idée émise et demander au groupe de l'expliciter ainsi que de la rendre opérationnelle.
- Supprimer les idées non recevables.
- Classer les idées intéressantes en catégories.
- Reprendre par la suite chaque catégorie d'idées et les transformer en solutions concrètes.
- Évaluer pour chaque solution concrète ainsi identifiée son opportunité et sa faisabilité technique.

EN PRATIQUE

C'est à vous qu'il revient d'ouvrir et de conclure la séance, de stimuler le groupe et de veiller à ce que tout ce qui est dit soit noté (même ce qui à première vue peut paraître insignifiant).

Contrôlez le respect des règles et notamment les travaux de dépouillement.

Concrétisez les idées en solutions, cela permet de constater que des idées considérées au départ comme farfelues peuvent en fait se transformer en d'excellentes solutions.

Dans certains cas, créez deux groupes : le premier pour imaginer des idées et le second pour les transformer en solutions opérationnelles. Il peut pareillement être très intéressant de changer les rôles entre les participants des deux groupes.

LE PLAN D'ACTION

Le plan d'action constitue la traduction opérationnelle des recommandations présentées dans le rapport d'audit interne ou demandées par le contrôle permanent. L'objectif du plan d'action est de présenter les actions devant être mises en œuvre par les métiers afin de développer la performance de leur dispositif de contrôle interne.

Protocole de définition d'un plan d'action

- Traduire les recommandations en actions et pour cela :
  - demander aux personnes concernées comment elles pensent s'y prendre pour répondre aux recommandations présentées dans le rapport ;
  - évaluer la pertinence de leurs actions en regard des faiblesses et recommandations.
- Formaliser ces actions dans un planning et faire valider ce planning par le responsable du domaine audité ou contrôlé.
- Contrôler régulièrement l'avancement des actions.

EN PRATIQUE

Le B.A.-BA d'un plan d'action est : qui ? doit faire quoi ? pour quand ?

Dans certains cas, il est utile de faire figurer les attendus réciproques entre les personnes (certaines actions nécessitent en effet en amont la réalisation d'autres actions par d'autres personnes).

OUTILS TECHNIQUES

LA CARTE DES FORCES

La carte des forces est un outil issu des travaux sur la sociodynamique réalisés par Christian Fauvet. Elle permet à l'auditeur interne ou au contrôleur permanent d'évaluer la capacité de changement des personnes d'une entité auditée ou contrôlée au niveau individuel de chacune des personnes qui la composent et pareillement au niveau collectif.

En effet, le changement est un processus complexe qui nécessite, pour les personnes concernées :

- la compréhension et l'acceptation de la cible visée (résultat et délai) ;
- la connaissance de la façon d'arriver à cet objectif (démarche) ;
- le renoncement aux bénéfices secondaires du maintien de la situation présente (gain).

Face à un changement, une personne et un groupe adoptent une attitude composée de synergie et d'antagonisme.

Protocole d'utilisation de la carte des forces

Identifier les catégories de personne concernées par la mise en œuvre du changement.

Repérer leurs positions à l'aide de questions types :

- Quelle est l'attitude prévisible de X ou de Y à l'égard du projet ?
- Comment se positionnent globalement les différentes catégories de personnes concernées par le projet ?
- Sont-elles plutôt favorables ou défavorables ?
- Passives ou actives ?
- Qu'ont-elles à gagner avec le projet, et à perdre ?
- Quelles concessions est-on prêt à faire ?
- Quelles influences sont en mesure de s'exercer au sein de l'entreprise ?
- Existe-t-il un ou plusieurs leaders ?
- Peut-on dès à présent repérer des personnes influencées par d'autres ?...

Représenter leurs positions sur la carte des forces.

Définir les actions de communication, de lobbying... à entreprendre.

Différentes positions sont possibles.

Positions alliées par rapport au changement

- Le «triangle d'or»: leur côté synergique fait avancer les choses et leur côté antagoniste leur fait garder du recul et proposer des améliorations. Cette catégorie de personnes doit avoir des responsabilités dans la conduite du changement, notamment pour convaincre les hésitants.
- Les «engagés»: ils adhèrent au changement sans retenue ni capacité critique. Totalement hermétique aux stratégies de compromis, cette catégorie de personnes doit être utilisée pour porter le changement et dans des contextes à faible résistance au changement.

Positions «flottantes» vis-à-vis du changement

- Les «hésitants»: ils sont parfois qualifiés de «faux jetons» car s'intéressent au changement (même s'ils s'intéressent également à celui des opposants s'il existe), ce sont des soutiens conditionnels au projet et ils ont une forte influence sur les passifs. Cette catégorie de personnes doit être associée au changement pour en devenir acteur.
- Les «passifs»: ils sont considérés comme des poids morts: la «force tranquille». Ils n'aiment pas se poser des questions et n'aiment pas l'incertitude; ils ne sont pas intéressés par le changement: l'intéressement passe par son voisin. Cette catégorie de personne doit être accompagnée de près.

Positions en opposition avec le changement

- Les «grognons»: ce sont des passifs qui rouspètent mais leur antagonisme se limite aux paroles. Ils constituent à ce titre un bon baromètre de ce que pense l'opinion publique par rapport au changement. Cette catégorie de personne doit être plutôt ignorée.
- Les «opposants»: ils ne cherchent jamais l'accord, manient l'art de la critique négative mais doivent être respectés dans leur opposition car elle est le plus souvent légitime. Cette catégorie de personne peut se soumettre moyennant quelques compensations.
- **Les «révoltés»**: ils ont un autre projet, une autre vision de la vie. Heureusement, cette catégorie de personne est très minoritaire: elle doit être soumise, voire exclue.
- Les «déchirés»: ils sont considérés comme des cas pathologiques, s'impliquant à l'extrême dans le changement et en même temps s'y opposant avec force.

OUTILS TECHNIQUES

EN PRATIQUE

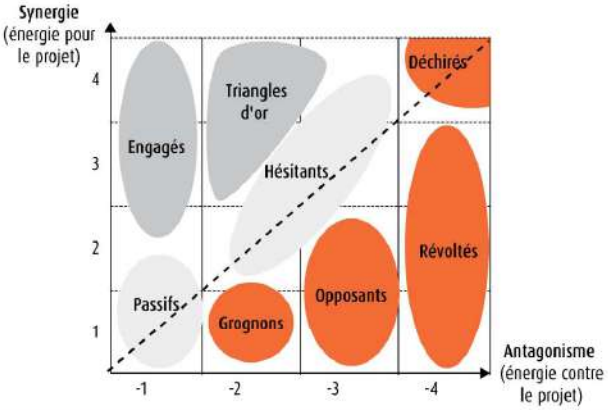
N'oubliez pas que, face à un changement, il est normal de se poser les questions suivantes: qu'est-ce que j'y gagne? Qu'est-ce que j'y perds? Quel est l'enjeu? Que se passera-t-il si je refuse?...

Souvenez-vous que face à un changement, la position d'une personne n'est pas figée, ce qui veut dire que celle-ci peut évoluer positivement ou négativement.

En matière de conduite du changement, utilisez les cinq piliers de la conduite du changement:

- la description précise de l'organisation et des processus cibles;
- la formation à la nouvelle organisation, processus, règles de gestion, procédures, modes opératoires, logiciels...
- la communication;
- le choix des personnes (celles retenues pour la cible, le reclassement de celles non retenues);
- le passage du *gap* (en une fois, tout d'abord sur un site test puis partout, en biseau...).

Figure 9.15 – Présentation des sous-populations caractéristiques



L'ANALYSE SWOT

L'analyse SWOT (*strengths weaknesses opportunities threats*) permet de réaliser des analyses stratégiques. Il est cependant également possible aux auditeurs internes et contrôleurs permanents d'utiliser cette technique dans l'analyse des risques par la réalisation de deux diagnostics concomitants.

Un diagnostic externe

Il identifie les opportunités et les menaces présentes dans l'environnement. Celles-ci peuvent être déterminées à l'aide d'une série de modèles d'analyse stratégique, tels que le modèle Pestel, le modèle des cinq forces de la concurrence de Michael Porter ou encore une analyse de scénarios. Il peut s'agir par exemple de l'irruption de nouveaux concurrents, de l'apparition d'une nouvelle technologie, de l'émergence d'une nouvelle réglementation, de l'ouverture de nouveaux marchés, etc.

Un diagnostic interne

Il identifie les forces et les faiblesses du domaine d'activité stratégique. Celles-ci peuvent être déterminées à l'aide d'une série de modèles d'analyse stratégique, tels que la chaîne de valeur, l'étalonnage (*benchmarking*) ou l'analyse du tissu culturel.

Il peut s'agir par exemple d'un portefeuille technologique, d'une notoriété, d'une présence géographique, d'un réseau de partenaires, d'une structure de gouvernement d'entreprise, etc.

Il est alors possible de comparer avec profit :

- la perception des forces et des faiblesses de l'entreprise par elle-même ;
- la perception des forces et des faiblesses de l'entreprise par ses clients, concurrents, fournisseurs et autres acteurs externes.

C'est alors la confrontation entre les résultats du diagnostic externe et ceux du diagnostic interne qui permet de formuler des options stratégiques. Cette formulation d'options stratégiques constitue l'intérêt de l'analyse SWOT.

OUTILS TECHNIQUES

Figure 9.16 – La matrice SWOT

Origine interne (Organisation)	Forces (*Strengths*)	Faiblesses (*Weaknesses*)
Origine externe (Environnement)	Opportunités (*Opportunities*)	Menaces (*Threats*)

EN PRATIQUE

La matrice SWOT n'apporte cependant une aide pertinente que dans la mesure où les questions initiales sont convenablement posées, où l'on peut y répondre, et où l'on a ensuite bien analysé chaque domaine en termes de performance mais aussi d'importance. La justesse des résultats dépend de la justesse de l'analyse sur le court, moyen et long terme et de la conscience que l'environnement interne ou externe peut rapidement changer, ce qui nécessite de régulièrement mettre à jour l'analyse.

Mettez en regard les quatre composants de la matrice.

Ne cherchez pas à être le plus exhaustif possible car la matrice n'est pas une science exacte. En revanche, inspirez-vous de grilles réalisées précédemment afin de ne pas oublier un thème à évaluer.

PAROLE D'EXPERT

Lawrence B. Sawyer, huitième commandement : connaître les personnes

« L'inspecteur moderne rencontre des personnes beaucoup plus souvent que ne le faisaient les inspecteurs d'autrefois. Il peut évoluer dans des domaines étranges et étrangers, où la langue est nouvelle, où le jargon professionnel est inintelligible et où les systèmes et les méthodes sont parfois mystérieux. S'il essaye avec arrogance d'agir seul, il pourrait bien aller tout droit vers un échec humiliant. Aussi doit-il comprendre ce que les gens éprouvent en face d'une critique et doit savoir qu'il est naturel pour eux d'être sur la défensive. Il doit comprendre qu'il ira beaucoup plus loin s'il cherche à former avec les gens une équipe pour la recherche de solutions aux problèmes que s'il garde un air de supériorité ou s'il a l'aspect sévère du censeur. Il doit éviter les conflits de front ou les discussions "gagne ou perd" au cours de son travail dans les services, il ferait alors reculer l'inspection ou lieu de la faire avancer. Il devra essayer de susciter de l'empathie avec les personnes avec qui il travaille, s'efforcer de se mettre vraiment à leur place. Elles ressentiront cette empathie et l'apprécieront et cela fera progresser la recherche des faits. Il devra faire des compliments lorsqu'ils sont mérités. Les gens "boivent du petit-lait" lorsque l'on reconnaît leurs mérites. Des mots d'éloge bien placés et la compréhension font voir à celui qui est inspecté l'inspecteur sous un nouveau jour, non comme un critique invétéré, mais comme un expert conseil. Lorsqu'il cherchera honnêtement et sincèrement à comprendre les gens et leurs problèmes, ils l'aideront et il pourra les aider. Et, surtout, il servira mieux la direction. »

TÉMOIGNAGE

Éric Guilhou, directeur général finance, groupe Socotec

Le contrôle interne est un levier clé d'amélioration de la performance dans une entreprise de services.

La mise en place d'un référentiel de contrôle interne dans une entreprise de services est souvent considérée comme un encadrement bloquant les initiatives et l'autonomie. Ceci est d'autant plus vrai dans une entreprise de services où le capital humain, son savoir-faire et son expérience représentent souvent la valeur principale de l'actif de l'entreprise.

Mettre en place un référentiel de contrôle interne et l'animer avec une équipe d'audit interne, c'est remettre en question des pratiques existantes depuis de nombreuses années, gage de la performance actuelle ou passé de l'entreprise.

Sauf que le monde change, le *go to market* des services s'accélère et la durée de vie des offres se raccourcit en particulier par la remise en cause technologique de la dématérialisation et du digital.

Comment la mise en place d'une structure de contrôle interne peut-elle donc aider à améliorer la performance de l'entreprise ?

- Au sens de ses processus opérationnels et de gestion, un nouveau référentiel de contrôle interne clarifie les rôles et responsabilités des personnes et des services, établit la pertinence des flux transactionnels et améliore la fluidité de l'échange des informations et des données.
- Au sens des coûts de fonctionnements, le référentiel de contrôle interne réduit, voire supprime, des redondances inutiles établies avec le temps.
- Au sens de l'efficacité de l'organisation, le contrôle interne permet de réduire des strates de décision inutiles, permet de déléguer des échelles de responsabilités plus complètes dans les différents niveaux de l'organisation à l'instar d'autonomies sauvages ou d'usages.
- Au sens de la performance financière, tout point de contrôle clé du référentiel de contrôle interne doit se traduire et peut se traduire dans sa définition et dans sa mise en œuvre par une baisse des coûts de fonctionnement et/ou de production et une amélioration du *cash-flow* correspondant.

La motivation et la démarche du contrôleur interne, tout en respectant les fonctions régaliennes qui lui sont attachées, doivent viser de façon permanente à l'amélioration de la performance de l'entreprise. Il pourra la mesurer et fournir à l'entreprise une meilleure maîtrise de ses risques.

Au-delà de la mise en place d'un référentiel de contrôle interne, l'auditeur interne deviendra plus naturellement un interlocuteur clé sur les enjeux de changements qui sont souvent porteurs de développement et de remise en cause dans les entreprises.

CHAPITRE 10

Les compétences relationnelles et comportementales

CE CHAPITRE VOUS PERMETTRA DE :

- connaître les compétences relationnelles et comportementales nécessaires pour la pratique des deux fonctions.

La véritable difficulté des métiers d'auditeur interne et de contrôleur permanent ne concerne pas les aspects techniques mais plutôt ce qui a trait à l'humain. L'humain va se rencontrer dans les relations avec sa hiérarchie et celle de l'entreprise (comité d'audit, président, *top management*), mais également et surtout au quotidien avec les personnes auditées et/ou contrôlées. Difficultés à faire coopérer dans le diagnostic, difficulté à faire admettre les faiblesses, difficulté à obtenir des idées d'amélioration, des engagements de changement et des réalisations concrètes…

1. LE POINT DE VUE DE L'APEC

L'Apec a défini les compétences techniques que doit posséder un auditeur interne.

Compétences techniques

- La maîtrise des techniques d'audit fondées sur les normes professionnelles : planification, vérification, conclusion.
- La maîtrise des techniques de management de projet.
- La connaissance des risques de l'entreprise.
- Les connaissances en comptabilité générale et analytique.
- La connaissance de l'anglais.
- La bonne connaissance de l'ensemble des métiers de l'entreprise (les entreprises recherchent désormais des auditeurs internes ayant une vue d'ensemble de l'entreprise).
- La maîtrise des systèmes d'information de l'entreprise.

D'après l'Apec, un auditeur interne doit posséder les traits de personnalité suivants :

- la capacité d'encadrement et d'animation d'équipe pour le directeur de l'audit interne ;
- la rigueur pour justifier et documenter chaque constat ;
- l'aisance relationnelle et l'aptitude au travail en équipe ;
- l'esprit d'initiative, la capacité à proposer des recommandations afin d'améliorer les process existants ;
- la disponibilité et une forte capacité de travail ;
- la curiosité et un sens critique développé dans la recherche d'approfondissement des sujets ou pour être attentif à toute information qui pourrait s'avérer importante ;
- la déontologie, l'intégrité, qualité essentielle à l'auditeur interne afin d'avoir un jugement impartial ; il doit en outre respecter la confidentialité des informations qu'il récolte ;
- le goût pour la mobilité. L'auditeur interne est souvent en déplacement au sein des filiales de l'entreprise.

2. LE POINT DE VUE DU SITE INTERNET LETUDIANT.FR

D'après le site Internet Letudiant.fr, les qualités d'un auditeur interne sont :

- la diplomatie ;
- les capacités d'analyse et de synthèse ;
- un bon contact et un sens pédagogique.

Tableau 10.1 – Les connaissances et compétences transverses d'un auditeur, banque commerciale

CONNAISSANCES	Connaissance de base	Connaissance approfondie	Maîtrise
CONNAISSANCES GÉNÉRALES			
Environnement économique et financier			X
Stratégie, objectifs et plan d'actions de l'entreprise			X
Organisation du Groupe et de l'entreprise			X
Organisme et interlocuteurs externes (acteurs externes intervenant dans le champ d'activité)			X
Normes de sécurité			X
Circuits d'information, procédures et habilitations			X

.../...

.../...

CONNAISSANCES	Connaissance de base	Connaissance approfondie	Maîtrise
Cadre législatif, réglementaire et juridique dans son domaine d'activité			X
Base de données et logiciels dédiés		X	
Gamme de produits et services	X		
CONNAISSANCES MÉTIER			
Règles de déontologie et règles d'entreprise			X
Contexte social et accords d'entreprise			X
Dans les domaines informatiques, engagements, financiers, comptables			X
Méthodes et outils statistiques		X	
Mécanismes financiers		X	
Techniques d'analyse financière		X	
Techniques d'audit		X	
Techniques de conduite de projet		X	

COMPÉTENCES TRANSVERSES	Niveaux attendus dans le cadre de sa propre activité
COMPÉTENCES TRANSVERSES	
Sens du résultat	A la volonté permanente de dépasser ses objectifs
Organisation et coordination	Planifie son activité en intégrant les contributions d'autrui et détermine le cas échéant les missions de chacun
Analyse et synthèse	Transpose les acquis de ses analyses à d'autres situations
Adaptabilité	Crée les conditions permettant aux autres de s'adapter aux changements
Sens de l'innovation	Trouve des solutions nouvelles et opérationnelles
Force de persuasion	Développe un argumentaire ciblé en fonction de ses interlocuteurs
Communication	Utilise des modes de communication variés et adaptés selon ses interlocuteurs
Compréhension des autres	Favorise l'expression des autres
Développement des compétences	Crée et organise les conditions favorisant le développement des compétences
Coopération et esprit d'équipe	Suscite et favorise les échanges

FORMATION
Formation initiale souhaitée : Baccalauréat +5 années universitaires ou expérience équivalente
Formation professionnelle interne

3. LE POINT DE VUE DE L'OBSERVATOIRE DES MÉTIERS, DES QUALIFICATIONS ET DE L'ÉGALITÉ PROFESSIONNELLE ENTRE LES FEMMES ET LES HOMMES DANS LA BANQUE

L'Observatoire des métiers, des qualifications et de l'égalité professionnelle entre les femmes et les hommes dans la banque a déterminé plusieurs types de connaissances et de savoir-faire nécessaires dans l'exercice du métier d'auditeur dans une banque.

Les connaissances générales des collaborateurs d'une banque

- Connaissance des métiers bancaires, des produits et services.
- Maîtrise des risques liés aux opérations bancaires (marché, contrepartie, liquidité, taux, opérationnel, etc.).
- Connaissances des normes de l'établissement.
- Connaissance des problématiques et des enjeux propres à l'entreprise.
- Connaissance des processus bancaires, des gammes de produits, des services applicatifs et des circuits de validation.

Les connaissances spécifiques des métiers du contrôle

- Connaissance des normes professionnelles liées à la pratique de l'audit interne (IFACI, IIA...).
- Connaissance des problématiques de lutte anti-blanchiment.
- Connaissances en comptabilité, fiscalité, juridique.
- Expertise sur des sujets de modélisation/mesure du risque.
- Maîtrise de langues étrangères (anglais courant *a minima*).
- Maîtrise des outils informatiques.
- Maîtrise des textes réglementaires en vigueur (CRBF 97-02 modifié relatif au contrôle interne).
- Modalités de mise en place de contrôles.
- Réglementation bancaire.

Les savoir-faire des métiers du contrôle

- Analyser les informations.
- Assurer le rôle d'interface avec les autorités bancaires.
- Assurer un rôle d'alerte à tous les niveaux hiérarchiques.
- Communiquer des règles de fonctionnement.
- Conduire des projets.
- Conseiller des actions pour améliorer les process.
- Contrôler les droits d'accès aux informations financières.
- Coordonner des chantiers transversaux.
- Coordonner la circulation des informations entre les différents services de l'entreprise.
- Coordonner les activités liées à la gestion des risques.
- Coordonner les opérations de communication et de sensibilisation en matière de risque.
- Développer et garantir la cohérence des méthodologies et des outils de mesure des risques.
- Élaborer des mesures correctrices, partagées avec les audités.
- Élaborer des méthodes d'évaluation
- Être force de proposition dans l'évaluation des risques de l'entreprise.
- Évaluer les processus et fonctions grâce à une bonne vision transversale de l'organisation.
- Identifier et évaluer les risques.
- Identifier l'origine des anomalies éventuelles.
- Maîtriser l'analyse et la rédaction juridique.
- Mener des études préalables à la mise en place de projets.
- Mettre en œuvre le système d'assistance et d'approbation préalable à la diffusion des procédures.
- Mettre en œuvre les moyens nécessaires afin que les salariés soient formés à la conformité.
- Mettre en place les actions nécessaires à l'amélioration continue du dispositif interne.
- Piloter les missions de surveillance et de maîtrise des risques.
- Proposer et mettre en place des règles et des procédures.
- Rapporter aux autorités compétentes
- Réaliser des missions de contrôle.
- Réaliser un reporting exhaustif et fiable des risques.
- Rédiger et diffuser des actions correctives.
- Rédiger les rapports des missions de contrôle.
- Réunir et présenter les éléments utiles à la prise de décision de la Direction générale.
- Savoir imposer son analyse d'une situation à risque avec fermeté et objectivité.
- Suivre et mettre à jour le dispositif de maîtrise des risques.

.../...

.../...

- Tenir les délais procéduraux.
- Travailler en coordination avec les autres entités.
- Travailler en réseau.
- Veiller à ce que les risques pris se situent à un niveau acceptable et cohérent avec les objectifs de rentabilité de la banque.
- Veiller à la bonne application des règles et procédures internes.
- Vérifier la bonne diffusion des procédures au sein des équipes.

Les savoir-faire relationnels des métiers du contrôle

- L'adaptabilité.
- L'aisance dans la prise de parole en public.
- L'aisance relationnelle.
- L'animation d'équipe (manager).
- L'aptitude à la communication.
- L'autonomie.
- La capacité à argumenter.
- La capacité à convaincre.
- La capacité à travailler en équipe.
- La capacité d'analyse.
- La capacité d'assimilation rapide de problématiques variées.
- La capacité d'écoute.
- La capacité de conceptualisation.
- La capacité pédagogique.
- L'esprit critique.
- L'esprit d'analyse et de synthèse.
- La faculté d'alerte.
- L'organisation.
- L'ouverture d'esprit.
- Le pragmatisme.
- La prise de décision (manager).
- Les qualités rédactionnelles.
- Les qualités relationnelles.
- La rigueur.

4. L'ENQUÊTE DU CBOK

L'enquête du CBOK a révélé les compétences comportementales attendues des professionnels de l'audit interne.

Compétences comportementales des professionnels de l'audit interne

- Le leadership.
- L'aptitude à générer du changement.
- La qualité de persuasion.
- La sensibilité au gouvernement d'entreprise et à l'éthique.
- La facilitation.
- L'aptitude relationnelle.
- La gestion du personnel.
- La capacité à travailler avec tous les niveaux du management.
- L'aptitude à créer un esprit d'équipe.
- La confidentialité.
- Le sens de la communication.
- Le jugement.
- L'objectivité.
- L'autonomie.
- La capacité à avoir un esprit d'équipe.

5. NOS OBSERVATIONS

Nos observations montrent que la dimension comportementale devient la compétence numéro 1 pour un auditeur interne ou un contrôleur permanent. En effet, plus que jamais, leur travail ne se limite pas à faire des constats mais à conduire le changement.

Conduire le changement n'est pas chose facile, et il n'est pas rare de constater que peu d'auditeurs internes et de contrôleurs permanents sont à l'aise dans le traitement des résistances à celui-ci, et notamment dans l'acculturation des personnes concernées à la nécessité de maîtrise des opérations. Pourtant, la conduite du changement est la partie la plus intéressante car elle correspond à la finalité du contrôle. Il ne s'agit pas simplement de constater et proposer, mais de surtout faire progresser durablement, en acculturant peu à peu l'organisation au contrôle.

LA COMMUNICATION VERBALE ET NON VERBALE

Parce qu'ils sont en relation permanente avec de nombreux interlocuteurs, l'auditeur interne et le contrôleur permanent doivent maîtriser l'art de la communication verbale et non verbale. Dans toute communication, les phrases et les mots sont importants, mais la signification des mots est donnée par le non-verbal et le ton. En effet, le non-verbal et le ton traduisent nos émotions et nos pensées, ce qui est très important en situation d'entretien pour un auditeur interne ou un contrôleur permanent pour comprendre réellement son interlocuteur.

Dans une communication, ces trois critères ont une importance indéniable :

- Le non-verbal : 55 %.
- Le ton : 35 %.
- Les mots : 10 % (seulement).

Les indices du non-verbal se composent de la voix, de la position du corps, de la respiration, du visage, des gestes et du langage.

Tableau 10.2 – La voix

La tonalité	Le rythme	Le volume
Aiguë	Saccadé	Fort
Normale	Lent	Bas
Grave	Rapide	Peu audible

Tableau 10.3 – La position du corps

Le buste	L'ensemble du corps
En avant	Rigide
Droit	En mouvement
En arrière	Souple

Tableau 10.4 – La respiration

Amplitude	Sonorité	Rythme
Profonde	Bruyante	Saccadé
Faible	Inaudible	Rapide
		Lent

Tableau 10.5 – Le visage

Coloration de la peau	Paupières	Yeux	Expression
Claire	Fixes	Fixes	Souriante
Rosée	Clignotantes	Mobiles	Ouverte
Sueurs			Fermée

Tableau 10.6 – Les gestes

Mains ou doigts	Tête	Bras et jambes
Fixes	Fixe	Fixes
Mobiles	Mobile	Mobiles
Agités		Agités

Tableau 10.7 – Le langage

Phrases	Silences
Longues	Rares
Courtes	Absents
Ponctuées	Longs
Saccadées	Courts

Comment faire concrètement ?

- Repérer les indices du non-verbal.
- En tenir compte dans sa communication.

EN PRATIQUE

Comme dit le sage : « On ne peut pas ne pas communiquer. » Sigmund Freud ajoutait : « Ce que les mots ne disent, les mains le disent. »

Pour favoriser la relation avec un interlocuteur, adoptez la même posture physique que lui.

BONNES PRATIQUES

LA PROGRAMMATION NEUROLINGUISTIQUE (PNL)

Cette méthode est constituée d'un ensemble coordonné de connaissances et de pratiques dans le domaine de la psychologie, fondées sur une démarche pragmatique de modélisation en ce qui concerne la communication et le changement. Elle a été élaborée par Richard Bandler et John Grinder dans les années 1970, aux États-Unis. Cette méthode est fondée sur l'observation et peut être utilisée à profit par l'auditeur et le contrôleur permanent. Elle propose un modèle reproductible de communication qui vise à établir une synchronisation entre un individu et les filtres de son interlocuteur. Un des postulats de base est que chaque personne utilise une catégorie de filtre préférée pour percevoir son environnement. Le repérage de ces catégories s'effectue à l'aide de grilles de lecture de la forme de la communication plutôt que du fond, c'est-à-dire de ce qui est exprimé. De même, l'observation d'une personne montre qu'elle utilise des schémas répétitifs pour la motivation, la prise de décision, l'apprentissage, la mémorisation et la créativité.

En ce qui concerne l'audit interne et le contrôle permanent, cette démarche est très utile à l'oral en situation de communication en face-à-face ou devant un groupe et également à l'écrit dans le cadre des rapports par exemple.

Nous renvoyons le lecteur qui souhaiterait approfondir le sujet à l'ouvrage *Animer une équipe projet avec succès*, Henri-Pierre Maders, Éditions Eyrolles, 2012.

Comment utiliser la programmation neurolinguistique ?

Commencer par identifier la structure de la communication du (des) destinataire(s) de l'information puis adapter ses messages en conséquence.

- Les critères : équivalence complexe (une chose est égale à une autre chose)/cause/effet (une chose en entraîne une autre).
- La direction de l'attention : soi (être centré sur soi-même, parler de soi)/autres (être tourné vers les autres, écouter, poser des questions).
- Le système de représentation : visuel (voir le côté visuel d'une situation et utiliser des mots visuels)/auditif (être sensible aux paroles, aux sons, parler et utiliser des mots auditifs)/kinesthésique (ressentir les émotions, l'ambiance et utiliser des mots propres aux émotions).
- Les catégories de tri : personnes (focaliser sur les personnes)/activités (focaliser sur les activités)/lieux (focaliser sur les lieux)/choses (focaliser sur les choses)/informations (focaliser sur les informations).
- La taille de découpage : informations globales (utiliser des informations de grande taille)/informations spécifiques (utiliser des informations de petite taille).

.../...

.../...

- Le filtre de relation : similitude (porter son attention sur ce qui est identique, ce qu'on connaît)/différence (porter son attention sur ce qui est différent, être attiré par le changement, la nouveauté).
- Le cadre de référence : référence interne (évaluer par rapport à soi-même)/référence externe (évaluer par rapport au point de vue d'autres personnes, de normes ou de standards).
- Le processus de relation : accord (être d'accord avec le point de vue de l'autre, voir ce qui va bien, rechercher l'harmonie)/comparaison (comparer le point de vue de l'autre par rapport à une échelle ou une norme)/désaccord (être en désaccord avec le point de vue de l'autre (polarité inverse), donner des contre-exemples (oui, mais...), voir ce qui ne va pas, rechercher l'opposition, le conflit).
- Le filtre d'orientation : aller vers (agir pour aller vers un but, un objectif, pour obtenir quelque chose)/s'éloigner de (agir pour s'éloigner de quelque chose, être loin de cette chose, ne pas rencontrer telle ou telle situation ou régler un problème).
- Les opérateurs modaux : possibilité (penser, agir, se motiver en termes de choix, d'options, d'alternatives)/nécessité (agir par sens du devoir, ou en fonction d'obligations ou de règles).
- L'organisation de l'action : option (faire plusieurs choses en même temps, avoir un comportement simultané)/procédure (faire une chose après l'autre, planifier ses activités, avoir un comportement séquentiel).
- La modalité d'engagement : actif (initialiser ses actions, s'en sentir responsable, avoir besoin de peu d'informations et de réflexion pour prendre la décision d'agir)/passif (suivre le mouvement, ne pas initialiser ses actions, ne pas s'en sentir responsable, avoir besoin de beaucoup d'informations et de réflexion pour prendre la décision d'agir).
- L'orientation du temps : passé (utiliser des verbes conjugués au passé, expliquer ses actions présentes et futures par référence au passé, aux traditions)/présent (utiliser des verbes conjugués au présent, agir sans tenir compte du passé et du futur)/futur (utiliser des verbes conjugués au futur, agir au présent pour des conséquences futures).
- Le schéma d'installation des convictions : intensité (une fois)/répétition (plusieurs fois)/fréquence (un certain nombre de fois dans une durée)/intervalle (la durée entre deux événements)/séquence (un certain ordre).

EN PRATIQUE

La structure de la communication vous en apprendra souvent beaucoup plus sur vos interlocuteurs que le contenu de leurs messages.

Dans un même contexte, une personne a tendance à adopter le même comportement. À ce titre, toute personne est prévisible...

BONNES PRATIQUES

L'ÉCOUTE ACTIVE

L'écoute active se compose du verbal et du non-verbal. Avec une écoute active, il est possible à l'auditeur interne et au contrôleur permanent d'obtenir quatre choses de la personne interviewée : de l'information, de la confiance, du confort, de la volonté à continuer à communiquer.

Quatre règles à respecter pour faire une bonne écoute active

Règle 1 – Utilisation du non-verbal

- Hocher la tête.
- Regarder la personne dans les yeux.
- Se rapprocher de la personne.
- Sourire...

Règle 2 – Questionnement

- Utiliser des questions ouvertes pour recueillir de l'information.
- Utiliser des questions fermées pour rechercher un fait précis, un chiffre, un accord, une opinion franche.
- Utiliser des questions de vérification pour s'assurer que l'information reçue ou donnée a été bien comprise.

Règle 3 – Écoute d'approfondissement

- Faire préciser des informations.

Règle 4 – Reformulation

- Utiliser la reformulation pour vérifier que l'on a compris ce que l'interlocuteur a dit.

La reformulation présente plusieurs avantages pour la personne que l'on interview :

- Relance : elle l'entraîne à poursuivre son message, à en dire plus.
- Clarification : elle lui permet de clarifier sa pensée par des synthèses successives. Elle le débarrasse du superflu pour ne retenir que l'essentiel.
- Réajustement : elle lui permet de repréciser sa pensée si ce qu'elle a exprimé ne correspond pas tout à fait à ce qu'elle a voulu dire.

- Approfondissement : elle l'incite à changer progressivement de niveau pour atteindre le noyau du message important pour elle.
- Compréhension : elle suscite le sentiment d'être compris par son interlocuteur.
- Apaisement : elle réduit la tension psychologique éventuelle et l'amène à une certaine détente.

La reformulation présente également plusieurs avantages pour la personne qui conduit l'entretien :

- Écoute : elle la conduit à une plus grande concentration sur la logique de l'autre.
- Exploration : elle lui permet un balayage plus exhaustif du terrain de l'autre.
- Neutralité : elle l'incite à ne formuler ni avis, ni jugement, ni interprétation.
- Mesure : elle est un moyen de vérifier l'écart entre ce qu'elle a compris et ce que l'autre a voulu dire.
- Initiative : elle lui donne, malgré les apparences, la maîtrise du processus de communication, et donc, l'initiative de son évolution.
- Précision : elle lui permet d'obtenir de l'autre un certain nombre de précisions sans avoir recours aux questions.
- Accompagnement : elle l'amène à fonctionner au rythme de l'autre.

EN PRATIQUE

Les questions commençant par « pourquoi ? » peuvent déranger la personne interviewée car ce type de question renvoie à des valeurs et des croyances.

Les questions rhétoriques de type : *« Cette recommandation est bonne, n'est-ce pas ? »* sont de fausses questions car la personne interviewée se sent obligée malgré elle de dire « oui ». Dans ce cas, la personne peut se sentir manipulée.

Dans le cas où une situation difficile se produit, il est important de ne pas l'ignorer mais au contraire de la nommer (Exemples de situations : l'interlocuteur montre son hostilité, son anxiété, ses doutes ou ses craintes ; l'interlocuteur ne réagit pas, reste silencieux ou indifférent ; l'interlocuteur est trop fatigué pour continuer à suivre le déroulement de la conversation ; l'interlocuteur est surpris par ces propos). Deux possibilités s'offrent alors à vous.

1. Ignorer l'existence des sentiments et des émotions de l'interlocuteur :
- Reportez la conversation à plus tard.
- Arrêtez-vous un moment pour laisser l'interlocuteur se remettre de ses émotions.
- Essayez d'aborder le problème sous un nouvel angle.
- Reconnaissez que vous devez faire un compromis.

BONNES PRATIQUES

2. Nommer précisément ce qui préoccupe l'interlocuteur :
- Nommez le sentiment.
- Offrez une solution à l'interlocuteur (exemples de phrases : « J'ai l'impression que vous êtes préoccupé par ce que je viens de dire. Souhaitez-vous que l'on approfondisse ce point ? » « Il me semble que vous êtes contrarié. Peut-être devrions-nous en parler ? » « Ce sujet semble vous avoir surpris. Voulez-vous prendre le temps d'y réfléchir un peu ? »).

▶ Exemples de questions d'écoute active

Questions ouvertes : « Comment… ? » ; « Pourquoi… ? » ; « Que pensez-vous… ? » ; « Je souhaiterais que vous me parliez de… » ; « Qu'est-ce que… ? » ; « Pourriez-vous… ? »
Questions fermées : « Depuis combien de temps… ? » ; « Combien en avez-vous… ? » ; « Êtes-vous d'accord… ? »
Questions de vérification : « Résumons… ? »
Écoute d'approfondissement : « Que voulez-vous dire par cela ? » ; « Vous évoquiez tout à l'heure… ? » ; « Pourriez-vous m'en dire davantage ? »
Reformulations : « Voulez-vous dire que… » ; « En d'autres mots… » ; « Laissez-moi résumer pour voir si j'ai compris… » ; « Si je vous suis… »

L'ENTRETIEN

Dans une mission d'audit interne ou de contrôle permanent, l'entretien a pour objectifs d'obtenir de l'information (investigation), de diffuser de l'information (annonce), de vendre une idée et de la faire valider (persuasion).

L'entretien est organisé uniquement en vue d'un objectif à atteindre : généralement prendre connaissance d'un sujet (en rapport avec la mission) ou d'une opinion. Ce n'est ni un interrogatoire, ni une conversation. L'entretien constitue un outil de base de la panoplie de l'auditeur interne et du contrôleur permanent. Il n'est pas obligatoire par nature mais pratiquement incontournable à un moment ou un autre dans une mission d'audit. La réalisation d'entretien exige un ensemble de règles à respecter lors de sa préparation et de son déroulement.

Trois règles pour mener un bon entretien

Règle 1 – Préparation

- Définir le sujet de l'entretien.
- Lister les points à aborder.
- Établir un guide d'entretien à partir des points ordonnés et hiérarchisés.
- Choisir le bon interlocuteur : celui qui détient l'information, qui a un pouvoir de décision ou d'influence.
- Prendre rendez-vous avec l'interlocuteur en lui précisant l'objet, la durée et le lieu de l'entretien, et vos coordonnées.

Règle 2 – Déroulement

- Choisir le meilleur moment pour ne pas trop gêner la personne dans son travail.
- Réaliser l'interview de préférence sur le lieu de travail de l'interviewé.
- Ne pas dépasser 2 heures.
- Se présenter et repréciser l'objet de l'entretien.
- Inviter l'interlocuteur à se présenter et à préciser sa fonction.
- Suivre le guide d'entretien en notant tout ce qui est dit par l'interlocuteur.
- Reformuler les informations qui ne paraissent pas claires ou qui doivent être détaillées.
- Faire une synthèse rapide à la fin de l'entretien pour s'assurer de n'avoir rien oublié ou de ne pas avoir mal interprété une information.
- Clôturer l'entretien en remerciant l'interlocuteur.

Règle 3 – Conclusion

- Rédiger un compte rendu, en veillant à être factuel.
- Faire valider le compte rendu par la personne interviewée.
- Valider les informations collectées à l'aide d'autres sources d'information.

EN PRATIQUE

Le questionnement d'une personne est l'un des exercices les plus difficiles qui soit et nécessite beaucoup de bienveillance et de respect :

- Restez ouvert, l'interlocuteur peut fournir des informations importantes qu'on ne lui a pas forcément demandées, le guide d'entretien n'est pas un cadre rigide.
- Soyez actif pendant l'entretien, analysez les informations données pour pouvoir orienter au mieux les questions tout au long de l'entretien.
- Gardez les questions commençant par « Pourquoi ? » qui peuvent conduire à des points de vue, des opinions, des interprétations pour la deuxième partie de l'entretien.

Préparez vos entretiens. Planifiez leur réalisation et pilotez leur déroulement.

Rédigez des comptes rendus d'entretien et faites les valider par les personnes interviewées.

BONNES PRATIQUES

▶ Exemple de règles relatives aux entretiens, société industrielle

Règles relatives à la préparation de l'entretien

- Définir au préalable le sujet d'interview.
- Connaître son sujet en s'informant sur la personne et sa structure.
- Collecter les éléments clés de son activité.
- Élaborer les questions.
- Prévoir le nombre de personnes requis (une ou deux personnes au maximum).
- Prendre rendez-vous.

L'entretien doit être :

- D'une durée moyenne d'une heure (maximum deux heures) ; il doit être soigneusement préparé, adapté à l'interlocuteur et mené principalement avec des questions ouvertes.
- Organisé et réalisé en respectant la voie hiérarchique. Cette information préalable peut se faire au cours de la réunion d'ouverture par un rappel de la liste des personnes à interviewer.
- Entamé par un rappel de la mission et de ses objectifs.
- Axé sur les difficultés, les points faibles, les anomalies rencontrées avant tout autre chose.
- Mené en conservant l'approche système, en vertu du principe que l'auditeur ne s'intéresse pas aux hommes.
- Mené dans une logique d'écoute et une technique de « facilitateur ». L'auditeur doit éviter d'être celui qui parle le plus. L'entretien est un moment privilégié de la relation entre l'auditeur et l'audité qui peut détendre une situation, favoriser une confidence, etc.
- Mené en considérant son interlocuteur comme un égal. Non pas égal au sens hiérarchique du terme, mais un égal dans la conduite du dialogue.
- Terminé par une conclusion qui résume la conversation, valide les principales observations relevées et « maintient la porte ouverte » pour des questions ou des demandes de précisions ultérieures.
- Organisé de façon à permettre l'acceptation du silence, la reformulation et la prise de note.
- Consigné dans un compte rendu dès sa fin ou au plus tard 24 heures après les notes prises.

LA CONDUITE DE RÉUNION

Dans le cadre d'une mission d'audit interne ou de contrôle permanent, la réunion est un outil de communication souvent utilisé.

La réunion permet de :

- favoriser la circulation de l'information (lancement de la mission, point d'avancement ou d'approfondissement, restitution…) ;
- travailler en groupe sur la résolution d'un problème, la construction d'une solution ;
- prendre des décisions (point intermédiaire, validation des recommandations, adoption de plans d'action).

Trois règles pour faire une bonne réunion

Règle 1 – Préparation

- Définir avec précision le « TOP » de la réunion : Thème (sujet de la réunion) ; Objectif (but à atteindre dans la réunion) ; Plan (points à aborder pour atteindre l'objectif).
- Déterminer la liste des participants, le lieu et l'heure de la réunion.
- Adresser des convocations aux intéressés.
- Préparer les aspects logistiques (tableau de papier, rétroprojecteur, micro-ordinateur, projecteur…).

Règle 2 – Animation

- Commencer à l'heure prévue.
- Noter sur le tableau de papier, le thème, l'objectif, le plan, la durée de la réunion.
- Faciliter la progression du travail.
- Faciliter les interactions entre les personnes et la participation.
- Rechercher un équilibre du temps de parole animateur/participants.
- Recentrer en cas de hors sujet.
- Pratiquer les reformulations et les synthèses intermédiaires.
- Rappeler régulièrement les objectifs de la réunion.
- Conclure la réunion en résumant les points clés et préciser la suite à donner.

Règle 3 – Suivi

- Effectuer une mini-analyse de la réunion : respect du TOP de départ (Thème, Objectif, Plan), choix des participants.

.../...

BONNES PRATIQUES

.../...

- Rédiger le compte rendu (animateur ou secrétaire s'il y en a un) : sujets et objectifs de la réunion, participants, décisions prises, points clés de la prochaine réunion.
- Diffuser rapidement le compte rendu. (Il est possible dans certains cas de rédiger le compte rendu en cours de réunion. Cette façon de faire permet aux participants de quitter la réunion avec le compte rendu validé par l'ensemble des personnes présentes.)
- Veiller au respect de la mise en application effective des décisions prises et à la réception des informations demandées au cours de la réunion.

EN PRATIQUE

- Tenez la réunion dans une pièce calme.
- Faites taire les téléphones portables et, surtout, ceux permettant de recevoir et d'envoyer des e-mails…
- Pensez à faire des interruptions lorsque la réunion dépasse 2 heures.
- En situation d'animateur, ne prenez pas position et laissez plutôt les participants s'exprimer librement, adoptez une attitude d'écoute active, reformulez les idées, synthétisez les points de vue, questionnez, faites préciser, traduisez les informations implicites…
- Travaillez toujours avec l'ensemble du groupe et non avec chaque participant successivement.
- Définissez un code de conduite.
- Définissez une fréquence adaptée et un calendrier.
- Placez les réunions en début ou en fin de demi-journée.
- Au cas où des déplacements sont nécessaires, faites des réunions d'une durée d'une demi-journée avec une pause en milieu de séance.
- Désignez une personne pour l'organisation matérielle (réservation de la salle, disponibilité des moyens).
- Communiquez les comptes rendus aux membres du groupe dans la semaine qui suit la réunion.
- Déterminez un quorum pour les réunions de validation.
- Désignez un animateur et un secrétaire en début de séance.
- Reprenez le compte rendu de la réunion précédente en début de réunion.
- Distribuez les travaux à faire en fin de réunion.
- Interdisez les agressions personnelles.
- Quantifiez les points débattus pour limiter la part de la subjectivité.
- Tenez compte de tous les points de vue et de toutes les opinions.
- Ne refusez aucune idée et examinez tous ses avantages et inconvénients.
- Faites prendre les décisions au consensus, et, en cas de désaccord persistant, malgré les explications, utilisez les techniques de rationalisation des choix.
- Interdisez pendant les réunions : la cigarette, le téléphone, la lecture des e-mails…

LA PRÉSENTATION ORALE

Les règles de présentation orale constituent un ensemble de conseils permettant de se sentir à l'aise et de réussir une communication orale face à un auditoire qui peut être nombreux ou plus ou moins acquis et parfois intimidant.

Quatre règles pour faire un bon exposé oral

Règle 1 – Préparation de l'exposé

- Identifier l'auditoire, ses attentes, son langage, sa disposition d'esprit.
- Déterminer l'objectif de la présentation.
- Recenser toutes les informations à transmettre.
- Les ordonner.
- Préparer les supports de présentation.

Règle 2 – Introduction du propos

- Présenter un plan structuré (construit comme une démonstration rigoureuse) et équilibré (deux ou trois parties principales ayant chacune autant de sous-parties).
- Mettre le plan en évidence en l'annonçant en fin d'introduction et en le rappelant à chaque changement de partie ou sous-partie.
- Accrocher l'auditoire dès le début de la présentation par une information appropriée.

Règle 3 – Exposé du sujet

- Surveiller la qualité de l'expression orale (le ton, le rythme...).
- Changer de position physique.
- Contrôler son exposé (utiliser des exemples, des illustrations, de l'humour...).
- Rester dans le contenu (ne pas se noyer dans les détails pour éviter les risques de questions techniques précises).
- Faire preuve d'esprit critique constructif (avantages et inconvénients) et de réalisme.
- S'appuyer sur des données chiffrées « parlantes » et sur les questions fondamentales (utilisation ? coût ?...).

Règle 4 – Conclusion

- Faire une synthèse de la présentation.
- Annoncer la suite des événements.
- Remercier l'auditoire.

BONNES PRATIQUES

EN PRATIQUE

Étayez la présentation de supports écrits et notamment de graphes/tableaux de synthèse (avantages, inconvénients, coûts/gains...) pour ne pas lasser l'auditoire.

Pensez à réserver du temps à la fin de la présentation pour les questions/réponses.

Évitez toute ambiguïté sur les points importants.

Reformulez régulièrement.

Exprimez-vous avec chaleur et conviction pour convaincre votre auditoire.

Évitez de lire vos notes, utilisez plutôt un schéma heuristique comme guide.

LES CRITÈRES DE LISIBILITÉ

Si la langue française comporte plus de 75 000 mots, un adulte ayant fait des études supérieures connaît environ 10 000 mots et en utilise 5 000 à l'écrit et 1 500 à l'oral dans la vie de tous les jours… Par ailleurs, la langue française est ainsi faite que, dès qu'un mot est supérieur à deux syllabes, la probabilité qu'il soit difficile à comprendre est forte. Comment s'étonner alors que beaucoup de documents professionnels soient hermétiques aux non-initiés ? C'est la raison pour laquelle l'auditeur interne et le contrôleur permanent doivent soigner tout particulièrement cet aspect. Les critères de lisibilité appelés aussi les indices de brouillard permettent de qualifier un texte sous l'angle de sa facilité de compréhension et de mémorisation.

Pour déterminer cette « lisibilité », on utilise les formules suivantes :

Indice de compréhension : Nombre de verbes/Nombre de phrases < 1,5

Indice de « brouillard » : (X + Y) × 0,4 < 12

Avec :

- X = % de mots > 3 syllabes (mots difficiles) ;
- Y = longueur moyenne des phrases en nombre de mots.

Protocole à respecter pour tenir compte des critères de lisibilité dans ses écrits

- Rédiger une première version du texte.
- Calculer les indices de brouillard.
- En fonction des résultats, rédiger une version corrigée avec :
  - des phrases plus courtes ;
  - des mots plus simples ;
  - un lexique (« étude d'opportunité » ; « étude de faisabilité » ; « cahier des charges » ; « maître d'œuvre » ; « maître d'ouvrage » ; COPIL ; « site pilote »…) ;
  - des schémas.

EN PRATIQUE

Faites attention aux mots techniques et encore plus aux mots anglais : ils ne sont compréhensibles que par les initiés. Et cela est vrai pour tous les métiers.

Identifiez le lexique des mots techniques à utiliser avec chaque catégorie d'experts et le tronc commun à utiliser avec tout le monde.

Dans les procédures et les modes opératoires, n'utilisez qu'une seule instruction par phrase et accompagnez le texte de schémas et de graphiques.

BONNES PRATIQUES

LES SUPPORTS DE PRÉSENTATION

Les supports de présentation sont très utilisés au cours des missions d'audit interne et de contrôle permanent dans le cadre des nombreuses réunions dans lesquelles il faut présenter des faits, des diagrammes de circulation, des données montrant des enjeux et/ou des évolutions, expliquer des imbrications de causes et proposer des recommandations.

Deux règles pour concevoir des supports efficaces

Règle 1 – Analyse de la pertinence de chaque support

- Le support est-il cohérent avec le TOP de la réunion ?
- Apporte-t-il un plus à l'animation de la réunion ? Une information complémentaire ? Des chiffres clés ? Un exemple caractéristique ? Un élément de contradiction ?…
- N'est-il pas contradictoire avec un autre ?

Règle 2 – Conception des supports

- Noter les idées à faire partager avec l'auditoire.
- Écrire gros, de préférence en lettres capitales : le support doit pouvoir être lu de loin.
- Se limiter à une idée forte.
- Utiliser des phrases courtes et des mots simples (cf. p. 247).
- Alterner graphiques et textes pour alléger la lecture.
- Utiliser des mots-clés : tout ne doit pas être noté sur le support, garder des idées, des arguments pour la présentation orale.

EN PRATIQUE

Utilisez des méthodes de classement des idées de type ESPRIT ou Minto.

Ne faites figurer qu'une idée-force par support.

Limitez le nombre total de supports.

Rappelez par une symbolique sur chaque support où vous en êtes dans votre présentation.

Distribuez les documents en début de séance afin que l'auditoire soit en mesure de compléter les documents par des notes personnelles. Et tant pis si vous constatez que certains sont en train de lire une autre page que celle que vous projetez, au moins, ils sont toujours dans le sujet !

LES NOTES PROFESSIONNELLES

La communication écrite doit, pour être lue et comprise, suivre des règles d'écriture particulières, propres au monde professionnel. Communiquer par écrit, c'est non seulement informer mais aussi former, animer, faire mémoriser, motiver…

Il faut savoir que sur 100 personnes placées devant un texte bien rédigé :

- 90 personnes ne lisent que le titre ;
- 75 personnes lisent le titre et l'introduction ;
- 40 personnes lisent le texte jusqu'à la fin du premier paragraphe ;
- 20 personnes lisent la totalité en diagonale ;
- 5 personnes seulement lisent le texte intégralement.

Et cela ne veut pas dire que les cinq personnes en question ont compris le texte, et encore moins l'ont mémorisé !

Deux règles pour rédiger une note lisible

Règle 1 – Rédiger d'une façon concise

- Alléger au maximum le corps du rapport pour être sûr qu'il soit lu.
- Privilégier les analyses, les conclusions et les préconisations, aux constats.
- Présenter en annexe les informations secondaires (détails, chiffres, calculs intermédiaires) pour permettre au lecteur de s'y référer s'il le souhaite.

Règle 2 – Rédiger d'une façon claire

- Aérer la présentation.
- Utiliser des phrases courtes, simples.
- Structurer les idées, trouver des titres de paragraphes parlants.
- Au-delà de 5 pages, insérer un sommaire.
- Illustrer les idées fortes par des exemples, des graphes, des schémas…

EN PRATIQUE

Proposez plusieurs niveaux de lecture (cf. comme dans la presse : titre parlant, chapeau, texte, encarts).

Utilisez de préférence des verbes actifs et évitez les participes présents afin de rendre le texte dynamique. Utiliser le présent permet d'ancrer le rapport dans la réalité et implique plus le lecteur.

Rédigez une synthèse du rapport et la placer en début de rapport.

BONNES PRATIQUES

Copyright © 2014 Eyrolles.

LA MÉTHODE « E.S.P.R.I.T. »

La méthode « E.S.P.R.I.T. », créée par Louis Timbal-Duclaux, constitue une aide précieuse dans la rédaction de livrables à caractère technique tel qu'un document technique. En effet, cette méthode, par un ordonnancement des informations, suscite l'intérêt du lecteur. Cette méthode n'est pas une technique d'influence, mais une technique qui permet au lecteur de comprendre le point de vue du rédacteur et de se positionner au regard de celui-ci.

Protocole pour utiliser la méthode « E.S.P.R.I.T. »

- Identifier le destinataire du livrable.
- Rédiger le livrable en utilisant un plan vendeur de type « E.S.P.R.I.T. ».
- Tester le texte avant diffusion.

E : « Entrée en matière » (1 paragraphe)

- Rappel du contexte et de l'objectif.
- Objectif : cadrer le sujet.

S : « Situation » (1 paragraphe)

- Description de la situation.
- Objectif : mettre l'interlocuteur sur la bonne longueur d'onde.

P : « Problème » (1 page)

- Présentation des conséquences et enjeux de la situation actuelle et de son évolution prévisible.
- Objectif : neutraliser les préjugés de l'interlocuteur par la présentation de la situation présente insatisfaisante et de la situation future satisfaisante.

R : « Résolution » (3 à 4 pages)

- Recommandations pour traiter le problème.
- Objectif : présenter en quelques lignes la proposition ainsi que les points forts et les points faibles de chaque solution, puis indiquer la préférence.

…/…

.../...

I: « Information » (quelques dizaines de pages)

- Description technique de la solution.
- Objectif : prouver que techniquement, la solution est adaptée à la situation.

T: « Terminaison » (1 paragraphe)

- Conclusion.
- Objectif : Rappeler l'intérêt de la mise en œuvre de la solution.

EN PRATIQUE

La séquence SPR peut être, dans certains cas, avantageusement remplacée par la séquence SRP, ou encore PSR, PRS ou même RSP ou RPS.

À la fin de chaque paragraphe, le lecteur doit se dire : « Oui, je suis d'accord avec ce que je lis. »

BONNES PRATIQUES

LA MÉTHODE MINTO

La méthode Minto, mise au point par Barbara Minto, constitue une aide précieuse à la présentation de supports visuels. Cette technique est très utilisée par certaines équipes de consultants. Elle peut également s'avérer très utile aux auditeurs internes et contrôleurs permanents.

Elle permet d'aider à la détermination d'un fil conducteur favorisant la démonstration et suscitant l'attention et l'adhésion d'un groupe lors de la présentation de résultats ou de conclusions.

Protocole pour utiliser la méthode Minto

- Définir avec précision la conclusion à laquelle on souhaite que le lecteur ou l'auditeur (dans le cas d'une présentation orale) arrive au terme de la lecture ou de la présentation. Cette conclusion doit se résumer à une idée maîtresse.
- Inventorier tous les arguments et toutes les informations qui seront utilisées dans le cadre du texte.
- Classer les arguments selon une logique claire.
- Définir l'argumentation logique permettant d'y arriver. Utiliser pour ce faire des relations entre les idées :
  - relation de cause à effet ;
  - relation temporelle : passé/présent/futur ;
  - relation global/détail ;
  - avantages/inconvénients.
- Rédiger les titres : ils doivent raconter une histoire.
- Sélectionner des informations caractéristiques permettant d'illustrer chaque titre de l'histoire.

EN PRATIQUE

Sans « téléphoner » à l'avance la conclusion, faites en sorte que le lecteur soit suffisamment guidé jusqu'à la conclusion.

Ne cherchez pas à faire passer plus d'une idée par page. Illustrez ces idées.

Évitez les présentations trop longues : 2 à 5 minutes par page, soit 12 à 30 pour une heure de présentation. N'oubliez pas que, plus une présentation est longue, et plus il est difficile de tenir un auditoire en haleine...

Ne cherchez pas à prouver les choses par une démonstration au sens mathématique. Cette démarche anglo-saxonne vise plutôt à illustrer par l'exemple que de prouver scientifiquement. En effet, elle sous-entend que l'émetteur du texte a fait le nécessaire en amont.

LES PROFILS CARACTÉRISTIQUES

La performance d'un groupe repose sur la qualité des personnes qui le constituent ainsi que sur leurs complémentarités. Il est donc très important pour les contrôleurs internes et les contrôleurs permanents de décrypter les rôles joués par les personnes auditées dans le cadre de missions d'audit interne ou de contrôle permanent. Les profils caractéristiques de Mérédith Belbin peuvent les y aider.

Protocole pour utiliser les profils caractéristiques dans le cadre des missions d'audit et de contrôle interne :

- Identifier les compétences et comportements des membres de l'équipe auditée ou contrôlée.
- Évaluer ces profils au regard de ses missions.

Tableau 10.8 – Présentation des huit profils caractéristiques

Profil « Organisateur »	■ Structure le projet de l'équipe en lui donnant une forme réalisable. ■ Créé des situations stables : planning, organigramme… ■ Travaille de manière efficace, systématique et avec méthode. ■ N'est pas sensible aux idées spéculatives, « farfelues », qui n'ont pas une portée directe et visible sur le travail en cours.
Profil « Président »	■ Préside l'équipe et coordonne ses efforts pour accomplir les différents objectifs et les buts externes. ■ A de l'autorité, est dominant mais sans agressivité. ■ Détermine les rôles et les limites du travail des autres, clarifie les objectifs de l'équipe et établit le planning. ■ Trie les problèmes à soumettre à l'équipe et fixe les priorités. ■ Pose les bonnes questions en début de projet. ■ Écoute, résume les sentiments de l'équipe. ■ Si une décision s'impose, la prend sans hésiter, après avoir donné la possibilité à chacun de s'exprimer.
Profil « Moteur »	■ Bouillonne d'énergie nerveuse. ■ Relève facilement les défis. ■ Donne forme aux efforts de l'équipe, fournit un apport personnel très important. ■ Cherche toujours le fil conducteur des débats et essaie d'intégrer les idées, les objectifs et les considérations d'ordre pratique en un projet unique et réalisable, qu'il cherche à traduire très rapidement en décision et en action. ■ Recherche l'action et les résultats. ■ Grâce à lui, les choses se réalisent.
Profil « Planteur »	■ Constitue pour l'équipe la source d'idées, de suggestions et de propositions originales : c'est l'homme à idées. ■ Est le plus imaginatif des membres, est le plus à même de déclencher la recherche d'une approche toute nouvelle d'un problème lorsque l'équipe s'enlise ou d'apporter un nouvel élan dans la réalisation d'une action déjà décidée.

.../...

BONNES PRATIQUES

.../...

	■ Est plus préoccupé par l'essentiel ou les points fondamentaux que par les détails. ■ Est entreprenant et sans complexe.
Profil « Explorateur »	■ Détendu, sociable, son intérêt s'éveille facilement, ses réactions tendent à être positives et enthousiastes. ■ Se rend à l'extérieur de l'équipe, rapporte de l'information, des idées. ■ Est le vendeur, le diplomate, l'officier de liaison, toujours en train d'explorer de nouvelles possibilités dans le monde extérieur. ■ Voit très vite la pertinence d'idées nouvelles. ■ Préserve l'équipe de la stagnation, l'empêche de se scléroser et de perdre le contact avec la réalité.
Profil « Rationnel »	■ Analyse sans passion et empêche l'équipe de s'engager dans un projet mal dirigé. ■ Est l'esprit le plus objectif de l'équipe. ■ À la capacité d'assimiler, interpréter et évaluer les jugements et les informations des autres membres de l'équipe. ■ Est solide et fiable, mais manque d'imagination et de spontanéité. ■ Son jugement est rarement pris à défaut
Profil « Équipier »	■ Est le communicateur interne le plus actif. ■ Constitue le ciment de l'équipe. ■ Apporte son soutien à tous les autres et se bat pour l'unité et l'harmonie de l'équipe, apaisant les frictions et les désaccords. ■ Indispensable en temps de stress ou de pression.
Profil « Perfectionniste »	■ Se préoccupe de tout ce qui pourrait éventuellement aller de travers. ■ Vérifie chaque détail. ■ Maintient un sens permanent d'urgence. ■ Cherche à tout prix à respecter les détails dans le planning. ■ Forte capacité à persévérer.

EN PRATIQUE

Ayez conscience dans vos missions d'audit interne ou de contrôle permanent de l'impact du rôle joué par chaque personne de l'équipe sur la performance du dispositif de contrôle interne :

- Les organisateurs permettent de structurer les choses.
- Les présidents cherchent à diriger.
- Les moteurs font avancer les choses.
- Les planteurs apportent des idées.
- Les explorateurs entretiennent les relations avec l'extérieur.
- Les rationnels évitent de rêver.
- Les équipiers permettent le travail en équipe.
- Les perfectionnistes permettent d'aller au niveau de détail souhaitable…

LES TYPES DE BESOIN

La satisfaction de besoins caractéristiques est recherchée par toute personne, dans la vie de tous les jours et dans le milieu professionnel. Cela explique les comportements individuels et collectifs.

Cela est vrai pour l'auditeur interne et le contrôleur permanent. Et cela est vrai également pour les membres d'une équipe concernée par une mission d'audit interne ou de contrôle permanent.

En effet, selon la pyramide des besoins d'Abraham Maslow :

- le comportement d'une personne peut s'expliquer par la recherche de la satisfaction de besoins caractéristiques ;
- le besoin le plus important pour une personne est celui que celle-ci cherche à satisfaire ici et maintenant ;
- une fois un besoin satisfait, une personne cherche à en satisfaire un autre, dans un certain ordre.

Connaître les besoins recherchés par les membres d'une équipe permet à ce titre :

- de comprendre ce qui motive chaque personne (attrait pour certaines tâches et responsabilités par exemple) ;
- d'expliquer les mécontentements, le niveau de qualité du travail, la productivité…

Protocole pour utiliser le modèle

- Identifier, à l'aide de questions anodines et pour chaque personne, ce qui la motive dans le fonctionnement de l'entité en matière de management et de travail d'équipe :
  - besoins physiologiques (salaire, primes et avantages divers…) ;
  - besoin de sécurité (carrière…) ;
  - besoin d'appartenance à un groupe (vie sociale) ;
  - besoin de reconnaissance (ego) ;
  - besoin de réalisation psychologique (quête de sens).
- Voir dans quelle mesure ces types de besoins individuels et collectifs peuvent être satisfaits, soit dans le cadre du projet d'organisation, soit dans la nature des solutions organisationnelles que le projet mettra en œuvre.

EN PRATIQUE

Ne sous-estimez jamais les besoins recherchés par les membres d'une équipe.

La motivation d'une personne et/ou d'un groupe n'est jamais acquise définitivement. En revanche, un style de management et/ou une organisation adaptée permettent le plus souvent d'apporter suffisamment de motivation.

BONNES PRATIQUES

LE MANAGEMENT SITUATIONNEL

Le management d'une équipe nécessite un management approprié sachant que :

- Le niveau de performance d'un collaborateur dépend en grande partie du style de management que son responsable hiérarchique adopte à son égard.
- Il n'y a pas de style de management idéal, mais des styles plus ou moins adaptés aux situations.
- L'utilisation par le manager du style approprié dans la bonne situation permet une optimisation des efforts produits par ce dernier et garantit la réussite pour le collaborateur. *A contrario*, l'utilisation d'un style moins approprié entraîne une consommation d'énergie supérieure pour le manager et peut aller à l'encontre de la réussite pour le collaborateur.
- Les deux facteurs qui permettent de déterminer le style de management à adopter sont le niveau de compétence et le niveau de motivation du collaborateur.

Le management situationnel de Hersey et Blanchard permet à un auditeur ou un contrôleur interne de réaliser un diagnostic rapide sur l'adéquation du style de management d'une entité.

Tableau 10.9 – Présentation des quatre styles du modèle

Le style directif	Ce style est adapté pour un équipier pas compétent et pas motivé. ■ Pas compétent, il n'a pas de savoir-faire, attend les informations de l'extérieur, ne sait pas utiliser ses connaissances de base, attend qu'on lui dise ce qui est à faire et qu'on lui montre comment le faire. ■ Pas motivé, il n'a pas envie, ne se sent pas prêt, pense que c'est aux autres de faire ce qu'on lui demande, pense que c'est inutile, sans intérêt, trop difficile, risqué, vague, flou ; il est réticent et inactif.
Le style persuasif	Ce style est adapté pour un équipier pas compétent mais motivé. ■ Pas compétent, il n'a pas de savoir-faire, attend les idées et les explications, pose des questions : comment faire ? Pourquoi faire ? ■ Motivé, il témoigne d'une bonne volonté générale, est ouvert, s'intéresse au projet mais sans être actif ni moteur, a besoin d'aide, d'encouragements et de reconnaissance.
Le style participatif	Ce style est adapté pour un équipier compétent et peu ou pas motivé. ■ Compétent, il possède un véritable savoir-faire, a des idées, émet des propositions, est centré sur ses conceptions, peut manquer d'esprit de synthèse. ■ Pas motivé, il peut manquer de confiance et ne pas vouloir assumer seul la responsabilité, souhaite un appui, sa motivation reste conditionnelle, il pose ses conditions, demande des moyens, plus de liberté et d'indépendance.
Le style délégatif	Ce style est adapté pour un équipier compétent et motivé. ■ Compétent, il possède une expertise réelle, se comporte en « pro », situe son action dans un contexte d'ensemble (équipiers, manager, entreprise), prend du recul et sait analyser son action de façon critique. ■ Motivé, il est actif, dynamique, intéressé, il communique sa motivation et son intérêt pour l'activité aux autres.

Protocole pour utiliser le modèle

- Identifier le style naturel du responsable hiérarchique du domaine audité ou contrôlé.
- Évaluer pour chaque membre de l'équipe auditée ou contrôlée et pour chacun des travaux qui leur sont confiés leurs niveaux de compétence et de motivation.
- Identifier les écarts entre le style dominant du responsable hiérarchique et les caractéristiques de chaque membre de son équipe.
- Rédiger des recommandations visant à un degré d'autonomie plus approprié pour chacun des collaborateurs en fonction de leurs critères de motivation et de compétence.

EN PRATIQUE

Le processus d'apprentissage et de motivation d'une équipe est de la responsabilité du responsable hiérarchique.

La non-adéquation entre le style naturel d'un responsable et les niveaux de motivation et de compétences de ses collaborateurs expliquent souvent les carences du dispositif de contrôle permanent d'une entité.

BONNES PRATIQUES

Tableau 10.10 Grille de repérage des niveaux de motivation et de compétence d'une personne

	A 1 Absence d'autonomie	A 2 Autonomie faible	A 3 Autonomie moyenne	A 4 Autonomie forte
Compétence	**Ne sait pas**	**Ne sait pas**	**Sait faire**	**Sait faire**
	■ Compétence faible. ■ Pas de savoir-faire. ■ Attend les informations de l'extérieur. ■ Ne sait pas utiliser ses connaissances de base. ■ Attend qu'on lui dise ce qui est à faire et qu'on lui montre comment faire.	■ Compétence faible. ■ Pas de savoir-faire. ■ Attend les idées et explications du manager. ■ Pose des questions : comment faire ? ■ Pourquoi faire ?	■ Compétence moyenne à forte. ■ Savoir-faire. ■ A des idées, des projets, des propositions. ■ Centré sur ses conceptions. ■ Peut manquer d'esprit de synthèse.	■ Expertise réelle. ■ Se comporte en « pro ». ■ Situe son action dans un contexte d'ensemble (équipiers, manager, entreprise). ■ Prend du recul et sait analyser son action de façon critique.
Motivation	**Ne veut pas**	**Veut bien**	**Veut bien mais**	**Veut bien**
	■ N'a pas envie. ■ Ne se sent pas prêt. ■ C'est aux autres de faire. ■ C'est inutile, sans intérêt. ■ Trop difficile, risqué. ■ Vague, flou, réticent et inactif.	■ Motivation moyenne. ■ Bonne volonté générale. ■ Est ouvert. ■ S'intéresse aux projets et aux activités mais sans être actif ni moteur. ■ Besoin d'aide, d'encouragements et de reconnaissance.	■ Motivation moyenne. ■ Peut manquer de confiance et ne pas vouloir assumer seul la responsabilité. ■ Souhaite un appui. ■ La motivation reste conditionnelle. ■ Pose ses conditions, demande des moyens, plus de liberté et d'indépendance.	■ Solide motivation. ■ Actif, dynamique. ■ Intéressé. ■ Communique aux autres sa motivation et son intérêt pour l'activité.

Tableau 10.11 – Grille des objectifs et méthodes des quatre styles de management

	M 1 Style directif	M 2 Style persuasif	M 3 Style participatif	M 4 Style délégatif
Organisationnel	+	+	–	–
Relationnel	–	+	+	–
Objectif	▪ Encadrer de près des jeunes collaborateurs, peu expérimentés et peu compétents.	▪ Souder l'équipe autour d'objectifs communs.	▪ Rappeler le respect des contrats et des zones d'autonomie. ▪ Créer une ambiance de travail conviviale.	▪ Partager la responsabilité et développer la prise d'initiative en accordant le droit à l'erreur.
Méthodes	▪ Ordres précis et instructions individualisées. ▪ Plannings et programmes. ▪ Définitions de fonction. ▪ Procédures. ▪ Contrôles réguliers. ▪ Parle beaucoup et écoute peu. ▪ Connaît le travail et peut l'expliquer. ▪ Communication *top/down* individualisée.	▪ Beaucoup d'explications (les causes, les enjeux). ▪ Décide et met en valeur les projets et les objectifs. ▪ Encourage et soutient les individus. ▪ Apprécie les améliorations. ▪ Suscite les questions et même les objections. ▪ S'assure que chacun a compris ce qu'on attend de lui et se sent motivé. ▪ Communication *top/down* et *bottom/up* individualisée.	▪ Conseille et aide à résoudre les difficultés. ▪ Négocie des solutions prenant en compte les intérêts généraux et ceux des individus. ▪ Analyse les limites de ce qui est négociable. ▪ Négocie les objectifs et travaille par contrat avec ses collaborateurs. ▪ Rencontres prévues dans les contrats. ▪ Écoute, s'adapte, tient compte des attentes et des conseils. ▪ Permet aux collaborateurs de se mettre en avant et les soutient Communication *top/down* et *bottom/up* individualisée et par groupe.	▪ Définit les missions et attend les propositions pour réaliser. ▪ Définit des rencontres périodiques. ▪ Apporte une aide indirecte. ▪ Échange. ▪ Accepte les propositions nouvelles. ▪ Analyse le processus et les résultats avec le collaborateur. ▪ Communication *top/down* et *bottom/up* individualisée et par groupes et communication entre les personnes.

BONNES PRATIQUES

6. LES DIFFICULTÉS COMPORTEMENTALES CLASSIQUES

Les métiers d'auditeur interne et de contrôleur permanent comportent des difficultés classiques spécifiques comme pourraient en avoir d'autres professions (enseignant, urgentiste, juge…).

Il est à la fois utile de les connaître pour les gérer au mieux mais aussi pour en comprendre le caractère essentiel (si vous ne supportez pas la vue du sang et l'expression de la douleur mieux vaut probablement ne pas se lancer dans le métier d'urgentiste) et sa « normalité » (vous n'avez rien d'anormal en vivant mal le dilemme du juge s'interrogeant sur la vérité et la capacité à la faire « éclater »).

6.1. Posture de l'auditeur interne

5.1.1. Les aspects valorisants

L'auditeur interne est investi de l'autorité du « chef ». Il est donc légitime. Il est indépendant des services et, à ce titre, peut aborder les problèmes et les blocages des deux côtés. Il peut apporter idées, recul et médiation : c'est une source d'aide.

Il est dédié à l'analyse du fonctionnement, l'appréciation des risques et de la performance. À ce poste d'observation il a tous les atouts pour mieux comprendre et mieux contribuer à la réussite et apparaître pertinent.

Il visite l'ensemble des services et développe une compréhension à la fois théorique (mission, standards d'organisation, grilles d'évaluation ou de performance…) et concrète (il est sur le terrain) des tenants et aboutissants de l'organisation. Il a du recul et de la vision.

Il travaille en contact avec les opérationnels et leur hiérarchie : il développe un « carnet d'adresses », des contacts à la fois valorisants et utiles. Le poste est de ce fait prestigieux. Il est en vue… il est visible… on est susceptible de penser plus facilement à lui.

5.1.2. Les aspects dévalorisants

L'auditeur interne ne fait que passer. Il filtre la réalité à l'aune de son programme de travail et de ses grilles d'évaluation. Il peut avoir une image de superficialité.

Il rédige des rapports qui font la part belle aux (voire n'aborde que les) points négatifs. Il choisit indépendamment, voire secrètement, ses thèmes et objets d'audit, à la discrétion de la direction générale ou des actionnaires ou du groupe. Il peut être perçu comme l'envoyé de la direction pour « régler des comptes » ou pour « faire son compte »

à quelqu'un, un service ou un responsable. Son indépendance et son objectivité peuvent être questionnées.

Il présente ses conclusions en accentuant soit la référence à une norme, soit aux observations de terrain. Dans le premier cas, il pourra être taxé d'être théorique, voire irréaliste, ou de faire un « procès d'intention ». Dans l'autre cas, il est considéré comme sans hauteur de vue, s'attachant à des détails…

Il diagnostique de vrais problèmes, suggère de vraies solutions mais ne s'attarde pas sur le caractère réalisable, sur les questions de moyens nécessaires pour mettre en œuvre les solutions proposées pour les priorités de la gestion courante, des projets en cours, de l'action supplémentaire recommandée : « Il charge la barque. » L'auditeur interne n'est pas considéré comme une aide mais comme « une plaie ».

Il analyse la situation, l'évalue et rédige son rapport. Mais cette situation c'est le fruit du travail de tel ou tel responsable qui analyse facilement le rapport comme une mesure de sa performance. L'auditeur interne est dérangeant et peut être vu comme un « ennemi » ou au moins un « danger ».

Il revisite perpétuellement les différents services et examine l'existant au regard des normes et des standards. Facteur aggravant, les équipes évoluent vite et le poste d'auditeur interne est souvent tenu par de jeunes collaborateurs bien formés et à fort potentiel… mais considérés comme jeunes et inexpérimentés. Les audités les considèrent facilement comme du personnel à former et sans valeur ajoutée.

EN PRATIQUE

Auditeur interne, vous devez :

- choisir et comprendre un référentiel pertinent pour le domaine audité ;
- déployer des méthodes d'analyses, des sondages et des enquêtes pertinents et probants ;
- établir et discuter vos constats et leur évaluation au regard du référentiel ;
- développer votre objectivité au travers d'une analyse factuelle et structurée ;
- conclure en proportion de l'enjeu de vos constats ;
- formuler des recommandations pertinentes et réalistes discutées avec les services ;
- hiérarchiser avec soin vos constats.

6.2. Posture du contrôleur permanent

5.2.1. Les aspects valorisants

Le contrôleur permanent a une connaissance terrain développée : c'est un partenaire de référence consulté pour connaître et comprendre les réalités du terrain.

Il est proche du terrain. Il est apte à faire passer les messages, à assurer du suivi mais aussi à faire remonter les messages du terrain, à obtenir les directives, les explications, les arbitrages manquants.

Il a accès à l'information sur les modes de fonctionnement des autres services, sur les inventaires d'incidents.

5.2.2. Les aspects dévalorisants

Le contrôleur permanent est souvent vu comme un employé administratif sans beaucoup de pouvoir de sanction dans le cas où on refuse de coopérer. Les actions qu'il demande pour renforcer le dispositif de contrôle interne sont souvent perçues comme non obligatoires…

Il est souvent moins craint que l'auditeur interne qui bénéficie de l'oreille du président et du directeur général… et dont les recommandations demandées sont des ordres !

EN PRATIQUE

Contrôleur permanent, vous devez :

- vous faire accepter par l'encadrement opérationnel et les personnels d'exécution comme un partenaire qui aide à la réalisation des opérations et au développement de l'efficacité et de l'efficience des traitements ;
- développer des relations de proximité avec les auditeurs internes afin de mutualiser votre expérience terrain ;
- vous situer dans une logique de transfert de connaissance et d'aide aux métiers plutôt que dans une logique simplement répressive.

PAROLE D'EXPERT

Lawrence B. Sawyer, neuvième commandement : savoir comment communiquer et à quel moment

« J'utilise ici le terme en son sens le plus large. Je parle de communication depuis le moment où l'inspection commence, en passant par l'examen des différentes opérations, jusqu'aux rapports finaux à la direction. L'inspecteur moderne est en rapport avec celui qu'il inspecte dès le début de l'inspection. Il a des entretiens préliminaires bien structurés qui se déroulent facilement, et non des parties de "pêche aux renseignements" décousues ou à bâtons rompus, et qui montrent que l'inspecteur a préparé son travail. Il est en rapport avec le personnel de contrôle lorsqu'il fait un tour d'horizon préliminaire et cherche à savoir :

- Quel est le travail ?
- Qui le fait ?
- Comment il est fait ?
- Pour quoi il est fait ?

Il est en rapport avec le personnel d'exécution lorsqu'il inspecte les opérations et cherche à connaître les conséquences et les raisons des erreurs. Il sait parfaitement quelles sont ses propres limites dans un nouvel et parfois étrange environnement, et il veut s'assurer qu'il connaît toutes les données avant de tirer les conclusions. Il est normalement en relation avec la direction du service inspecté lorsque la situation nécessite un redressement. Ces relations peuvent avoir lieu par échanges oraux-visuels ou au moyen de rapports écrits de la situation. Il communique avec le directeur du service inspecté à la fin de son travail lors d'une présentation orale-visuelle de toutes les découvertes faites en cours d'inspection, des bonnes comme des mauvaises. Et c'est à ce moment qu'il discute des mesures de régularisation prises ou en cours. Il est en communication avec chaque directeur concerné de la société lorsqu'il rédige son rapport définitif, net et incisif, qui expose les résultats de son inspection, qui indique ce qui est insatisfaisant dans le secteur qu'il a inspecté et qu'il invite à régulariser ce qui est erroné. »

TÉMOIGNAGE

Patrick Georgelin, conseiller de dirigeants d'entreprises PME-PMI

Mon activité consiste à conseiller les dirigeants de PME/PMI en gestion financière, fiscale, administrative et organisationnelle et à les assister *via* un accompagnement opérationnel. Si le contrôle interne n'est pas mon activité principale, je suis amené à le pratiquer en diverses occasions.

Il y a à peu près autant de définitions du contrôle interne que d'intervenants et d'organisations professionnelles qui ont traité ce sujet. Ceci s'explique par la diversité des préoccupations de chacun. À sa manière, Henri Fayol a sans doute apporté la première pierre du contrôle interne en affirmant que l'administration était l'une des fonctions essentielles de l'entreprise : « Administrer, c'est prévoir, organiser, commander, coordonner et contrôler. Contrôler, c'est veiller à ce que tout se passe conformément aux règles établies et aux ordres donnés. » C'est un bon début (nous sommes à l'aube du XX^e^ siècle) mais c'est un peu court !

Une définition synthétique et universelle du contrôle interne serait de dire qu'il s'agit de rechercher, d'identifier et de gérer les risques au sein d'une entreprise. Vaste programme ! Les risques sont multiples.

Le dirigeant de PME/PMI a, le plus souvent, une compétence « métier » et rarement une attirance pour la gestion administrative. Par manque de temps (et d'intérêt), il va négliger l'examen de nombreux risques dont les conséquences peuvent être fatales à la survie de son entreprise.

Parmi ces risques, j'en retiendrai deux : les détournements de fonds et les contrats d'assurance.

J'ai connu trois entreprises victimes de détournements de fonds. À chaque fois, le dirigeant était stupéfié car il n'aurait jamais imaginé que l'auteur en était capable. Il n'avait pas su déceler les failles de procédure et avait sans doute oublié le vieux dicton : « L'occasion fait le larron. » Pour déceler les risques, il faut être imaginatif, curieux et méfiant. Presque toutes les victimes d'un escroc déclarent : « Je n'aurais jamais imaginé cela de lui, il était tellement sympathique et inspirait confiance »...

Quant aux contrats d'assurance (multirisques des locaux, responsabilité civile professionnelle, pertes d'exploitation...), il est fréquent, par souci d'économie, que le dirigeant ne prenne pas en compte des garanties qui lui paraissent superflues ou encore omette d'ajuster des garanties en fonction de la croissance de son activité. Le jour où survient un sinistre, le dirigeant apprend qu'il est peu ou pas couvert et c'est la catastrophe financière.

Pour finir, je dirai que toute entreprise, quelle que soit sa taille, doit disposer d'un dispositif de contrôle interne *a minima*. Ce dispositif ne peut être de la responsabilité opérationnelle du dirigeant qui a déjà fort à faire. Par contre, il doit être confié à une personne proche en qui il a toute confiance.

Chapitre 11

La démarche de conduite d'une mission d'audit interne

CE CHAPITRE VOUS PERMETTRA DE :

- connaître les différentes phases et étapes de conduite d'une mission d'audit interne : la préparation, l'étude préliminaire, la réalisation des travaux, la conclusion et restitution.

Si le contrôleur permanent réalise les mêmes contrôles selon une fréquence régulière sur un terrain connu, il n'en est pas de même pour l'auditeur interne. En effet, la diversité des missions qui lui sont confiées ainsi que la fréquence aléatoire de celles-ci font que chaque mission peut être considérée comme unique. À ce titre, elles demandent une démarche structurée et un formalisme documentaire. C'est l'objet de ce chapitre que de décrire la démarche spécifique de conduite d'une mission d'audit interne.

La conduite d'une mission d'audit interne se déroule selon une démarche classique en trois temps et la répartition du temps total de la mission est le plus souvent de 20 % pour la préparation de la mission, 60 % pour la réalisation de la mission à proprement parler et 20 % pour la rédaction du rapport d'audit.

Une mission d'audit interne prend la forme d'un diagnostic. L'auditeur interne étudie les pratiques du domaine audité en vue d'apprécier la qualité de son contrôle interne. Le cas échéant, il repère les éventuels dysfonctionnements ou insuffisances, en recherche les causes et en démontre les conséquences, puis développe, en collaboration avec les personnes auditées, des recommandations et des plans d'action aptes à améliorer la situation. Il revient ensuite aux responsables concernés de s'engager sur la mise en œuvre de ces plans d'action.

Certaines missions d'audit interne peuvent nécessiter le recours à des profils de compétences spécifiques, pas toujours présentes au sein de l'entreprise. Dans ce cas, il sera nécessaire d'évaluer les budgets correspondants.

1. LA PRÉPARATION DE LA MISSION D'AUDIT INTERNE

L'objectif de la phase de préparation de la mission d'audit interne est d'organiser celle-ci. À ce titre, les travaux à réaliser et les résultats attendus sont de constituer l'équipe et de planifier la mission d'audit interne : équipe disponible et logistique, et de collecter les informations disponibles sur le domaine à auditer.

1.1. Le choix de l'équipe d'auditeurs internes

La réalisation des missions d'audit requiert compétence et conscience professionnelle. La composition de l'équipe doit s'appuyer sur une évaluation de la nature et de la complexité de chaque mission, des contraintes de temps et des ressources disponibles. Une équipe est constituée d'un chef de mission et d'auditeurs internes. L'équipe peut être complétée d'assistants et d'experts externes.

Le directeur de l'audit interne doit s'assurer pour chaque mission que :

- l'équipe d'auditeurs internes possède collectivement les connaissances, le savoir-faire et les compétences nécessaires pour mener correctement la mission ;
- le dimensionnement de l'équipe affectée à la mission, en nombre de personnes, est adapté à l'ampleur ou la complexité du sujet.

2. L'ÉTUDE PRÉLIMINAIRE

Préalablement à la réalisation de la mission, les auditeurs internes étudient les informations utiles qu'il est possible de collecter concernant le domaine à auditer. Ces travaux vont permettre de constituer un référentiel du domaine à auditer, de mener une analyse de risques et de préciser l'objectif de la mission.

L'étude préliminaire peut se faire, exceptionnellement par téléphone, mais implique généralement un « travail de terrain ». Comme il s'agit du premier contact avec les personnes auditées concernant la mission prévue, ce contact peut s'avérer déterminant pour la suite et la bonne fin de la mission ; et le face-à-face, les discussions/digressions et les observations « physiques » constituent un excellent investissement.

À l'issue de cette étape, il peut être décidé de réorienter la mission initialement prévue, d'en changer le périmètre, de redimensionner l'équipe et le temps à y consacrer, de la planifier ultérieurement, voire de l'abandonner.

2.1. La prise de connaissance

L'étude préliminaire, initialisée par le chef de mission, consiste à :

- préciser le champ de l'audit avec ses commanditaires si des questions subsistent ;
- identifier les personnes à rencontrer ;
- collecter la documentation sur les disciplines à auditer et sur les techniques d'audit existantes ;
- consulter les bases documentaires de l'entreprise, les procédures, etc.
- collecter et consulter les rapports d'audit antérieurs et autres analyses du sujet audité ;
- obtenir des informations chiffrées ou caractéristiques du domaine audité ;
- collecter et adapter ou créer le programme de travail.

2.2. L'entretien avec le management de l'entité auditée

Avant de démarrer l'audit, le chef de mission doit programmer un entretien d'ajustement avec les responsables de la structure auditée afin de :

- se concerter sur l'intérêt et les objectifs de la mission d'audit interne à réaliser et en définir les grandes lignes (attendus, périmètre, calendrier…) ;
- discuter la coordination de l'audit avec le fonctionnement opérationnel de l'entité auditée ;
- collecter toute information analytique actualisée/complémentaire/additionnelle significative ;
- s'accorder sur les objectifs clés de l'entité auditée ;
- recueillir auprès du management son auto-évaluation succincte de l'entité auditée.

Cette discussion doit permettre :

- de valider les risques préalablement identifiés et leur probabilité d'occurrence ;
- de décider de la réalisation ou non de la mission ;
- d'adapter le programme d'audit interne ;
- d'améliorer l'efficacité en estimant éventuellement plus exactement les jours/hommes budgétés.

Les conclusions de cette réunion doivent être consignées par écrit dans le « compte rendu d'entretien préliminaire avec le management ».

2.3. La préparation du programme de travail

Le programme de travail s'établit sur la base de la note d'orientation. Il est destiné à définir, répartir, planifier et suivre les travaux des auditeurs. Le programme doit être revu et validé avant le démarrage des travaux sur le terrain par le chef de mission et conservé dans le dossier de mission.

Le plan de travail constitue le guide méthodologique de conduite de la mission. Son objectif est de constituer le planning des tâches à réaliser dans le cadre de la mission. C'est pour cela qu'il précise :

- la répartition du travail entre les auditeurs internes ;
- la planification des phases en termes de délais et d'échéances à respecter ;
- les outils à utiliser ;
- la manière de conduire la mission (qui est fonction des caractéristiques et des objectifs de la mission).

3. LA RÉALISATION DES TRAVAUX

L'objectif de la phase de réalisation des travaux est d'inventorier les points positifs et les points négatifs (faiblesses réelles) de l'entité auditée.

À ce titre, les travaux à réaliser et résultats attendus sont les suivants :

- Identifier les forces et faiblesses apparentes du domaine audité.
- Tester celles-ci sur le terrain : papiers de travail et feuilles de risques validées par le chef de mission ; identification des faiblesses compensées par des forces réelles et des faiblesses réelles ; identification des causes explicatives des faiblesses réelles ; précision des conséquences en termes de risques réels ou potentiels de chaque faiblesse identifiée ; détermination des recommandations qui, une fois mises en place, permettront d'annuler les faiblesses en question.
- Formaliser les résultats sous la forme de composants élémentaires validés par le chef de mission.

3.1. La réunion d'ouverture

La réunion d'ouverture se tient au sein du domaine audité, sur le lieu de la mission. Les participants sont :

- l'encadrement du domaine audité ;
- le chef de mission ou le directeur de l'audit interne ;
- l'équipe d'auditeurs.

Cette réunion doit permettre au chef de mission :

- de présenter les auditeurs, leur expérience, leur fonction ;
- de demander à l'encadrement du domaine audité de présenter celui-ci ;
- d'exposer/de rappeler la définition du rôle de la fonction audit interne et sa place dans l'entreprise, en faisant éventuellement référence à la charte de contrôle interne ;
- d'annoncer le déroulement prévisionnel de la mission et de discuter de la note d'orientation en prenant en compte les éventuelles remarques des personnes auditées ;
- d'affiner la logistique (bureau, horaires, ligne téléphonique, espace de rangement sécurisé…) et de prendre les premiers rendez-vous ;
- de rappeler la procédure d'audit et de décrire le déroulement des phases suivantes.

Les conclusions de cette réunion peuvent éventuellement conduire à une mise à jour de la note d'orientation.

3.2. Les tests d'audit

Les travaux de vérification sont effectués par les auditeurs internes et les informations recueillies permettent de répondre aux objectifs de la mission. Ces informations doivent être suffisantes, fiables, pertinentes et utiles pour fournir une base saine et sûre aux constatations et recommandations.

Le travail sur le terrain consiste à conduire les contrôles prévus dans le programme de travail en utilisant les outils d'audit interne adéquats : mener des entretiens, élaborer des diagrammes de circulation, réaliser des observations physiques, effectuer des rapprochements et des reconstitutions, interroger des fichiers informatiques… et établir les papiers de travail.

3.3. La formalisation des constats et leur présentation

Après chaque étape de travail, des conclusions partielles sont rédigées par l'auditeur interne sous forme de FRAP. Ce sont les constats des déficiences identifiées. L'auditeur les présente au chef de mission ainsi qu'aux personnes du domaine audité.

3.4. La réunion de clôture de phase de vérification

Une réunion doit être tenue en aparté entre le chef de mission et les auditeurs afin de s'assurer que les objectifs ont été atteints et que l'ensemble des points du programme de travail ont été réalisés.

Avant de quitter le site, une réunion est organisée avec l'encadrement de l'entité auditée afin de clôturer la phase de vérification par une restitution orale (néanmoins un document préparé à cet effet peut également être distribué). Les participants sont les mêmes que ceux de la réunion d'ouverture.

Cette réunion de clôture sur place doit permettre au chef de mission :

- de remercier les personnes auditées pour leur accueil et coopération lors de la mission ;
- de présenter les constats qui ont été validés avec les différents échelons hiérarchiques du domaine ;
- de discuter des recommandations et des plans d'action, de recueillir les commentaires ;
- d'aborder les éventuels points en suspens et obstacles à la réalisation de la mission (il ne s'agit pas d'évoquer les difficultés résolues mais les éléments qui ont conduit à limiter la mission initialement prévue) ;
- de décrire le déroulement des phases suivantes.

EN PRATIQUE

Bien menée, cette réunion doit permettre de valider au maximum le futur rapport et d'obtenir l'accord de l'audité sur les constats et les recommandations. Elle ne remplace pas la réunion de validation, mais contribue à la préparer.

Les conclusions de cette réunion, doivent être consignées dans le « Compte rendu de réunion de clôture ».

4. LA CONCLUSION ET LA RESTITUTION

Cette dernière partie de la mission n'en est pas la moins complexe. En effet, il revient à l'équipe d'audit de rédiger et faire valider par les personnes auditées les faits observés et les recommandations en mettant en avant la priorité de mise en œuvre de chacune d'entre elles.

En ce sens, le rapport final est un document très impliquant :

- Il note les faits indiscutables constatés par les auditeurs internes, au regard de standards, de bonnes pratiques, de niveaux de performance attendus. Cette partie n'est pas très engageante pour les auditeurs car elle constitue un simple procès-verbal.

L'erreur serait d'y faire figurer des faits sans importance et qui pourraient irriter inutilement les personnes auditées et décrédibiliser la fonction d'audit interne.

- Il précise également les recommandations que les auditeurs proposent, ce qui est plus engageant car toute recommandation inadaptée pourra se retourner contre eux. C'est la raison pour laquelle les auditeurs veillent à ne pas être trop précis en matière de solution à mettre en œuvre…
- Il indique pour finir l'ordre dans lequel les recommandations doivent être mises en œuvre, ce qui est également impliquant car cela montre ce qui est le plus important pour les auditeurs. Là encore, ils ne doivent pas se tromper sous peine de voir leur compétence remise en cause.

4.1. La réunion de restitution

Dès le retour de mission, les auditeurs internes s'entretiennent avec leur hiérarchie (chef de mission et directeur de l'audit interne) des événements, des faits et des observations remarquables (positives, négatives ou connexes) afin de définir rapidement la suite à donner à chaque situation.

4.2. La réunion de validation

Une réunion de validation est tenue entre les personnes auditées et les auditeurs, selon les circonstances en présence (facultative) du commanditaire, au cours de laquelle tous les aspects du projet de rapport sont discutés.

Lors de la réunion, les « destinataires » des recommandations sont désignés et un délai de réalisation proposé. Les minutes et les conclusions de cette réunion doivent être consignées dans le « compte rendu de réunion de validation » qui sera adressé aux participants de la réunion.

L'objectif de la validation est d'intégrer la réponse des personnes auditées dans le rapport et d'obtenir leur accord tacite pour les observations et les axes de recommandation proposés. L'accord formel viendra de la réponse des personnes auditées au « projet » de rapport permettant de s'assurer qu'il n'y a pas eu d'interprétation involontaire des faits ou d'ambiguïté dans la formulation de leur restitution, pour permettre à l'audité d'exercer son droit de réponse et pour recueillir le plan d'action qu'il s'engage à mettre en œuvre.

EN PRATIQUE

La validation n'est pas une négociation ni une recherche de compromis.

Lorsque les contraintes géographiques liées à l'éloignement ne permettent pas de tenir une réunion de validation, le principe reste cependant intangible. Cette réunion sera tenue par téléphone, *a minima* avec le responsable du management audité.

PAROLE D'EXPERT

Lawrence B. Sawyer, dixième commandement : connaître les méthodes modernes

Nous vivons dans un univers constamment en évolution. La direction moderne comprend bien que rien ne reste immobile. Si cela ne progresse pas, cela rétrograde. Et si l'inspecteur ne comprend pas ce principe tout aussi parfaitement, il ne sera pas en mesure de garder le rythme de ceux pour lesquels il travaille. Aussi, l'inspecteur moderne doit-il posséder une connaissance solide de l'informatique. Il doit connaître l'échantillonnage statistique, il ne devrait pas être perturbé par un problème d'analyse de régression multiple. Il doit avoir en plus des notions en matière de recherche opérationnelle et ses dérivés, comme la méthode P.E.R.T., la programmation linéaire ou la simulation de Monte Carlo. Il devrait être versé en mathématiques tout comme une Direction moderne est versée en mathématiques. Et il doit être prêt à "manœuvrer ses voiles aux vents du changement" afin de ne pas "sombrer sur les récifs" de l'ignorance ou de « demeurer encalminé sur les bancs de l'apathie. »

TÉMOIGNAGE

Olivier Faujour, président de Yoplait

Le métier d'auditeur interne apporte beaucoup de valeurs ajoutées car il consiste à observer la vie de l'entreprise de manière fiable et objective et de définir des plans d'action pour gérer les risques au mieux. Ce métier permet de protéger l'entreprise et ainsi de mieux sécuriser sa croissance.

Cette fonction revêt une importance particulièrement grande dans une entreprise comme Yoplait suite à son acquisition par le groupe américain General Mills en 2011. « La Petite Fleur » a su s'adapter aux méthodes de reporting des entreprises cotées à Wall Street ainsi qu'aux contraintes réglementaires (mise en place de SOX). Pour cela, les auditeurs internes ont reçu le soutien direct de la direction générale. Au cours de l'intégration, les auditeurs internes de Yoplait ont joué un rôle central pour renforcer la fiabilité des processus. Ils ont aussi travaillé étroitement avec les cabinets d'audits externes qui ont mesuré les progrès de l'entreprise dans l'amélioration et la fiabilisation des processus de reporting et d'approbation. Au final, Yoplait a pu consolider la maîtrise de sa croissance, la plus rapide dans le marché des produits laitiers frais en France depuis quatre ans. Cette consolidation a renforcé aussi la confiance des actionnaires, encore plus disposés à investir pour accroître la compétitivité de l'entreprise.

La fonction d'auditeur interne appelle des profils de managers rigoureux, déterminés et ayant de bonnes qualités de communication et de persuasion. À l'aise avec les chiffres, ils doivent être précis, méthodiques et analytiques. Ils doivent être capables d'aller en profondeur pour réaliser et interpréter le *check-up* de l'entreprise sous toutes ses facettes et pour cela poser les bonnes questions aux bonnes personnes au bon moment. L'auditeur interne doit aussi savoir persévérer pour mettre en œuvre les plans d'amélioration résultant des différents audits. Ces plans requièrent des initiatives de l'ensemble des services de l'entreprise. Compte tenu de la diversité de leurs interlocuteurs, ils doivent être flexibles dans leur style de communication. Ils doivent savoir se positionner comme des « partenaires d'affaires » avec leurs collègues en interne, être à leur écoute et se montrer convaincants pour les amener à réaliser des projets auxquels ils n'auraient pas spontanément pensé.

L'une des richesses de ce poste est aussi de faire face à des problématiques extrêmement variées car les auditeurs internes doivent couvrir l'ensemble des cycles de l'entreprise (achat, vente, finance, ressources humaines, IT...) et côtoient des interlocuteurs de tous niveaux (des opérationnels aux membres du COMEX). À titre d'exemple, leurs analyses et leurs recommandations peuvent aussi bien porter sur la gestion opérationnelle des pièces de maintenance d'une usine que sur le processus de production des états financiers destinés aux actionnaires.

C'est donc un métier central et passionnant qui contribue au développement de l'entreprise dans sa globalité et sa durée.

CHAPITRE 12

Les livrables spécifiques de conduite d'une mission d'audit interne

CE CHAPITRE VOUS PERMETTRA DE :

- connaître les livrables caractéristiques à produire dans le cadre d'une mission d'audit interne.

La conduite d'une mission d'audit interne nécessite un formalisme documentaire qui l'accompagne de son lancement à son archivage.

Les « livrables » sont :

- la lettre de mission ;
- les papiers de travail ;
- le dossier permanent et le dossier de mission ;
- la note d'orientation ;
- la feuille de couverture ;
- le rapport d'audit.

Ces « livrables » sont autant des outils de travail internes que des outils de pilotage et de communication.

Les livrables concrétisent le travail de vigilance et d'analyse des contrôleurs et auditeurs internes. Le travail est en effet moins aisément perceptible que celui des commerciaux ou des producteurs, voire des comptables. L'auditeur interne existe donc pour une bonne part par ses livrables. Il faut se rendre compte que certains interlocuteurs considèreront que les observations et recommandations orales des contrôleurs n'ont pas de « réalité » tant qu'on ne les retrouve pas dans un rapport écrit… ou qu'elles n'engagent pas. La part de communication orale et écrite doit ainsi être adaptée aux circonstances.

Le livrable est également un ouvrage où se concrétisent la compréhension et la maîtrise par le contrôleur/l'auditeur du contexte, de sa mission, des faits et de sa méthode. Il constitue donc pour l'apprenti un exercice et une preuve de compétence. Les meilleures directions d'audit ou de contrôle attachent une importance significative à la qualité des restitutions et au processus de production et surtout de revue des travaux et livrables. La revue qualité est surement une épreuve… mais c'est aussi le chemin du professionnalisme.

Recherchez la revue des plus expérimentés et tirez en le meilleur profit.

La démarche de contrôle est un raisonnement et un discours et doit donc être logique. La construction se réalise progressivement. Chaque livrable apporte sa pierre à l'édifice. Les écueils classiques sont :

- se ruer sur les contrôles par peur de « manquer » et omettre l'analyse des risques… le plan d'audit ou la cartographie des risques doit y remédier ;
- réaliser les contrôles par habitude ou mimétisme. Il n'y a finalement pas le lien attendu entre l'analyse des risques et le plan de contrôle. Rien de tel qu'une bonne note d'orientation ;
- réaliser un test… mais qui n'a que peu à voir avec le risque ciblé. Un programme de travail suffisamment détaillé et bien relier à la note d'orientation préviendra ce problème ;
- omettre de conclure sur son test en fonction des observations. Des papiers de travail bien structurés guideront la formalisation et, pour peu que l'on soit attentif au guide, éviteront l'écueil ;
- ne pas « remonter » et suivre une observation significative et ainsi altérer le diagnostic en réduisant l'apport de la mission. Les standards de conclusion et de formulation (et de gestion) des recommandations y pourvoiront.

LA LETTRE DE MISSION

La lettre de mission constitue la matérialisation du mandat donné par la direction générale à l'audit interne, qui informe les responsables du domaine concerné de l'intervention prochaine des auditeurs. Lorsque la nature de la mission le permet (ce qui n'est pas toujours le cas, pour une fraude par exemple), il est d'usage que l'auditeur informe l'audité de sa venue. Au plus tard 15 jours à un mois avant le démarrage de la mission d'audit, le directeur de l'audit adresse au responsable concerné une « lettre de mission » officielle pour informer les audités qu'un audit va être réalisé.

Cette lettre de mission annonce l'audit, sa date de début, sa durée prévue ainsi que le nom du chef de mission et des auditeurs qui vont intervenir. Elle fait référence au plan d'audit approuvé par le président.

Il est précisé que l'information sur l'imminence de la mission doit permettre aux personnes auditées de s'organiser pour :

- prendre en compte et réduire le risque de perturbation du fonctionnement du domaine potentiellement induit par la venue des auditeurs ;
- contribuer aux travaux des auditeurs : libre accès aux documents, biens et personnes en rapport avec l'objet de la mission, facilitation logistique (espace de travail, communication, hébergement…).

EN PRATIQUE

Une copie de la lettre de mission est conservée dans la section « Préparation de la mission » du dossier d'audit interne.

La lettre de mission doit être signée par une personne d'un grade suffisamment élevé dans l'entreprise pour que les personnes auditées ne puissent pas refuser la mission : président du groupe, président d'une des sociétés du groupe, président d'une filiale… qui sera le signataire.

La lettre de mission est le « sésame ouvre-toi » de la mission à condition de bien faire figurer les objectifs et le périmètre de celle-ci, ainsi que la liste des auditeurs.

LIVRABLES SPÉCIFIQUES

LES PAPIERS DE TRAVAIL

Les papiers de travail permettent :

- de conserver la trace du travail réalisé et de fournir la preuve des conclusions tirées durant l'audit (notions de piste d'audit, de force probante) ;
- d'exercer et de documenter la supervision ;
- de faciliter les revues croisées ;
- de structurer et enregistrer l'information qui pourrait être utilisée pour de futurs audits.

La quantité, le type et le contenu des documents de travail dépendent de la nature de l'audit. Le niveau de documentation doit être le minimum nécessaire pour satisfaire ces attentes. Les auditeurs doivent éviter d'inclure des informations inutiles dans les documents de travail. Les conclusions des tests sont rédigées dans une « feuille de couverture de test ». Les synthèses des entretiens sont rédigées dans un « compte rendu d'entretien ».

EN PRATIQUE

Ces documents doivent également être archivés dans le dossier de mission. Les documents de travail électroniques doivent faire référence, chaque fois que possible, aux documents de travail papiers, et réciproquement.

Restez à l'écoute des élargissements, approfondissements d'investigation qui peuvent apparaître intéressants.

Demandez-vous en permanence s'il ne serait pas plus rentable de réorienter le travail (le résultat recherché apparaît impossible à obtenir ; il est déjà suffisamment atteint sans avoir effectué tous les travaux prévus).

Périodiquement et au moins à la fin de chaque section du programme, présentez, pour information et revue, vos papiers de travail avec suggestions de recommandations à la hiérarchie de la mission.

À la fin de chaque section, référencez les papiers de travail conformément à la norme en vigueur pour archivage ultérieur.

LES DOSSIERS PERMANENTS ET LE DOSSIER DE MISSION

Véritable mémoire de la direction de l'audit, les dossiers permanents regroupent toutes les informations connues sur chacun des domaines de l'entreprise. Le dossier de mission a lui pour objectif de constituer un lieu unique de rangement de toutes les informations relatives à une mission.

Les objectifs des dossiers permanents et du dossier de mission sont :

- de constituer la mémoire d'un domaine (dossiers permanents) ;
- de centraliser toutes les informations concernant une mission (dossier de mission).

Les dossiers permanents et le dossier de mission s'utilisent de la façon suivante :

- Les dossiers permanents contiennent : la réglementation, les procédures internes de l'entreprise et les précédents rapports de mission effectués sur le même domaine, ou effectués transversalement, mais concernant en partie le domaine.
- Le dossier de mission se compose d'une chemise dans laquelle figurent des sous-chemises. Chaque sous-chemise contient : un type d'informations concernant le domaine audité (souvent issue du dossier permanent) et les travaux réalisés pendant les phases de terrain.

EN PRATIQUE

Tenez bien à jour les dossiers permanents et le dossier de mission, ce sont des investissements pour toute l'équipe d'audit, et non pas une perte de temps.

Le papier prend beaucoup de place, n'hésitez pas à stocker les informations sous forme électronique, ce qui permet, dans le cadre d'intranet ou de l'extranet, de pouvoir y accéder dans le monde entier.

LIVRABLES SPÉCIFIQUES

LA NOTE D'ORIENTATION

La note d'orientation, rédigée par le chef de mission et revue par son responsable, définit et formalise les axes d'investigation de la mission et ses limites : elle les exprime en objectifs à atteindre par l'audit interne pour le commanditaire et les personnes auditées. À la fin de la phase d'étude de la mission et juste avant que ne démarre la phase de vérification de l'audit, un document synthétique présente dans une « note d'orientation », les objectifs poursuivis et les zones de risques que les auditeurs vont examiner. Il délimite ainsi précisément le champ de l'intervention. Il est le plus souvent envoyé au commanditaire initial de la mission pour avis, puis présenté aux personnes du domaine audité pour information.

EN PRATIQUE

La note d'orientation doit être conservée dans le dossier de mission. Elle vient, en complément de la lettre de mission, préciser les objectifs et le périmètre qui sera audité. Elle ne se substitue pas à celle-ci mais la complète.

La direction de l'audit Interne pourra, à ce stade, proposer de ne pas continuer la mission, si en fin d'étude préliminaire, l'enjeu apparaissait ne plus/ne pas justifier la charge d'une mission d'audit.

LA FEUILLE DE COUVERTURE

La feuille de couverture est le document qui, établi en deux temps, décrit les modalités de mise en œuvre d'une tâche définie dans le programme de travail et met par la suite en évidence les conclusions qui en ont été tirées. En deux temps signifie qu'avant d'effectuer une tâche, par exemple un test ou une interview, l'auditeur interne en spécifie les modalités. Ensuite, après la réalisation des travaux détaillés, il rédige ses conclusions directement sur la feuille de couverture. La feuille de couverture comporte uniquement l'objectif poursuivi, la méthode utilisée et les résultats et conclusions le reste se trouve sur les papiers de travail produits au cours de la tâche. Elle est produite au fur et à mesure des besoins, ce qui évite d'établir les spécifications d'actions devenues caduques (conclusion établie autrement ou réorientation des travaux).

Avec le programme de travail, la feuille de couverture permet de suivre de façon synthétique l'état d'avancement du travail sur le terrain et facilite la concertation entre les auditeurs et la supervision :

- la supervision « quotidienne » qui s'assure que les conclusions sont étayées (approbation de la méthode utilisée, allers-retours entre la feuille de couverture et ses papiers de travail détaillés) ;
- la supervision « globale » qui vise à dégager les conclusions de la mission au fur et à mesure de l'avancement des travaux sans aller plus en détail que les feuilles de couverture.

EN PRATIQUE

Cet outil permet de savoir où en sont les travaux au jour le jour, ce qui est très pratique pour la supervision de la mission ; Il permet donc de corriger toute éventuelle dérive au regard des objectifs ou des échéances, notamment en rajoutant d'éventuelles ressources supplémentaires.

L'outil permet également de calculer un indicateur pouvant figurer dans le tableau de bord de la mission.

LIVRABLES SPÉCIFIQUES

LE RAPPORT D'AUDIT

Il est recommandé que l'essentiel, voire la totalité, du projet de rapport soit rédigé en cours de mission et avant la tenue de la réunion de clôture. Au plus tard dès la fin de la phase de vérification, l'auditeur interne rédige un « projet de rapport » formalisant ses constats et recommandations. Le soin apporté à la relation des faits constatés et à la rédaction des recommandations est d'une grande importance : les remarques qui figurent dans un rapport s'adressent à des personnes totalement engagées dans des activités opérationnelles et qui attendent de l'auditeur interne une parfaite objectivité. Le rapport constitue un relevé des lacunes, des faiblesses et des dysfonctionnements identifiés au cours de la mission. Il est pour les responsables l'occasion d'affiner, voire de remettre en cause les méthodes de gestion de leurs domaines d'activité ; il n'établit pas un bilan d'une gestion car cette appréciation relève du ressort de la hiérarchie.

Le projet de rapport est diffusé aux responsables concernés par le champ de l'audit. Il reprend la forme des FRAP rédigées à la fin de la phase de vérification et comporte à la suite de l'exposition des problèmes (faits, causes et conséquences) des recommandations adaptées à l'attention des responsables capables de les prendre en charge, qu'ils soient à l'intérieur ou à l'extérieur du domaine audité. Le rapport d'audit constitue le livrable présentant les forces et les faiblesses ainsi que les recommandations. L'objectif du rapport est de constituer le procès-verbal de l'état des lieux et également un avis de l'auditeur sur l'évaluation des forces et des faiblesses, et également de ce qu'il pense que l'audité doit mettre en œuvre, notamment pour renforcer l'efficacité de son dispositif de contrôle interne.

Le projet de rapport, après la réunion de validation et les mises à jour, constitue le « rapport définitif ». Il se compose d'une synthèse destinée à être lue par les dirigeants, des fiches FRAP examinées lors de la réunion de validation et d'une liste des recommandations classées par destinataires précisant la position des audités et constituant de fait leur première réponse à l'audit. Il est souhaitable de joindre le plan d'action mais ceci ne doit pas se faire au détriment du délai de finalisation du rapport définitif. Réduire le délai d'envoi de ce rapport après la fin de mission est un objectif prioritaire, l'adjonction du plan d'action est un plus appréciable mais non indispensable. Le rapport est envoyé aux responsables audités en charge de mettre en œuvre les plans d'action, à leur supérieur hiérarchique membre du comité exécutif ainsi qu'au président-directeur général. Le commanditaire initial de la mission fait nécessairement partie de cette liste de destinataires.

Le principe de l'information du président-directeur général n'est pas discutable, néanmoins les modalités pratiques de cette information sont possibles. Ainsi, sous réserve d'accord du président, cette information sera entièrement gérée par le directeur

de l'audit interne qui transmettra au président une «synthèse des synthèses» avec ses commentaires. Le président aura alors la possibilité de se faire communiquer, à sa demande et sans délai, la copie de tout rapport d'audit qu'il souhaiterait consulter *in extenso*. Le rapport d'audit matérialise le travail des auditeurs.

Un rapport d'audit n'est pas neutre :

- Il analyse une situation, mais, comme un devis de réparation, il met l'accent sur les dysfonctionnements, pour faire développer des actions de progrès. « Au moins une page sur ce qui ne va pas, au plus une ligne sur ce qui va. »
- Il contient des recommandations. Une recommandation n'est pas une critique, elle n'implique pas de faute : c'est une amélioration proposée au responsable habilité à mener l'action. Il est en charge de développer et mettre en place une solution au problème soulevé : la solution proposée, une solution équivalente ou une meilleure solution.

Après lecture ou sur demande du directeur de l'audit interne, le président-directeur général peut inscrire l'examen du rapport à l'ordre du jour d'un comité exécutif ou d'une réunion thématique avec, selon les besoins, la présence des responsables du domaine audité et de l'équipe d'audit. Seuls les commanditaires et le président-directeur général peuvent décider d'une diffusion plus large du rapport.

Le rapport d'audit permet de formaliser la synthèse des faiblesses et des recommandations accompagnées des plans d'action appropriés. C'est une trace et également un document qui doit guider l'action.

Protocole de rédaction du rapport d'audit

- Classer les feuilles de révélation et d'analyse de problème : faiblesses classées par ordre de gravité décroissante et recommandations classées par ordre de priorité et d'insistance décroissantes.
- Rédiger le rapport : rapport validé par le chef de mission et le directeur de l'audit.
- Valider le rapport : rapport validé par le responsable de l'activité audité.
- Définir les plans d'action associés : actions définies par le responsable de l'entité auditée.

LIVRABLES SPÉCIFIQUES

EN PRATIQUE

Faites une première rédaction du rapport, sans censure, comme vous le sentez, cela fait du bien...

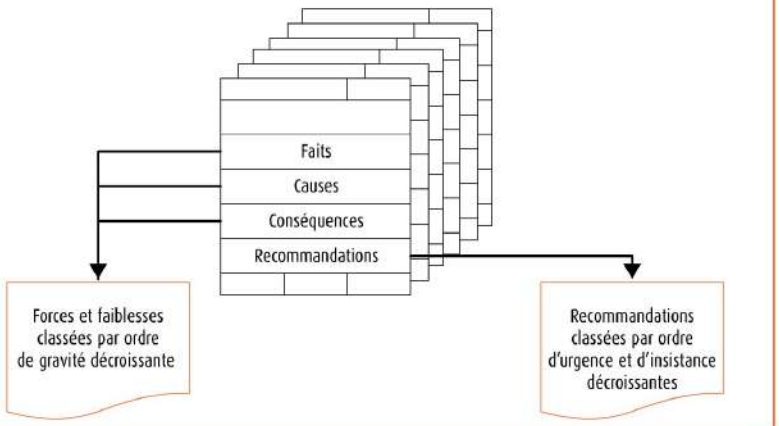
Assurez-vous que toutes les FRAP ont bien été reprises dans le rapport.

Reprenez une seconde fois le projet de rapport et adaptez ce que vous avez rédigé pour que celui-ci soit le plus utile possible.

Faites relire votre rapport par votre superviseur ou effectuez une lecture « à quatre yeux ».

Le Président est la seule personne à pouvoir autoriser la communication d'un rapport d'audit à l'extérieur de l'entreprise. Toute demande dans ce sens doit donc lui être soumise.

Figure 12.1 – Le processus de rédaction du rapport d'audit



LES STANDARDS DE QUALIFICATION

Les standards de qualification correspondent à des mots facilitant la rédaction de la partie « forces et faiblesses » du rapport d'audit. Leur objectif est de qualifier les forces et les faiblesses à une date donnée ou pour une période considérée et de rédiger des rapports d'audit homogènes les uns par rapport aux autres.

Protocole d'utilisation des standards de qualification

- Classer les forces et les faiblesses identifiées par ordre d'importance décroissante.
- Choisir pour chaque force et faiblesse le mot le plus adapté.
- Rédiger la partie « forces et faiblesses » en présentant :
  - les forces, de la plus importante à la moins importante ;
  - les faiblesses classées de la plus grave à la moins grave.

Figure 12.2 – Les standards de qualification d'une situation à un moment donné (exemple)

Très mauvaise	Désespérée Catastrophique Dramatique Critique Alarmante Déplorable Dangereuse
Mauvaise	Difficile Sérieuse Grave Inquiétante Préoccupante Épineuse Délicate Médiocre
Bonne	Passable Acceptable Convenable Honorable Positive Satisfaisante
Très bonne	Remarquable Exemplaire Excellente Parfaite Idéale

LIVRABLES SPÉCIFIQUES

EN PRATIQUE

Définissez et utilisez au sein de l'équipe un référentiel de standards de qualification unique. Attention, méfiez-vous des faux amis si vous traduisez votre liste dans une autre langue.

Figure 12.3 – Les standards de qualification de l'évolution d'une situation (exemple)

En détérioration constante (- vers --)	Délabrement (décisif) Dégradation (immense) Détérioration (capitale)
En détérioration (+ vers -)	Affaiblissement (important) Altération (sensible)
Sans évolution (- ou +)	Évolution (infime, insignifiante non significative)
En amélioration (- vers +)	Mieux (léger) Amélioration (modeste)
En amélioration constante (+ vers ++)	Redressement (marqué, significatif) Progrès (net)

LES TERMES DE HIÉRARCHISATION

Les termes de hiérarchisation sont des mots facilitant la rédaction du rapport d'audit. Leur objectif est de lier les informations entre elles dans un ordre logique, ce qui permet ensuite de rédiger un rapport d'audit structuré.

Protocole d'utilisation des termes de hiérarchisation

- Identifier les liens existant entre les idées.
- Choisir le terme le plus approprié.
- Rédiger les phrases en conséquence.

EN PRATIQUE

Définissez et utilisez au sein de l'équipe un référentiel de termes de hiérarchisation unique.

Figure 12.4 – Les termes de hiérarchisation (exemple)

Une idée peut en expliquer une autre	En effet Car Parce que
Une idée peut s'opposer à une autre, ou faire une concession	Mais Toutefois Cependant Pourtant Néanmoins En revanche Certes Par contre Au contraire À l'opposé Si Sauf que Excepté Malgré
Une idée peut être la conséquence d'une autre idée	Ainsi Alors Par suite Donc Par conséquent C'est pourquoi C'est la raison pour laquelle De ce fait
Une idée peut avoir une relation chronologique avec une autre	En premier lieu... En second lieu En premier... En dernier Tout d'abord... Puis... Ensuite... Enfin D'une part... D'autre part Hier, aujourd'hui, demain
Une idée peut s'additionner à une autre	Et Également En outre Par ailleurs De plus De surcroît De même Aussi En sus
Une idée peut être l'aboutissement des précédentes	Finalement En somme Au total En fin de compte En bref En conclusion Pour finir En résumé Pour conclure

LIVRABLES SPÉCIFIQUES

Copyright © 2014 Eyrolles.

LES EXPRESSIONS DE RECOMMANDATION

Les expressions de recommandation sont des mots facilitant la rédaction de la partie « Recommandations » du rapport d'audit. Leur objectif est de donner une priorité aux recommandations et de préciser le niveau d'engagement de l'auditeur.

Protocole d'utilisation des expressions de recommandation

- Classer les recommandations par ordre d'urgence et d'importance.
- Choisir dans les listes les termes les plus appropriés.
- Rédiger la partie « Recommandations » en présentant les recommandations classées par ordre décroissant d'importance.

EN PRATIQUE

Définissez et utilisez au sein de l'équipe un référentiel d'expressions de recommandation unique.

Figure 12.5 – Les expressions de recommandations caractérisant l'importance (exemple)

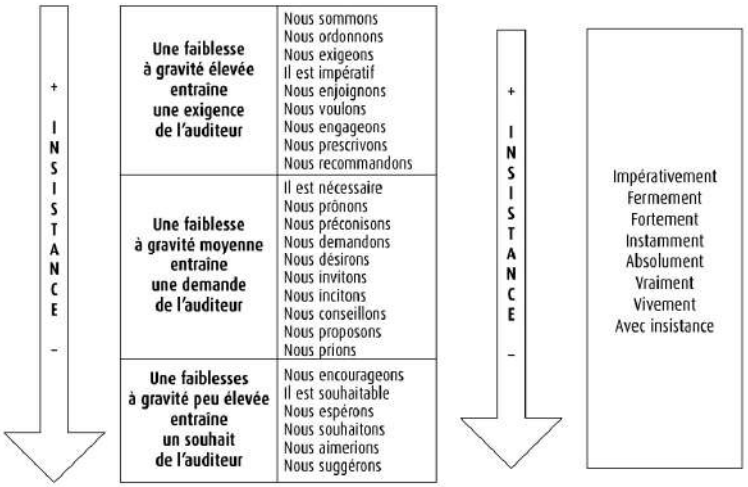
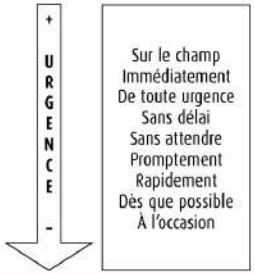


Figure 12.6 – Les expressions de recommandations caractérisant le degré d'urgence



Exemple

Rapport d'audit concernant l'évaluation des techniques de rédaction d'une équipe d'inspecteurs avec utilisation de standards de qualification, termes de hiérarchisation et expressions de recommandation.
FRAPs :

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 01
FAITS	CONSÉQUENCES
Les rapports ont un volume important : plus de 100 pages.	La lecture demande un temps très important. Le nombre de pages peut décourager le lecteur. Difficulté à distinguer ce qui est important de ce qui ne l'est pas.
CAUSES	RECOMMANDATIONS
Le nombre de pages est souvent synonyme de qualité. Les rapports sont essentiellement descriptifs.	Réduire le nombre de pages. Mettre tout ce qui est descriptif en annexes.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 02
FAITS	CONSÉQUENCES
Le contenu des rapports est essentiellement descriptif.	Le lecteur risque de lire des choses qu'il connaît déjà.
CAUSES	RECOMMANDATIONS
Le nombre de pages est souvent synonyme de qualité. Les rapports sont essentiellement descriptifs.	Réduire le nombre de pages. Mettre tout ce qui est descriptif en annexes.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 03
FAITS	CONSÉQUENCES
Les titres ne sont pas toujours explicites.	Cela renforce le côté littéraire, et donc peut orienter vers l'action.
CAUSES	RECOMMANDATIONS
Les titres sont considérés comme des introductions et non comme des conclusions partielles.	Utiliser systématiquement des titres journalistiques.

.../...

Copyright © 2014 Eyrolles.

.../...

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 04
FAITS	CONSÉQUENCES
Les informations ne sont pas hiérarchisées et classées par destinataire.	Impossibilité d'envoyer facilement le rapport vers plusieurs destinataires.
CAUSES	RECOMMANDATIONS
Volonté de rédaction littéraire.	Rédiger le rapport sous la forme de fiches indépendantes.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 05
FAITS	CONSÉQUENCES
La calligraphie n'est pas homogène (caractères fins, gras, en italique, encadrés, ...).	Ne facilite pas pour le lecteur l'identification de ce qui est important.
CAUSES	RECOMMANDATIONS
Absence de référentiel.	Définir des normes calligraphiques.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	Fiche n° : 06
FAITS	CONSÉQUENCES
Des jugements de valeur sur des personnes.	Risque de manque d'objectivité.
CAUSES	RECOMMANDATIONS
Difficulté à donner un jugement sur un comportement ou un style de management.	Être factuel.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	**Fiche n° : 07**
FAITS	**CONSÉQUENCES**
L'essentiel des rapports est consacré à la description des faiblesses.	Image du service de contrôle de policier.
CAUSES	**RECOMMANDATIONS**
Décrire est plus facile que proposer. Rôle historique du service du contrôle ?	Développer les recommandations et les points positifs.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	**Fiche n° : 08**
FAITS	**CONSÉQUENCES**
Feuille de synthèse des recommandations ne présente pas « qui ? » et « pour quand ? ».	Ne facilite pas le passage à l'action. Ne permet pas de savoir à quelle date les inspecteurs sont en droit d'estimer que les recommandations seront mises en place.
CAUSES	**RECOMMANDATIONS**
Volonté de laisser l'établissement libre de déterminer cela ?	Préciser « qui ? » et « pour quand » ?

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	**Fiche n° : 09**
FAITS	**CONSÉQUENCES**
La structure et les informations contenues ne permettent pas de comparer l'entreprise à une moyenne nationale.	L'entreprise ne peut se comparer qu'à elle-même.
CAUSES	**RECOMMANDATIONS**
Historiquement non demandé aux inspecteurs.	Sélectionner une dizaine de chiffres permettant de situer l'établissement par rapport à une moyenne nationale.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	**Fiche n° : 10**
FAITS	**CONSÉQUENCES**
Le vocabulaire utilisé n'est pas homogène.	Le lecteur ne peut pas comparer un rapport avec un autre. Une même faiblesse peut être qualifiée différemment selon l'inspecteur.
CAUSES	**RECOMMANDATIONS**
Absence de règles.	Définir des listes de mots pour qualifier la gravité des faiblesses ainsi que l'urgence et l'insistance des recommandations.

Audit rédaction rapports d'inspection	30/06/2014
Service du contrôle	**Fiche n° : 11**
FAITS	**CONSÉQUENCES**
Certaines séquences sont incomplètes : certains faits ne sont pas expliqués en terme de causes ou de conséquences ; certains faits ne donnent pas lieu à recommandation.	Le rapport peut être remis en cause, car il paraît incomplet. Certaines recommandations peuvent être inadaptées car ne traitant pas les causes.
CAUSES	**RECOMMANDATIONS**
Absence de validation systématique des séquences. Manque de méthodes de travail ?	Utiliser un support de classement de l'information garantissant la qualité des séquences « fait/conséquences/causes/recommandations ».

LIVRABLES SPÉCIFIQUES

Copyright © 2014 Eyrolles.

Rapport final :

Introduction

Nous avons procédé le 30 Juin à un rapide audit portant sur la qualité de rédaction des rapports d'inspection rédigés par les Inspecteurs de l'Inspection générale.
Cet audit, qui a porté sur trois rapports, nous conforte dans notre sentiment qu'il est souhaitable de revoir en profondeur la façon de rédiger les rapports d'inspection.

Principales faiblesses identifiées

Tout d'abord, il est inquiétant que les rapports d'inspection soient orientés vers la description des faiblesses plutôt que des recommandations, présentent des informations non hiérarchisées et non classées par destinataires et ne permettent pas de situer les performances de l'entité inspectée par rapport à des normes de performance nationales.

Ensuite, leur volume trop important, leur contenu essentiellement descriptif, les jugements de valeur qu'ils présentent, les informations incomplètes auxquelles ils font référence et des feuilles de synthèse ne présentant pas « qui ? », « doit faire quoi ? », « pour quand ? » rendent **délicate** la mise en œuvre des recommandations présentées.

Enfin, l'utilisation de titres pas toujours explicites, de règles calligraphiques et d'un vocabulaire non homogènes rend **difficile** la reconnaissance par les entités contrôlées d'un style « Inspection générale », véritable marque de fabrique.

Recommandations

Nous vous recommandons tout d'abord fortement et sans délai de donner aux rapports une orientation plutôt « recommandations » que « faiblesses », de hiérarchiser les informations (par gravité, par urgence et par insistance) et de les classer par destinataires et de situer les performances de l'entité inspectée par rapport à des normes de performance nationales.

Ensuite, nous vous invitons vivement et sans attendre à réduire le volume des rapports, à rendre leur contenu moins descriptif, à éviter tout jugement de valeur, à s'assurer que toute faiblesse soit complète : le fait, les conséquences, les causes et la recommandation et à présenter dans les feuilles de synthèse : « qui ? » doit faire « quoi ? », « pour quand ? ».

Enfin, nous vous encourageons à utiliser des titres explicites, des règles calligraphiques et un vocabulaire homogènes.

Conclusion

Le séminaire de formation des inspecteurs à la rédaction du rapport d'inspection intervient à une période favorable à une remise en cause, non seulement du contenu des rapports en particulier, mais aussi des méthodes de travail du service du contrôle en général.
C'est pourquoi le séminaire devra être suivi d'un certain nombre de travaux : conception d'imprimés, d'un référentiel de vocabulaire, de normes calligraphiques, mais aussi d'outils d'investigation et de règles d'intervention, ...

PAROLE D'EXPERT

Lawrence B. Sawyer, conclusion

« Eh bien, voilà mes dix commandements. Je suis sûr que certains vont chicaner, et diront qu'il y a un plus grand nombre de commandements ou qu'il y en a moins. Mais les dix commandements dont j'ai parlé m'ont été d'un grand secours depuis de nombreuses années. Je les recommande à chacun d'entre vous qui désire chercher à évaluer les opérations pour la direction, ce qui constitue le travail d'inspection moderne.

Lorsque l'inspecteur se conformera à ces commandements, en en suivant les principes de façon intelligente et avec imagination, il fera un pas de géant et sera bien près d'évaluer les opérations comme le ferait le président de la société, si celui-ci en avait le temps et savait le faire. »

TÉMOIGNAGE

Xavier Tremblay, expert-comptable, commissaire aux comptes, associé Rexco Conseils

Après une formation préparant au DEC (diplôme d'expertise comptable), j'ai intégré un grand cabinet d'audit français, Salustro-Reydel/KPMG, en tant qu'auditeur débutant. Au sein de ce cabinet, j'ai évolué pour devenir responsable de mission où j'ai pu développer mes compétences en gestion d'équipes et de dossiers de taille *middle market*. Ensuite, j'ai donné une nouvelle orientation à ma carrière en intégrant en tant qu'associé, la société Rexco Conseils, cabinet d'expertise comptable basé à Boulogne-Billancourt regroupant deux associés, cinq experts-comptables/commissaire aux comptes, une vingtaine de collaborateurs regroupés dans différents pôles : expertise comptable, commissariat aux comptes, fiscal et juridique, et externalisation.

Les métiers de l'expertise comptable et du commissariat aux comptes partagent des socles de connaissance et des voies d'accès communs. Néanmoins, ces métiers demeurent très différents. L'expert-comptable tient la comptabilité et présente les comptes. Quant au commissaire aux comptes, il intervient dans un cadre légal, en respectant des normes d'exercice professionnel, issues des normes internationales d'audit, adaptées au contexte national de la Compagnie nationale des commissaires aux comptes (CNCC) et homologuées par le ministère de la Justice. Le commissaire aux comptes certifie la régularité et la sincérité des comptes. Il apprécie le contrôle interne et les systèmes d'information des entités qu'il contrôle. Le commissaire aux comptes a aussi d'autres prérogatives notamment le droit d'alerte sur des faits de nature à compromettre la continuité de l'exploitation de la société et le cas échéant la révélation au procureur de la République de tout fait délictueux qu'il aurait découvert au cours de sa mission.

Ce rôle comporte de grandes responsabilités et requiert :

- de larges compétences techniques dans les domaines notamment de la comptabilité, de la fiscalité, de la finance, du droit et de l'informatique ;
- une ouverture sur le monde économique ;
- une capacité d'analyse et de synthèse ;
- un sens de l'esprit critique ;
- de bonnes capacités relationnelles et rédactionnelles.

En résumé

Cette troisième partie a présenté l'activité des métiers d'auditeur interne et de contrôleur permanent au quotidien et plus précisément :

- la description des travaux à réaliser dans le cadre du cycle annuel de l'audit interne et du contrôle permanent ;
- les outils communs aux deux métiers :
- les compétences que les auditeurs internes et contrôleurs permanents doivent posséder ou développer ;
- la démarche de conduite d'une mission d'audit interne et les outils spécifiques correspondants ;
- cinq témoignages illustrant nos propos :
  - Manon Mourier des Gayets a montré en quoi l'audit interne et les Commissaires aux Comptes permettent de donner aux contributeurs la garantie d'une gestion rigoureuse et transparente des fonds collectés par l'ONG SOS Sahel International France,
  - Éric Guilhou a montré l'importance de disposer d'un référentiel de contrôle interne dans une entreprise de service telle Socotec, notamment dans un contexte de changements permanents,
  - Patrick Georgelin a montré quant à lui que le contrôle interne ne se limite pas aux organisations de taille importante mais concerne également les PME-PMI et suppose d'être confié à une personne de toute confiance,
  - Olivier Faujour a insisté sur les profils et qualités que les auditeurs internes doivent posséder pour être en mesure de contribuer pleinement au développement d'une entreprise internationale telle que Yoplait,
  - Xavier Tremblay a présenté l'exercice des métiers d'expert comptable et de commissaire aux comptes tels que normés par la Compagnie nationale des commissaires aux comptes ;
- les septième, huitième, neuvième et dixième commandements de Lawrence B. Sawyer : « connaître l'effet », « connaître les personnes », « savoir communiquer et à quel moment » et « connaître les méthodes modernes ».

Le questionnaire qui termine cette troisième partie va maintenant vous permettre de tester vos connaissances…

TEST DE CONNAISSANCE

Ce questionnaire a pour objectif de vous aider à faire le point sur vos connaissances des métiers de l'audit interne et du contrôle permanent et plus précisément sur l'exercice des métiers d'auditeur interne et de contrôleur permanent au quotidien.

Pour ce faire :

- répondez aux questions ci-après en choisissant pour chacune d'entre elles : « je pense » ou « je ne pense pas » ;
- à chaque fois que vous avez répondu : « je ne pense pas », à une question, relisez le passage du livre indiqué.

Questions

1. Le programme d'audit présente les contrôles de troisième niveau dits « périodiques » qui seront réalisés sous la forme de missions d'audit par l'audit interne dans l'année. Le plan de contrôle présente les contrôles de deuxième niveau dits « permanents » qui seront réalisés sur place ou à distance selon une périodicité déterminée par les équipes du contrôle permanent.

   (Réponse : chapitre 8, le programme d'audit et le plan de contrôle, p. 159.)

2. La fiche de risque constitue la carte d'identité d'un risque.

   (Réponse : chapitre 8, la fiche de risque, p. 167.)

3. La méthode AMDEC est une technique multidisciplinaire d'analyse de risque utilisée pour déterminer les modes de défaillance potentiels d'un procédé ou d'un produit (la sévérité de leurs effets et la probabilité d'occurrence) et les causes et mécanismes associés avec chaque mode de défaillance (l'habileté à les détecter).

   (Réponse : chapitre 9, la méthode AMDEC, p. 169.)

4. Dans le cadre d'un domaine comptable, les auditeurs internes et contrôleurs permanents réalisent des tests afin de s'assurer que celui-ci est juste et sincère.

   (Réponse : chapitre 9, les fondamentaux du domaine comptable, p. 173.)

5. La sécurité des systèmes d'information repose sur quatre facteurs qui s'appliquent aux flux, aux traitements et aux données et que sont la disponibilité, l'intégrité, la confidentialité, le contrôle et la preuve.

   (Réponse : chapitre 9, les fondamentaux d'un système d'information, p. 174.)

6. La moyenne, la médiane, le mode, l'étendue et l'écart type sont des valeurs qui permettent à l'auditeur interne ou au contrôleur permanent de caractériser une distribution de résultats autour d'une valeur centrale.

   (Réponse : chapitre 9, les indicateurs de tendance centrale, p. 180.)

7. Le sondage, effectué sur une partie de la population, permet à l'auditeur interne ou au contrôleur permanent de déterminer une caractéristique particulière qu'il est possible d'extrapoler au niveau de la population tout entière. Ils peuvent être réalisés sur des populations dénombrées ou non dénombrées.

   (Réponse : chapitre 9, les sondages, p. 189.)

8. L'hexamètre de Quintilien est un outil constitué d'une check-list de questions types permettant à l'auditeur interne ou au contrôleur permanent de guider l'analyse exhaustive d'une situation.

   (Réponse : chapitre 9, l'hexamètre de Quintilien, p. 195.)

9. Le diagramme de circulation (*flow-chart*) est une représentation schématique et symbolique d'un processus qui permet à l'auditeur interne ou au contrôleur permanent de faire apparaître très clairement : les tâches effectuées, leur chronologie et les différents acteurs qui y participent ; les documents qui les transcrivent, leur nombre d'exemplaires, leur distribution et leur classement ; les contrôles associés aux différentes tâches.

   (Réponse : chapitre 9, le diagramme de circulation, p. 204.)

10. La feuille de révélation et d'analyse de problème (FRAP) est le papier de travail synthétique qu'utilise l'auditeur interne ou le contrôleur permanent pour présenter et documenter chaque « révélation ».

    (Réponse : chapitre 9, la feuille de révélation et d'analyse de problème, p. 212.)

TEST DE CONNAISSANCE
Copyright © 2014 Eyrolles.

11. La carte des forces permet à l'auditeur interne ou au contrôleur permanent d'évaluer la capacité de changement des personnes d'une entité auditée ou contrôlée au niveau individuel de chacune des personnes qui la compose et pareillement au niveau collectif.

    (Réponse : chapitre 9, la carte des forces de Christian Fauvet, p. 220.)

12. La véritable difficulté des métiers d'auditeur interne et de contrôleur permanent n'est pas l'aspect de diagnostic mais plutôt ce qui a trait à l'humain.

    (Réponse : chapitre 10, les compétences relationnelles et comportementales, p. 227.)

13. L'auditeur interne et le contrôleur permanent doivent maîtriser l'art de la communication, et celle-ci est verbale et non verbale.

    (Réponse : chapitre 10, la communication verbale et non verbale, p. 234.)

14. Avec une écoute active, il est possible à l'auditeur interne et au contrôleur permanent d'obtenir quatre choses de la personne interviewée : de l'information, de la confiance, du confort et de la volonté à continuer à communiquer.

    (Réponse : chapitre 10, l'écoute active, p. 238.)

15. Les critères de lisibilité, appelés aussi les indices de brouillard, permettent de qualifier un texte sous l'angle de sa facilité de compréhension et de de mémorisation.

    (Réponse : chapitre 10, les critères de lisibilité, p. 247.)

16. La méthode « E.S.P.R.I.T. » constitue une aide précieuse dans la rédaction de livrables à caractère technique tel qu'un document technique. En effet, cette méthode suscite l'intérêt du lecteur de par la disposition des informations.

    (Réponse : chapitre 10, la méthode « E.S.P.R.I.T. », p. 250.)

17. La méthode Minto permet d'aider à la détermination d'un fil conducteur favorisant la démonstration et de faciliter l'attention et l'adhésion d'un groupe lors de la présentation de résultats ou de conclusions.

    (Réponse : chapitre 10, la méthode Minto, p. 252.)

18. La performance d'un groupe repose sur la qualité des personnes qui le constituent ainsi que sur leurs complémentarités.

    (Réponse : chapitre 10, les profils caractéristiques de Mérédith Belbin, p. 253.)

19. Le niveau de performance d'un collaborateur dépend en grande partie du style de management que son responsable hiérarchique adopte à son égard. Il n'y a pas de style de management idéal, mais des styles plus ou moins adaptés aux situations.

(Réponse : chapitre 10, le management situationnel d'Hersey et Blanchard, p. 256.)

20. Préalablement à la réalisation de la mission, les auditeurs internes étudient les informations utiles qu'il est possible de collecter concernant le domaine à auditer. Ces travaux vont permettre de constituer un référentiel du domaine à auditer, de mener une analyse de risques et de préciser l'objectif de la mission.

(Réponse : chapitre 11, l'étude préliminaire, p. 266.)

21. Le programme de travail s'établit sur la base de la note d'orientation. Il est destiné à définir, répartir, planifier et suivre les travaux des auditeurs.

(Réponse : chapitre 11, la préparation du programme de travail, p. 268.)

22. Le travail sur le terrain consiste à conduire les contrôles prévus dans le programme de travail en utilisant les outils d'audit interne adéquats.

(Réponse : chapitre 11, les tests d'audit, p. 269.)

23. Avant de quitter le site, une réunion est organisée avec l'encadrement de l'entité auditée afin de clôturer la phase de vérification par une restitution orale.

(Réponse : chapitre 11, la réunion de clôture de la phase de vérification, p. 269.)

24. L'objectif de la validation est d'intégrer la réponse des personnes auditées dans le rapport et d'obtenir leur accord tacite pour les observations et les axes de recommandation proposés.

(Réponse : chapitre 11, la réunion de validation, p. 271.)

25. La lettre de mission constitue la matérialisation du mandat donné par la direction générale à l'audit interne, qui informe les responsables du domaine concerné de l'intervention prochaine des auditeurs.

(Réponse : chapitre 12, la lettre de mission, p. 277.)

TEST DE CONNAISSANCE

26. La note d'orientation, rédigée par le chef de mission et revue par son responsable, définit et formalise les axes d'investigation de la mission et ses limites : elle les exprime en objectifs à atteindre par l'audit interne pour le commanditaire et les personnes auditées.

(Réponse : chapitre 12, la note d'orientation, p. 280.)

27. La feuille de couverture est un document établi en deux temps qui décrit les modalités de mise en œuvre d'une tâche définie dans le programme de travail et met par la suite en évidence les conclusions qui en ont été tirées.

(Réponse : chapitre 12, la feuille de couverture, p. 281.)

28. Le projet de rapport, après la réunion de validation et les mises à jour constitue le « rapport définitif ». Il se compose d'une synthèse destinée à être lue par les dirigeants, des fiches FRAP examinées lors de la réunion de validation et d'une liste des recommandations classées par destinataires précisant la position des audités et constituant de fait leur première réponse à l'audit.

(Réponse : chapitre 12, le rapport d'audit, p. 282.)

29. Les standards de qualification correspondent à des mots facilitant la rédaction de la partie « Forces et faiblesses » du rapport d'audit. Leur objectif est de qualifier les forces et les faiblesses à une date donnée ou pour une période considérée et de rédiger des rapports d'audit homogènes les uns par rapport aux autres.

(Réponse : chapitre 12, les standards de qualification, p. 285.)

30. Les termes de hiérarchisation sont des mots facilitant la rédaction du rapport d'audit. Leur objectif est de lier les informations entre elles dans un ordre logique, ce qui permet ensuite de rédiger un rapport d'audit structuré.

(Réponse : chapitre 12, les termes de hiérarchisation, p. 287.)

31. Les expressions de recommandation sont des mots facilitant la rédaction de la partie « Recommandations » du rapport d'audit. Leur objectif est de donner une priorité aux recommandations et de préciser le niveau d'engagement de l'auditeur.

(Réponse : chapitre 12, les expressions de recommandation, p. 288.)

Conclusion

Les métiers d'auditeur interne et de contrôleur permanent font partie du dispositif de maîtrise des risques de l'entreprise. Ils permettent le suivi du fonctionnement au quotidien et également la revue périodique des organisations et des systèmes sous l'angle de leurs risques, de leur conformité réglementaire et également de leur efficacité et de leur efficience.

Comme l'ont illustré les personnes qui ont apporté leur témoignage dans cet ouvrage, ces deux métiers peuvent s'exercer aussi bien dans le secteur privé qu'au sein des administrations publiques, dans les associations, les sociétés de conseil en management et en organisation d'entreprises ou encore les cabinets d'audit. Ils apportent aux professionnels exerçant des métiers à risques et également aux conseils d'administration, présidents et dirigeants d'entreprise des informations précieuses pour prendre des décisions.

Leurs champs d'intervention sont très variés et vont des processus de pilotage de l'entreprise (stratégie, gouvernance, budgets…) aux processus supports (comptabilité, ressources humaines, achats, moyens généraux, système d'information…) en passant par les processus opérationnels (recherche et développement, marketing, commercial, production…).

Ce sont des métiers passionnants, que l'on peut choisir de pratiquer pour un temps, comme en début, en milieu ou en fin de carrière, ou encore même d'y faire toute sa carrière. Ils demandent quelques prédispositions de base, telles l'honnêteté intellectuelle, la capacité d'engagement, le sens de la relation, le goût du travail bien fait, le goût de l'analyse et de la synthèse, la résistance à une lourde charge de travail permanente…

Ils permettent d'acquérir des connaissances variées. En ce sens, ils ne peuvent être considérés comme des métiers reposants mais plutôt comme des métiers exigeants. En contrepartie, ils permettent de passer ses journées à faire des choses intellectuellement intéressantes (analyser, apprendre, comprendre, rechercher), utiles, et accessoirement pas trop mal rémunérées… autant de raisons méritant que l'on s'y attarde un peu, non ?

Le sinistre de Fukushima

Le vendredi 11 mars 2011 à 14 h 46 min 23 s heure locale, a lieu le plus important séisme mesuré au Japon. Son épicentre se situe à 130 kilomètres à l'est de Sendai, chef-lieu de la préfecture de Miyagi, dans la région du Tohoku, ville située à environ 300 kilomètres au nord-est de Tokyo. Cinquante et une minutes plus tard, un tsunami provoqué par le tremblement de terre aborde la côte orientale. La vague atteint une hauteur estimée à plus de 30 mètres par endroits, parcourant jusqu'à 10 kilomètres à l'intérieur des terres, ravageant près de 600 kilomètres de côtes et détruisant partiellement ou totalement de nombreuses villes et zones portuaires. Le séisme entraîne un arrêt automatique des réacteurs nucléaires en service, la perte accidentelle de l'alimentation électrique et le déclenchement des groupes électrogènes. L'observation d'émissions de xénon, avant même la première dépressurisation volontaire du premier réacteur nucléaire, indique des dommages structurels probables dans la partie nucléaire des installations immédiatement après le séisme. À la suite du tsunami provoqué par le séisme, des groupes électrogènes de secours tombent en panne. Ces défaillances, couplées à plusieurs erreurs humaines aussi bien de fond que concernant les pratiques, causent l'arrêt des systèmes de refroidissement de secours des réacteurs nucléaires ainsi que ceux des piscines de désactivation des combustibles irradiés. Le défaut de refroidissement des réacteurs induit des fusions partielles des cœurs des trois réacteurs nucléaires puis d'importants rejets radioactifs. Il s'agit d'un accident nucléaire majeur classé au niveau 7 (le plus élevé) de l'échelle internationale des événements nucléaires, ce qui le place au même degré de gravité que la catastrophe de Tchernobyl (1986), compte tenu du volume important des rejets. À ce jour, trois ans après l'accident, les conséquences du tsunami sur le site de Fukushima ne sont pas traitées à 100 % ne sont toujours pas stabilisées…

ANNEXES

Le vocabulaire du contrôle

Analyse des risques – Démarche d'audit visant à recenser les risques et les sources potentielles d'anomalies concernant le « produit »/« service » audité.

Analyse qualitative – Analyse des causes, contrôles, effets et facteurs de quantification des incidents potentiels recensés dans le cadre de l'évaluation des risques opérationnels.

Analyse quantitative – Détermination de la fréquence et de la sévérité du cas vraisemblable (*likely case*) et du pire des cas (*worst case*) dans le cadre de l'évaluation des risques opérationnels.

***Appétence pour le risque (*risk appetite)** – Reflet de l'approche du management des risques d'une entité. Elle influence sa culture et son style de management. La définition de la stratégie doit tenir compte et rester cohérente avec l'appétence pour le risque. L'appétence pour le risque de l'entité est un point de repère dans le cadre de la détermination de la stratégie. Elle guide l'affectation des ressources. Elle permet la mise en adéquation de l'organisation, des hommes, des processus et de l'infrastructure de l'organisation.

Archivage – Conservation d'informations pendant une durée déterminée en vue d'une éventuelle consultation ultérieure.

Assurance – Technique qui permet de transférer un risque moyennant le paiement d'une prime à un tiers qui accepte, en contrepartie, de prendre ce risque à sa charge. En matière de finance, prendre une « option » revient à prendre une assurance.

Assurance raisonnable – Concept selon lequel le dispositif de management des risques, aussi clairement défini et appliqué soit-il dans l'organisation, ne peut garantir l'atteinte systématique des objectifs en raison de ses limites inhérentes.

Audit d'efficacité (ou audit de performance) – Opinion sur la qualité des procédures. Le référentiel devient une abstraction, résultante de l'appréciation de l'auditeur.

Audit de management – Évaluation de la mise en œuvre sur le terrain des politiques et stratégies de l'entreprise.

Audit de régularité (ou audit de conformité) – Vérification de la bonne application des règles et procédures de l'entreprise.

Audit de stratégie – Évaluation de la cohérence globale des politiques et stratégies d'entreprise avec l'environnement de l'entreprise.

Audit interne – Entité ayant la responsabilité d'évaluer le fonctionnement du dispositif de contrôle interne et de faire toutes les préconisations pour l'améliorer, dans le champ couvert par ses missions.

Back-up – Existence d'une solution de repli en cas d'indisponibilité de la personne ou du système en charge du contrôle.

BCM (Business Continuity Management) – Ensemble des solutions permettant d'assurer la continuité des activités critiques d'une entreprise.

BCP (Business Continuity Program) – Processus continu de gestion et de gouvernance soutenu par la direction de l'entreprise et qui dispose des moyens adéquats pour garantir, en cas de survenance d'un incident, la continuité des activités à un niveau de performance conforme à ce qui a été défini. Ce processus conduit à passer par différentes étapes, et en particulier : l'identification des impacts, l'expression des besoins en continuité, la définition et la maintenance des stratégies et des plans de secours, la réalisation d'exercices.

BIA (Business Impact Analysis) – Étude qualitative et quantitative des impacts et des pertes pouvant résulter d'un incident majeur. Elle est complétée par une analyse des risques que des menaces avérées ou potentielles font peser sur l'entreprise.

Blanchiment de capitaux – Processus qui consiste à injecter de l'argent d'origine criminelle dans les circuits réels ou fictifs d'une activité en apparence respectable afin d'en dissimuler l'origine.

Cartographie des processus – Représentation de l'entreprise à travers les liens entre ces différents processus métiers, de pilotage et supports.

Cartographie des risques opérationnels – Outil indispensable de gestion des risques opérationnels dont la responsabilité et la mise à jour sont confiées au management opérationnel des entités/*business unit*. Processus dynamique et adapté à l'activité, à ses évolutions et au niveau de tolérance au risque que les entités ont défini (concept de *risk tolerance*). La cartographie des risques opérationnels constituée doit permettre de :

- disposer d'une première vision macro des principales zones de risque d'une entité, par processus, grand domaine fonctionnel ou nature de risque ;
- mettre en regard de ces risques le dispositif de contrôle au sens large (principes organisationnels, procédures, contrôles…) et juger de son efficacité en fonction de la tolérance au risque de l'entreprise ;
- fournir un outil de suivi dynamique du profil de risque de l'entreprise ;
- définir les actions de prévention et de correction des risques et assurer le suivi de leur mise en œuvre.

Les grandes étapes de la cartographie des risques sont :

- l'analyse des risques sous-jacents, dont l'objet est de mettre en lumière les principales zones d'exposition récurrente au risque, par grand type d'événement et d'obligations réglementaires ;
- l'analyse du dispositif de contrôle, qui vise à évaluer la qualité des mesures mises en place afin de réduire le niveau de risque sous-jacent ;
- l'analyse d'indicateurs dynamiques de risques, qui doivent permettre d'évaluer les distorsions, existantes ou à venir, par rapport aux situations évaluées lors des étapes précédentes.

Cas vraisemblable (likely case) – Cas le plus fréquent de l'incident potentiel de risque opérationnel. Il représente la situation que l'on rencontrera le plus couramment lorsque l'incident potentiel se produira.

Catégorie d'objectifs – L'une des quatre catégories d'objectifs d'une organisation, à savoir : l'atteinte des objectifs stratégiques ; la réalisation et l'optimisation des opérations ; la fiabilité des reportings ; la conformité aux lois et règlements applicables. Ces catégories se recoupent. Ainsi un objectif donné peut appartenir à plusieurs catégories.

Cause – Le ou les facteurs internes ou externes à l'entreprise qui sont à l'origine d'événements avérés ou potentiels de pertes. L'étude et la résolution des causes permettent de diminuer la fréquence d'occurrence des événements et la sévérité de leurs impacts lorsqu'ils surviennent.

Comité d'audit – Groupe de travail issu de l'organe de contrôle d'une société (le conseil d'administration ou le conseil de surveillance) chargé de surveiller la gestion confiée au dirigeant (le directeur général ou le directoire). Il est souvent chargé d'analyser les comptes et le dispositif de contrôle arrêtés par le dirigeant.

Commissaire aux comptes – Personne habilitée par la loi à vérifier la régularité, la sincérité et l'image fidèle des comptes en certifiant les documents comptables.

Confidentialité (C) – Propriété qui assure la tenue secrète des données d'un système d'information avec accès aux seules entités autorisées.

Copyright © 2014 Eyrolles. © Groupe Eyrolles

Contrefaçon – Reproduction à l'identique. Elle consiste à refabriquer entièrement un support non authentique, différent de l'original qui contient des signes de sécurité. Les éléments de sécurité peuvent être imités, mais les faux sont assez aisément repérables pour les initiés de base. Aux yeux de la loi, la contrefaçon constitue un délit.

Contrôle – Vérification de la conformité des opérations et des processus à une ou à des normes ou règles ainsi que de la bonne mise en œuvre des procédures internes. Le contrôle consiste en une vérification qui peut être le résultat d'un processus automatisé ou non réalisé préalablement à l'exécution de l'opération ou du processus (contrôle *a priori*, permettant d'éviter la matérialisation d'un risque ou un incident) ou postérieurement (contrôle *a posteriori*, permettant de limiter, voire d'annihiler, l'impact d'un incident). La mise en place d'un contrôle découle de l'identification et de l'analyse en profondeur d'un risque, de ses causes et de ses effets. Les contrôles sont mis en place pour assurer que les opérations ou les processus sont conformes aux standards, règlements ou procédures internes. Les principaux objectifs des contrôles sont :

- la prévention ou la mitigation d'un risque est prise en compte conformément à la tolérance au risque de l'entité ;
- la prévention d'un risque ou la limitation de son impact en le détectant précocement ; le positionnement de chaque contrôle au meilleur endroit du processus ;
- l'organisation du contrôle de façon formelle et décrite en détail dans une procédure, démontrant l'existence d'un dispositif formalisé de mitigation du risque.

Un contrôle est forcément lié à un risque quelle qu'en soit la nature. Un contrôle doit être proportionné au risque considéré et à la tolérance au risque définie par l'entité. Les contrôles doivent être : en adéquation avec les plans de contrôle définis par les responsables opérationnels et fonctionnels ; adaptés à leur environnement ; décrits dans des procédures.

Contrôle et preuves (P) – Faculté de vérifier le bon déroulement d'une fonction d'un système d'information. Non-répudiation : impossibilité pour une entité de nier avoir reçu ou émis un message.

Contrôle de troisième niveau – Contrôles exercés par l'audit interne. On parle de contrôle périodique.

Contrôle interne – Dispositif de l'entreprise défini et mis en œuvre sous sa responsabilité qui vise à assurer :

- la conformité aux lois et règlements ;
- l'application des instructions et des orientations fixées par la direction générale ou le directoire ;
- le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde de ses actifs ;

- la fiabilité des informations financières et, d'une façon générale, qui contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources.

En contribuant à prévenir et maîtriser les risques de ne pas atteindre les objectifs que s'est fixés la société, le dispositif de contrôle interne joue un rôle clé dans la conduite et le pilotage de ses différentes activités. Toutefois, le contrôle interne ne peut fournir une garantie absolue que les objectifs de la société seront atteints. Le contrôle interne est donc un processus mis en œuvre par le conseil d'administration ou le conseil de surveillance, les dirigeants et le personnel d'une organisation qui est destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs. Les grands principes du contrôle interne :

- le contrôle interne est un processus ; il est assuré par des personnes et il est l'affaire de tous ;
- le contrôle interne ne peut fournir qu'une assurance raisonnable ;
- le contrôle interne est adapté à la réalisation d'objectifs. Le contrôle interne est complété par le contrôle externe (régulateurs, commissaires aux comptes…).

Contrôle majeur (ou contrôle clé) – Contrôle couvrant un risque majeur, c'est-à-dire un risque dont la matérialisation aurait un effet important sur les résultats, les actifs ou la réputation de l'entreprise ou de l'une de ses entités. Les contrôles permettent de répondre à un risque sous-jacent évalué lors de l'exercice de cartographie des risques.

Contrôle périodique – Contrôle assuré par l'audit interne qui conduit des missions d'investigation dans tout domaine, résultant soit du plan d'audit, soit d'une demande de la direction générale ou d'un responsable opérationnel ou fonctionnel, soit de son autosaisine ; qui évalue le dispositif de contrôle permanent du groupe ; qui évalue la bonne mise en œuvre des stratégies définies par le groupe ; plus généralement, qui formule toute recommandation permettant d'améliorer le fonctionnement de l'entreprise.

Contrôle permanent – Contrôle au quotidien réalisé par les opérationnels et leur hiérarchie dans le cadre du traitement des opérations ; par le contrôle interne (deuxième niveau), la gestion des risques et le contrôle de la conformité.

Contrôler – Action de réguler, d'établir ou mettre en place une politique qui génère un ou plusieurs contrôles.

Contrôles de premier niveau – Autocontrôles exercés par les opérationnels sur leurs opérations/transactions :

- contrôles indépendants exercés par d'autres opérationnels (*middle office* et *back office*, contrôles croisés…) ;
- contrôles hiérarchiques exercés par l'encadrement.

Les contrôles de premier niveau relèvent du contrôle permanent. Ils sont du ressort des directions opérationnelles, commerciales et financières. Ils font partie intégrante des procédures des directions concernées. Ils sont constitués de bonnes pratiques, d'autorisations préparées (tiers, opérations, ressources, conditions…) et d'autocontrôles sélectionnés pour assurer à eux seuls la bonne régularité et la bonne fin des opérations. Ils sont effectués et documentés systématiquement et au fil de l'eau par les collaborateurs dans le cadre de leur travail et par certains collaborateurs à qui la hiérarchie peut les déléguer.

Ces contrôles peuvent s'appuyer sur les applications de traitement, grâce notamment aux éléments de sécurité logique (profils utilisateurs, gestion des droits…). La hiérarchie assure le management opérationnel des contrôles de premier niveau (analyse de risque, proposition de contrôles de premier niveau, documentation des procédures, recherche des validations nécessaires, attribution/formation/surveillance des contrôles de premier niveau, enregistrement et analyse des incidents, exploitation des reportings des risques et de contrôle de second et troisième niveaux). Ce dispositif de premier niveau doit s'ajuster en fonction de l'organisation, de l'activité et de la stratégie de l'entreprise.

Contrôles de deuxième niveau – Contrôles exercés par des fonctions de contrôle permanent indépendantes des entités. Ils permettent de vérifier la conformité, la sécurité et la validation des opérations réalisées ainsi que le respect des autres diligences liées à la surveillance des risques de toute nature qui leur sont associés. Ces contrôles portent sur l'ensemble des directions opérationnelles, commerciales et financières. Le seuil et la fréquence de ces contrôles de second niveau sont fondés sur une évaluation des risques et ajustés aux moyens de contrôle à disposition. Le plan de contrôle annuel est présenté aux organes de gouvernance de l'entreprise. Les contrôles sont effectués au travers d'investigations indépendantes, à l'aide d'outils spécifiques si nécessaire, portant :

- Soit sur les procédures (vérification par sondage de l'application des contrôles de premier niveau prévus aux procédures), dans le cadre de programmes de contrôles déterminés ou dans celui de revues plus globales aboutissant à un rapport sur telle ou telle activité. L'objectif est de tenir à disposition des managers opérationnels, de la direction et de la gouvernance une photo d'ensemble du fonctionnement du dispositif de contrôle interne.
- Soit sur les opérations elles-mêmes (analyse de la nature et des conditions de réalisation de certaines opérations), au fil de l'eau ou dans le cadre de l'analyse d'alertes développées au sein du dispositif de contrôle interne ou d'enquêtes appropriées à la compréhension d'incidents éventuels, à leur remédiation et à leur suivi. Le contrôle de deuxième niveau peut prendre la forme d'un « deuxième regard » sur des opérations, transactions et activités. Ce « deuxième regard » permet à la fonction qui l'exerce d'« escalader », si nécessaire, les décisions à un niveau supérieur de l'organisation.

Contrôles de troisième niveau – Contrôles exercés par l'audit interne.

COSO – Committee of Sponsoring Organizations of the Treadway Commission.

Crise – Situation caractérisée par une instabilité remettant en cause le fonctionnement normal d'une organisation et obligeant à adopter une gouvernance spécifique dite « de gestion de crise » pour revenir à un mode normal.

Criticité d'un risque – Produit de la fréquence par la sévérité. Elle correspond à l'espérance mathématique de la gravité. La criticité d'un risque est donc un indicateur de l'acuité du risque.

Criticité des contrôles – Échelle de mesure de 1 à 3 cohérente avec l'évaluation des risques correspondants. Pour les contrôles de premier niveau, on aura une distinction majeur/non majeur. Pour les contrôles de deuxième niveau, on appliquera cette notion de criticité du contrôle selon une échelle de 1 à 3 (élevé, moyen, faible).

Critique – Niveau d'un risque qui entraînerait des pertes financières, commerciales et organisationnelles importantes, voire inacceptables, ou des préjudices majeurs d'ordre judiciaire, et qui obligerait à prévoir des mesures de sécurité.

Culture du risque – Attitudes et croyances partagées par la direction d'une entreprise caractérisant sa stratégie et la perception du risque au sein des activités. Elle est le reflet des valeurs de l'entité. Elle influence sa culture au sens large et son style de management. Elle impacte la façon dont les éléments du management des risques sont mis en œuvre. Elle impacte également la manière dont les événements sont identifiés, le type de risques qui sont acceptés et la façon dont ils sont gérés. Elle doit être déployée et comprise, et bénéficier de l'adhésion de tous les collaborateurs de l'organisation. Elle transparaît dans les politiques, les communications orales et écrites, ainsi que dans le processus de prise de décision. Le management véhicule cette culture non seulement par ses paroles mais également par ses actions quotidiennes.

Défaillance de processus – Rupture ou défaut dans les chaînes de traitement ou dans les enchaînements d'activités ayant pour conséquence la non-réalisation de l'objectif attendu.

Degré d'automatisation – Caractère plus ou moins automatisé d'un contrôle, en général *via* une solution informatique ; l'automatisation peut être complète ou partielle.

Délégation de pouvoir – Signifie que la direction générale abandonne le contrôle de certaines décisions à des niveaux hiérarchiques inférieurs, c'est-à-dire aux personnes plus directement impliquées dans les transactions quotidiennes. La délégation de pouvoirs fixe la mesure dans laquelle les individus et les équipes sont autorisés et encouragés à faire preuve d'initiative afin de résoudre certaines questions ou problèmes. Par ailleurs, elle permet de définir les limites du pouvoir délégué. Ces délégations déterminent les relations

hiérarchiques et les protocoles d'autorisation. Les politiques décrivent les pratiques professionnelles appropriées, le savoir-faire et l'expérience des collaborateurs clés ainsi que les ressources nécessaires. Les individus savent de quelle manière leurs actions sont liées les unes aux autres et contribuent à l'atteinte des objectifs.

Développement durable – Développement qui répond aux besoins du présent sans compromettre la capacité des générations futures de répondre aux leurs. Deux concepts sont inhérents à cette notion : le concept de besoins, et plus particulièrement des besoins essentiels des plus démunis, à qui il convient d'accorder la plus grande priorité, et l'idée des limitations que l'état de nos techniques et de notre organisation sociale impose sur la capacité de l'environnement à répondre aux besoins actuels et à venir.

Disponibilité (D) – Aptitude des systèmes d'information à remplir une fonction dans des conditions prédéfinies d'horaires, de délais et de performances.

Dispositif de maîtrise des risques (DMR) – Réponses prudentielle (limites d'activités), organisationnelles, de procédures et de systèmes visant à réduire un risque.

Données historiques (*historical data*) – Incidents avérés de risque opérationnel internes ou externes. Elles constituent l'un des piliers de l'infrastructure de gestion du risque opérationnel. L'analyse de leurs causes et effets doit permettre de prendre des mesures correctrices, avec l'objectif d'améliorer et de sécuriser les processus.

Données prospectives (*forward looking*) – Informations sur l'exposition aux événements et risques potentiels.

Échantillon – Petite quantité d'une population, destinée à faire apprécier le tout. L'échantillon est donc une fraction représentative d'un certain type de population. L'échantillonnage est réalisé pour des raisons de coûts ou de délais. L'objectif est alors de construire un échantillon tel que les observations pourront être généralisées à l'ensemble de la population. Il existe deux méthodes pour constituer un échantillon :

- méthode probabiliste : sélection de l'échantillon par tirage aléatoire dans la population-mère. Chaque individu statistique doit avoir exactement la même chance que les autres de participer à l'enquête ;
- méthode non probabiliste : identifier dans la population mère, quelques critères de répartition significatifs puis essayer de respecter cette répartition dans l'échantillon d'individus interrogés.

Effectif – Se dit d'un contrôle, conçu et maintenu.

Effet – Conséquence d'un événement de risque opérationnel, se matérialisant par un impact financier (perte, gain, manque à gagner).

Efficacité d'un contrôle – Capacité à maîtriser un risque (en limiter sa survenance et/ou ses effets). Les deux principaux facteurs de mesure de cette efficacité sont son adéquation au risque du contrôle (ses caractéristiques permettent-elles de maîtriser le risque ?) et la qualité de sa mise en œuvre (le contrôle est-il exécuté conformément à la procédure qui le définit ?).

Environnement de contrôle – Environnement dans lequel les personnes accomplissent leurs tâches et assument leurs responsabilités ainsi que les qualités individuelles des collaborateurs et surtout leur intégrité, leur éthique et leurs compétences constituent le socle de toute organisation.

Évaluation des risques – Lors de celle-ci, le management prend en compte à la fois les événements prévisibles (du fait d'une occurrence certaine) et potentiels (du fait d'une occurrence possible mais incertaine).

Événement – Événements potentiels identifiés par le management susceptibles d'avoir un impact (négatif, positif ou les deux) sur la mise œuvre de la stratégie ou sur la réalisation des objectifs. Même les événements dont la probabilité d'occurrence est faible sont pris en compte s'ils ont un impact significatif sur la réalisation d'un objectif majeur. L'événement de risque opérationnel est au cœur d'un incident. Il s'agit de ce qui survient, ce qui arrive, en interne à la suite d'une défaillance de processus interne, ou d'un événement extérieur. Il a pour conséquence un impact financier. L'événement peut être lui-même une défaillance de processus, dans le cadre des réactions en chaîne.

Événement avéré – Événement ayant réellement eu lieu et dont il faut identifier les causes et les effets. Les événements avérés font partie des données historiques.

Événement extérieur – Événement délibéré, accidentel ou naturel qui est externe au groupe mais qui l'impacte financièrement. Sous certaines conditions, ces événements extérieurs constituent des incidents de risque opérationnel pour le groupe. Il peut s'agir par exemple de fraudes externes, de catastrophes naturelles, d'émeutes, etc.

Falsification – Voler des documents originaux *via* des réseaux organisés. Les documents sont authentiques mais certains éléments en sont modifiés. Les éléments de falsification les plus courants sont la photo et les dates (naissance, émission du document). Aux yeux de la loi, la falsification est un crime. Aujourd'hui, la falsification est plus courante que la contrefaçon, qui reste réservée aux opérations avec des enjeux plus importants. Elle est également plus repérable.

Formalisation des contrôles – Formalisation dans une ou des procédures qui en définissent l'objectif, les modalités de mise en œuvre, de matérialisation et de suivi par le management *via*, notamment, une information de gestion. Le niveau de formalisation doit

être proportionné à la criticité des risques concernés. Un contrôle doit être spécifié selon deux axes :

- Caractéristiques générales : statut (contrôle majeur ou non) ; périmètre couvert ; caractère *a priori* ou *a posteriori* ; niveau du contrôle (1 ou 2) et personnes ou services responsables de l'exécution ; personnes ou services en charge de l'analyse des résultats.
- Mode opératoire (degré d'automatisation) : sélectivité (intégralité ou échantillon avec ses modalités de détermination) ; fréquence ; spécification fonctionnelle du contrôle, tâches à exécuter ; matérialisation du résultat ; évaluation des résultats du contrôle (grille de notation/*scoring*) ; diffusion des résultats.

Fréquence (ou probabilité) – Probabilité de survenance d'incidents. La fréquence permet de déterminer le taux d'occurrence. Multipliée par la sévérité, elle permet de mesurer la criticité d'un risque.

Gain – Incident de risque opérationnel se traduisant par un impact financier positif.

Gestion des risques (*risk management*) – « Processus mis en œuvre par le conseil d'administration d'une entité, par ses dirigeants et par d'autres employés, utilisé pour la mise en œuvre de la stratégie et conçu pour identifier des événements potentiels qui pourraient affecter l'entité, pour gérer le risque dans les limites fixées, et pour fournir une assurance raisonnable quant à l'atteinte des objectifs » (COSO). Les principaux objectifs de la gestion des risques sont la mobilisation de tous les acteurs, la réduction de la probabilité de survenance d'événements de risque, la mise en place d'un dispositif homogène et le juste équilibre entre les risques pris et le coût du dispositif.

Gestion du risque opérationnel (*operational risk management*) – Identification, évaluation, contrôle et maîtrise de l'exposition aux pertes de risque opérationnel.

Gestionnaire de risque – Responsabilité conceptuelle visant d'une part à identifier, expliciter et estimer le risque et à concevoir et mettre en place un dispositif de contrôle et de reporting sur le risque et, d'autre part, à exploiter les reportings et alertes issues du dispositif.

Gravité – Mesure de l'impact de la survenance d'un risque (1/100/1 000 K euros – effet sur l'image sensible ou désastreux…).

Impact – Résultat ou effet d'un événement. Un même événement peut se traduire par différents impacts possibles. L'impact d'un événement peut avoir un effet positif ou négatif sur la réalisation des objectifs de l'organisation.

Impact financier – Impact engendré par un incident de risque opérationnel : une perte, un gain, un manque à gagner, un *near-miss*.

Incertitude – Incapacité de connaître à l'avance, avec exactitude, la probabilité ou l'impact des événements futurs.

Incident de risque opérationnel (*operational risk incident*) ou incident historique – Événement avéré résultant de l'inadéquation ou de la défaillance de processus internes ou d'événements extérieurs, qui a, pourrait ou aurait pu entraîner une perte, un gain ou un manque à gagner.

Incident potentiel (*potential incident*) – Événement de risque opérationnel qui résulterait de l'inadéquation ou de la défaillance de processus internes ou d'événements extérieurs et entraînerait une perte, un gain ou un manque à gagner. Les principaux incidents potentiels sont étudiés aux différents niveaux du groupe : une analyse qualitative (analyse des causes, des contrôles et des effets) et une analyse quantitative (estimation de la fréquence et de la gravité) sont réalisées. Les incidents potentiels, une fois analysés, constituent des données prospectives utilisées dans la gestion et la mesure du risque opérationnel. Les incidents potentiels participent à l'élaboration de la cartographie des risques des métiers et des fonctions. À la différence des incidents historiques (avérés), les incidents potentiels sont des risques identifiés et quantifiés mais qui ne se sont pas nécessairement produits par le passé et dont l'occurrence est aléatoire.

Incidents potentiels majeurs (*major potential incidents*) – Incidents potentiels dont l'impact sur l'exposition du Groupe au risque opérationnel serait majeur.

Indicateurs clés de risques (*key risk indicator*) – Indices numériques, sélectionnés *via* l'expertise des managers, qui donnent une indication avancée de l'exposition au risque opérationnel pour une entité donnée. Pour être « clé », un indicateur doit soit fournir aux managers une information essentielle pour la gestion quotidienne du risque, soit être particulièrement sensible au risque de pertes.

Indicateurs d'analyse des contrôles – Indicateur de réalisation des contrôles, mesurant la proportion de réalisation effective des contrôles, dans le respect des modalités prévues, rapportée à la réalisation attendue et indicateur de résultat des contrôles, évaluant la conformité de l'opération ou du processus vérifié, sur la base d'une cotation ou d'une grille de scoring prédéfinie.

Infrastructure de gestion du risque opérationnel (*operational risk framework*) – Ensemble des éléments qui permettent de gérer et de mesurer le risque opérationnel : politiques, processus, organisation, ressources, procédures, méthodologies et systèmes dédiés.

Instructions aux collaborateurs – Terme générique pour décrire les procédures détaillées d'application de la politique générale de gestion des incidents rédigées par les analystes risque opérationnel et applicables au périmètre qui les concerne.

Intégrité – Principes moraux tels que l'honnêteté, l'incorruptibilité, la probité, le souhait de bien faire, d'exprimer et de respecter un ensemble de valeurs et d'attentes.

Intégrité (I) – Propriété qui assure que les données d'un système d'information sont identiques en deux points, dans le temps et dans l'espace ;

Key risk indicator *(KRI)* – Voir *indicateurs clés de risques.*

Les 4 « T » – Comportements que l'on peut adopter face à un risque en fonction de sa nature :

- Tolérer : décider d'accepter le risque en l'état, autrement dit endosser les conséquences si le risque se transforme en sinistre.
- Terminer : cesser l'activité qui est à l'origine du risque.
- Transférer : confier le risque à quelqu'un d'autre, notamment à une compagnie d'assurances, un client ou un fournisseur. Ce comportement relève essentiellement du domaine de l'assurance de l'entreprise.
- Traiter : amener le risque au niveau décidé par la fonction de pilotage de l'entreprise. C'est sur ce comportement qu'agit principalement le contrôle interne.

Lignes de défense – Caractéristique d'un dispositif de contrôle interne composé de contrôles de premier degré, deuxième degré et troisième degré.

***Manque à gagner* (opportunity cost)** – Incident de risque opérationnel se traduisant par une perte de revenus. Ils peuvent par exemple être provoqués par l'indisponibilité pendant une journée d'un système critique de l'entreprise (tel qu'un système de traitement des instructions clients).

Matérialisation des contrôles – Existence d'une trace matérielle de la réalisation du contrôle ou d'un ensemble de contrôles. La matérialisation peut être partielle (une signature, une check-list cochée, etc.), ou complète, *via* un rapport de contrôle formalisé incluant une piste d'audit. Le degré de matérialisation est fonction de la criticité du contrôle, définie au regard du risque qu'il couvre.

Menace – Relation entre un événement d'origine naturelle, accidentelle ou volontaire et un élément du système d'information susceptible d'en subir les atteintes.

Mesure de prévention – Mesure de sécurité qui agit sur la probabilité d'un sinistre (ex. : chiffrement).

Mesure de protection – Mesure de sécurité qui agit sur l'impact d'un sinistre (ex. : *back-up*).

Mesure du risque opérationnel – Quantification du risque opérationnel à travers diverses données quantitatives y compris les données chiffrées sur le capital économique et réglementaire, élaborées à partir des données historiques et prospectives.

***Near-miss* –** Incident de risque opérationnel où l'événement a eu lieu mais pour lequel, par chance, aucun impact financier ne s'est matérialisé.

Objectifs opérationnels associés – Objectifs déclinés des objectifs stratégiques et contribuant à la mise en œuvre de la stratégie choisie. Chaque niveau d'objectifs stratégiques est précisé par des objectifs plus spécifiques. Les objectifs stratégiques sont ainsi déclinés au sein de l'ensemble de l'organisation. Les objectifs sont compréhensibles et mesurables. Ils sont en adéquation avec l'appétence pour le risque.

Objectifs stratégiques – Objectifs fixant les lignes directrices en accord avec la mission/vision de l'organisation. Ils reflètent les choix stratégiques du management quant à la manière dont l'organisation cherche à créer de la valeur pour ses parties prenantes. Le management identifie les risques associés aux choix stratégiques et étudie les impacts.

Opportunité – Possibilité qu'un événement se produise et ait une incidence positive sur la réalisation des objectifs.

Périodicité des contrôles – Fréquence de réalisation d'un contrôle (annuelle, hebdomadaire…) ou, dans le cas d'un contrôle exécuté en continu, délai maximum entre l'exécution du contrôle et l'opération.

***Perte* (loss)** – Incident de risque opérationnel qui a un impact financier négatif.

***Pire des cas* (worst case)** – Cas le plus adverse qui puisse être raisonnablement envisagé dans le cadre de l'incident potentiel considéré.

Plan d'action – Ensemble d'actions structurées préventives et/ou correctives visant à corriger une ou des défaillances(s) constatée(s). Il doit être distingué de l'« action immédiate » qui correspond, quant à elle, à une correction ponctuelle de la défaillance, sans planification dans le temps. Les caractéristiques principales sont les suivantes : nom, description, entête propriétaire du plan d'actions, dates clés, le ou les déclencheurs, responsable du suivi, décisionnaire, niveau de criticité, le ou les sponsors du plan d'action, famille de risque. Les différents statuts d'un plan d'actions (cycle de vie) : en cours de documentation, initialisé, clôturé, abandonné, supprimé.

Plan de contrôle – Ensemble organisé de contrôles à exécuter couvrant l'ensemble des processus propres à une entité ainsi que les processus partagés ou délégués par une autre entité. L'identification des contrôles qui forment le plan de contrôle d'une entité doit obéir à une approche systématique d'analyse des risques liés à chaque processus dont l'entité est responsable. Elle s'appuie donc sur un exercice de cartographie des risques. Les contrôles sont documentés et formalisés au sein de plans de contrôles : la constitution de plans de contrôle structure le dispositif (homogénéisation). Ce plan comprend un nombre raisonnable de contrôles majeurs ; une validation formelle par le management de l'entité est obligatoire. Une mise à jour périodique est nécessaire pour suivre l'évolution des risques.

Politique – Ensemble des directives du management sur ce qui doit être fait pour mettre en place un contrôle. Une politique sert de fondement aux procédures destinées à sa propre mise en œuvre.

Probabilité – Possibilité qu'un événement donné se produise. La probabilité indique un pourcentage ou une mesure quantitative telle qu'une fréquence de survenance d'un événement ou toute autre mesure numérique.

Procédure – Action permettant la mise en œuvre d'une politique. Une procédure est un document : actant une (ou plusieurs) instructions(s) permanente(s) et de toute nature aux collaborateurs d'une entité ou de plusieurs entités, de leur hiérarchie directe ou supérieure ; décrivant un (ou plusieurs) processus détaillé(s) de traitement. Les procédures sont une preuve évidente de l'organisation et de la structuration des activités. Elles jouent un rôle clé dans l'organisation du groupe, dans l'encadrement de ses activités dont elles sont un des supports, et dans la formation par leur exemplarité. Elles sont un facteur essentiel de la maîtrise des risques, de la qualité du service client, de la protection de la réputation du groupe et de ses résultats. Elles répondent à une obligation réglementaire. Les procédures doivent être exhaustives, à jour et de qualité, et couvrir l'ensemble du périmètre d'activités.

Processus (process) – Série de tâches coordonnées qui font appel à des ressources humaines, une infrastructure, de la technologie et des procédures, et ayant pour but d'atteindre un objectif donné. Les processus sont gérés par les métiers et les fonctions supports. Ils peuvent entre autre avoir des objectifs liés à une rentabilité ou à la qualité du service aux clients. Un processus a un commencement (souvent dénommé facteur ou événement déclencheur) et une fin. Un processus doit être transversal et indépendant de l'organisation de l'entité.

Processus clé (key process) – Processus critique à la réalisation des objectifs d'une entité, et/ou pour lequel on estime que le niveau de risque opérationnel est significatif. C'est un processus dont la défaillance mettrait en danger ou perturberait gravement la réalisation des objectifs de l'entreprise. L'appréciation des processus clés se fait sur appréciation à dire d'experts et sur la base de données comme :

- le montant du chiffre d'affaires en jeu ;
- l'importance des clients concernés en nombre ou en revenus générés ;
- le niveau des obligations réglementaires attachées ;
- l'impact en termes d'image et de réputation ;
- le nombre de collaborateurs impliqués et/ou le montant de coûts engendrés ;
- le processus ou activité critique au titre de la continuité d'activité.

Processus de pilotage – Ils définissent la stratégie, organisent l'action et contrôlent les réalisations.

Processus opérationnels (appelés aussi processus « métier ») – Ils contribuent directement à la réalisation du produit ou de la prestation. Ils délivrent un produit à un client final externe à l'entreprise.

Processus support – Ils contribuent au bon déroulement des processus métier en leur apportant les ressources et informations nécessaires.

Profil de risque d'une entreprise – Positionnement d'une entreprise sur son marché se traduisant par un niveau de risques connu et accepté (rapport « opportunités/risques »).

Profil de risque opérationnel (risk profile) – Exposition globale de tous les processus d'une entité à des incidents potentiels.

Réduction des risques – Actions permettant de réduire la fréquence de survenance d'un risque (ex. : principe des quatre yeux) ou d'en atténuer la gravité (ex. : PCA, assurance).

Référentiel des processus – Inventaire exhaustif des processus d'une entreprise en distinguant différents niveaux d'agrégation.

Référentiel des produits et services – Inventaire exhaustif des produits et services commercialisés par une entreprise.

Reporting – Ensemble des informations de gestion qu'un responsable rend disponible à un niveau supérieur pour mesurer sa performance et/ou la qualité du dispositif de contrôle interne de son périmètre. Le terme se rapporte à la fiabilité du reporting de l'organisation, y compris la communication externe ou interne, des informations financières ou non financières. On distingue les reportings internes (à usage interne) et les reportings réglementaires (à destination des régulateurs). Les principaux objectifs de tout reporting sont de :

- fournir une vision transparente au niveau du groupe et de l'ensemble des entités en matière de risques et de dispositif de contrôle permanent ;
- mettre en avant les points d'attention ;
- permettre la consolidation dans un cadre homogène ;
- matérialiser l'engagement du responsable de l'entité.

Un reporting doit être exhaustif et fiable et une validation formelle par le management doit être obtenue.

Responsabilité sociale de l'entreprise (RSE) – Concept dans lequel les entreprises intègrent les préoccupations sociales et environnementales dans leurs activités et dans leur interaction avec leurs parties prenantes sur une base volontaire.

Risk appetite/risk tolerance – Voir *tolérance au risque*.

Risk management – Voir *gestion des risques*.

Risque – Possibilité qu'un événement se produise et ait une incidence défavorable sur la poursuite et/ou contrarie l'atteinte des objectifs et/ou les actifs de l'entreprise. L'événement doit être potentiel et sa potentialité de survenance doit être évaluée. Le risque peut être considéré comme la combinaison d'un aléa et d'une conséquence. Un risque est à la fois un aléa, une incertitude, une vulnérabilité, mais aussi une opportunité… Dans le secteur bancaire, les trois grandes catégories de risques sont les risques de crédit, les risques de marché et les risques opérationnels.

Risque acceptable (ou seuil de tolérance ou risque) – Risque acceptable dans l'atteinte des objectifs définis par la direction générale. Ce sont les objectifs qui déterminent les risques acceptables et en conséquence le dispositif de contrôle à déployer pour circonscrire les risques.

Risque brut ou inhérent – Risque évalué avant tout dispositif de maîtrise des risques. Exposition de l'organisation à son univers des risques intrinsèques à ses activités.

Risque de conformité – Risque de pertes résultant de l'inadaptation ou de la défaillance de procédures internes, de personnes et de systèmes ou résultant d'événements extérieurs.

Risque de réputation – Risque d'atteinte portée à la confiance dans l'entreprise de ses clients, de ses fournisseurs ou contreparties, de ses actionnaires ou collaborateurs, de ses régulateurs et plus généralement de toute personne dont la confiance, à quelque titre que ce soit, est une condition nécessaire à la poursuite normale de l'activité.

Risque majeur – Risque dont la matérialisation aurait un effet important sur les résultats, les actifs ou la réputation de l'entreprise ou de l'une de ses entités.

Risque maximum tolérable – Événement unitaire ou addition d'événements qui, a un moment donné, dépasse ce que l'entreprise peut supporter. Le risque maximum tolérable est de nature à remettre en cause l'existence même de l'entreprise.

Risque net ou résiduel – Risque évalué après avoir apprécié le dispositif de réponses aux risques maîtrisables. Évaluation du risque tenant compte des différentes étapes de l'exercice de cartographie des risques : risque sous-jacent ; qualité du dispositif de contrôle permanent ; indicateurs de risques. Il peut faire l'objet d'une cotation reflétant l'appréciation globale du management.

Risques opérationnels – Risques résultant de l'inadéquation ou de la défaillance de processus opérationnels de l'entité. L'étude et la résolution des causes permettent de diminuer la fréquence d'occurrence des événements et la sévérité de leurs impacts lorsqu'ils surviennent.

Scénario – Description narrative d'une situation hypothétique représentative d'un incident. Remarque : Les scénarios retenus permettent d'évaluer les vulnérabilités, de guider les *business cases* et les exercices.

Sélectivité – Quote-part d'opérations que le contrôle doit couvrir (on parle dans ce cas d'échantillon). Si le contrôle ne couvre pas toutes les opérations, les modalités de sélection des opérations doivent être spécifiées : le contrôle peut couvrir une proportion fixée, choisie de façon aléatoire, ou une proportion variable, selon une modalité de sélection fixée (dépassement d'un montant de transactions, etc.).

Self-audit – Dispositif de contrôle mettant à disposition des opérationnels un moyen d'évaluer la manière dont ils emploient le dispositif de contrôle et donc leur exposition au risque et leurs axes d'amélioration.

Sensible – Niveau d'un risque qui entraînerait des pertes financières, commerciales et organisationnelles significatives, ou des préjudices mineurs d'ordre judiciaire, et qui obligerait à prévoir des mesures de sécurité.

Séparation des tâches – Attribution à des personnes ou à des services distincts des fonctions qui, si elles étaient accomplies par la même personne ou le même service, augmenteraient les risques d'erreur ou de fraude.

Seuil de tolérance au risque – Voir *risque acceptable*.

Sévérité (ou gravité) – Correspond à la gravité d'un incident. Elle mesure les conséquences pour l'entreprise.

Spécifications – Définition concrète des caractéristiques du contrôle (organisation et mode opératoire), dans une procédure.

Stratégique – Niveau d'un risque qui entraînerait la perte d'une activité de l'entreprise ou des poursuites judiciaires à l'encontre d'un haut responsable de l'entreprise, et qui obligerait à prévoir des mesures de sécurité.

Taxonomie des risques – Bibliothèque des risques possibles pouvant concerner une entreprise.

Tolérance au risque (*risk tolerance *ou* risk appetite*) – Niveau de variation acceptable dans l'atteinte d'un objectif. Le niveau de tolérance au risque doit être mesurable. Sa mesure s'effectue de préférence à l'aide des mêmes unités que celles utilisées pour mesurer les objectifs opérationnels. Elle doit être en adéquation avec l'appétence pour le risque. La tolérance au risque opérationnel correspond au niveau de pertes de risque opérationnel auquel l'entreprise accepte d'être exposée aux divers échelons de l'organisation. L'expression de la tolérance au risque opérationnel ne suit pas le chemin classique utilisé pour les autres risques. Si la tolérance au risque opérationnel ne se formalise pas sous forme de limites, elle s'exprime à travers divers actes et décisions de management, dont :

- les politiques générales, formalisées sous forme de procédures ;

- les comités de validation des nouvelles activités, nouveaux produits, nouvelles organisations ou processus ;
- les différents reportings sur l'état des risques opérationnels ;
- les processus de délégation et/ou d'escalade.

Traitement des risques – Mode de traitement du risque sélectionné par le management parmi les alternatives suivantes : évitement, réduction, partage et acceptation du risque.

***Type d'événement* (event type)** – Catégories dans lesquels les événements sont classés. Dans le cadre d'une analyse cause/événement/effet, l'événement de l'incident doit être identifié et catégorisé en fonction de la liste des types d'événements.

Liste des témoignages

Bibliographie

OUVRAGES

EMMERICH Jean-Pierre, LEJEUNE Gérard, *Audit et commissariat aux comptes*, Gualino Éditeur, 2007.

IFACI et PRICEWATERHOUSSECOOPERS, *COSO, référentiel intégré de contrôle interne*, Paris, Eyrolles, 2014.

MADERS Henri-Pierre, *Audit opérationnel dans les banques*, Éditions d'Organisation, 1994.

MADERS Henri-Pierre et MASSELIN Jean-Luc, *Piloter les risques d'un projet*, 2009.

MADERS Henri-Pierre et MASSELIN Jean-Luc, *Contrôle interne des risques*, 2004, 2006, 2014.

RENARD Jacques et NUSSBAUMER Sophie, *Audit interne et contrôle de gestion*, Paris, Éditions d'Organisation, 2011.

RENARD Jacques, *Théorie et pratique de l'audit interne*, Paris, Eyrolles, 2013.

SARDI Antoine, *Audit et contrôle interne bancaires*, Paris, AFGES, 2002.

SCHICK Pierre, BOURROUIH-PAREGE Olivier, VERA Jacques, *Audit interne et référentiels de risques*, Paris, Dunod, 2010.

ARTICLES

CHAMBERS Richard F., ELDRIDGE Charles B. et PARK Paula, THE KORN/FERRY INSTITUTE AND THE INSTITUTE OF INTERNAL AUDITORS, « Une âme de leader, les sept qualités personnelles qui maximisent l'impact des directeurs de l'audit interne les plus performants », 2010.

LEMANT Olivier, « Un outil pour améliorer l'efficacité des missions d'audit : la FRAP », *Travail et méthodes*, 1988.

MADERS Henri-Pierre, « Le management des risques », *La Revue de Centre de formation au management du ministère de la Défense*, octobre 2012.

MADERS Henri-Pierre, « En Afrique, la raison principale des faillites des banques est la mauvaise gestion », *L'Analyste* (Bénin), avril 1996.

MADERS Henri-Pierre, « Comment mener un audit opérationnel ? », *La Lettre du CFPB*, octobre 1994.

MADERS Henri-Pierre, « Audit opérationnel dans les banques – un métier fondamental quoique redouté », *La Vie des agences*, octobre 1994.

MADERS Henri-Pierre et THEILLET Yves, « Contrôle des prestations externalisées – Des banques mutualisent leurs audits de leurs prestataires », *La Revue banque*, mars 2011.

MASSELIN Jean-Luc et MADERS Henri-Pierre, « Entre objectifs commerciaux et contrôle interne », *La Revue Banque*, juin 2006.

SAWYER Lawrence B., « Les 10 commandements de l'inspecteur moderne », *Internal Auditors*, 1973.

CONFÉRENCES

MADERS Henri-Pierre, « Le management des risques », Conférence EPIDE, Paris, 5 février 2013.

MADERS Henri-Pierre, « Cartographie des risques et dispositif de contrôle interne », Ministère de la défense, CFMD, Paris, 14 novembre 2013.

MADERS Henri-Pierre, « Conduire une mission d'audit », Conférence VIP, Alger, 27 mai 2012.

MADERS Henri-Pierre, « Cartographie des risques : les nouveaux enjeux – Focus sur le risque de fraude et le risque de liquidité », Conférence EFE, Paris, 23 mars 2009.

FILMS

Inside job, Charles Ferguson, 2010.

Capitalism : A Love Story, Michael Moore, 2009.

Cleveland contre Wall Street, Jean-Stéphane Bron, 2010.

NORMES PROFESSIONNELLES

Code de déontologie, The Institute of Internal Auditors, IFACI, 1er janvier 2009.

Normes internationales pour la pratique professionnelle de l'audit interne (extraits), The Institute of Internal Auditors, IFACI, octobre 2008, révision octobre 2012 :

- 1000 – Mission, pouvoir et responsabilités
- 1100 – Indépendance et objectivité
- 1200 – Compétence et conscience professionnelle

- 1300 – Programme d'assurance et d'amélioration de la qualité
- 2000 – Gestion de l'audit interne
- 2100 – Nature du travail
- 2200 – Planification de la mission
- 2300 – Accomplissement de la mission
- 2400 – Communication des résultats
- 2500 – Surveillance des actions de progrès
- 2600 – Acceptation des risques par la direction générale

Normes Internationales d'audit, CNCC-IRE-CSOEC, juin 2012 (extraits):

- ISA 200 – Objectifs généraux de l'auditeur indépendant et conduite d'un audit selon les normes internationales d'audit
- ISA 210 – Accord sur les termes des missions d'audit
- ISA 220 – Contrôle qualité d'un audit d'états financier
- ISA 230 – Documentation d'audit
- ISA 240 – Obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers
- ISA 250 – Prise en considération des textes législatifs et réglementaires dans un audit d'états financiers
- ISA 260 – Communication avec les personnes constituant le gouvernement d'entreprise
- ISA 300 – Planification d'un audit d'états financiers
- ISA 320 – Caractère significatif lors de la planification et de la réalisation d'un audit
- ISA 330 – Réponses de l'auditeur aux risques évalués
- ISA 450 – Évaluation des anomalies relevées au cours de l'audit
- ISA 500 – Éléments probants
- ISA 505 – Confirmations externes
- ISA 510 – Missions d'audit initiales – Solde d'ouverture
- ISA 520 – Procédures analytiques
- ISA 530 – Sondages en audit
- ISA 540 – Audit des estimations comptables, y compris des estimations comptables en juste valeur et des informations fournies les concernant
- ISA 550 – Parties liées
- ISA 560 – Événements postérieurs à la clôture
- ISA 570 – Continuité de l'exploitation
- ISA 580 – Déclarations écrites

- ISA 600 – Aspects particuliers : audits d'états financiers d'un groupe
- ISA 610 – Utilisation des travaux des auditeurs internes
- ISA 620 – Utilisation des travaux d'un expert désigné par l'auditeur
- ISA 700 – Fondement de l'opinion et rapport d'audit sur les états financiers
- ISA 710 – Données comparatives : chiffres correspondants et états financiers comparatifs
- ISA 720 – Obligations de l'auditeur au regard des informations dans des documents contenant des états financiers audités

Référentiel de compétences de l'audit interne de l'IIA, The Institute of Internal Auditors, IFACI, septembre 2013.

ÉTUDES ET RAPPORTS

«Audit des projets informatiques», AFAI.

«Cartographie des risques informatiques», AFFADI.

«CBOK – Common Body of Knowledge – Vos pratiques au regard des tendances mondiales», IFACI, juillet 2011.

«De la construction du contrôle interne à la communication sur son efficacité», Cahier technique DFCG, novembre 2010.

«Exemple de guide d'évaluation des auditeurs internes», Audit Committee Institute, KPMG, 2012.

«Guide d'audit des applications informatiques», AFFADI.

«Livre vert sur la politique et le rôle de l'audit», CNCC, 2010.

«Rapport mondial 2013 – Saisir les nouvelles opportunités», IFACI, avril 2013.

SITES INTERNET

Association française d'audit informatique (AFAI) : *www.afai.fr.*

Compagnie nationale des commissaires aux comptes : *www.cncc.fr.*

Conservatoire national des arts et métiers (CNAM) : *www.cnam.fr.*

Institut français de l'audit et du contrôle internes (IFACI) : *www.ifaci.com.*

Institut national des techniques économiques et comptables (INTEC) : *www.intec.cnam.fr.*

The Institute of Internal Auditors (IIA) : *www.theiia.org.*