ifaci
institut français de l'audit et du contrôle internes

AMRAE
ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE

Actes du colloque

Risk managers, auditeurs internes...

Comment les acteurs de la maîtrise des risques contribuent-ils ensemble à la valeur ajoutée des organisations ?

mardi 17 mai 2011

RISK MANAGERS, AUDITEURS INTERNES...

COMMENT LES ACTEURS DE LA MAITRISE DES RISQUES CONTRIBUENT-ILS ENSEMBLE A LA VALEUR AJOUTEE DES ORGANISATIONS ?

MARDI 17 MAI 2011

EN PARTENARIAT AVEC L'AMRAE

SOMMAIRE

PRESENTATION DU PROGRAMME, PAR LOUIS VAURS 4

POURQUOI CREER UN COLLOQUE IFACI/AMRAE ? QUELLE COOPERATION ENTRE LES DEUX ASSOCIATIONS 6

Claude VIET, ***Président de l'IFACI, Directeur de l'audit et des risques, La Poste*** 6

Gérard LANCNER, ***Président de l'AMRAE, Directeur des risques, de l'audit interne et des assurances, Groupe Yves Rocher*** 6

DISCOURS D'OUVERTURE, PAR SEVERIN CABANNES 9

ROLES RESPECTIFS DES RESPONSABLES D'AUDIT INTERNE ET DES RISK MANAGERS DANS LE PROCESSUS DE MANAGEMENT DES RISQUES 14

Annie BRESSAC, ***Directrice de l'audit et du contrôle internes, Fondation Apprentis d'Auteuil*** 14

Bénédicte HUOT de LUZE, ***Directrice scientifique, AMRAE*** 14

TABLE RONDE : CADRES ORGANISATIONNELS ET RELATIONS ENTRE L'AUDIT INTERNE ET LE RISK MANAGEMENT DANS LES SECTEURS BANQUES ET ASSURANCES 20

ANIMEE PAR REGIS MONFRONT, ***INSPECTEUR GENERAL AU SEIN DU CREDIT AGRICOLE CIB.*** 20

AVEC EDOUARD-MALO HENRY, ***INSPECTEUR GÉNÉRAL, SOCIÉTÉ GÉNÉRALE*** **;** 20

CHRISTOPHE HIOCO, ***CHIEF EXECUTIVE OFFICER, SOCIETE GENERALE CIB ;*** 20

ANNETTE DOLD, ***HEAD OF GLOBAL INTERNAL AUDIT, ALLIANZ ;*** 20

JUERGEN GUHE, ***GLOBAL HEAD OF RISK MANAGEMENT, ALLIANZ ;*** 20

PAUL-HENRI MEZIN, ***DIRECTEUR DE L'AUDIT, MALAKOFF MEDERIC ;*** 20

THOMAS COLIN, ***DIRECTEUR DES RISQUES, MALAKOFF MEDERIC.*** 20

TABLE RONDE : CADRES ORGANISATIONNELS ET RELATIONS ENTRE L'AUDIT INTERNE ET LE RISK MANAGEMENT DANS LES SECTEURS DE L'INDUSTRIE, DU COMMERCE ET DES SERVICES 38

ANIMEE GERARD LANCNER, ***PRESIDENT DE L'ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE (AMRAE).*** 38

AVEC FLORENCE VINCENT, ***DIRECTRICE DE L'AUDIT INTERNE ET DES RISQUES, MICHELIN ;*** 38

PHILIPPE HATRON, ***DIRECTEUR DE L'AUDIT INTERNE GROUPE, AREVA ;*** 38

PHILIPPE OBERT, ***DIRECTEUR DE L'ASSURANCE ET DE LA GESTION DES RISQUES, AREVA ;*** 38

BRUNO DUNOYER DE SEGONZAC, *DIRECTEUR DE L'AUDIT INTERNE ET DE LA GESTION DES RISQUES, BOUYGUES TELECOM.* **38**

QU'ATTEND-ON DE L'AUDITEUR INTERNE ET DU RISK MANAGER ? LES ROLES PERÇUS PAR LES DIFFERENTES PARTIES PRENANTES **57**

ANIMEE PAR CLAUDE VIET, *PRESIDENT DE L'IFACI, DIRECTEUR DE L'AUDIT ET DES RISQUES, LA POSTE*. **57**

AVEC ALDO CARDOSO, *PRESIDENT DE COMITE D'AUDIT* **57**

DIDIER ELBAUM, *SECRETAIRE GENERAL ADJOINT, AUTORITE DE CONTROLE PRUDENTIEL* **57**

PHILIPPE GUILLAUMIE, *DIRECTEUR FINANCIER, 3 SUISSES INTERNATIONAL* **57**

JEAN-MARC LUMET, *COMMISSAIRE AUX COMPTES, CHAMBRE REGIONALE DES COMPTES DE VERSAILLES* **57**

DISCOURS DE CLOTURE : LES RISQUES HORS CADRE, PAR PATRICK LAGADEC **68**

CLOTURE DU COLLOQUE, PAR LOUIS VAURS **70**

PRESENTATION DU PROGRAMME, PAR LOUIS VAURS

Louis VAURS, *Conseiller du Président, IFACI*

Mesdames et messieurs, bonjour. J'ai le grand plaisir de vous accueillir au nom de l'AMRAE et de l'IFACI pour ce premier colloque commun. Il devrait intéresser les auditeurs internes et les *risk managers* dès lors qu'il s'agira de voir comment les acteurs de la maîtrise des risques contribuent à la valeur ajoutée des organisations.

La semaine dernière, le journal *Les Echos* publiait une interview de Stéphane Walter, le secrétaire général du comité de Bâle. Celui-ci affirmait que *« nous continuons à vivre dans un monde dangereux avec un horizon chargé de risques* ». Il aurait pu ajouter que ces risques sont de plus en plus imprévisibles. On constate en effet que des risques, qui ont un impact élevé mais un potentiel jugé faible, finissent de plus en plus par se concrétiser, avec des conséquences dévastatrices pour les organisations.

En analysant les deux catastrophes industrielles majeures qui viennent de se produire en l'espace d'un an, la marée noire du golfe du Mexique et l'accident nucléaire de Fukushima, Antoine de BOISSIEU note dans un récent article :

- que l'enchaînement qui a causé chacune de ces catastrophes n'avait pas été envisagé ;
- que les dispositifs de lutte étaient déficients ;
- que la couverture du risque par les assurances était insuffisante.

A la question de savoir si l'on peut avoir une idée de la prochaine crise, Stéphane Walter répond par la négative « *car par définition, une crise n'est pas anticipée* ». Faut-il admettre dès lors que l'on sera toujours en retard d'une crise ou d'une catastrophe ? Faut-il considérer que dorénavant, pour certains types de risques, notamment nucléaires, l'on doit accepter de se préparer à des situations inimaginables comme vient de le déclarer, lors de son audition au Parlement, le directeur général de la sûreté nucléaire ?

Je crois personnellement que nous nous retrouverons de plus en plus devant de telles situations et qu'il faudra alors faire preuve de réactivité, de créativité, aucun des scénarios qui auraient pu être envisagés précédemment ne pouvant par définition être mis en œuvre. Les acteurs de la maîtrise des risques doivent bien intégrer cette évolution inéluctable.

En matière de finance, les crises commencent par un pays, puis se répandent petit à petit dans beaucoup d'autres, voire dans tous. Ce phénomène a été expérimenté avec la crise des *subprimes* et sa propagation par le mécanisme de la titrisation.

Dans l'aveuglement général qui a caractérisé cette période, on peut se demander quelle a été la part de responsabilité des acteurs de la maîtrise des risques, les *risk managers* et les auditeurs internes confondus. Ceux-ci avaient-ils suffisamment de compétences et d'indépendance d'esprit pour voir venir la crise ? Si oui, avaient-ils suffisamment de crédibilité et de légitimité auprès des organes dirigeants pour leur faire accepter leurs recommandations ? De leur côté, les organes

dirigeants avaient-ils la capacité d'entendre et de comprendre les diagnostics et recommandations que pouvaient formuler les acteurs de la maîtrise des risques ? A cette double question qui avait été posée dans le cadre d'un colloque IFA IFACI sur le rôle de l'audit interne par la gouvernance, je pense que nous ne pouvons répondre que par la négative.

A leur manière, les législateurs et les régulateurs ont rapidement tiré des conséquences de cette crise. En France, la loi sur la régulation bancaire et financière a été votée. L'Europe a récemment établi un *green paper* qui parle de la gestion des risques. Dans le secteur bancaire, dans le cadre de la réglementation 97-02, une filière risques et compétences élargis rattachée au plus haut niveau a été créée.

Pour les auditeurs internes et les *risk managers*, la leçon à tirer de cette crise et des catastrophes qui reviennent à présent est qu'ils doivent se sentir concernés, plus encore que par le passé, par les risques jugés par d'aucuns comme les plus improbables.

La montée en puissance de la gestion des risques comme discipline autonome à l'égal de l'audit interne, observée dans tous les secteurs d'activités, doit être considérée comme une chance pour une plus grande maîtrise des activités des organisations et l'amélioration de leur performance. Encore faut-il bien comprendre le rôle de chacun, bien appréhender leur différence et jouer sur la complémentarité des auditeurs et des *risk managers* pour apporter plus de valeur aux organisations. C'est tout l'enjeu de ce colloque.

La matinée débutera par les interventions des deux présidents. Le discours d'ouverture sera ensuite prononcé par Séverin CABANNES, directeur général délégué de la Société Générale. Il sera suivi de la présentation des rôles respectifs des directeurs d'audit internes et des *chief risk officers*. La première table ronde portera sur l'audit interne et le *risk management*. Une deuxième table ronde se tiendra dans l'après-midi. Elle portera sur l'activité industrie-commerce et service. Enfin, la dernière table ronde sera consacrée aux attentes des parties prenantes qui sont essentiellement la direction générale, les comités d'audit, les commissaires aux comptes et le régulateur. Le discours de clôture sera prononcé par Patrick LAGADEC, directeur de recherche à l'Ecole Polytechnique.

Claude VIET, président de l'IFACI depuis 2008, est diplômé de l'école nationale supérieure des postes et télécommunications. Il a exercé différentes hautes responsabilités à la Poste : directeur de cabinet du directeur général à ses débuts, directeur de différentes postes départementales, directeurs des ressources humaines, directeur du courrier puis directeur général. En 1998, il devient président-directeur général de l'Aéropostale. En 2004, il est nommé conseiller auprès du président de La Poste et en 2005, il devient directeur de l'audit groupe. En 2009, il est nommé directeur de l'audit et des risques. Je lui cède la parole.

POURQUOI CREER UN COLLOQUE IFACI/AMRAE ? QUELLE COOPERATION ENTRE LES DEUX ASSOCIATIONS

Claude VIET, *Président de l'IFACI, Directeur de l'audit et des risques, La Poste*

Gérard LANCNER, *Président de l'AMRAE, Directeur des risques, de l'audit interne et des assurances, Groupe Yves Rocher*

Claude VIET

Je voudrais dire tout le plaisir que j'ai d'être auprès de Gérard LANCNER, le président de l'AMRAE pour ouvrir ce colloque qui est l'aboutissement d'une démarche que nous avions initiée il y a quelque temps. Cette démarche se poursuivra de manière encore plus concrète à l'issue de nos travaux, sous la forme d'une prise de position.

Dans un contexte de crise financière mondiale, nous avons assisté ces dernières années à des changements importants qui impactent à la fois la direction générale des entreprises, leur management et leur gouvernance. L'évolution du cadre des entreprises est marquée par la mondialisation. Cette dernière s'est notamment traduite par de nouvelles exigences financières, sociales, sociétales et environnementales. Par ailleurs, il existe une forte demande de transparence de la part de l'opinion publique. Parallèlement, l'adaptation de la législation s'est matérialisée par un renforcement des règles prudentielles, des organes de contrôle, des exigences nouvelles en matière de gestion des risques et une responsabilité accrue de la gouvernance, notamment à l'échelle des comités d'audit.

Ces deux évolutions ont mis en exergue l'importance du contrôle interne dans son acception large. Il est donc logique, voire indispensable, que l'IFACI et l'AMRAE proposent une démarche commune et une prise de position partagée à la lumière des réflexions qui émergeront dans le cadre de ce colloque et de celles ayant été engagées auparavant.

Pour l'IFACI, ce colloque intervient à l'issue d'un certain nombre de réflexions et de prises de position. La réflexion engagée le 9 septembre 2008 a abouti à une prise de position sur l'urbanisme de contrôle interne, de façon globale et de façon plus ciblée sur le secteur bancaire en 2010. En 2009, une table ronde mondiale a été organisée par l'IIA. Cette réflexion menée avec le patronat américain a conduit à rendre plus forte l'exigence pour l'audit interne de prendre en compte l'ensemble des risques au niveau des entreprises. L'ECIIA et le FERMA – qui représentent les instituts nationaux en matière d'audit interne et de risques au niveau européen – ont également pris position pour montrer la synergie de l'audit interne et du *risk management*. Enfin, la transposition et l'application des quatrième, septième et huitième directives européennes a eu lieu en France. Cela s'est traduit par un guide pour les comités d'audit et par une révision profonde du cadre de référence en matière de risques et de contrôle interne.

L'ensemble de ces travaux a montré l'importance d'une coordination accrue, plus étroite et efficace entre les différents acteurs de la maîtrise des risques. L'étape suivante consistera à intégrer cette démarche de management des risques dans l'entreprise même et dans son

pilotage. Il est certain que nos deux fonctions sont très liées, d'une part parce que l'audit s'appuie sur la cartographie des risques pour établir son plan d'audit, d'autre part parce qu'il apporte un certain nombre d'éclairages au *risk managers* pour l'élaboration de la cartographie des risques.

Notre objectif commun aujourd'hui est d'approfondir les contours et les contenus de la collaboration entre audit interne et *risk management,* dans la recherche de la plus grande efficacité des systèmes de contrôle interne.

Louis VAURS

Avant que Gérard LANCNER ne prenne la parole, je souhaite rappeler qu'il est diplômé de l'Ecole supérieure de commerce de Rouen et qu'il a débuté sa carrière au sein du cabinet juridique et fiscal Arthur Andersen. En 1981, il rejoint le département juridique et fiscal du groupe Yves Rocher, dont il prend rapidement la direction. En 2001, il est directeur du département *risk management* et assurance, auquel il agrégera rapidement l'audit interne et les affaires réglementaires. Gérard LANCNER est président de l'AMRAE depuis 2008.

Gérard LANCNER

L'AMRAE est très heureuse de cette première conférence organisée avec l'IFACI, qui traduit la synergie que nous avons amorcée depuis plusieurs mois et la volonté que nous avions de travailler ensemble et de trouver le bon équilibre entre nos différentes démarches.

Je crois, effectivement, que nous avons le même objectif : assurer le contrôle par l'interne de nos entreprises afin qu'elles puissent atteindre leurs objectifs. C'est la mission qui nous est donnée quels que soient le titre et la fonction que nous avons dans nos entreprises. Nous avons la même feuille de route : assurer le contrôle interne de notre entreprise, prévoir les incidents, anticiper les difficultés, envisager des plans d'actions et assurer leur efficacité.

C'est donc tout naturellement, après s'être cherchés pendant quelques années, que nous nous sommes retrouvés avec une mission commune. Nous avons le même objectif. Partageons la même vision afin qu'à l'issue de cette journée, nous puissions promouvoir la vision commune de l'IFACI et de l'AMRAE sur les rôles respectifs des gestionnaires de risques, des auditeurs internes, des responsables du contrôle interne et des autres fonctions de l'entreprise.

Nous nous complétons les uns les autres comme nous le verrons au cours de la journée. Nous sommes amenés à travailler ensemble pour assurer le contrôle interne de nos entreprises. L'organisation de l'IFACI a toujours été un modèle pour l'AMRAE. De son côté, l'AMRAE a participé à des travaux au cours des six dernières années sur la gestion des risques, dès lors que nous avons admis que celle-ci devait être globale. Nous nous sommes retrouvés ensemble à différentes occasions, notamment dans le cadre du groupe de travail de l'AMF. Tout naturellement, nous avons défendu devant l'AMF et d'autres acteurs, le fait que l'identification des risques et la mise en place d'un système relèvent des fonctions des *risk managers* mais que la

recherche de l'efficacité et le *reporting* sont le fait des auditeurs internes. Voilà la raison pour laquelle nous sommes rassemblés aujourd'hui.

Nous sommes tous amenés à devoir gérer l'ingérable. Dans ces conditions, il vaut mieux que nous soyons ensemble plutôt qu'opposés les uns les autres. Je vous remercie et je cède la parole à notre intervenant.

Louis VAURS

Séverin CABANNES est un ancien des Mines, il est directeur général délégué de la Société Générale depuis 2008. Séverin a exercé pendant une dizaine d'années des responsabilités chez ELF Atochem, dont celle de directeur de la stratégie. Il a ensuite rejoint le groupe La Poste en 1997 en tant que directeur de la stratégie. L'année suivante, il est nommé directeur général adjoint stratégie et finances et membre du comité exécutif. En 2001, il rejoint le groupe Société Générale en tant que directeur financier et membre du comité de direction. En 2009, il est directeur des ressources et membre du comité exécutif avant d'être nommé en 2008, directeur général délégué du groupe Société Générale.

DISCOURS D'OUVERTURE, PAR SEVERIN CABANNES

Séverin CABANNES, *Directeur général délégué de la Société Générale*

Merci Messieurs les présidents de m'avoir invité ce matin. En tant que membre d'une équipe de direction générale, j'ai le sentiment d'être membre d'une équipe de gestionnaires de risques et de contrôle interne. La Société Générale est par ailleurs un membre actif de l'IFACI.

Qu'est-ce qu'une direction générale attend d'une équipe de maîtrise des risques ? Pour une part, j'attends que cette dernière collabore à la sécurité du fonctionnement de l'entreprise, qu'elle collabore efficacement à cette sécurité et qu'elle collabore efficacement à la sécurité de son développement. Pour les banques, qui ont connu un certain nombre de difficultés depuis quelque temps, la sécurité du développement de l'entreprise est un point clé qui a été parfois oublié.

I. La sécurité du fonctionnement

Un des principaux risques que nous devons gérer est le risque de destruction de valeur au sein de l'entreprise. Malheureusement, dans l'industrie bancaire dans son ensemble, nous avons connu depuis trois ans une véritable destruction de valeur. Nous devons donc nous demander si les dispositifs généraux de contrôle interne de l'entreprise sont suffisamment protecteurs de ses actifs et de son fonctionnement permanent. La protection des actifs physiques de l'entreprise est un sujet traité depuis longtemps. La préoccupation que nous avons aujourd'hui est la protection des actifs incorporels. Parmi ceux-ci figurent le risque de réputation, le risque lié à la protection des fonds de commerce, sachant que la relation client a été considérablement affectée par la crise systémique, et enfin, le risque de distension de la communauté humaine que représente l'entreprise et du lien entre les collaborateurs et l'entreprise. Votre contribution au fonctionnement sûr de l'entreprise devrait ainsi être davantage orientée sur la protection des actifs incorporels.

La Société Générale a vécu deux crises majeures au cours des trois dernières années, dont une crise spécifique au Groupe due à une fraude massive. Nous avons travaillé depuis trois ans sur nos dispositifs de contrôle, avons enrichi ces derniers qualitativement et quantitativement. Les acteurs du Groupe qui traitent de la maîtrise des risques et du contrôle interne représentent aujourd'hui 8 000 personnes, soit 5 % des effectifs. Nous avons en parallèle investi sur l'accroissement du niveau de compétences et d'expertise métiers de nos gestionnaires de risques. Depuis trois ans, nous avons également accru l'attractivité de ces métiers dans l'entreprise. Aujourd'hui, nous mettons en place un nouvel équilibre, entre les équipes métiers et les équipes de contrôle. La sécurité du fonctionnement quotidien de l'entreprise passe par un tel équilibre et j'attends des équipes de maîtrise de risques qu'elles y contribuent fortement.

II. L'efficacité

J'aimerais à présent revenir sur l'efficacité, ou plutôt l'efficience des systèmes de contrôle. L'exigence d'efficience s'impose à l'ensemble des entités de l'entreprise. Les équipes de contrôle interne n'échappent pas à cette règle. En tant que responsables de maîtrise des risques ou du contrôle interne, nous avons aussi une responsabilité en termes d'efficacité.

L'efficacité passe d'abord par la pertinence des actions. Au cours des dix dernières années, le secteur bancaire a développé des dispositifs de contrôle interne et de maîtrise des risques qui ont été parfois, d'abord dictés par les contraintes réglementaires. Nous avons ainsi plaqué sur des organisations opérationnelles des dispositifs lourds de contrôle, pour répondre aux exigences des régulateurs plutôt qu'en vertu des exigences stratégiques du pilotage de l'entreprise. Ainsi la question de savoir si la pertinence des systèmes de contrôle permanent correspond réellement aux risques majeurs que nous devons gérer se pose. Par ailleurs, ces dispositifs présentent le risque de créer une image bureaucratique des organisations et donc, un risque d'opposition potentielle entre les responsables opérationnels et les corps de contrôle.

Nous avons engagé la correction de ces deux faiblesses. Nous essayons d'utiliser un outil qui est utilisé depuis longtemps dans d'autres industries et qui n'est autre que l'optimisation des processus. J'ai la conviction que la meilleure façon de s'assurer de la pertinence des dispositifs de contrôle est de se fonder sur des démarches d'optimisation des processus. Dans l'industrie, le processus est physique et il peut sembler plus aisé d'identifier les risques, dans certains cas vitaux, y afférents. Dans la banque, les processus sont intangibles et sont très rarement vitaux. La diffusion d'une approche d'optimisation des processus dans une entreprise comme la Société Générale est un travail difficile que nous avons engagé depuis trois ans. Toutefois, il s'agit de garantir la pertinence de nos contrôles et d'accroître la qualité des services que nous offrons à nos clients. Accessoirement, je me suis toujours demandé pourquoi les référentiels normant le contrôle interne et la qualité n'étaient pas confondus.

La deuxième dimension de cette efficacité est le rapport coûts-résultats. Est-ce optimal d'avoir 5 % des effectifs dédiés à la maîtrise des risques ? Nous ne disposons pas de réponse satisfaisante à cette question. Plutôt que d'augmenter les moyens, je pense aujourd'hui que nous devons faire en sorte que le temps passé par les managers opérationnels sur les problématiques de risques et de contrôle interne soit plus important.

Enfin, un dispositif de contrôle interne n'est pas efficace si le risque de déresponsabilisation des opérationnels n'est pas suffisamment pris en compte. Sous le développement nécessaire et voulu des corps de contrôle, on a vu s'établir une distinction trop nette entre le preneur de risque et le contrôleur des risques. Il s'agit là pour moi de l'un des principaux points sur lesquels nous devons être vigilants.

Dans notre organisation, nous avons établi trois lignes de défense contre les risques :

- les responsables opérationnels (contrôle permanent de niveau 1) : il s'agit de l'individu, quelle que soit sa fonction dans l'entreprise ;
- les grandes fonctions (contrôle permanent de niveau 2) : il s'agit de la direction financière, de la direction des risques et de l'ensemble des directions dites fonctionnelles ;

- le contrôle périodique (contrôle de niveau 3) par l'inspection générale et par les équipes d'audit interne.

Ainsi, nous n'avons pas souhaité dédier d'équipes au contrôle permanent de premier niveau pour éviter le risque de déresponsabilisation des opérationnels.

III. La sécurité du développement de l'entreprise

La deuxième crise majeure que nous ayons dû gérer est la crise systémique. Le développement de la complexité de nos produits d'une part, l'accroissement rapide des volumes sur la période 2002-2007 associé à une durée assez longue d'un cycle économique porteur qui a fait diminuer le niveau de vigilance d'autre part, ont fait perdre des repères aux acteurs de l'industrie.

L'une des erreurs que nous avons commise a été de négliger l'un des risques de contrepartie majeurs de toute entreprise : la solidité de ses compagnies d'assurance. Or ce sont les compagnies d'assurance spécialisées dans la couverture des risques financiers qui ont fait défaut aux Etats-Unis et qui ont mené à la catastrophe. Le risque de concentration était en effet très important. Les monolines étaient notées triple A par les agences de rating, tout comme les produits qu'elles assuraient. Nous avons eu aussi un excès de confiance dans les notations extérieures.

Il existe deux moyens de se développer pour les entreprises. Le premier est la croissance organique. Dans les industries lourdes, le développement organique et la maîtrise des risques sont associés. Dans la banque, le gestionnaire des risques n'a pas suffisamment été, dans le passé, associé à la conception des produits. Ceci a été changé. Nous avons mis en place des «Comités Nouveaux Produits» dans lesquels toutes les parties prenantes sont associées pour une analyse ex ante des risques. La sécurité du développement suppose donc que les équipes de recherche, de vente, de production, de contrôle et de maîtrise des risques travaillent ensemble. Le deuxième moyen de se développer pour une entreprise est la croissance externe. La prise de risques est plus tangible lors d'une acquisition externe. C'est pourquoi nous associons depuis longtemps l'ensemble des corps de contrôle au processus de croissance externe.

Avant de conclure, je souhaite partager un certain nombre de convictions personnelles. Une entreprise est d'abord une communauté d'hommes et de femmes qui ont décidé d'associer leur destin en vue d'un projet commun. Je pense que la première condition d'un dispositif de contrôle interne efficace réside dans le partage de valeurs profondes et d'une culture risque commune au sein de cette communauté. Il est essentiel que les gestionnaires de risques et les équipes de contrôle interne contribuent tous les jours à l'élévation de la « culture risque » de l'entreprise. Quand on embauche un jeune qui devient agent d'accueil dans une agence, il n'a pas de conscience a priori du risque que représente son activité pour l'entreprise et pour le client. Nous devons consentir un effort considérable de formation et de sensibilisation. D'ailleurs, le processus de recrutement est également un sujet central de la réflexion sur la maîtrise des risques. La deuxième condition d'un dispositif sûr, en plus de la qualité des hommes, est la qualité des relations entre les hommes, les valeurs managériales du Groupe, leur diffusion et leur partage. A

partir du moment où les relations entre les membres de l'entreprise sont réellement fondées sur la confiance, les risques diminuent sensiblement. Trop souvent, les personnes ont eu peur d'exprimer leur point de vue, de peur de paraître idiotes à cause de la complexité des sujets. Il relève de la responsabilité des managers de faire en sorte que chaque membre de la communauté ait cette capacité à exprimer son point de vue et à être un véritable acteur libre de sa responsabilité. Ainsi, la «bonne» culture d'entreprise est pour moi la première condition d'un système de maîtrise des risques efficace et pertinent.

Enfin, pour conclure une dernière réflexion : la responsabilité d'une direction générale est de choisir les hommes et les femmes et de définir une organisation qui permette, avec un niveau de sécurité suffisant, l'atteinte des objectifs stratégiques qui ont été fixés. Une question fondamentale se pose à l'heure de fixer les objectifs stratégiques de l'entreprise. Quel est le niveau de rentabilité que nous proposons à nos différentes parties prenantes ? Si ce niveau est trop élevé, il devient un facteur essentiel de génération de risques. Une des causes de la crise des subprimes réside sans doute dans le fait que les exigences de rentabilité de certains acteurs économiques, en particulier aux Etats-Unis, étaient devenues telles que la prise de risques associée était devenue énorme. Il est essentiel de partager avec ses actionnaires, les enjeux rendement/risques et pas seulement de partager des objectifs de rentabilité. Dans le secteur bancaire, les nouvelles règles auront comme effet majeur une baisse structurelle des rentabilités. Au-delà de ces éléments, l'espérance de retour de toute communauté humaine est liée aux taux d'intérêt des individus qui la composent. Quel est notre taux d'intérêt individuel ?

Questions de la salle

Louis VAURS

Je souhaite revenir sur la peur de l'expression chez les employés de la banque. J'ai lu dans la presse que, dans le cadre de la crise des *subprimes*, les différences des connaissances entre les managers et les administrateurs étaient trop importantes. Est-ce une réalité que vous avez ressentie ou n'est-ce qu'une vision de journaliste ?

Séverin CABANNES

Cette vision est partiellement exacte. Les conseils d'administration réunissent des personnes ayant une longue expérience bancaire et se répartissant les responsabilités. Nous avions dans notre banque des administrateurs très compétents. En revanche, tous n'étaient pas associés aux sujets pointus. Ce qui est vrai est que très peu de monde dans l'entreprise était au fait de la complexité de ces sujets. Cette situation est porteuse de risques dès lors qu'elle réduit la capacité du corps de l'entreprise à produire une analyse pertinente des risques. Nous avons donc élargi le nombre de personnes capables de s'exprimer sur les risques liés aux produits complexes. Avant, les personnes ne s'exprimaient pas.

Depuis trois ans, le *board* a pris en main de nombreux sujets et a développé sa présence dans le fonctionnement quotidien de l'entreprise. Nous avons en outre initié une démarche holistique sur l'ensemble des risques à gérer et sur le processus de fixation de l'appétit au risque. Le *board* est associé à cette définition d'appétit au risque. Nous disposons de scénarios macroéconomiques et de scénarios de développement de notre activité avec des hypothèses de rentabilité et de croissance. Nous stressons ensuite ces scénarios dans des hypothèses de chocs économiques. Le conseil d'administration débat des hypothèses de chocs et de l'appétit de la société en termes d'impacts sur le résultat au niveau du Groupe. La difficulté réside dans le fait qu'entre la décision quotidienne d'une prise de risque et l'appétit global au risque se situe la déclinaison de l'appétit risque.

Ainsi, le *board* est beaucoup plus impliqué sur les questions de pilotage de l'entreprise.

ROLES RESPECTIFS DES RESPONSABLES D'AUDIT INTERNE ET DES RISK MANAGERS DANS LE PROCESSUS DE MANAGEMENT DES RISQUES

Annie BRESSAC, *Directrice de l'audit et du contrôle internes, Fondation Apprentis d'Auteuil*

Bénédicte HUOT de LUZE, *Directrice scientifique, AMRAE*

Louis VAURS

Annie BRESSAC est directeur de l'audit et du contrôle internes de la Fondation Apprentis d'Auteuil. Elle a plus de 30 ans d'expérience dans le domaine de l'audit, du contrôle interne et de la maîtrise des risques. Elle a été auditeur, consultant externe à l'IFACI, chez Ernst & Young, chez Deloitte. Elle est formatrice et enseignante, professeur affiliée d'ESCP Europe, cofondatrice de la chaire de contrôle interne avec l'IFACI. Enfin, elle codirige l'*executive master* de *risk management*, audit et contrôle interne. Annie BRESSAC est diplômée de l'ESCP Europe et d'expertise comptable. Elle est titulaire du CIA.

Bénédicte HUOT de LUZE est diplômée d'expertise comptable et de management des risques, de l'Insurance Institute of America. Depuis janvier 2009, elle est directrice scientifique de l'AMRAE en charge du contenu et des publications de l'Institut. Elle a travaillé pendant 12 ans chez KPMG et a cofondé en 2001 le département *internal audit service*.

Anne BRESSAC

Mesdames et messieurs, c'est un plaisir de vous retrouver pour évoquer des fonctions auxquelles nous portons un vif intérêt. Bénédicte portera les couleurs du *risk manager* et je me chargerai de représenter l'audit interne.

Notre propos sera axé sur les normes, les référentiels et visera à clarifier les pratiques du *risk manager* et de l'auditeur interne au regard du processus de management des risques. Nous nous attacherons à mettre en évidence les synergies ayant été évoquées et à pointer quelques sujets de débats en préambule aux tables rondes qui suivront.

Bénédicte HUOT de LUZE

Avant d'entrer dans le vif du sujet, il nous a semblé important de réaliser un état des lieux de la profession et de comparer les niveaux de maturité de ces deux fonctions en matière de gestion des risques et d'audit interne. La gestion des risques organisée est un fait relativement récent et encore non normé. La loi de sécurité financière de 2008 a mis au goût du jour l'actualité juridique concernant la gestion des risques. Avant cela, nous ne pouvions nous reporter qu'à une évocation de la gestion des risques dans les NRE de 2001.

Annie BRESSAC

L'audit interne est normé depuis de nombreuses années. Il existe un cadre de référence international des pratiques professionnelles qui est régulièrement revu et enrichi. Il comporte une définition des normes, leur modalité pratique d'application, des guides pratiques, etc. Cette capitalisation d'expérience n'interdit pas l'évolution de nos métiers pour en améliorer la performance. Il convient à présent de rappeler les objectifs des deux fonctions.

Bénédicte HUOT de LUZE

La gestion des risques est un dispositif dynamique de la société défini et mis en œuvre sous sa responsabilité. Cette définition est issue du cadre de référence de l'AMF. On dit également que la prise de risques est inhérente à chaque société. L'objectif est de prendre des risques maîtrisés pour l'entreprise et, *in fine*, d'anticiper les risques pour ne pas les subir. La sécurisation de la prise de décision et la favorisation de l'atteinte des objectifs permettent d'allouer efficacement les ressources de l'entreprise. Il s'agit ensuite de favoriser la cohérence des actions avec les valeurs de la société et de fiabiliser la réputation de l'entreprise et sa crédibilité. Une gestion des risques efficace implique une mobilisation des collaborateurs sur une prise de risques globale, ce qui favorise l'appropriation du système de gestion des risques. L'atteinte de ces objectifs généraux demande du temps, l'appropriation du système par les opérationnels, leur responsabilisation et la compréhension de la prise de risques par tous les collaborateurs. Elle nécessite donc un travail en profondeur et une diffusion de la culture du risque qui n'est pas rapide.

Annie BRESSAC

En matière d'audit interne, la définition internationale a fixé le cap en 2000 afin que celui-ci puisse contribuer à créer de la valeur ajoutée. Pour cela, elle lui assigne une double mission : une mission relative à l'assurance sur le degré de maîtrise des opérations et une mission de conseil pour aider l'organisation à atteindre ses objectifs. Cette définition propose également un triple champ d'évaluation, au premier rang desquels figure le processus de management des risques. A celui-ci s'ajoutent le gouvernement d'entreprise et le contrôle interne. Ainsi, la contribution de l'audit interne à la performance de l'entreprise est très ambitieuse. Cette ambition renforce d'emblée la double exigence d'indépendance et de compétence. Entrons à présent dans la définition des missions du gestionnaire des risques ou *chief risk officer*.

Bénédicte HUOT de LUZE

Nous avons identifié six rôles pour le *chief risk officer* :

- la définition du système de gestion des risques et la garantie du bien-fondé de la méthodologie ;
- l'animation relative aux correspondants, à la diffusion de la culture du risque, à la périodicité, à l'élaboration des *reportings* et au contrôle du système ;
- la promotion des compétences en management des risques et la diffusion de la culture du risque dans l'entreprise ;
- la contribution à la définition de l'appétence de la gestion des risques et la rédaction de la politique de gestion des risques ;
- l'assistance aux propriétaires de risques dans leur plan de remédiation lorsque le risque a été qualifié d'inacceptable ;
- le compte rendu à la direction générale et au comité d'audit des risques majeurs, de leur traitement, de leurs évolutions et du système de gestion des risques dans son ensemble.

Le baromètre du *risk manager* de l'AMRAE est un document essentiel concernant les qualités personnelles attendues du *risk manager*. Celui-ci doit avoir un fort esprit de conviction, un esprit de synthèse développé, une vision globale de l'entreprise et un sens de la communication aiguisé.

Annie BRESSAC

Le rôle de l'auditeur interne en matière de management des risques est de plusieurs ordres. L'auditeur interne est à la fois utilisateur et parfois acteur de l'identification et de l'évaluation des risques. Il est contributeur au dispositif de management des risques. Enfin, il est évaluateur du dispositif. Ce champ d'action dépend en grande partie de l'existence et de la maturité du processus de management des risques dans l'organisation. En tout état de cause, il doit s'inscrire dans des limites définies par les normes professionnelles et clarifiées par les modalités pratiques d'application.

Les normes posent bien l'analyse des risques comme le double point d'entrée dans nos missions. Le plan d'audit doit être élaboré à partir d'une analyse des risques selon la norme 2010. La même phase d'analyse des risques doit accompagner chaque audit et être réalisée par l'auditeur lui-même ou par le *risk manager*. L'analyse des risques est également l'élément central de toutes les missions. Avant même de parler d'évaluation du dispositif, chaque mission d'audit doit comporter une évaluation de la gestion des risques. Ainsi, les constats d'audit comportent toujours une description et une évaluation des risques. Les recommandations que nous formulons concernent les mesures préventives, correctives et protectives qui permettront de mieux maîtriser les risques. Enfin, nous pouvons être amenés à détecter de nouveaux risques à l'occasion de ces missions.

L'évaluation de l'efficacité du processus de management des risques se produit au niveau de chacune des compétences du dispositif ou du processus. On voit donc que le risque constitue un sujet central pour nos deux fonctions qui ont nécessairement vocation à interagir.

Bénédicte HUOT de LUZE

Comment les fonctions peuvent-elles interagir ? Le gestionnaire de risques va construire la cartographie, les *reportings*, hiérarchiser les risques et travailler sur les plans d'actions avec les opérationnels. Une fois que les informations ont été validées par la direction, il les transmet à l'audit interne. Qu'en fait ce service ?

Annie BRESSAC

L'audit est utilisateur de cette cartographie. Il s'appuie sur ces éléments pour élaborer son plan d'audit et donne en retour de l'information aux *risk managers*. Il valide l'analyse de la cartographie mais peut également la compléter par des éléments nouveaux afin d'actualiser l'analyse des risques.

Bénédicte HUOT de LUZE

Les *risk managers* aident également la direction et les administrateurs à définir l'appétence pour le risque. Il revient en effet au gestionnaire de risque de formuler des propositions à la direction qui se prononcera avec les administrateurs. Ces éléments sont également transmis à l'audit interne.

Annie BRESSAC

L'audit interne a besoin de cette appréciation et de cette définition de l'appétence pour le risque pour apprécier l'efficacité du traitement des risques. Lorsque nous évaluons le contrôle interne, il est très difficile d'appréhender le niveau de risque cible, de ne pas tomber dans un excès de contrôle ou en déficit de contrôle. Nous avons besoin de connaître cette ligne pour mener à bien notre évaluation. Nous identifions par ailleurs au cours des missions des risques insuffisamment maîtrisés et formulons des recommandations qui peuvent intéresser le gestionnaire des risques.

Bénédicte HUOT de LUZE

Cela nous permet en effet de recueillir des informations sur des risques qui n'auraient pas été identifiés par les opérationnels ou au cours des entretiens. Nous pouvons ainsi fiabiliser notre cartographie des risques et notre évaluation des risques résiduels.

Annie BRESSAC

L'évaluation du dispositif de gestion des risques peut contribuer à la surveillance et au pilotage du dispositif de management des risques.

Bénédicte HUOT de LUZE

En effet, l'audit nous permet d'avoir un regard externe sur nos activités, de prendre du recul, d'avoir des recommandations pertinentes et intéressantes. Ainsi, nous pouvons mieux répondre aux exigences de la direction générale. Nous allons à présent nous intéresser à nos objectifs partagés.

Nos fonctionnements sont différents, nous interagissons et nous avons des objectifs partagés. Parmi ceux-ci, nous veillons à ce que la stratégie soit en adéquation avec la politique de risque. L'audit interne aura un regard de deuxième niveau sur ce sujet alors que la gestion des risques y veillera au premier niveau.

Annie BRESSAC

Notre deuxième objectif commun est la maîtrise des risques. Les auditeurs internes parlent de manière préférentielle du contrôle interne. Les gestionnaires des risques évoquent de manière plus globale la gestion des risques. Quoi qu'il en soit, nous devons couvrir la totalité de la palette. Ainsi, les auditeurs internes doivent également s'intéresser aux processus et aux dispositifs d'assurance, aux processus et aux dispositifs de gestion de crise.

Bénédicte HUOT de LUZE

Ensemble, nous contribuons aussi à la diffusion de la culture du risque et à l'appropriation des risques par les collaborateurs.

Annie BRESSAC

Enfin, nous participons au processus d'information des managers, des dirigeants et du comité d'audit sur l'exposition au risque, chacun apportant son éclairage spécifique sur le sujet. Parfois,

cette grande proximité peut poser question. Pour la bonne compréhension de nos rôles respectifs, il nous paraît important de mettre en évidence plusieurs points de vigilance.

Bénédicte HUOT de LUZE

Il nous semble important de disposer d'un langage commun et d'outils partagés. Un vocabulaire univoque permettra une meilleure diffusion de la culture du risque. L'univers de risque et les éléments de *reporting* doivent également être partagés.

Annie BRESSAC

La cartographie est précisément un point qui peut faire débat. Les deux fonctions doivent être indépendantes l'une de l'autre même si cela n'est pas toujours facile. Cette indépendance suppose un positionnement clair, pose la question du rattachement. La question de l'indépendance de l'auditeur par rapport à sa mission d'évaluation du dispositif est importante.

Bénédicte HUOT de LUZE

Il est également essentiel de développer des compétences spécifiques pour l'amélioration et la compréhension du mécanisme de gestion des risques.

Annie BRESSAC

Enfin, il convient de veiller à la bonne coordination des différents acteurs de la gestion et de la maîtrise des risques, ainsi que d'éviter les superpositions. Il est important de développer un esprit de synergie autour des objectifs partagés. Les exemples pratiques qui seront présentés lors des tables rondes permettront de débattre sur ce point comme sur les autres.

TABLE RONDE : CADRES ORGANISATIONNELS ET RELATIONS ENTRE L'AUDIT INTERNE ET LE RISK MANAGEMENT DANS LES SECTEURS BANQUES ET ASSURANCES

ANIMEE **PAR REGIS MONFRONT**, *INSPECTEUR GENERAL AU SEIN DU CREDIT AGRICOLE CIB.*

AVEC **EDOUARD-MALO HENRY**, *INSPECTEUR GÉNÉRAL, SOCIÉTÉ GÉNÉRALE* ;

CHRISTOPHE HIOCO, *CHIEF EXECUTIVE OFFICER, SOCIETE GENERALE CIB ;*

ANETTE DOLD, *HEAD OF GLOBAL INTERNAL AUDIT, ALLIANZ GLOBAL CORPORATE & SPECIALITY ;*

JUERGEN GUHE, *GLOBAL HEAD OF RISK MANAGEMENT, ALLIANZ ;*

PAUL-HENRI MEZIN, *DIRECTEUR DE L'AUDIT, MALAKOFF MEDERIC ;*

THOMAS COLIN, *DIRECTEUR DES RISQUES, MALAKOFF MEDERIC.*

Louis VAURS

Régis MONFRONT est depuis novembre 2009 Inspecteur Général du Crédit Agricole CIB, banque d'investissement et de financement. Il a débuté sa carrière professionnelle en 1981 à la banque Indosuez où il a successivement travaillé à la direction des risques puis comme responsable grande clientèle à Chicago avant de devenir directeur des financements d'actifs à New York puis directeur des risques actions à Paris. Après cinq ans passés à Hong-Kong, il était depuis 2002 responsable pays du Crédit Agricole Indosuez, puis de Calyon, au Royaume-Uni. Il possède donc une grande expérience internationale. Régis Monfront est également diplômé de HEC et titulaire d'une licence en droit.

Régis MONFRONT

Je voudrais simplement ajouter à cette présentation très complète que cette fonction d'inspecteur m'a été proposée cette fonction d'inspecteur en m'expliquant que les braconniers faisaient les meilleurs policiers. C'est donc la raison pour laquelle je me trouve devant vous.

J'ai aujourd'hui le privilège de vous présenter un panel de six personnes composé de praticiens distingués et éprouvés en matière de risques et d'audit interne, qui réunissent ensemble 100 à 150 ans d'expérience dans ces domaines.

Christophe HIOCO est *Chief Operating Officer* pour la Société Générale CIB. Spécialiste de la conduite de changement, il y assume actuellement la responsabilité de fonctions ressources humaines, risques opérationnels, risques de crédit et de gestion de portefeuille de crédit. Avant de rejoindre la Société Générale, Christophe HIOCO a exercé d'importantes responsabilités commerciales et opérationnelles au sein de McKinsey et JP Morgan en Europe et en Asie.

Édouard-Malo HENRY est Inspecteur Général pour l'ensemble du groupe Société Générale. Il dirige la direction du contrôle périodique regroupant mondialement 1500 inspecteurs et auditeurs. Il assume cette responsabilité depuis janvier 2010 après avoir occupé des fonctions très diverses au sein du groupe Société Générale depuis 1984, notamment celles de Secrétaire Général de la division grandes entreprises et institutions financières, et de Responsable des activités de la Société Générale au Canada.

Juergen GUHE is the Global Head of Risk Management of Allianz Global Corporate and Specialty, one of the key activities of the Allianz Group, specializing in providing insurance solutions across the whole spectrum of corporate and specialty risks worldwide. Prior to this role, he was the Chief Risk Officer of Fireman's Fund Investors Company, a US firm. Juergen GUHE joined Allianz Group in 2001, serving in various positions within Group planning and Group risks.

Anette DOLD has been Head of Global Internal Audit of Allianz Global Corporate and Specialty since 2008. She is in charge of audit services for all entities of AGCS globally. Prior to this role, Anette DOLD was in charge of risk control of asset management and banking entities within the Allianz Group from 2002 to 2008. Before joining Allianz, she spent 11 years at Citibank, mainly in credit finance and consumers with a focus on the credit card division.

Thomas COLIN est Directeur des risques à Malakoff Médéric. Il a débuté sa carrière à l'inspection de la Société Générale et a ensuite réalisé l'essentiel de son parcours chez BNP-Paribas Assurances. Après un passage chez PwC, il a rejoint le groupe Malakoff Médéric en 2010.

Dans ce groupe mutualiste, la gouvernance est assurée par des représentants des employeurs ainsi que par les cinq grandes confédérations syndicales de salariés. Le groupe exerce à ce titre deux métiers historiques : gestion des retraites complémentaires par répartition (caisses AGIRC et CARCO) pour 2,7 millions de retraités et 3 millions de salariés et une activité assurantielle plus classique et concurrentielle.

Paul-Henri MEZIN, Directeur de l'audit du groupe Malakoff Médéric possède une expérience de 20 ans en cabinet et en entreprise, dans l'audit et la maîtrise des risques en entreprises et en systèmes d'information.

The issue today is to determine how audit and risk management interact.

I. Exemple du Groupe Allianz

Juergen GUHE

First of all, I would like to thank you for the opportunity of talking to this audience today on the topic of risk management and audit. I will begin with a short introduction on Allianz Global Corporate and Specialty, or AGCS. We are a dedicated provider of insurance solutions for all types of corporate and specialty risks within the Allianz Group. We have an AA rating from S&P and an A+ from AM Best. Our GWP attains €4 billion and we are represented with branch offices or legal

entities in many countries. Even when we are not represented, we can use the global network of the Allianz Group.

I will begin with the three lines of defence approach taken at AGCS, and will then share some insights into how we define risk management responsibilities. Anette will then discuss the responsibilities and approach taken by internal audit, as well as the way in which internal risk management and internal audit cooperate with each other.

The three lines of defence approach has been defined not only for AGCS but also for the Allianz Group as a whole.

- In the first line of defence, process owners are responsible for managing their risks, and implementing and executing the controls for which they are responsible.
- The second line of defence consists of the oversight functions. Risk management is part of that second line of defence. Key responsibilities are first of all to define the framework in which the process or risk owners operate, but also to provide independent oversight, thereby ensuring that the functions operate within that framework.
- The third line of defence is basically internal audit. Its responsibility is to provide independent quality assurance of the processes. It reviews both the first and second lines of defence.

With respect to the risk management area, it is important to be aware of the fact that the AGCS board of management is ultimately responsible for appropriate risk management. It can to some extent delegate this responsibility, but in the end it has ultimate responsibility for the decisions taken. At AGCS, we create more visibility with respect to this ultimate responsibility by allocating certain top risks – that are identified in an annual process – to specific board members.

As I said earlier, the board of management may decide to delegate certain risk-relevant decision making to either certain functions or committees. It has in fact decided to delegate the responsibility for developing the risk management framework and the continuous monitoring of the risk profile to the risk management department and to the risk committee.

From an organisational perspective, the Chief Risk Officer of AGCS is a board member, which is not usual in the insurance sector. At AGCS, a deliberate decision was made to allocate a board seat to the CRO. This reflects the fact that, as a company, we deal with considerable corporate risks.

Three departments report to the CRO: actuarial, reinsurance and risk management. I am the Global Head of Risk Management and my key responsibility is thus to provide independent risk oversight that also covers the two other departments (actuarial and reinsurance). One could argue that there is a possibly of a conflict of interest in having reinsurance report to the CRO. However, at AGCS, neither the Head of Reinsurance nor the CRO can make any decisions about reinsurance. They can propose reinsurance programs to the reinsurance committee, and it is that latter body that makes the decision. Similarly, on the actuarial side, when it comes to the setting

of reserves, neither the CRO nor the Chief Actuary can make any decisions on reserves. Those decisions are made by the loss reserve committee.

All three departments and the CRO have global responsibilities. We do not operate in a country or regional mode, but for all the entities operating within AGCS.

One of the responsibilities of the risk management function is to develop the AGCS risk policy and risk strategy. Risk policy defines the universe of our risks and specifically addresses risk governance questions. In contrast, risk strategy defines AGCS's risk tolerance and appetite at a high level.

Our second responsibility is the development of globally consistent risk management processes. As I said earlier, we are not focused on one particular country. We are responsible for developing globally consistent risk management processes, which are then applied globally. We try to overcome the separation that often exists between risk management and the businesses. We therefore define our risk management processes in close cooperation with AGCS's different business lines and functions. It is not a closed doors exercise.

The risk strategy contains a definition of risk tolerance at the highest level of aggregation. This high level definition of risk tolerance is then broken down into more manageable elements, which are relevant for the lines of business and individual functions. We thus have to develop proposals on how to break down this definition into more granular limits that can be used for day-to-day management decisions. Again, we do not decide on those limits; we propose them to the risk committee which makes the ultimate decision.

We are also responsible for providing oversight and verifying that we stay within those limits. To that end, we report to the risk committee on how the actual exposure compares to the limits that have been defined.

We are involved in a number of day-to-day risk management activities, which are part of the first line of defence. When it comes to important problems or material risks, we help and support the business owner in developing an appropriate solution.

Another important responsibility of the risk management department is the review of new products. This means that we have full internal transparency with respect to the risk profile of a new product. In some cases, the risk profile may have to be mitigated.

Finally, we also have to ensure that we comply with regulatory requirements, in particular, Solvency 2.

In order to strengthen our role in independent risk oversight, the Global Head of Risk Management is represented in all committees as a non-voting member but has the right to veto decisions, escalating either to the AGCS board of management or the Allianz Group if necessary.

Anette DOLD

I will present the cooperation that takes place between internal audit and risk management. These are two different functions that do not overlap but cooperate with each other.

As in many other organisations, our mission statement describes the tasks of internal audit. We adopted a mission statement to make clear the fact that we are not a police function. The message is that we undertake an objective assurance function, which provides added value and assists the company. Our target is therefore the success and well-being of the company rather than teaching people what to do.

The second part of the mission statement shows that internal audit is an equal partner. We want to handle diverging opinions constructively and provide clear recommendations because we believe that collaboration is the best way to achieve results.

Our audit function reports directly to the Chief Executive Officer (CEO) in order to maintain independence. This means that we are in close liaison with the CEO, with regular meetings and one-on-ones in which we discuss what we observe.

Our on-going activities obviously include audit assignments. We look at the entire process – from end to end – in order to analyse the risks and understand the internal controls implemented within those processes. We assess those processes and their controls, and determine if they are working in reality. We ensure that they comply with our internal and external rules and guidelines, and we also consider whether or not the controls add value. We do not ask "What went wrong?" but "What could go wrong?"

While the audit assignment can be linked to *ex-post* detective work, we are able to take a preventative approach in our advisory and consulting role. We can help the business lines identify best practices within the Group, and apply them to their own circumstances.

Last but not least, our third area of activity is fraud prevention and detection. We are involved in awareness-raising programs by analysing controls within the company. We coordinate fraud risk assessments and, where suspicious cases arise, carry out investigations.

Our audit engagements follow a risk-based approach. Our first concern is always to detect if there is any risk at all. We then follow the usual approach for an audit function: we identify an audit plan, prepare for an audit, perform the audit, draw up a report and, finally, carry out follow-up.

At each and every step of this process, we look at the risk. We first carry out a risk assessment in order to prioritize audit topics. It is based on the same risk values that apply throughout the Allianz Group, as defined by risk management. However, we make our own assessment. We then prepare for the specific audit topic, going into a more detailed risk assessment through our interviews with different partners and stakeholders. We identify what could be considered as a sort of "control to be". We confront what we expect from the experience with the existing control processes, and ask "can certain risks materialise?"

Coming to the audit report, we focus on what could happen because a control is missing. We rate all of our observations in a type of "risk-rating", considering the potential frequency and severity of a given risk. We then provide an overall assessment to management of the effectiveness of the

area that has been audited. Finally, in our follow-up, we focus particularly on those issues that could result in a high risk for the company. The higher the risk, the more rapidly we should implement appropriate solutions.

You can therefore see that, while we obviously take input from risk management, we provide our own assessment, which is indeed the purpose of the exercise.

In terms of the cooperation between the two functions, we work hand-in-hand with each other, which avoids duplication. We use the input from risk management to define our annual audit plans. We exchange on the audits we are planning for the next year to ensure that we do not go into the same areas at the same time. We hold quarterly meetings between internal audit, risk management and the compliance function, as well as a wide range of informal meetings. We exchange information on operational losses and suspicious or fraudulent activities, perform joint fraud risk assessments, and provide each other with copies of our reports. I am also invited as a guest in each risk committee meeting.

There is thus close cooperation between our two functions, with no overlap or duplication of efforts.

Régis MONFRONT

You mentioned the important exercise of risk mapping for the audit function. Obviously, you work very closely with risk management. Would you elaborate on the respective roles of the two divisions in the risk mapping task? Who has ultimate responsibility for the audit plan?

Anette DOLD

Risk-mapping is carried out by risk management. We provide our input but we are not responsible for setting up the risk map or the risk universe. When we perform our audit plan, we define a risk universe, using the input of the risk management department.

Régis MONFRONT

Regarding the independence of the two functions, would you also elaborate on the reporting line of the audit function?

Anette DOLD

As I mentioned, we report directly to the CEO but there is also a link to the audit committee and, in Germany, to the supervisory board. I meet the Head of the supervisory board on a quarterly basis. Both the risk management and audit functions are represented in the audit committee.

Régis MONFRONT

Does the audit committee include other functions of the Group?

Anette DOLD

It does not include functions *per se*, but this will depend on what the audit committee is interested in. For example, if the audit committee wanted to gain insight on a specific topic, it could invite that function to its next meeting. However, the standard agenda topics concern internal and external auditors and risk management.

Question de la salle (personne travaillant chez Bouygues Telecom)

You stated that best practices were shared within the Allianz Group. What is your view on sharing best practices with other companies?

Juergen GUHE

That very much depends on the circumstances. There may be areas where we are prepared to share best practices. In other cases, we may prefer to keep our best practices within the Group as they may, at least in the short-term, provide us with a competitive advantage.

Anette DOLD

I believe that best practices can certainly be shared when it comes to our own work or our own implementation. However, when it comes to specific risk topics in insurance, we are not really willing to share.

II. Exemple de la Société Générale

Christophe HIOCO

J'ai commencé ma carrière en tant qu'auditeur interne chez JP Morgan, à l'époque des débuts d'IFACI. Je peux constater que vous avez connu un développement phénoménal. Nous avions commencé à l'époque à proposer quelques formations qui ont visiblement montré la voie si je me reporte à vos propositions en ce domaine.

Cette expérience autour des risques que l'on peut rencontrer dans une entreprise et en particulier dans une banque d'investissement m'est très précieuse dans le poste que j'occupe actuellement. Les spécificités d'une banque d'investissement en termes de contrôle interne et de risques tiennent tout d'abord à un environnement extrêmement compétitif et dans la capacité d'un tel établissement à concevoir de nouveaux produits ou à les faire évoluer. Les cycles de développement de nouveaux produits sont beaucoup plus courts (de l'ordre de quelques heures à quelques jours parfois) que dans l'industrie. Les banquiers et traders sont par ailleurs extrêmement créatifs et motivés par la réalisation de profits concrets. Il existe donc des zones de risque considérables. Une autre particularité de la banque d'investissement est le caractère binaire de sa valeur ajoutée : on peut gagner comme perdre beaucoup d'argent. Le risque y est donc omniprésent, particulièrement dans notre banque, réputée mondialement pour ses produits structurés et sur-mesure. Le risque y est aussi pervers, car à la différence de l'industrie, il n'est pas vital. Des risques se développent sans que l'on en prenne conscience.

Un nouveau challenge se présente aux banques d'investissement : celui que constitue le changement de leur environnement. En effet, à la suite de la crise financière, le monde des banques d'investissement ne sera plus jamais le même. Auparavant, une crise offrait l'opportunité de se repositionner, d'investir sur de nouveaux produits ou de nouvelles activités. Cette fois-ci, l'embellie post-crise n'a duré que quelques mois. Les nouveaux règlements légitimement mis en place par les Etats vont impacter significativement nos activités. Nous devrons revoir nos portefeuilles de produits et il est très prévisible que la rentabilité de nos activités diminue.

L'ensemble des banques d'investissement ont pour préoccupation de s'adapter à cette nouvelle réalité, d'augmenter leur efficacité pour maintenir le niveau de profitabilité, le *return on equity*, à un niveau satisfaisant. De nouveaux risques vont apparaître, du point de vue du contrôle interne, en raison d'un certain nombre de coupes liées à la nécessité d'augmenter la productivité. Un équilibre doit cependant être trouvé entre la maîtrise de notre risque opérationnel et la nécessité d'accroître notre efficacité. Ces deux objectifs n'entrent pas en conflit selon moi.

J'ai rejoint la Société Générale il y a deux ans pour travailler sur le projet « Résolution » qui avait déjà pour objectif de nous préparer à ce nouvel environnement. Ce projet s'articulait autour de quatre axes :

- le développement de notre activité ;
- le développement de nos collaborateurs ;
- la question de la productivité et de l'efficacité ;
- le risque opérationnel.

Le quatrième point de ce programme de changement me paraît essentiel. Le risque opérationnel est en outre le levier le plus important en termes d'efficacité. Un risque élevé signifie en effet que les *process* ne sont pas suffisamment définis, que le personnel n'est pas correctement formé ou que le *straight through processing* n'est pas complètement transparent. Ces facteurs de risques sont aussi des facteurs d'inefficacité. S'attaquer au problème du risque permet donc d'augmenter significativement la productivité.

Dans le métier du contrôle interne, les réglementations sont une base importante en vue de définir les principes de contrôle. Le comité de Bâle qui réglemente nos banques a défini des principes qui ont ensuite été adaptés dans l'environnement français. A nous non seulement de les suivre, mais aussi d'aller jusqu'au niveau le plus pertinent dans l'intérêt de nos clients et actionnaires. Deux grands axes constituent le contrôle interne : le contrôle permanent et le contrôle périodique, dont Edouard-Malo Henry parlera plus précisément ensuite.

Le contrôle interne permanent relève de notre responsabilité en tant que managers, responsables, avant même d'être de la responsabilité des auditeurs. Malheureusement, il est nécessaire de répéter inlassablement cette idée pour que les personnels soient suffisamment responsabilisés. Le contrôle permanent est une question de procédures et de *process* mais aussi, et l'on a tendance à l'oublier, une affaire de personnes. Il s'agit de s'assurer que chacun est compétent dans le métier exercé (ce qui est un challenge puisque nos métiers évoluent très vite), que le personnel est bien formé et alerte en ce qui concerne les risques. La responsabilisation de chacun est indispensable et ne doit pas souffrir d'un fonctionnement bureaucratique dans lequel on appliquerait « religieusement » les contrôles mais sans en retirer la substance.

Le contrôle permanent intégré d'une part aux *process* et aux responsabilités de chacun comme je viens de le décrire, bénéficie aussi d'autre part de fonctions dédiées : le contrôle permanent de la conformité, celui de la sécurité des opérations (une fonction essentielle qui est occupée dans notre banque par un membre de la direction générale) et l'ensemble de la filière risques.

En tant que *Chief Operating Officer*, confronté à de nombreux risques inhérents aux activités que je supervise, je m'appuie sur une direction que nous avons créée au niveau de la banque d'investissement, dédiée à la sécurité des opérations et à la prévention de la fraude. L'acronyme en anglais de cet intitulé, SAFE, traduit parfaitement notre objectif. Cette organisation regroupe près d'une centaine de personnes mondialement, au sein de cette direction et parmi les *Operation Security Managers.* Il s'agit bien sûr d'une fonction globale dédiée à la gestion des risques opérationnels, domaine dans lequel il m'apparaît essentiel de faire des progrès continus.

Les grands rôles de cette fonction sont :

- **L'évaluation des risques**

  Cette évaluation s'effectue à partir de scénarios qui nous permettent de nous remettre continuellement en cause et d'améliorer le contrôle.

- **La définition et la surveillance d'indicateurs clés**

Ces indicateurs sont revus au niveau de la direction générale et de l'*Operating Committee* de la banque d'investissement.

- **L'analyse des incidents**

Cette démarche s'inscrit dans une logique de formation permanente et se décline au travers d'un dispositif que j'ai mis en place il y a 18 mois. Lors de chaque incident, qu'il s'agisse d'une perte opérationnelle dépassant un certain montant ou d'un incident révélant un comportement inadapté relativement à un *process* ou de la part d'un manager, l'équipe SAFE produit une analyse détaillée et indépendante. Ces rapports sont ensuite étudiés par l'*Operating Committee* qui rencontre les managers concernés avec pour objectifs essentiels l'apprentissage et la responsabilisation de chacun.

Comme je l'ai dit, le risque est plus important dans notre secteur d'être plus laxiste que dans l'industrie. Le groupe SAFE a donc aussi pour vocation d'observer d'autres secteurs économiques pour s'en inspirer. Nous avons ainsi fait intervenir un pilote, chef instructeur d'Air France, qui nous a fait des présentations passionnantes sur les rapports d'incidents, la maîtrise des risques à partir des paramètres d'un vol. Tous nos managers ont l'obligation de suivre régulièrement des présentations proposées par le groupe SAFE avec la contribution de l'audit. Le processus d'amélioration des procédures et des compétences des personnels est donc continu.

Notre dispositif de surveillance permanente nous permet d'avoir une maîtrise de nos risques tout à fait satisfaisante pour nos clients et nos actionnaires.

Edouard- Malo Henry

J'ai été nommé il y a un an, c'est-à-dire environ deux ans après l'affaire Kerviel, qui a représenté un risque quasi fatal pour notre banque. Ma nomination est intervenue dans un contexte difficile, à une époque où les équipes d'audit étaient éparpillées dans les lignes de métiers et dans le monde. On m'a demandé de les regrouper avec également l'Inspection Générale en une Direction de manière à accroître très concrètement la compétence, le professionnalisme et l'efficacité dans ces fonctions.

Je voudrais dire quelques mots tout d'abord sur la culture de contrôle, puis sur les interactions entre le contrôle permanent, la filière risques et l'audit, et vous indiquer enfin quels sont selon moi les écueils à éviter pour la direction audit d'une banque ou d'une entreprise.

Séverin CABANNES expliquait ce matin que, même lorsqu'elle affecte 5 % de ses effectifs à la fonction de contrôle, une banque n'est pas à l'abri de problèmes. Le bon fonctionnement de l'entreprise repose avant tout sur sa culture de contrôle. Les corps de contrôle peuvent être multipliés ou renforcés, mais ils ne sont là qu'à titre de dernier rempart, pour renforcer encore le fonctionnement sécuritaire de l'entreprise. En effet, il n'est pas pertinent de considérer que l'entreprise exerce deux types de métiers : celui de gagner de l'argent et celui de ne pas en perdre. Le bon pilote doit savoir manier à la fois l'accélérateur et le frein. De plus, cette culture de contrôle doit venir d'en haut et non de la base. La direction de l'entreprise doit montrer à quel

point l'environnement de contrôle est important et « toucher au portefeuille » les managers qui ne le respecteraient pas.

J'en arrive aux trois niveaux de contrôle que sont le contrôle permanent, la filière risques et l'audit. Leur challenge commun est d'être branchés sur le vivant de l'entreprise.

Dans cette logique, le contrôle permanent doit aider chaque manager mais non se substituer à lui, En effet, les managers sont ici responsables comme l'a expliqué Christophe Hioco. La filière risques est plus proche du vivant de l'entreprise car elle s'intéresse aux flux, donne son accord sur les dossiers et surveille précisément les stocks. Contrairement au contrôle permanent qui est intrinsèquement lié au manager, la filière risques est indépendante par nature dans ses décisions mais doit investir beaucoup dans la fluidité des échanges avec les opérationnels qu'elle accompagne. L'audit est bien sûr indépendant, mais doit se nourrir, à plusieurs stades, de ses relations avec le contrôle permanent et la filière risques.

A la première étape du *risk assessment*, des débats existent sur la provenance de la cartographie utilisée par l'Audit. Je suis d'avis qu'il faut utiliser le même langage et les mêmes outils que la Direction des Risques, mais cela ne signifie pas que l'on s'en contente. Ensuite, dans la conduite des missions, le dialogue doit être engagé en amont de la mission, tandis que l'écart entre les perceptions et la réalité doit être discuté en aval. Pour être utiles et mises en œuvre, les recommandations émises doivent être comprises par le contrôle permanent qui doit également se les approprier.

La question des relations devient plus actuelle en raison de la montée en puissance de la Direction des risques, elle-même liée à l'augmentation des risques qui résulte de l'accroissement de la complexité des opérations. Le *Chief Risk Officer* est membre du comité exécutif, tandis que le responsable de l'audit ne peut pas l'être de mon point de vue, pour des raisons d'indépendance. L'audit, cependant, reporte au *Chief Executive Officer*, ce qui est un élément clé.

Je voudrais terminer en vous présentant les points de vigilance que j'ai identifiés pour la fonction d'audit.

Le premier écueil consisterait à considérer d'un point de vue salutaire l'impact des régulateurs sur la crédibilité ou la reconnaissance de la fonction audit. Ne nous contentons pas d'être là parce que le régulateur nous le demande et de faire ce qu'il nous demande de faire. Un véritable audit s'affirme par sa compétence, qui s'apprécie à sa capacité à vérifier que les risques sont bien identifiés, encadrés et que le pilotage et le suivi sont bien réalisés.

Le second écueil serait de trop se concentrer sur la production d'indicateurs d'ordre statistique de la performance de l'audit, par exemple des taux ou durées de réalisation des plans d'audit annuels. Ne perdons pas de vue l'essentiel : il s'agit de mettre en évidence vis-à-vis de la direction générale les angles morts et les risques d'accidents. Un audit ne doit pas se contenter d'effectuer des vérifications formelles de procédures, mais porter un jugement d'ensemble sur les pratiques. La légitimité de l'audit dans l'entreprise tient aussi à cette fonction de jugement et d'alerte. Un CEO doit échanger avec son responsable d'audit régulièrement et la crédibilité de l'audit se joue à la capacité de son responsable à mettre en valeur les points de vigilance les plus importants.

Régis Monfront

Selon vous, quels éléments ont-ils le plus influencé l'audit interne et la gestion des risques depuis deux ou trois ans ? Est-ce la crise de 2008 ou la présence accrue du régulateur ?

Edouard-Malo HENRY

Tout concorde en réalité. De nombreuses banques ont disparu, d'autres ont fusionné ou ont été rachetées. Le régulateur a pris conscience qu'il était trop lointain dans sa manière de superviser les banques. Par la conjugaison des instincts de survie des organismes financiers comme des régulateurs, le monde a changé définitivement. Il s'agit bien d'un mouvement de fond qui ne doit pas se vivre comme une réponse bureaucratique à une question réglementaire. Soyons au contraire des organismes vivants au service du vivant de l'entreprise.

Régis Monfront

Quel impact la montée en puissance de la direction des risques a-t-elle eu sur l'audit interne ?

Edouard-Malo HENRY

Cette montée en puissance est relativement récente. Alors qu'auparavant, l'audit réalisait son évaluation des risques de son côté, il est désormais challengé de deux côtés : par la filière risques qui se professionnalise et se dote de vrais outils et par les exigences du régulateur. L'audit ne doit donc pas rester passif, mais se poser les bonnes questions. Cet environnement peut être un stimulant très positif.

Régis Monfront

Christophe Hioco nous a livré un plaidoyer pour la conduite du changement. Qu'en est-il du lancement de nouveaux produits ?

Christophe HIOCO

Le sujet des nouveaux produits est essentiel dans notre environnement et tout lancement suppose un renforcement de notre contrôle interne.

Quasiment tous les jours, nous tenons un comité de nouveaux produits à travers le monde. Nous avons mis en place un *process* très rigoureux pour les nouveaux produits, amenant à des décisions tout à fait indépendantes du *business*. L'objectif est d'abord d'identifier l'ensemble des risques résultant de ces nouveaux produits. Nous demandons dans cet esprit un mémo formel de présentation du nouveau produit avec tous ses risques inhérents. Avant de nous réunir en ce comité, nous demandons à chacune des fonctions qui contribuent à notre environnement de contrôle interne et de développement de l'évaluer par rapport à des grilles de critères. En outre, le comité de nouveaux produits est présidé par la direction des risques et par le CEO ou son représentant. La décision ultime est prise de manière complètement indépendante par les deux co-présidents du comité.

Cette démarche exige que nous soyons très réactifs au *business*. En effet, si la procédure devient trop bureaucratique, nous courons d'autres types de risques, commerciaux cette fois-ci. La mobilisation de toutes les ressources compétentes pour évaluer de nouveaux produits, parfois en 48 heures, doit être très rapide et efficace.

L'an dernier, nous avons défini 1 900 conditions de mise en place en rapport avec ces 200 à 250 approbations de nouveaux produits. Nous devons aujourd'hui nous assurer que ces conditions sont respectées.

Régis Monfront

Qui assure la sécurité des systèmes d'information à la Société Générale ?

Christophe HIOCO

De la même manière que pour les fonctions décrites tout à l'heure, le premier contrôle s'effectue au niveau des groupes IT eux-mêmes. Nous avons une fonction dédiée à la sécurité informatique, qui entretient des relations étroites avec le groupe SAFE dont j'ai parlé tout à l'heure.

III. Exemple de Malakoff Médéric

Thomas COLIN

Malakoff Médéric est, comme l'a rappelé Régis Monfront, un groupe de protection sociale à double gouvernance, paritaire et mutualiste, ce qui entraîne certaines obligations et contraintes spécifiques. La première de nos deux activités majeures concerne la gestion des cotisations et le versement de prestations de retraite complémentaire, activité pour laquelle nous sommes en délégation de service, sous une réglementation propre. Notre deuxième activité, l'assurance de personnes, est concurrentielle, régie par les codes de la sécurité sociale, des assurances, et de la mutualité, sous gouvernance et revue de l'autorité de contrôle prudentiel.

L'enjeu majeur, dans le cadre de cette deuxième activité, pour une organisation comme la nôtre consiste à mettre en œuvre, à l'horizon 2013, la directive Solvabilité 2. Dans nos environnements de l'assurance et de la mutualité, les obligations réglementaires ont vu le jour plus tardivement que dans le secteur bancaire et vont prendre une importance plus significative encore dans le cadre de Solvabilité 2. Cette directive nous impose de trouver un équilibre entre une prise de risque inhérente à l'activité d'assurance et la préservation de l'intérêt des différentes parties prenantes à l'organisation. Pour un groupe paritaire ou mutualiste comme le nôtre, les parties prenantes vont au-delà des clients ou des investisseurs, puisqu'elles incluent les organisations syndicales, patronales, les entreprises clientes, les assurés finaux. Nous avons une vocation sociale qui prend tout son relief dans ce cadre.

Solvabilité 2 met en avant l'équilibre de la gouvernance entre différentes parties prenantes, à la fois organes de direction et fonctions clés qui vont prendre de plus en plus d'importance au sein des compagnies : gestion des risques, conformité, fonction actuarielle, et audit interne. Notre paysage est donc plus large que les seules fonctions gestion des risques et audit interne.

Paul-Henri MEZIN

Nous sommes en effet un groupe composé de multiples institutions (Institutions de Retraite complémentaire, Institutions de Prévoyance, Mutuelles, Compagnie d'assurance, société de gestion d'actifs, …) et donc soumis à un certain nombre de codes. Nous avons deux commissions d'administrateurs dédiées à l'audit et au contrôle des risques, respectivement sur le secteur de la Retraite complémentaire et sur le secteur Assurantiel... En termes de gouvernance, ce sont ces commissions qui font le lien entre la partie audit et la partie contrôle des risques.

Au niveau organisationnel, nous avons séparé de manière classique la fonction de contrôle permanent et celle de contrôle périodique. Cette dernière a en charge pour l'ensemble des entités la revue générale et indépendante de tous les dispositifs et elle est rattachée directement à la délégation générale.

Les activités opérationnelles sont rattachées en fonction des activités aux différentes structures du groupe. Au sein du contrôle permanent, la direction des risques comporte plusieurs pôles : le *risk management* qui fixe le cadre méthodologique du dispositif ; le contrôle interne qui pilote le dispositif ; le pôle conformité chargé de la gestion du risque, de la fraude et de la lutte anti-blanchiment et, enfin le pôle sécurité des systèmes d'information.

Afin que ce système fonctionne, nous avons mis en place deux comités internes – à la différence des commissions, ceux-ci ne comprennent pas d'administrateurs – chargés pour l'un des risques et pour l'autre de l'audit. Plus précisément, le comité d'audit a en charge le suivi des plans d'actions et programmes d'audit et le comité des risques suit le travail de cartographie des risques. A ce dispositif s'ajoutent des comités de coordination au niveau du contrôle interne.

Thomas COLIN

La direction des risques a pour vocation d'accompagner les opérationnels et d'être au cœur de l'activité.

Sur les quatre domaines d'activités de la fonction risques (contrôle interne, pôle conformité, pôle sécurité et *risk management*), nous nous référons sans grande originalité aux référentiels connus et utilisons deux outils principaux. Nous avons tout d'abord mis en place une base d'incidents. A cet égard, je ne peux que souscrire aux propos tenus par Christophe Hioco sur l'importance de l'identification et de l'analyse des incidents pour l'amélioration de la maîtrise des risques. Notre deuxième outil est un registre des risques qui a vocation à prévenir ou anticiper sur des risques émergents. Nous misons beaucoup sur l'intelligence collective et le croisement de regards, de professionnels d'autres secteurs notamment, qui peuvent nous apporter un éclairage intéressant sur des évolutions comportementales ou juridiques.

Dans l'évaluation des risques ensuite, nous mêlons approches quantitatives et qualitatives : modèles de calcul de solvabilité ou de capital économique, coordonnés avec l'usage des cartographies, soit au niveau des risques majeurs qui doivent attirer l'attention d'une délégation générale, soit au niveau des processus dans une démarche plus opérationnelle.

L'approfondissement des travaux et des réflexions en matière de gestion des risques suscite des questionnements relativement nouveaux pour nos métiers. Par exemple, la formulation par une direction générale de son appétit au risque n'est pas une question simple.

Le dernier point essentiel consiste bien sûr à faire vivre le dispositif au moyen d'un système de pilotage, de *reporting* et d'indicateurs.

Cette approche se décline naturellement dans les opérations, avec des relais qui ont en charge de diffuser cette culture du risque et cette méthodologie sur différents sujets.

Paul-Henri MEZIN

La mission classique de la direction de l'audit est d'apporter aux différentes entités de gouvernance une évaluation, des conseils et des recommandations sur les processus internes de gestion des risques.

Nous sommes amenés à nous exprimer sur trois axes essentiels : l'efficacité, la sécurité et le bon respect de la réglementation.

Notre deuxième objectif vise à informer les entités de gouvernance sur leur exposition au risque au travers des dysfonctionnements identifiés dans le cadre de nos missions. Cette évaluation sert aussi de base pour l'échange avec la direction des risques.

Enfin, notre mission consiste aussi à évaluer les plans d'actions mis en place relativement aux recommandations de l'audit. Notre intervention peut également en cas de besoin particulier être ponctuelle et concerner une activité spécifique.

Dans notre fonctionnement classique, il est intéressant de noter nos échanges avec les différents organismes de contrôle, dont les commissaires aux comptes, mais aussi les autorités de contrôles propres à nos activités de retraite complémentaire et d'assurance. Nous n'en sommes cependant pas leurs interlocuteurs permanents.

Le périmètre de l'activité d'audit couvre toutes les entités du Groupe. Nous ne sommes pas une société capitalistique, si bien qu'il est difficile d'en définir les limites. En quelque sorte, nous allons là où la délégation générale nous dit d'aller.

Il est également intéressant de souligner que notre organisation s'appuie sur deux pôles : un pôle support et un pôle métier qui se décompose lui-même en un pôle Retraite complémentaire et un pôle Assurance. Notre pôle support est constitué de manière classique d'auditeurs dans les domaines de la comptabilité, de la finance, de l'informatique ou d'activités plus transverses. Au sein de notre pôle métiers, nous avons renforcé nos forces avec des équipes spécifiques en Assurances (avec par exemple 2 actuaires au sein de l'équipe d'audit de ce pôle)

Notre dispositif est structuré au travers d'une charte d'audit, d'un code de déontologie, de plans d'audit construits à partir d'une cartographie de l'audit confrontée à la cartographie des risques du Groupe établie par la direction des risques, ainsi qu'une procédure d'audit classique faisant intervenir lettres de mission et rapports contradictoires.

Tous nos rapports et plans d'actions sont transmis à la direction des risques. Nos rapports alimentent la cartographie des risques et les plans de contrôle suivis par la direction des risques. Nous challengeons la cartographie des risques puisque notre regard est différent.

Le travail de coordination est également important car les opérationnels sont confrontés à de multiples plans d'actions. Ces derniers doivent être coordonnés pour ne pas multiplier les actions à suivre sur un sujet donné.

Pour notre groupe, le premier enjeu des 24 prochains mois sera de trouver un équilibre entre les enjeux du *business* et la nécessité de maîtriser les risques. Notre deuxième enjeu, qui représentera un travail important, consistera à ancrer la gestion des risques dans les processus de décision, une habitude qui n'est pas encore bien intégrée dans notre secteur d'activité.

Il faudra aussi développer une culture du risque à tous les niveaux de l'organisation, de la direction aux niveaux les plus opérationnels. En particulier, la direction des risques a été créée en 2008. Elle se met donc peu à peu en place et doit s'installer.

Notre quatrième enjeu sera de pouvoir mobiliser des ressources humaines suffisantes, en nombre et en compétences. Nous avons déjà renforcé le pôle métiers au sein de l'audit interne, tandis que Thomas Colin monte actuellement une équipe dédiée au *risk management*.

Nous devrons enfin nous adapter aux nouvelles qualités de pilotage requises, c'est-à-dire les notions de vision prospective, d'anticipation et de réactivité nécessaires dans nos métiers.

Je voudrais ajouter un point entendu lors d'une conférence à l'IFACI. Souvent, les directions de l'audit ont été les premières à aborder ces questions de risques. Aujourd'hui apparaissent dans

notre secteur d'activité ces notions de contrôle permanent, de contrôle périodique qui nous viennent de la banque. L'audit interne doit savoir laisser à la direction des risques la possibilité de s'exprimer et de prendre son envol. Malgré l'envie parfois de suivre les aspects opérationnels, la direction de l'audit doit savoir prendre du recul et laisser à la direction des risques la charge de développer cette activité.

Question de la salle

Vous évoquiez une cartographie des risques appliquée par l'audit. Pourriez-vous décrire par un ou deux exemples la nature de cette adaptation ?

Paul-Henri MEZIN

Notre cartographie relève d'une vision par macro-*process* et qui est établie sur une douzaine de risques. Cet outil est simple et ne rentre pas dans un niveau de détail précis, mais donne une vision globale de l'ensemble des activités du groupe par rapport à ces douze critères de risques. Par exemple, sur les sujets de pilotage ressources humaines, nous avons un macro-*process* nommé « pilotage ressources humaines » et une problématique réglementaire, une problématique systèmes d'information et qualité des données, une problématique sur le contrôle interne, etc…. Nous plaçons l'équivalent de gommettes – quatre niveaux de gommettes - sur chacune de ces activités pour indiquer si elles présentent ou non un risque.

La cartographie des risques de la direction des risques, quant à elle décrit beaucoup plus finement la vision risques, notamment au travers de scénarios.

Notre niveau de cartographie des risques est bien différent, mais ces différents éléments nous permettent de construire notre plan d'audit, alimenté par la cartographie du risque majeur et par celle de la direction des risques. Dans le même temps, nous challengeons donc la cartographie de la direction des risques.

Question de la salle

Etant moi-même directeur de l'audit interne, je souhaiterais poser une question en forme de provocation. Si un système de contrôle permanent, une direction des risques fait parfaitement son travail et que l'on dispose d'une base de remontées d'accidents parfaitement exploitée, est-ce que cela ne retire pas l'essentiel ou en tout cas une grande partie des champs de travail de l'audit interne ?

Edouard-Malo HENRY

Si les opérationnels faisaient parfaitement leur travail et étaient complètement conscients des enjeux de contrôle, aurait-on besoin d'un contrôle permanent ?

L'expérience montre que ces trois niveaux de protection sont nécessaires. Séverin Cabannes identifiait ce matin trois risques ou trois enjeux pour nos fonctions : la destruction de valeur, le risque de réputation et la protection du fonds de commerce. De nombreuses entreprises ont disparu ces dernières années, ce que l'on n'observait pas auparavant. Le niveau des risques n'a jamais été aussi élevé, puisqu'en quelques jours, on peut perdre sa valeur ou son fonds de commerce. Ces filets de sécurité sont donc tous nécessaires.

En outre, l'avantage de l'audit tient à ce qu'il n'est pas plongé dans le stress de l'activité quotidienne. Pour avoir constaté qu'il n'est déjà pas évident pour le contrôle périodique de détecter les « éléphants dans les couloirs », je peux affirmer que le recul et le détachement sont absolument nécessaires pour repérer les angles morts, les gros accidents potentiels. Les personnels des directions des risques sont épuisés par le flux quotidien des tâches urgentes. Au niveau du contrôle permanent, les ressources humaines sont, elles aussi, épuisées par l'urgence, comme celle des comités nouveaux produits. Le recul et la capacité à analyser objectivement les enjeux sont d'autant plus nécessaires.

Si la question du principe n'est pas en jeu, celle des moyens se pose, car nous n'aurions dans le cas évoqué peut-être pas besoin d'autant de ressources qu'auparavant.

Régis MONFRONT

Il est temps de conclure. Les débats et présentations ont été très riches et l'échange transparent. Je voudrais apporter très rapidement quatre commentaires :

Tout d'abord, les fonctions de risque comme d'audit sont confrontées à un environnement passionnant mais difficile. Nos fonctions sont plus que jamais au cœur de la gouvernance.

Ensuite, les processus sont très importants et les intervenants ont souligné la nécessité de clarifier les responsabilités et les rôles de chacun.

En outre, l'intervention avec le vivant et la qualité de jugement ne doivent pas être négligées comme l'a souligné Edouard-Malo Henry. Nos fonctions participent à la vie quotidienne de l'entreprise.

Enfin, la notion de culture est très importante. L'exemple en la matière doit venir d'en haut. Le management définit l'appétit de risque tandis que le comportement des opérationnels définit la capacité de l'entreprise à réaliser un retour sur capital satisfaisant et à éviter les écueils et angles morts.

Je remercie chacun de cette matinée très enrichissante.

TABLE RONDE : CADRES ORGANISATIONNELS ET RELATIONS ENTRE L'AUDIT INTERNE ET LE RISK MANAGEMENT DANS LES SECTEURS DE L'INDUSTRIE, DU COMMERCE ET DES SERVICES

ANIMEE **GERARD LANCNER,** *PRESIDENT DE L'ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE (AMRAE).*

AVEC **FLORENCE VINCENT**, *DIRECTRICE DE L'AUDIT INTERNE ET DES RISQUES, MICHELIN ;*

PHILIPPE HATRON, *DIRECTEUR DE L'AUDIT INTERNE GROUPE, AREVA ;*

PHILIPPE OBERT, *DIRECTEUR DE L'ASSURANCE ET DE LA GESTION DES RISQUES, AREVA ;*

BRUNO DUNOYER DE SEGONZAC, *DIRECTEUR DE L'AUDIT INTERNE ET DE LA GESTION DES RISQUES, BOUYGUES TELECOM.*

Louis VAURS,

La table ronde de cet après-midi sera consacrée aux cadres organisationnels et aux relations entre l'audit interne et le *risk management* dans l'industrie, le commerce et les services. Des intervenants représentant les sociétés Michelin, Areva et Bouygues Telecom participeront à cette table ronde, qui sera animée par Gérard LANCNER, président de l'AMRAE.

Gérard LANCNER

Nous tenterons de démontrer en quoi les équipes d'audit interne et de gestion des risques peuvent être complémentaires et de mettre en lumière le rôle et les responsabilités respectives de ces acteurs. L'objectif de cette table ronde n'est pas de rappeler ce que sont nos missions mais de clarifier les rôles des équipes d'audit et de gestion des risques. Si nos objectifs et nos missions sont communs, quelle doit être la répartition des tâches entre l'audit et les risques ?

J'ai le plaisir d'accueillir à cette table ronde Florence VINCENT, Directrice de l'audit interne et des risques du groupe Michelin. Comme vous le constatez, Florence VINCENT est responsable tant de l'audit interne que des risques. Je vous présente également Philippe HATRON, Directeur de l'audit interne et Philippe OBERT, Directeur de l'assurance et de la gestion des risques du groupe Areva. Contrairement à la société Michelin, Areva a opté pour la séparation de ses fonctions d'audit interne et de risques et a décidé de rattacher l'assurance à la Direction de la gestion des risques. Bruno DUNOYER de SEGONZAC, Directeur de l'audit interne, des risques et du contrôle interne de la société Bouygues Telecom, nous rejoindra dans quelques instants.

Ces trois exemples montrent qu'il n'existe ni de modèle préconçu ni de modèle unique. En réalité, il est important de mettre en place une organisation qui corresponde à votre entreprise, à sa culture, à celle de ses hommes et de sa direction. L'organisation de l'audit interne et des risques doit être efficace, étant entendu que l'efficacité dépend étroitement de la culture d'une entreprise et de son histoire. Nous retrouvons à travers ces trois illustrations les quatre fonctions

principales que nous évoquons depuis le début de cette journée, c'est-à-dire l'audit interne, la gestion des risques, le contrôle interne et les assurances. La plupart des entreprises regroupent certaines de ces fonctions, compte tenu de leur culture et de leurs spécificités.

Nous avons privilégié aujourd'hui des interventions courtes afin de laisser la place aux échanges. Vous disposerez de trente minutes à la fin de chaque intervention afin de poser toutes les questions que vous jugerez utiles.

Le groupe Areva réalise un chiffre d'affaires de 9 milliards d'euros avec un effectif de près de 48 000 personnes. Areva est une société anonyme cotée à Paris, et elle est dotée d'un directoire, d'un conseil de surveillance et d'un comité d'audit. Ce groupe compte 14 directions fonctionnelles, soit une direction par métier, et exerce des activités à l'international.

Le groupe Michelin réalise un chiffre d'affaires de 18 milliards d'euros avec un effectif de 108 000 personnes. Société en commandite par actions, Michelin dispose de trois collèges pour les gérants, les commandités et les commanditaires, d'un conseil de surveillance et d'un comité d'audit, ce groupe étant coté au CAC 40. Les quatre lignes de produits de Michelin sont le tourisme, les poids lourds, les spécialités et les biens dédiés à la consommation intermédiaire. Ce groupe compte 13 directions opérationnelles et la couverture de ses activités est mondiale.

Le groupe Bouygues Telecom enregistre un chiffre d'affaires de 5,6 milliards d'euros avec un effectif de plus de 9 000 personnes. Société anonyme cotée à la Bourse de Paris, Bouygues Telecom dispose d'un comité d'audit et ne couvre que le marché français.

En ce qui concerne l'organisation, la Direction de l'audit interne d'Areva est rattachée à la Direction de la conformité, tandis que la Direction des risques et des assurances est rattachée à la Direction financière. Un chargé du contrôle interne rapporte à la Direction de la conformité. Au sein de Michelin, la Direction de l'audit interne et des risques est rattachée à l'un des co-gérants ; la Direction de l'assurance et le service de contrôle interne à la Direction financière. Chez Bouygues Telecom, le directeur de l'audit interne et de la gestion des risques est rattaché à la Direction financière ; le responsable de l'assurance à la Direction juridique.

L'organisation de la gestion des risques de ces trois groupes est relativement proche. En effet, Bouygues Telecom, Michelin et Areva ont chacun développé des organisations internes. Dans certains cas, les groupes peuvent confier la gestion des risques et l'audit interne à des sociétés de *consulting* extérieures. En outre, ces trois groupes disposent de *guidelines*, d'une méthodologie des risques et de systèmes de *reporting* interne et *corporate*. Ainsi, l'organisation de la gestion des risques est très mature.

De même, l'organisation de l'audit interne de ces trois groupes affiche un haut niveau de maturité, avec des services d'audit interne propres, des outils traditionnels tels que des référentiels de cartographie, et de systèmes de *reporting* classiques.

Quelles sont les spécificités de l'audit interne, de la gestion des risques et du contrôle interne au sein de vos organisations respectives ?

I. La spécificité des organisations

1. La spécificité de l'audit interne, du contrôle interne et de la gestion des risques au sein du groupe Michelin

Florence VINCENT

Le groupe Michelin présente trois spécificités.

Premièrement, la vision du contrôle interne englobe non seulement des sujets classiques, tels que la comptabilité et les finances, mais aussi l'environnement, la sécurité au travail et les produits. Notre groupe a choisi de confier la gestion du contrôle interne aux directions fonctionnelles : par exemple, la Direction des achats, la Direction des systèmes d'information et la Direction financière exercent leur propre contrôle interne. Le groupe Michelin a donc opté pour une vision large du contrôle interne. Le contrôle interne est l'affaire des opérationnels et des responsables qui pilotent les activités.

Deuxièmement, le groupe Michelin a décidé de pousser la logique de l'évaluation de la maîtrise des risques de la Direction de l'audit interne jusqu'au bout. Cette démarche nous a amenés à modifier notre approche de l'audit et la composition de notre équipe.

Troisièmement, nous considérons que la qualité, le *risk management* et le contrôle interne relèvent d'une même démarche, à ceci près que ces trois fonctions ont vocation à gérer des risques spécifiques. Nous nous sommes efforcés de marier ces trois fonctions et de capitaliser sur la culture et le réseau de qualité du groupe Michelin.

Gérard LANCNER

Dans quelle mesure la logique de l'évaluation de la maîtrise des risques a-t-elle influencé le rôle de l'audit interne ?

Florence VINCENT

Lorsque j'ai pris mes fonctions de directrice de l'audit interne et des risques, 80 % de cette équipe était composée de juniors et de collaborateurs provenant de cabinets d'audit. A cette époque, ma fonction était centrée sur la gestion des processus. Aujourd'hui, les risques auxquels le groupe Michelin est confronté portent davantage sur les produits eux-mêmes, l'approvisionnement et la santé des personnels. Ces sujets forment 80 % du contenu du programme d'audit, alors que les aspects comptables et financiers ne représentent que 15 % de ce programme.

Mon équipe compte actuellement 40 personnes et je travaille en coopération avec un médecin du travail, un ergonome, des directeurs qualité et des opérationnels, notamment. La moyenne

d'âge des collaborateurs est de 45 ans et ces derniers sont tous issus de métiers spécifiques (achats, ventes, production, etc.).

Gérard LANCNER

L'organisation de l'audit interne et des risques du groupe Michelin est donc très originale. Qu'en est-il du groupe Areva ?

2. La spécificité de l'audit interne, du contrôle interne et de la gestion des risques dans le groupe Areva

Philippe HATRON

Le groupe Areva s'est doté d'une charte de contrôle interne. Celle-ci stipule que le contrôle interne est l'affaire de tous, des organes de gouvernance à l'ensemble des collaborateurs du groupe. Nous avons mis en place un certain nombre de lignes de défense à partir de cette charte.

La première ligne de défense est celle des opérationnels : les 5 *business groups* d'Areva organisent eux-mêmes la gestion des risques en fonction d'un corpus de règles préétabli, selon un principe de subsidiarité.

La deuxième ligne de défense renvoie à celle des directions fonctionnelles : il s'agit de la Direction financière, qui inclut la Direction des risques et de l'assurance, et de l'Inspection, qui est en charge du suivi des risques industriels (ce qui recouvre la sécurité et la sûreté nucléaire).

La troisième ligne de défense est celle de la Direction de l'audit interne.

Gérard LANCNER

En quoi cette organisation est-elle originale ?

Philippe HATRON

L'organisation de l'audit interne et de la gestion des risques du groupe Areva est plutôt conventionnelle. Toutefois, je souhaiterais mettre en perspective la relation entre l'audit interne et le *risk management*, qui se caractérise par l'indépendance et la complémentarité.

Le rôle du directeur de l'audit interne est d'évaluer le niveau de maîtrise des risques au sein du groupe, en toute indépendance et d'émettre un avis sur les grands risques identifiés comme tels, lesquels sont testés dans le cadre des plans d'audit et des différentes missions de la Direction de l'audit interne.

Philippe OBERT

J'ajoute que les dispositifs mis en place par le groupe Areva ont été conçus simultanément, contrairement à certaines entreprises. Ainsi, le partage des rôles et des responsabilités entre la Direction de l'audit interne et la Direction de la gestion des risques est parfaitement clair.

Par ailleurs, le positionnement de la Direction de la gestion des risques et de l'assurance d'Areva est spécifique. Bien qu'elle soit rattachée à la Direction financière, cette direction peut intervenir directement auprès de la Direction générale. Si une anomalie nécessitant un traitement politique particulier est détectée, nous exerçons un devoir d'alerte auprès d'Anne Lauvergeon. Cette approche est fondée sur un dialogue simplifié et non formalisé, ce qui renforce l'efficacité de nos dispositifs internes.

Gérard LANCNER

Ce dispositif est très intéressant. Quelle est l'originalité de la démarche de l'audit interne et de la gestion des risques de Bouygues Telecom ?

3. La spécificité de l'audit interne, du contrôle interne et de la gestion des risques au sein du groupe Bouygues Telecom

Bruno DUNOYER de SEGONZAC

Bouygues Telecom est une entreprise monolithique et compte très peu de filiales internationales. L'originalité de la démarche d'audit interne et de gestion des risques de Bouygues Telecom repose sur la complexité des réseaux. Cette complexité nécessite en effet de mettre en place des dispositifs de veille et de contrôle très pointus, le moindre risque pouvant provoquer une réaction en chaîne. Ainsi, l'équipe de l'audit interne et de la gestion des risques est très spécialisée et se compose essentiellement d'ingénieurs des télécommunications.

A l'instar du groupe Michelin, seuls 15 % des audits que nous menons sont des audits comptables et financiers. 80 % des audits portent sur les risques opérationnels et les risques liés aux processus. Pour Bouygues Telecom, un des enjeux est de détecter les risques de faible niveau, ces derniers pouvant provoquer des incidents majeurs.

Gérard LANCNER

Le groupe Bouygues Telecom a décidé de regrouper au sein d'une même direction l'audit interne, la gestion des risques, le contrôle interne et la sécurité. Ces différentes fonctions sont-elles exercées par les mêmes personnes ?

Bruno DUNOYER de SEGONZAC

Deux équipes distinctes gèrent le plan de management général, lequel inclut la gestion des risques, et le plan d'audit. Le plan d'audit est fondé sur une cartographie des risques.

Gérard LANCNER

En est-il de même au sein de Michelin ?

Florence VINCENT

Oui. Deux équipes sont en charge respectivement de la gestion des risques et de l'audit interne. L'équipe de gestion des risques compte deux personnes ; le *Risk Manager* a été recruté en interne pour ses compétences et sa connaissance approfondie des lignes métiers et des produits. Cette personne est secondée par un spécialiste des audits. Compte tenu de la taille restreinte de cette équipe, j'ai confié aux auditeurs la mission de concevoir des outils pour la gestion des risques.

Gérard LANCNER

Qu'en est-il de l'indépendance entre l'audit interne et la gestion des risques ? Ces deux fonctions étant regroupées chez Michelin et Bouygues Telecom, comment gérez-vous cette contradiction ?

Florence VINCENT

A mon sens, l'indépendance est un faux problème.

La question de l'indépendance se pose lorsque nous sommes amenés à évaluer une action ou les conséquences d'une décision. Au sein de Michelin, le *risk management* ne fait pas et il ne décide pas. Ce matin, l'intervenant du groupe Société Générale soulignait que le pilote (en l'occurrence les *business units*), qui a la possibilité d'actionner l'accélérateur, peut aussi actionner le frein. Le *risk management* de Michelin a un rôle d'animation, d'élaboration des méthodes et de *reporting*.

Bruno DUNOYER de SEGONZAC

Je partage le point de vue de Florence Vincent. La Direction de l'audit interne et de la gestion des risques de Bouygues Telecom définit et anime les processus, mais elle ne gère pas les risques en tant que tels. Ces risques sont gérés au niveau opérationnel. En quelque sorte, les opérationnels sont propriétaires de ces risques et ils gèrent eux-mêmes leurs plans d'actions. Les directions opérationnelles sont ensuite auditées par notre direction.

Gérard LANCNER

En d'autres termes, vous auditez l'efficacité des systèmes de gestion des risques, qui sont la propriété des directions opérationnelles. Quel est le point de vue des représentants d'Areva sur ce point ?

Philippe HATRON

Les risques sont la propriété des opérationnels. L'indépendance de l'audit interne et de la gestion des risques est acquise *de facto*. En revanche, il importe aux services de gestion des risques de canaliser les risques et d'effectuer des *reportings*. Le processus même de la cartographie des risques fait partie intégrante du système de management des risques. Si ce processus n'est pas efficient, les risques ne bénéficieront pas de la visibilité qui leur est due.

Si je partage le point de vue des intervenants concernant l'analyse critique des risques, je suis plus réservé quant à l'analyse de l'efficacité de la gestion des risques.

Gérard LANCNER

Ce type d'organisations serait-il disqualifiant au regard des normes applicables aux services d'audit ?

Louis VAURS

Il est difficile de répondre à cette question. Les normes de la profession imposent aux services d'audit d'être indépendants. En d'autres termes, l'audit interne doit établir lui-même son plan d'audit et il doit se réserver la possibilité d'auditer un risque qui n'a pas été identifié préalablement dans la cartographie des risques. A mon sens, si elle est rattachée au plus haut niveau de l'entreprise, la fonction d'audit interne acquiert une crédibilité très importante. Cela lui permet de travailler en toute indépendance. Cependant, il n'existe pas de vérité absolue. En réalité, il convient de tenir compte des réalités et de la culture de l'entreprise.

Gérard LANCNER

J'en déduis qu'aucune des trois organisations qui nous a été présentée aujourd'hui ne serait disqualifiée dans le cadre d'une procédure d'obtention de certification.

Louis VAURS

Non, en effet. L'un des critères fondamentaux pour la certification repose sur l'indépendance de l'audit interne et de la gestion des risques.

II. Synergies, échanges et arbitrages

Gérard LANCNER

Est-il possible d'obtenir des effets de synergie et d'organiser les échanges dans des structures regroupant l'audit interne et la gestion des risques ? Comment s'assurer de la complémentarité de ces équipes ?

Florence VINCENT

Le groupe Michelin a créé le service de *risk management* en 2005. A cette époque, ce service a été rattaché à la Direction de la qualité du groupe, qui était alors dirigé par un membre de la famille Michelin. Lors du départ à la retraite du directeur de la qualité, la fonction d'audit interne m'a été confiée.

J'ai alors cherché à intégrer les fonctions d'audit interne et de gestion des risques. La Direction dont je suis responsable s'appuie sur une équipe de direction, qui compte un manager d'audit aux Etats-Unis et un manager d'audit en Ecosse. Cette équipe se réunit une fois par trimestre dans le cadre de réunions d'équipe de direction afin de travailler sur la gestion des risques et de faire le bilan des missions d'audit. Le *Risk Manager* fait partie de cette équipe et il participe pleinement à l'évaluation des auditeurs et à l'élaboration des plans d'audit. Les managers d'audit participent, pour leur part, à la mise en place d'outils de gestion des risques et à l'élaboration de la cartographie.

Il est intéressant de noter qu'avant la fusion de ces équipes, les directeurs des *business units* étaient confrontés à deux visions différentes des risques. Aujourd'hui, nous apportons une réponse unique et homogène et nous analysons une large part de risques non identifiés dans la cartographie. Si l'audit a évalué 40 % des positionnements dans la cartographie, cela donne une plus grande confiance aux patrons.

Bruno DUNOYER de SEGONZAC

Le plan d'audit de Bouygues Telecom est élaboré à partir de la cartographie des risques. De toute évidence, l'audit interne est parfaitement indépendant et nous ne retenons pas les différents thèmes de la cartographie de façon systématique. Si la cartographie est au fondement du plan d'audit, nous nous permettons des incursions dans d'autres types de risques. Il revient à chaque auditeur d'infirmer, de confirmer ou d'ajouter des risques qui n'ont pas été pris en compte initialement.

Gérard LANCNER

Les rapports d'audit font-ils l'objet d'échanges ? Sont-ils accessibles aux *Risk Managers* ?

Bruno DUNOYER de SEGONZAC

Oui.

Florence VINCENT

Chez Michelin, les rapports d'audit font l'objet d'une présentation de façon systématique.

Gérard LANCNER

Les missions et les objectifs des directions de l'audit interne et de la gestion des risques sont spécifiques. Lorsque ces fonctions sont distinctes, comment gérez-vous les échanges d'informations et dans quelle mesure pouvez-vous dégager des effets de synergie ?

Philippe HATRON

Philippe Obert a souligné que le groupe Areva avait mis en place un partage clair des responsabilités. Nous ne disposons que d'une seule cartographie des risques. L'animateur de ce processus est la Direction de la gestion des risques et de l'assurance, depuis 2003. La Direction de l'audit interne s'assure que la cartographie des risques a bien été communiquée et que les risques ont été correctement évalués. Ainsi, le partage des responsabilités entre l'audit interne et la gestion des risques est parfaitement clair.

Les échanges d'informations s'effectuent comme dans toutes les entreprises : la Direction de l'audit interne et la Direction de la gestion des risques se rencontrent une fois par mois, dans le cadre de la préparation du plan d'audit et de la synthèse des risques. Le groupe Areva étant certifié par l'IFACI, nous effectuons une réconciliation de la cartographie des risques et du plan d'audit. Quoi qu'il en soit, la Direction de l'audit assure effectue des missions d'audit qui ne sont pas liées directement à la gestion des risques.

Gérard LANCNER

Le programme d'audit est-il destiné à analyser des risques ?

Philippe HATRON

Oui. Nous auditons des risques et des processus. Ces processus n'ont d'intérêt que s'ils permettent de maîtriser certains risques. De plus, nous menons un audit des risques clés, des objectifs précis étant fixés en ce domaine.

Gérard LANCNER

La cartographie des risques vous permet donc d'orienter le programme d'audit des risques et des processus, en fonction des priorités établies par Philippe OBERT.

Philippe HATRON

Oui, entre autres. L'établissement de La Hague peut, par exemple, faire l'objet d'audits régulièrement. Les environnements de contrôle interne de certains établissements doivent être audités régulièrement, même si nous considérons que le niveau de risques n'y est pas très élevé.

Philippe OBERT

Nous avons mis en place des processus extrêmement collaboratifs, ce qui s'explique par la nature des activités du groupe Areva. Notre groupe est constitué d'une pluralité de métiers, dont la spécificité est très forte. En particulier, les métiers du cycle du combustible sont regroupés dans un modèle intégré, de l'extraction minière au retraitement. Les métiers d'ingénierie sont très spécifiques et recouvrent la conception, la maintenance des réacteurs et des installations nucléaires, et leur démantèlement. La fabrication d'un réacteur nécessite plusieurs dizaines de spécialités d'ingénierie différentes ! Ces exemples démontrent toute la complexité des réalités que nous devons couvrir.

Dans ce cadre, nous avons décidé d'élaborer les cartographies des risques dans le cadre d'un dispositif de *risk management*, lequel est intégré aux directions opérationnelles. Le rôle de la Direction de la gestion des risques et de l'assurance est d'animer ces processus et l'ensemble du réseau, afin de tirer profit de toutes les spécificités.

Le groupe Areva a privilégié, en outre, le principe de co-responsabilité. Nous avons déjà cité les directions opérationnelles, mais les directions fonctionnelles jouent également un rôle essentiel, dans la mesure où elles déterminent les politiques de maîtrise des risques dans le cadre de leur mission. Par exemple, la Direction de la sécurité, de la santé, de la sûreté et de l'environnement (D3SE) est en charge de la gestion du risque nucléaire. Cette direction établit la charte nucléaire en coopération étroite avec l'Autorité de sûreté nucléaire, et détermine les normes applicables au sein du groupe. De toute évidence, nous ne pouvons nous substituer à la D3SE en ce domaine. La collaboration entre les directions opérationnelles, fonctionnelles, les directions de la gestion des risques et de l'audit interne doit être permanente.

Gérard LANCNER

L'objectif est d'identifier les risques et de mettre en place un suivi de l'efficacité de la gestion des risques. Si le programme d'audit ne recouvre pas l'ensemble des risques prioritaires identifiés par la Direction de la gestion des risques, qui sera l'arbitre ?

Philippe HATRON

La discussion entre la Direction de l'audit interne et celle de la gestion des risques est continue. Nous travaillons ensemble et nous échangeons nos informations respectives. Je suis consulté sur l'élaboration du plan d'audit et, dans ce cadre, j'ai la possibilité d'y apporter un certain nombre d'éléments. Je rappelle que nous pouvons nous appuyer sur le devoir d'alerte. Si, par exemple, le programme d'audit ne me semble pas conforme, j'ai la possibilité de solliciter un arbitrage auprès de la Direction générale.

Gérard LANCNER

Pourriez-vous dresser un panorama des missions de la Direction de l'assurance en lien avec la gestion des risques ?

Philippe OBERT

Le rôle d'un assureur est d'évaluer le degré d'exposition de déterminer le risque pouvant être mutualisé, et donc transféré. Le rôle du directeur de la gestion des risques et de l'assurance

consiste, lui, à évaluer l'ensemble des risques, y compris ceux qui ne peuvent pas entrer dans la logique de la mutualisation. Le gestionnaire des risques et l'assureur exercent finalement le même métier, et ils se partagent la culture du diagnostic.

Au sein d'Areva, la Direction de l'assurance remplit aussi une mission d'acheteur dans le cadre d'une démarche d'optimisation de la gestion financière. La Direction de l'assurance gère également tous les aspects contractuels et elle participe à ce titre aux négociations avec les partenaires d'Areva.

Gérard LANCNER

Quelle est la part des risques couverts par une assurance au sein d'Areva ?

Philippe OBERT

Cette question est très délicate. Le référentiel de risques d'Areva comprend 42 familles, parmi lesquelles 17 familles éligibles à l'assurance, même si elles ne sont pas toutes assurables. *A priori*, la part des risques transférables est de l'ordre de 20 %, hors financements alternatifs.

Gérard LANCNER

Le fait qu'un risque n'est pas assurable signifie-t-il pour autant qu'aucune solution n'est possible ?

Philippe OBERT

Cela signifie soit qu'il n'y a pas de réponse ou d'opportunité, soit qu'il n'y a pas d'envie.

Gérard LANCNER

Quel est le rôle d'une direction des assurances au sein de Bouygues Telecom et de Michelin ?

Florence VINCENT

François Huche, directeur de l'assurance du groupe Michelin, était rattaché à la Direction de l'audit interne au début des années 90. Aujourd'hui, il est rattaché à la Direction financière. Ainsi, nous nous inscrivons également dans une logique d'optimisation financière. La Direction de

l'assurance utilise la cartographie des risques des différentes entités et elle sélectionne elle-même les risques devant être couverts par un contrat d'assurance. Je ne connais pas la part exacte des risques couverts au sein de Michelin. Celle-ci pourrait cependant être estimée à 20 %.

Bruno DUNOYER de SEGONZAC

La Direction de l'assurance doit être indépendante de la Direction de la gestion des risques, qui identifie et gère des processus extrêmement larges. Ces processus couvrent des risques stratégiques qui, par définition, ne peuvent être assurés. A notre sens, la Direction de la gestion des risques doit être indépendante parce qu'elle ne saurait être influencée par une vision assurantielle des risques.

Toutefois, nous parvenons à trouver des synergies et lorsque la cartographie des risques est achevée, la définition des risques assurables fait l'objet d'une réflexion commune. Si un risque est jugé trop élevé, nous demandons à la Direction de l'assurance d'examiner les différentes opportunités d'assurance. Celle-ci s'appuie sur les services d'un courtier. Dans certains cas, les risques peuvent être couverts par un contrat d'assurance sur mesure.

Philippe OBERT

Comment protégez-vous la confidentialité de certaines informations ?

Bruno DUNOYER de SEGONZAC

Le courtier n'a connaissance de la cartographie des risques à aucun moment. La cartographie des risques est présentée à la Direction générale, qui décide des risques devant faire l'objet d'un contrat d'assurance.

Gérard LANCNER

Comment gérez-vous les relations avec les commissaires aux comptes, au sujet de la cartographie des risques ?

Philippe HATRON

Les commissaires aux comptes ont accès à l'ensemble de la cartographie des risques.

Bruno DUNOYER de SEGONZAC

Il en est de même au sein de Bouygues Telecom.

Florence VINCENT

Les commissaires aux comptes ne participent pas aux comités d'audit de Michelin. En tout cas, ils n'y assistent pas lorsque la cartographie des risques est présentée.

III. Les rapports avec le comité d'audit

Gérard LANCNER

Le comité d'audit, dans les sociétés cotées, a pour obligation d'assurer le suivi de l'efficacité et d'en rendre compte. Comment parvenez-vous à démontrer l'efficacité de vos dispositifs respectifs ?

Philippe OBERT

Au groupe Areva, la Direction de la gestion des risques travaille en étroite coopération avec le président du comité d'audit. Le président du comité d'audit m'a notamment demandé de mettre en place une méthode d'évaluation de la part des risques bruts et des risques nets. Nos relations avec le comité d'audit se limitent à des échanges techniques, méthodologiques et au *reporting*.

Philippe HATRON

La Direction de l'audit interne rédige chaque année un rapport détaillé sur l'audit interne du groupe, dans lequel nous faisons un point sur le système de *risk management*. L'analyse des grands risques intervient dans ce cadre. La présentation de la cartographie des risques s'accompagne d'une information des plans d'action et d'un bilan de l'évolution de la maîtrise des risques. La présidente du comité d'audit interne d'Areva est de nationalité canadienne. Sa conception des risques est très large et ne se limite donc pas aux risques financiers.

Par ailleurs, la 8ème directive et les travaux qui ont suivi n'ayant pas abouti à des recommandations précises, il a été nécessaire de discuter avec les membres du conseil de surveillance pour trouver un niveau de « *confort* » adéquat.

Philippe OBERT

Le processus de cartographie des risques donne naissance à deux systèmes. Il s'agit d'une cartographie *top down*, qui couvre les 10 risques majeurs définis par la Direction générale et 5 risques majeurs définis par les 6 *business groups*. Ces 40 risques et leur plan d'actions sont présentés au comité exécutif et au comité d'audit. La Direction de l'audit interne évalue le niveau de réalisation de chaque plan d'actions et rend compte de leur bilan dans le cadre de la présentation du plan pluriannuel d'audit.

Gérard LANCNER

Comment la présentation du bilan de l'efficacité de la gestion des risques et de l'audit est-elle effectuée à Bouygues Telecom et Michelin ?

Florence VINCENT

En général, nous partons toujours de la cartographie des risques (qui comprend 14 familles de risques), puis nous présentons au comité d'audit le bilan des audits et le suivi des plans d'actions. Aujourd'hui, un seul support sert à présenter la cartographie des risques et les conclusions de l'audit.

Bruno DUNOYER de SEGONZAC

Je suis représenté au comité d'audit et des comptes de Bouygues Telecom. Je présente généralement les évolutions de la cartographie des risques (qui comprend 9 familles de risques). Toute la difficulté est ici de faire comprendre aux administrateurs, qui sont pour la plupart des administrateurs indépendants, la réalité des risques. Dans ce cadre, l'intervention des commissaires aux comptes est relativement limitée dans la mesure où je travaille très en amont avec ces derniers. Les commissaires aux comptes ont, par exemple, la possibilité d'apporter des modifications aux rapports d'audit.

Questions / Réponses

Monsieur RENARD

Je souhaiterais apporter des précisions au sujet des assurances, qui laissent planer un certain doute. Quel est l'apport des assurances au *risk management* ? En fait, les assurances n'apportent rien à ce niveau. A l'inverse, c'est la politique de *risk management* qui permet de définir la politique d'assurances. En effet, c'est en fonction des limites qui auront été fixées à l'acceptation du risque que le montant des franchises est fixé dans les polices d'assurance. De même, le seuil

de tolérance au risque constitue un point de repère pour la décision de souscrire un contrat d'assurances.

Vous avez évoqué, par ailleurs, la question de la confidentialité. Si un problème de confidentialité se pose sur un sujet grave, la meilleure solution est de détenir sa propre société de courtage.

Gérard LANCNER

Le marché est relativement restreint en matière de risques. Dans certaines activités ou certaines sphères géographiques, il semble que les assureurs soient réticents à couvrir les risques, en particulier lorsque ces derniers sont avérés. Les cartographies des risques permettent d'illustrer la maturité des entreprises dans leur diagnostic des risques assurables. Ainsi, les sociétés d'assurances peuvent être rassurées quant aux mesures de prévention mises en place.

Monsieur BERTRAND

Quelle approche utilisez-vous pour inciter les directions générales à définir leur appétit pour le risque ?

Florence VINCENT

Ce sujet est très complexe et nous n'avons toujours pas trouvé de méthode appropriée. Il faut, à mon sens, adopter un raisonnement *a contrario* en matière de risques et chercher à identifier les risques que les directions générales ne sont pas prêtes à prendre. Je serais intéressée de connaître les pratiques de mes confrères sur la gestion des profils de risques.

Bruno DUNOYER de SEGONZAC

Il est difficile de travailler selon une approche préventive. Nous travaillons plutôt en mode de crise. Lorsqu'une crise survient, quelles que soient ses conséquences, nous tentons de déterminer un seuil d'acceptabilité, ce qui amène la Direction générale à réfléchir aux limites de l'acceptation d'un risque. De notre point de vue, une crise n'ayant aucun impact sur les clients est une crise acceptable. A l'inverse, une crise ayant des impacts sur les clients n'est pas acceptable. Il est toujours plus facile de faire réfléchir une direction générale à partir d'un cas pratique.

Philippe HATRON

La gestion des risques est inhérente aux activités d'un groupe tel qu'Areva. Nous n'avons donc aucune difficulté à sensibiliser la Direction générale sur ces sujets. A l'inverse, la Direction générale fixe des objectifs stricts à ses managers sur la gestion des risques, ceci en permanence. Au-delà des risques industriels, des risques touchant à la sécurité et à la sûreté nucléaires, les cadres intermédiaires sont sensibles aux risques pesant sur l'image de l'entreprise et aux risques financiers. En outre, les managers sont de plus en plus conscients des impacts d'une dérive éventuelle de la charte des valeurs. En particulier, si un manager est sensibilisé à l'existence d'un environnement RH faible ou défaillant, l'alerte est rapidement déclenchée.

Un participant

Vos organisations respectives sont-elles dotées d'une base de données relative aux incidents ?

Florence VINCENT

Toutes les industries sont dotées de ce type d'outils. Nous disposons de bases de données relatives aux départs de feu, aux accidents du travail et à la qualité des produits. Le suivi des données sur la qualité nous permet notamment d'effectuer des rappels de produits si nécessaire.

Bruno DUNOYER de SEGONZAC

Bouygues Telecom a mis en place un système d'analyse des incidents ou des crises ayant un impact financier.

Philippe OBERT

Le groupe Areva s'est doté d'un dispositif qui permet de répertorier tous les incidents intervenant sur les sites. D'ailleurs, tous les incidents survenant dans un site nucléaire font l'objet d'une déclaration à l'Autorité de sûreté nucléaire.

Thierry POMMIER, groupe Caisse des Dépôts

Vos sociétés respectives sont-elles dotées de dispositifs d'évaluation du contrôle interne ? Quelle est l'évolution de ces dispositifs en termes de recueil des informations ?

Philippe HATRON

Nous avons mis en place à Areva un dispositif d'auto-évaluation du contrôle interne, qui concerne 80 % du chiffre d'affaires du Groupe et près de 130 entités. Nous envoyons aux équipes une liste de 200 questions sur la réciprocité des tâches, le respect des procédures du groupe et l'efficacité. Ces auto-évaluations donnent lieu à une synthèse, qui est reprise dans le rapport du conseil de surveillance sur l'examen du contrôle interne. Ces questionnaires sont pilotés par la Direction financière, mais ils sont tous signés par les directeurs des entités.

Florence VINCENT

Le dispositif d'évaluation du contrôle interne de Michelin est similaire à celui d'Areva. Une équipe de la Direction vérifie, en outre, la qualité des évaluations par cycles.

Bruno DUNOYER de SEGONZAC

De même, nous avons mis en place un dispositif d'auto-évaluation du contrôle interne, qui est fondé sur le référentiel de l'Autorité des marchés financiers. Ce dispositif permet d'évaluer 200 principes de contrôle interne. Ces principes sont évolutifs. Ainsi, les auditeurs ont la possibilité d'en supprimer un certain nombre (lorsqu'ils n'ont pas d'intérêt pour l'organisation), de les modifier et d'en ajouter.

Gérard LANCNER

Quelle est la valeur ajoutée des commissaires aux comptes dans les dispositifs d'audit interne et de gestion des risques ?

Bruno DUNOYER de SEGONZAC

Les commissaires aux comptes sont informés du plan d'audit de Bouygues Telecom et, réciproquement, je suis tenu informé de leurs travaux. Notre travail est complémentaire et nous tâchons d'éviter les audits redondants.

Philippe HATRON

Le travail de la Direction de l'audit interne d'Areva et celui des commissaires aux comptes sont complémentaires. Nous échangeons nos plans d'audit respectifs et nous nous rencontrons de 4 à 5 fois par an. La Direction de l'audit interne mène des audits de contrôle interne général (ce qui recouvre la gestion de crise, les processus RH, etc.), contrairement aux commissaires aux comptes, dont les audits portent sur le contrôle interne financier. Les commissaires aux comptes

et la Direction de l'audit interne présentent respectivement au comité d'audit un rapport sur le contrôle interne comptable et financier et un rapport sur le contrôle interne général. Quoi qu'il en soit, les commissaires aux comptes contribuent parfaitement aux démarches de contrôle interne et leur valeur ajoutée est importante.

Une participante, groupe France Télécom

France Télécom et Areva sont présents dans des pays réputés difficiles. Je souhaiterais savoir comment le groupe Areva mène sa politique de gestion des risques et comment il promeut la culture de la gestion des risques dans ces pays.

Philippe HATRON

Les filiales des pays dits difficiles sont soumises aux mêmes règles que l'ensemble des filiales du groupe. Les deux principes de management du groupe Areva sont la charte des valeurs, qui s'adresse à toutes les entités du groupe, et le développement durable. Les managers de ces régions obéissent à ces principes.

La Direction de l'audit interne est une direction *corporate* et compte une trentaine de collaborateurs. Nous n'avons pas opté pour des équipes délocalisées afin de garantir leur efficacité et leur indépendance. Ces implantations, telles que le Niger, le Kazakhstan ou la République Centrafricaine, sont auditées au même titre que l'ensemble des filiales du groupe.

Notre organisation du contrôle interne est décentralisée et est fondée sur le principe de subsidiarité. Ainsi, les *business groups* se sont dotés de coordinateurs du contrôle interne. Ces derniers participent aux comités de contrôle interne au niveau du groupe et possèdent leurs propres réseaux dans les entités opérationnelles. Les bonnes pratiques peuvent être échangées dans ce cadre.

En tant que directeur de l'audit interne, je m'intéresse particulièrement à ces filiales, qui sont soumises à davantage de risques, notamment du fait de leur éloignement.

Philippe OBERT

De la même manière, les dispositifs de gestion des risques sont rigoureusement identiques dans toutes les filiales du groupe Areva.

QU'ATTEND-ON DE L'AUDITEUR INTERNE ET DU RISK MANAGER ? LES ROLES PERÇUS PAR LES DIFFERENTES PARTIES PRENANTES

ANIMEE PAR **CLAUDE VIET**, *PRESIDENT DE L'IFACI, DIRECTEUR DE L'AUDIT ET DES RISQUES, LA POSTE*.

AVEC **ALDO CARDOSO**, *PRESIDENT DE COMITE D'AUDIT*

DIDIER ELBAUM, *SECRETAIRE GENERAL ADJOINT, AUTORITE DE CONTROLE PRUDENTIEL*

PHILIPPE GUILLAUMIE, *DIRECTEUR FINANCIER, 3 SUISSES INTERNATIONAL*

JEAN-MARC LUMET, *COMMISSAIRE AUX COMPTES, CHAMBRE REGIONALE DES COMPTES DE VERSAILLES*

Louis VAURS

La dernière table ronde de cette journée est consacrée aux attentes des parties prenantes dans les domaines de l'audit interne et de la gestion des risques. Les parties prenantes sont généralement les directions, les comités d'audit, les commissaires aux comptes et les régulateurs. Cette table ronde sera animée par Claude VIET.

Claude VIET

Je suis très honoré de présenter cette dernière table ronde. Les débats d'aujourd'hui ont montré qu'en matière de gestion des risques, les grandes entreprises, quel que soit leur secteur d'activités, adoptent des approches de recherche d'efficacité, mais que les organisations répondent à des objectifs différents. Dans tous les cas, les interactions entre les acteurs sont essentielles.

Nous avons souhaité organiser un débat faisant intervenir les parties prenantes, c'est-à-dire le management, la gouvernance et le régulateur, qui ont pris une importance croissante au cours des dernières années, ainsi que les cabinets d'audit extérieurs. Dans les entreprises cotées, il est nécessaire de s'assurer de l'efficacité des dispositifs de contrôle interne. De plus, la synergie entre les directions d'audit interne et les cabinets d'audit est importante pour le comité d'audit.

Monsieur Philippe GUILLAUMIE, CFO du groupe 3 Suisses International, participera à cette table ronde. Philippe GUILLAUMIE a débuté sa carrière au sein du cabinet Deloitte, puis a exercé des fonctions de Direction Financière au sein du Groupe Alcatel Alstom avant d'être Directeur administratif et financier des groupes Roullier et Segula Technologies. Sa riche expérience des finances nous sera très utile.

Je vous présente également Monsieur Aldo Cardoso, qui est administrateur indépendant dans de nombreuses sociétés, telles que Accor, Rhodia et Gaz de France. Aldo CARDOSO est diplômé de l'Ecole Supérieure de Commerce de Paris et a effectué une grande partie de sa carrière dans l'audit et le conseil.

Les régulateurs seront représentés par Monsieur Didier ELBAUM, Secrétaire général adjoint de l'Autorité de contrôle prudentiel. Cette structure montre toute l'importance que le régulateur attache au contrôle du secteur bancaire et du secteur des assurances. Monsieur ELBAUM a notamment travaillé à la Banque de France et à la Banque Européenne pour la Reconstruction et le Développement.

Enfin, Monsieur Jean-Marc LUMET, Commissaire aux comptes, est vice-président du conseil d'administration de Deloitte. Jean-Marc LUMET interviendra sur les interactions entre les directions d'audit interne et les cabinets d'audit.

Philippe GUILLAUMIE, comment percevez-vous l'organisation, la structuration et le positionnement des acteurs du contrôle interne au sens large ?

I. Le cadre général de la réflexion

1. Le témoignage d'un directeur financier

Philippe GUILLAUMIE

Les témoignages qui ont précédé ont concerné des grands groupes. J'interviendrai en tant que représentant d'une structure de taille plus modeste, où la gestion des risques et l'audit interne restent à construire. Le Groupe 3 Suisses International est une entreprise familiale et ses deux actionnaires, qui sont l'Association Familiale Mulliez et le groupe allemand Otto adoptent une logique patrimoniale. Le comité d'Audit et Finance du groupe 3 Suisses est actuellement centré sur la gestion des risques financiers, des liquidités, la fiabilité des systèmes de reporting et les relations avec les cabinets d'audit externes. La prochaine étape consistera à investir davantage le champ de la gestion des risques et de l'audit interne.

La démarche de gestion des risques devra être construite en partenariat avec les opérationnels et avec la Direction de l'audit interne en création.

Le processus de gestion des risques, pourra s'appuyer sur la fonction du contrôle de gestion.

Il nous appartiendra de faire émerger une culture du risque et de développer une démarche de connaissance et d'évaluation des risques opérationnels.

Claude VIET

Je suis surpris qu'une société telle que les 3 Suisses n'ait pas été dotée de cette organisation auparavant. Quelles sont les attentes des administrateurs en ce domaine ?

2. Le témoignage d'un administrateur

Aldo CARDOSO

L'implication des conseils d'administration en matière de gestion des risques et de contrôle est très hétérogène selon les sociétés. J'ai participé aux conseils d'administration de grandes sociétés et j'ai eu, à ce titre, l'opportunité de suivre l'évolution de cette implication dans les sociétés françaises. Pour ma part, je travaille en partenariat avec l'IFA depuis sa création et je préside un groupe d'échanges des présidents des comités d'audit, afin de partager les bonnes pratiques et de mettre au point de nouvelles méthodologies. Notre rôle est notamment de communiquer sur ces notions et de diffuser les bonnes pratiques.

Les conseils d'administration sont responsables des démarches de gestion des risques et d'audit. Il est important de souligner que les comités d'audit n'apportent que des modalités pratiques aux travaux des conseils d'administration. Aux termes de la 8ème directive, les rôles du conseil d'administration et du management doivent être distincts. Lorsque cette directive a paru, certains administrateurs ont considéré que le conseil d'administration ne jouait qu'un rôle de premier niveau. Le rapport de place précise ses responsabilités : il appartient au conseil d'administration de s'assurer de l'existence des dispositifs de gestion des risques et d'audit et de leur efficacité. De son côté, le rôle du management est de mettre en œuvre ces dispositifs.

Les comités d'audit ont évolué rapidement au cours des dix dernières années. Initialement, les comités d'audit étaient des comités de comptes qui ne se réunissaient pas plus de deux fois par an. Au-delà des comptes, ces comités d'audit ont progressivement pris la responsabilité du suivi du contrôle interne, de la communication financière, du document de référence, de l'analyse des litiges et de la gestion des risques. La multiplication des missions s'est accompagnée de l'augmentation de la fréquence des réunions et du nombre de participants. En général, les risques, le contrôle interne et le suivi des comptes sont regroupés au sein d'un seul comité afin de garantir la cohérence des approches.

La fonction d'audit interne est très répandue et elle bénéficie d'effectifs plus ou moins importants, selon les entreprises. Au contraire, la fonction de gestion des risques n'existe pas toujours et lorsqu'elle existe, elle est souvent limitée aux assurances. *De facto*, les directeurs de la gestion des risques sont souvent rattachés aux directeurs juridiques. De plus en plus, ces deux fonctions sont regroupées dans une direction des risques et du contrôle interne. Ce regroupement a suscité de nombreux débats, mais à mon sens, le fait de nommer un responsable pour chacune des fonctions permet d'assurer leur bonne coordination et garantit une certaine indépendance.

Les relations entre les comités d'audit et les responsables de fonction sont divergentes. Les auditeurs internes, à l'instar du commissaire aux comptes, sont de plus en plus présents aux réunions du comité d'audit, afin de présenter les plans d'audit et les conclusions de leur rapport. Les gestionnaires de risques interviennent aux comités d'audit de façon plus intermittente, afin de présenter la cartographie des risques et les processus de gestion des risques. Le comité d'audit attend des auditeurs internes et des gestionnaires des risques qu'ils exercent leur droit d'alerte, si nécessaire. Dans les grands groupes du CAC 40, les comités d'audit se réunissent une fois par trimestre, soit une vingtaine d'heures par an au maximum. Dans ces conditions, il est difficile pour les administrateurs membres du comité d'audit d'appréhender le travail du contrôle interne et de gestion des risques effectué par les équipes. Ainsi, les rôles respectifs doivent être correctement articulés et tant les auditeurs internes que les *Risk Managers* doivent être capables de mettre

l'accent sur les aspects les plus importants de leurs missions. A titre personnel, je ne suis pas intéressé par les processus qui fonctionnent de façon satisfaisante. Il me paraît plus important d'insister sur les dysfonctionnements et l'analyse de ces derniers.

Claude VIET

J'ai noté l'importance de la coordination entre l'audit interne et la gestion des risques. La plupart des sociétés industrielles et commerciales ont regroupé ces deux fonctions dans une seule direction, dans le respect des normes professionnelles. Le choix des banques et des sociétés d'assurance a été très différent. Monsieur ELBAUM, quelles sont les raisons de ce choix ?

3. Le témoignage du régulateur

Didier ELBAUM

L'Autorité de contrôle prudentiel (ACP) est une autorité administrative indépendante qui, avec son Secrétariat général (et ses quelque 1000 agents), est adossé à la Banque de France. L'Autorité de contrôle prudentiel regroupe plusieurs collèges, qui traitent, selon leur configuration, de la situation des secteurs bancaire et des assurances prises dans leur ensemble ou au travers de cas individuels. Une des missions de l'Autorité de contrôle prudentiel est de s'assurer de la conformité des pratiques des banques et des sociétés d'assurance à la réglementation. Il me paraît important de préciser que le terme de « régulation » revêt un caractère mixte en ce qu'il englobe tout à la fois les notions de réglementation et de supervision. Or, si l'Autorité de contrôle prudentiel n'est pas en charge de la réglementation en tant que telle, mais de son application, il est vrai qu'en revanche, elle exerce un pouvoir d'influence technique sur les textes adoptés par le Gouvernement français et les institutions européennes. Au niveau international, c'est également le cas s'agissant des principes élaborés par le Comité de Bâle (pour le secteur bancaire) et par l'IAIS (pour le secteur des assurances). En outre, l'ACP est en charge du suivi micro-prudentiel des établissements bancaires et des organismes assurances tout en veillant à la préservation de la stabilité financière, et à ce titre, nous avons le souci d'éviter le développement des bulles spéculatives dans le secteur des banques et des assurances. Enfin, l'ACP intervient au titre de la protection des consommateurs.

Parmi le corpus réglementaire applicable aux banques et aux assurances, un certain nombre de textes régissent la façon dont le système de contrôle interne doit être structuré et la manière dont il doit fonctionner. Certaines prescriptions concernent les organes délibérants et leur émanation (comité d'audit, comité des comptes, etc.), l'audit interne (qui est généralement désigné par le terme d'inspection dans les établissements bancaires) et les départements en charge de la mesure et du suivi des risques. En France, les textes mettent également en avant la notion de contrôle permanent. Le contrôle permanent, c'est-à-dire quotidien, rassemble les différents acteurs traitant de la gestion, des risques. Le contrôle périodique est incarné par les services d'inspection ou d'audit interne. Dans les banques, la gestion des risques est

nécessairement indépendante des opérationnels (notamment des départements qui octroient les crédits).

Claude VIET

Monsieur Lumet, comment voyez-vous les relations entre l'audit interne, la gestion des risques et les cabinets d'audit externes ?

4. Le témoignage du commissaire aux comptes

Jean-Marc LUMET

Les relations entre les cabinets d'audit externes et les structures de contrôle interne sont très contrastées. Tout d'abord, nos rapports avec les auditeurs internes et les *Risk Managers* sont très différents. Si nos relations avec les auditeurs internes sont relativement riches, celles que nous entretenons avec les responsables de la gestion des risques sont plus rares, même si elles sont nécessaires. Un des rôles des commissaires aux comptes est de comprendre comment les risques sont identifiés et couverts dans les entreprises. Nous ne rencontrons les *Risk Managers* qu'une fois par an, en général, lors de la présentation de la cartographie des risques ou des mises à jour des outils de pilotage des risques.

Nos rencontres avec les auditeurs internes sont plus fréquentes, mais nos relations avec ces derniers n'en sont pas moins hétérogènes. Dans certains cas, les rapports entre la direction de l'audit interne et le cabinet d'audit sont riches et ils se matérialisent à travers des échanges de programmes de travail, le partage des conclusions, voire des coopérations sur le terrain. L'auditeur interne peut déléguer une partie des tâches sous sa responsabilité, dans le cadre de missions accessoires. Pour autant, j'ai été confronté à des situations où l'auditeur interne et l'auditeur externe s'ignoraient, les objectifs assignés à l'audit interne ne correspondant pas toujours à ceux du commissaire aux comptes.

Ainsi, les relations entre les commissaires aux comptes, les auditeurs internes et les gestionnaires des risques sont très hétérogènes.

Claude VIET

Je vous remercie. Le rôle des associations professionnelles telles que les nôtres et des colloques est d'étendre les bonnes pratiques, au-delà de l'application des normes.

Comment la nouvelle responsabilité des comités d'audit, qui doivent s'assurer de l'efficacité des dispositifs de gestion des risques et de contrôle interne, est-elle mise en œuvre ?

II. Les interactions entre les acteurs de la gestion des risques et de l'audit interne sous l'angle de la coordination

Jean-Marc LUMET

La situation qu'Aldo Cardoso a décrite est juste : si nous voyons apparaître les auditeurs internes dans les comités d'audit, afin de partager leurs plans d'audit, la participation des responsables de la gestion des risques est moins fréquente.

Claude VIET

Monsieur Cardoso, comment les comités d'audit évoluent-ils et comment l'interaction avec les auditeurs internes et les responsables de la gestion des risques est-elle assurée ?

Aldo CARDOSO

En général, le fonctionnement n'est pas optimal dans les entreprises, probablement parce que les fonctions d'audit interne et de gestion des risques ne sont pas stabilisées ou parce qu'elles ne sont pas correctement gérées. Je souhaite que ces deux fonctions soient parfaitement identifiées et articulées et qu'une synthèse claire des risques, de leurs responsables et des processus de gestion soit présentée dans les entreprises où j'ai exercé. Malheureusement, on ne m'a jamais présenté de tableau ainsi articulé.

De plus, les auditeurs internes et les responsables de la gestion des risques doivent échanger leurs conclusions respectives en toute transparence. Le rôle du comité d'audit est de s'assurer que tous les risques sont identifiés et couverts. La redondance est moins le problème du conseil d'administration que celui du management. Quoi qu'il en soit, celle-ci doit être éliminée. L'un des problèmes majeurs auxquels un conseil d'administration pourrait être confronté est l'absence de coordination et le manque d'imprécisions du dispositif global de contrôle interne. Comment présenter de façon synthétique l'articulation de leurs travaux et la communication de ces travaux ?

Claude VIET

Ces sujets méritent en effet d'être approfondis. L'IFACI, l'IFA et l'AMRAE doivent œuvrer en ce sens. Monsieur GUILLAUMIE, l'IFACI est à votre disposition pour vous aider à mettre en place ces dispositifs. Au sein de la société Roullier, vous avez réalisé une cartographie des risques ; pourriez-vous nous faire part de cette expérience ?

Philippe GUILLAUMIE

Le groupe Roullier est une entreprise de l'industrie agroalimentaire et réalise 1,5 milliard d'euros de chiffre d'affaires, notamment à l'international. Son actionnaire a souhaité mieux maîtriser son développement et promouvoir celui-ci dans la sécurité. Ainsi, nous avons réfléchi à la création d'un dispositif d'audit interne et de gestion des risques, en dépassant le cadre strict des risques assurables et en privilégiant la complémentarité et les synergies.

Cette expérience a été concluante et elle a été rendue possible par l'impulsion de l'actionnaire et l'investissement de la Direction générale. Les objectifs de la cartographie des risques ont consisté à renforcer le contrôle des risques donnant lieu à une sinistralité importante et à définir des mécanismes opérationnels de protection de l'entreprise en cas de risque avéré.

Cette cartographie a été réalisée selon la méthode classique de priorisation des risques, de définition des risques inhérents et résiduels. Au-delà de cette démarche, nous avons mis en place un processus d'actualisation régulière, en responsabilisant les opérationnels, en identifiant les propriétaires des risques, et en mettant en œuvre des plans d'action adaptés. Un soutien de la Direction générale permanent est indispensable à la réussite de cette démarche.

La fonction d'audit interne a été créée simultanément et le responsable qui a été recruté alors a réussi à trouver immédiatement sa place dans une organisation très décentralisée – le groupe Roullier était en effet une fédération de PME relativement autonomes La mise en place de l'audit interne a reposé essentiellement sur la capacité du responsable à se faire accepter et à véhiculer les bons messages. Initialement, le travail du responsable de l'audit interne a été d'identifier les bonnes pratiques pouvant servir de base au développement d'un référentiel de contrôle interne renforcé et de socle pour améliorer la maîtrise des risques identifiés.

En définitive, nous avons réussi à mettre en place un dispositif d'évaluation et de réduction des risques, avec la participation du comité exécutif et des principaux responsables opérationnels.

A mon sens, il est important de retenir les éléments suivants :

- la complémentarité de la cartographie des risques et de l'audit interne ;
- la volonté managériale et l'adhésion des managers, qui passe par une communication régulière des plans d'action ;
- des plans d'audit fondés sur la cartographie des risques et tournés vers les enjeux des métiers.

Claude VIET

Cette expérience sera certainement utile à votre réflexion. Dans le secteur financier, ne faudrait-il pas rechercher des synergies entre l'audit interne et la gestion des risques ?

Didier ELBAUM

Le partage des responsabilités est clair dans le secteur des banques et des assurances, tout particulièrement dans le premier eu égard à l'ancienneté de la réglementation en ce domaine – la première ayant été édictée en 1997. Au cours des dernières années, la filière métier de l'audit interne s'est renforcée et nous voyons se dessiner la même tendance concernant la gestion des risques. Ce phénomène de constitution de la gestion des risques en une ligne métier à part entière s'impose compte tenu de la nécessité de disposer d'une vision consolidée des risques alors même que l'activité des banques et des assurances s'exerçant sur plusieurs continents et dans un grand nombre d'entités juridiques.

Les rôles de l'audit interne et de la gestion des risques sont complémentaires. Si la mise en œuvre d'une cartographie des risques, qui est obligatoire dans les banques et les assurances, est assurée par les départements de gestion des risques, le contrôle de celle-ci est réalisé par les services d'inspection générale.

Quel est le degré d'indépendance du département de la gestion des risques par rapport aux opérationnels ? Ce département doit-il se limiter à identifier les risques et à suivre leur évolution, ou doit-il participer davantage à la prise de décisions ? Les frontières entre le rôle des opérationnels et celui des *Risk Managers* doivent être précisées.

Nous pouvons également nous interroger sur l'opportunité de partager les responsabilités entre l'audit interne et la gestion des risques, en matière de contrôle des modèles internes. Dans les banques et les assurances, la gestion des risques et la comptabilisation des engagements reposent sur l'emploi de modèles mathématiques et statistiques, selon les règles de Bâle II et bientôt de Solvency II, respectivement. Or à quel département la responsabilité de valider ces modèles doit-elle être confiée ? S'il n'existe pas de réponse claire à ce sujet, le fait de nommer une entité distincte de celle qui a mis en place le modèle interne paraît en tout état de cause indispensable. Dans les cas où les départements de gestion des risques ont contribué au contrôle de la validité des modèles, il reviendra à l'inspection de les valider en dernier ressort.

Claude VIET

Quel serait le meilleur fonctionnement possible à l'avenir ? Quelles orientations la gouvernance des entreprises devrait-elle suivre ?

III. Les perspectives d'évolution

Aldo CARDOSO

Une réflexion doit être conduite sur les conséquences de la crise du secteur financier sur les sociétés industrielles et commerciales. Dans le secteur financier, le *risk management* est une fonction opérationnelle et celle-ci est de définir et d'encadrer un certain nombre d'opérations. Dans le secteur industriel et commercial, le *risk management* est aujourd'hui conçu comme une fonction support. Lorsque la cartographie des risques est établie, la responsabilité de la gestion des risques relève des opérationnels. Je ne suis pas certain que cette méthode soit appropriée. Ne faudrait-il pas confier à la gestion des risques une autorité dans un certain nombre de domaines ?

Les réflexions sur l'évolution de l'environnement des banques et des assurances, sur les conséquences de cette évolution sur la tolérance au risque et sur l'interdiction des opérations avant la réalisation du risque, devront être approfondies.

En outre, l'association des conseils d'administration et des comités d'audit dans les sociétés industrielles et commerciales me semble souhaitable. En effet, celle-ci permet de ne pas limiter les comités à une fonction de transcription de l'événement comptable et d'élargir leur rôle à la réflexion sur l'origine de cet événement, c'est-à-dire l'activité elle-même. Nous devons nous assurer que les comités d'audit disposent des moyens nécessaires à l'analyse des risques et à la compréhension des différentes activités. J'y suis très favorable, à la condition que les comités d'audit prennent le temps d'effectuer cette analyse. Il est illusoire de penser qu'un comité d'audit pourra jouer pleinement son rôle, s'il ne se réunit que trois ou quatre fois par an. De plus, les réunions des comités d'audit sont très liées au calendrier de la publication des comptes. Il ne faudrait pas que la gestion des risques soit pénalisée par ce calendrier. Ainsi, une meilleure participation à la gestion des risques suppose la fermeté du président dans la fixation des calendriers. Le président doit également s'assurer que les interlocuteurs sur ces sujets disposent du temps nécessaire pour exposer leurs points principaux.

Claude VIET

Quelle pourrait être l'évolution des rapports entre les auditeurs internes, les *Risk Managers* et les commissaires aux comptes ?

Jean-Marc LUMET

Nos ambitions doivent être réalistes et il me semble qu'une meilleure coordination entre les commissaires aux comptes et les auditeurs internes constituerait un axe intéressant. Je ne crois pas à une articulation idéale entre les fonctions d'audit externe et d'audit interne, même si nous devons tendre vers cet objectif. L'audit interne fixe lui-même son programme de travail avec la validation de la Direction générale. De plus, une articulation idéale supposerait que l'audit interne dispose d'une méthodologie idoine sur tous les sujets et d'une réelle indépendance. Quoi qu'il en soit, je considère que la coopération entre l'audit interne et les commissaires aux comptes doit

être plus étroite, ne serait-ce que pour des raisons d'efficacité, de coût et de couverture globale des risques.

Claude VIET

Monsieur GUILLAUMIE, nous n'avons pas évoqué les rapports entre les acteurs du contrôle interne et le pilotage d'une entreprise, voire le développement de l'entreprise. Comment percevez-vous la relation avec le contrôle de gestion au sein des entreprises que vous avez gérées ?

Philippe GUILLAUMIE

Je me pose cette question actuellement, en l'absence de dispositif de gestion des risques au sein du groupe 3 Suisses International. Mon diagnostic montre que le réseau des contrôleurs de gestion de l'entreprise peut constituer un levier d'action intéressant, au moins pendant une période intérimaire. L'utilisation de ce levier comporte un certain nombre de risques, notamment celui de la confusion des rôles entre le contrôle de gestion et l'audit interne, mais aussi des opportunités. Nous devons également veiller à ce que l'implication du contrôle de gestion ne nuise pas à la lisibilité des actions de contrôle interne pour les opérationnels.

Parmi les opportunités principales, je citerai la mise en place d'un relais permanent qui soit le plus proche possible des opérations. En outre, le contrôle de gestion bénéficie d'une certaine légitimité opérationnelle ; au-delà de l'identification des risques, il me semble que nous avons intérêt à intégrer les approches de gestion des risques dans les dispositifs d'amélioration de la performance. De plus, l'analyse des opérations par les contrôleurs de gestion leur permet de proposer des actions correctrices en matière de gestion des risques. Les contrôleurs de gestion peuvent également jouer un rôle important dans le suivi des indicateurs de risques, le contrôle de l'application des processus et l'établissement des prévisions, qui doivent être ajustées en fonction des risques. Si le contrôle de gestion n'est pas lui-même en charge du contrôle interne, il peut proposer des indicateurs de suivi et contribuer à la définition des procédures.

Ainsi, les actions de l'audit interne et du contrôle de gestion peuvent être complémentaires en matière de risques. Le contrôle de gestion dispose d'un réseau, qui est essentiel à la collecte d'informations. A mon sens, cela constitue un avantage supplémentaire permettant au contrôle de gestion d'être un des maillons importants du dispositif de maîtrise des risques, en particulier lors de la phase de mise en place.

Claude VIET

Je vous remercie. Compte tenu du rôle de l'Autorité de contrôle prudentiel, quels sont les facteurs de risques les plus importants dans le secteur des banques et des assurances ?

Didier ELBAUM

Vous ne serez pas surpris si je mentionne les risques présents dans un certain nombre de pays à la périphérie de la zone euro et également le fait que la valeur de certains actifs financiers des banques doit faire l'objet d'un suivi régulier. Nous devrons continuer à être vigilants, par ailleurs, sur l'évolution du secteur immobilier. Il ne s'agit pas de difficultés en tant que telles, mais de risques sur lesquels nous devons rester vigilants.

L'enjeu, pour les sociétés d'assurances, consistera à être à la hauteur de la nouvelle réglementation, qui est très exigeante. Les règles de Solvency II constituent un pas essentiel vers un recours accru aux modèles internes. Solvency II permettra, en outre, de mieux structurer les systèmes de contrôle interne dans les assurances. Quoi qu'il en soit, nous continuerons à être attentifs à la manière dont le management, l'organe délibérant et le comité d'audit suivront les risques. Je partage le point de vue d'Aldo Cardoso, selon lequel il faudra veiller au temps que les acteurs consacrent à cette mission.

En ce qui concerne les filières métiers, nous devons être conscients de la complexité croissante des organisations et du recours à des techniques de plus en plus sophistiquées. Pour l'audit interne et la gestion des risques, l'enjeu sera de disposer des ressources suffisantes, c'est-à-dire des ressources qui assurent leur indépendance. Le développement opérationnel des activités devra aller de pair avec les dispositifs permettant de les contrôler et il nous appartiendra de vérifier que ce principe soit bien appliqué dans les faits.

Claude VIET

Avant de céder la parole à Monsieur Patrick LAGADEC, je remercie l'ensemble des intervenants de cette table ronde de leur participation.

Louis VAURS

A présent, Patrick LAGADEC va clore cette journée, par une intervention sur les risques hors cadre. Patrick LAGADEC est directeur de recherche à l'Ecole Polytechnique et travaille particulièrement sur le pilotage de la gouvernance des sociétés complexes.

DISCOURS DE CLOTURE : LES RISQUES HORS CADRE, PAR PATRICK LAGADEC

Patrick LAGADEC, *Directeur de recherche à l'Ecole Polytechnique*

Je tiens à souligner, en préambule, la qualité des débats de ce séminaire. Les intervenants de ce matin ont mis l'accent sur les angles morts, sujet sur lequel je souhaite revenir aujourd'hui. A mon sens, nous allons jouer sur un nouvel échiquier et les stratégies devront être adaptées de plus en plus fréquemment. En quelque sorte, nous quittons les sentiers balisés pour nous aventurer dans l'inconnu. Au-delà de ce constat, il convient de s'interroger sur les actions à préconiser en matière de pilotage des risques.

En plongée sous-marine, le suivi des règles de sécurité doit être très rigoureux, sinon absolu. Il est recommandé aux plongeurs qui se sont perdus de suivre les bulles d'oxygène, lesquelles remontent toujours à la surface. En cas d'extrême urgence, il est vivement conseillé aux plongeurs de se regrouper et de définir ensemble l'attitude à adopter. Le piège principal à éviter est la sidération totale, comme cela a été le cas lors de l'accident nucléaire de Fukushima. J'ajoute que le FMI avait publié un rapport en 2006, louant la situation des banques mondiales. Deux ans plus tard, la crise éclatait sur les marchés financiers.

Quid du pilotage ? Quelles sont les pistes à envisager ? Il est possible de suivre les règles, mais celles-ci doivent être claires ou, *a minima*, non contradictoires. Qui doit prendre en charge l'analyse statistique ? Cette question soulève la problématique du *leadership* et de l'identification des acteurs qui vont prendre en charge le problème et qui vont afficher les valeurs, au détriment des outils. En outre, le paramètre de la vitesse devient essentiel, comme l'a montrée récemment l'opération de neutralisation d'Oussama Ben Laden, qui a été suivie en direct de la Maison Blanche. La cohésion doit aussi être consolidée immédiatement.

Aujourd'hui, l'enjeu des « méga-chocs » doit être pris en compte impérativement. Les directions doivent être préparées à la gestion de chocs majeurs, ce qui recouvre tant la prévention que la gestion des crises. Il convient de réaliser des *benchmarkings* et d'identifier les bonnes pratiques. Quelles ont été les bonnes idées ? Comment ces idées ont-elles été mises en place ? Ce sont autant de questions auxquelles une réponse doit être apportée, afin d'aider les directions à gérer les risques majeurs correctement.

Une interview du directeur de l'aéroport de La Nouvelle Orléans est projetée aux participants.

L'exemple du directeur de l'aéroport de La Nouvelle Orléans est remarquable. Lorsque l'ouragan Katrina a frappé cette ville, cette personne a fait face aux événements seule, pendant 72 heures, faisant preuve d'une capacité émotionnelle stupéfiante. Même après l'arrivée de 5 000 militaires, il n'a jamais perdu le contrôle de la situation et il saura reconfigurer en permanence sa capacité de pilotage, tout en maîtrisant ses ressources internes. La plupart des 1 000 collaborateurs avaient été évacués et il n'a conservé autour de lui qu'une cinquantaine de collaborateurs. Ces derniers ont été disponibles 24 heures sur 24, car leurs familles avaient été mises en sécurité dans l'aéroport.

Toutefois, certains professeurs de l'université de Berkeley estiment que la surprise présente certains avantages. Nous avons été recrutés, car nous sommes compétents dans l'utilisation des meilleurs outils. Aujourd'hui, les organisations sont surdimensionnées, et les dirigeants devront non plus afficher des capacités de *leadership*, mais des capacités de *méta-leadership*. L'objet n'est pas de prévoir l'imprévisible, mais de s'entraîner à faire face à l'imprévu. Ainsi, il convient non seulement de s'assurer de nos capacités à mettre en place les procédures prévues, mais aussi d'adopter des logiques de comportement, de décision et d'organisation dans une situation qui brise toutes les conventions. Il faut donc s'entraîner à être surpris. S'il est impossible d'avoir réponse à tout, il faut être capable d'être créatif sur des terrains qui ne sont plus ce qu'ils étaient. Dans les situations difficiles, il est essentiel de lancer des appels à l'intelligence créatrice.

Pour être à la hauteur de ces nouveaux enjeux, il convient de susciter la créativité et de donner aux collaborateurs la capacité d'être créatifs. Des stratégies, innovantes et porteuses d'avenir, doivent être mises en place. La double signification de l'idéogramme chinois « dangers et opportunités » est souvent rappelée lors des conférences, mais je précise que les opportunités sont plutôt réservées aux personnes exceptionnelles. En effet, une personne tétanisée face au danger ne peut saisir les opportunités. Cela renvoie à la question de la confiance envers les individus. Le *leadership* est essentiel, mais il convient aussi de construire la confiance au sein des organisations.

En matière d'audit et de maîtrise des risques, la rigueur dans la sécurité conventionnelle doit être préservée, compte tenu de la fragilité des terrains où nous nous situons aujourd'hui. Les frontières entre les situations conventionnelles et les situations non conventionnelles sont plus ténues, et les acteurs de la gestion des risques doivent jouer un rôle, en quelque sorte, de passeur de frontière. Il faut donc être capable d'écouter, d'accompagner, de proposer, d'ouvrir et d'aider. La légitimité à l'intérieur et à l'extérieur des organisations des acteurs résidera dans leur capacité à afficher de nouvelles perspectives, à proposer du sens, des démarches et de nouveaux théâtres d'opération pour inventer ensemble, ce qui revient à créer de nouvelles alliances.

Aux Etats-Unis, un certain nombre de pionniers avaient compris à la fin du XIXème siècle que les populations feraient face à de nouveaux risques de pandémie, et qu'il fallait donc préparer de nouveaux esprits inventifs. Ainsi, les entreprises américaines étaient prêtes à affronter des risques majeurs. Ce fut le cas lorsqu'une pandémie survint en 1918.

Préparons-nous à être créatifs sur ces sujets. Nous serons attendus sur nos capacités à réagir correctement sur de nouveaux terrains.

CLOTURE DU COLLOQUE, PAR LOUIS VAURS

Louis VAURS, *Conseiller du Président, IFACI*

J'ai noté que si nous ne pouvons prévoir l'imprévisible, nous devons nous entraîner à être surpris. Guillaume II disait à ses généraux qu'ils seraient peut-être pardonnés d'avoir perdu une bataille, mais qu'ils ne seraient jamais pardonnés d'avoir été surpris.

Aujourd'hui, nous avons souligné la nécessité de partager les mêmes valeurs, le même langage et la même approche des risques dans les entreprises. Nous avons également mis l'accent sur l'exemplarité des directions générales.

Incontestablement, la filière des risques connaît une montée en puissance, ce qui est considéré comme étant un fait normal par les entreprises du secteur bancaire, et très stimulant par les acteurs de l'audit interne. Néanmoins, la filière de gestion des risques apparaît toujours en retrait par rapport à l'audit interne, comme Aldo Cardoso et Jean-Marc Lumet l'ont indiqué à plusieurs reprises. Il semble que les comités d'audit et les commissaires aux comptes aient plus de contacts avec l'audit interne qu'avec la gestion des risques. Des progrès doivent être obtenus en ce sens.

En outre, il convient de s'adapter rapidement, car les risques évoluent en permanence, notamment les risques exceptionnels. La gestion des risques de cette nature nécessite non seulement de la réactivité, mais aussi de la créativité.

J'ai relevé, par ailleurs, que le contrôle interne, la gestion des risques et l'audit interne devaient être fondés sur tous les acteurs d'une entreprise. Ainsi, la connaissance des métiers de l'entreprise est essentielle. Le management opérationnel ne doit pas être occulté, car la gestion des risques est l'affaire de tous. Nous avons noté, toutefois, une différence entre le secteur financier et les secteurs de l'industrie, des commerces et des services. En effet, les *Risk Managers* gèrent les risques dans les banques, alors que le *risk management* joue davantage un rôle de support dans les autres secteurs, les opérationnels y étant considérés comme les propriétaires des risques.

Un consensus semble se dégager sur les trois de ligne de défense. J'ajouterais une quatrième ligne de défense, qui serait constituée des commissaires aux comptes et des autorités de régulation.

Il n'existe pas de modèle unique, comme l'ont montré les différents témoignages. Certaines entreprises font le choix de créer des directions de l'audit interne, de la gestion des risques et du contrôle interne, mais elles doivent alors séparer ces différentes fonctions en créant des départements distincts, pour garantir leur indépendance. Cela ne fait pas obstacle aux coopérations entre l'audit interne et la gestion des risques, qui ne sont pas toujours une évidence. Un article de Richard Chambers à paraître dans la prochaine revue de l'audit interne montre à cet égard que les analyses de l'audit interne et de la gestion des risques ne sont pas toujours convergentes.

Les qualités et les compétences nécessaires ont été citées. Je retiendrai plus particulièrement l'indépendance, le courage et le jugement. Aldo Cardoso a souligné la nécessité de hiérarchiser et de synthétiser les informations, ce qui permet aux comités d'audit d'aller à l'essentiel.

A mes yeux, ce séminaire a été très intéressant. Je remercie les présidents de l'AMRAE et de l'IFACI de nous avoir permis de travailler ensemble.