

Rôle de l'Administrateur dans la maîtrise des risques

en collaboration avec

PRICEWATERHOUSECOOPERS 

LANDWELL & ASSOCIÉS

Cabinet d'avocats correspondant de PRICEWATERHOUSECOOPERS 

Rôle de l'Administrateur dans la maîtrise des risques

en collaboration avec

PRICEWATERHOUSECOOPERS 

LANDWELL & ASSOCIÉS

Cabinet d'avocats correspondant de PRICEWATERHOUSECOOPERS 

Institut Français des Administrateurs

7, rue Balzac
75382 PARIS cedex 08
Tel : 01 55 65 81 32
contact@ifa-asso.com

www.ifa-asso.com

Association pour le Management des Risques et des Assurances de l'Entreprise

9/ 11, avenue F. Roosevelt
75008 PARIS
Tél : 01 42 89 33 16
Fax : 01 42 89 33 14

www.amrae.fr

PricewaterhouseCoopers

63, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 58 59
Fax : 01 56 57 58 60

www.pwc.fr

Landwell & Associés

61, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 56 57
Fax : 01 56 57 56 58

www.landwell.fr



Aux termes du Code de la propriété intellectuelle, toute reproduction ou représentation, intégrale ou partielle de la présente publication, faite par quelque procédé que ce soit (reprographie, micro filmage, scan-nérisation, numérisation...) sans le consentement de l'auteur ou de ses ayants droits ou ayant causes est illicite et constitue une contrefaçon sanctionnée par les articles L-335-2 et suivants du Code de la propriété intellectuelle. L'autorisation d'effectuer des reproductions par reprographie doit être obtenue auprès du Centre Français d'exploitation du droit de Copie (CFC) 20 rue des Grands-Augustins 75006 Paris Tél. : 01 44 07 47 70 Fax. : 01 46 34 67 19.

Sommaire

Composition du groupe de travail.....	1
Objectifs et méthodologie du groupe de travail.....	3
Avant propos	5
Executive Summary	7
Partie I : Contexte réglementaire.....	9
Chapitre 1 - Des interventions successives du législateur français pour amener les entreprises à améliorer leur gouvernance, le contrôle interne et la gestion des risques.....	9
1.1 Une évolution progressive des exigences réglementaires en France.....	9
1.2 Une tendance en France à privilégier en priorité la mise en place de « bonnes pratiques » et le suivi de « référentiels » et de « recommandations », autrement dénommés « Soft Laws ».....	12
Chapitre 2 - L'évolution du rôle du Conseil d'Administration en matière de contrôle interne et de gestion des risques	14
1.1 Rappel sur les fonctions essentielles du Conseil d'Administration.....	14
1.2 Les droits et obligations de l'administrateur, dont le rôle a été « professionnalisé ».....	15
Chapitre 3 - Les responsabilités de l'entreprise et de ses dirigeants en matière de contrôle interne et de gestion des risques	17
1.1 Les dirigeants et les administrateurs voient leur rôle se transformer face aux risques	17
1.2 Qui est responsable en cas de défaillance du contrôle interne ou de la gestion des risques ?	18

Partie II – Principes et fondamentaux de la surveillance des risques de l'entreprise.....	21
Chapitre 1 - Liens entre surveillance, pilotage et gestion des risques.....	21
1.1 Les fondamentaux	21
1.2 La maîtrise des risques, les plans d'actions, le contrôle interne et l'assurance : Interactions et liens.....	22
Chapitre 2 - Rôles et responsabilités des différents acteurs clés de l'entreprise ...	24
1.1 Principaux contributeurs à la surveillance des risques.....	24
1.2 Les interactions entre les principaux dispositifs participant à la surveillance des risques.....	29
Partie III – Qu'attendent aujourd'hui les dirigeants des entreprises ?	31
Partie IV – Propositions de bonnes pratiques.....	33
Chapitre 1 - Rôles et Responsabilités des membres du Comité du Conseil au regard de la réglementation en vigueur.....	33
1.1 Les conséquences de la transposition de la 8ème directive européenne	33
1.2 Périmètre d'intervention des administrateurs au titre du suivi des risques de l'entreprise	34
Chapitre 2 - Quelle organisation mettre en place ?.....	41
Chapitre 3 - Modalités de fonctionnement du Comité du Conseil et domaines de compétences.....	44
1.1 Fonctionnement opérationnel.....	44
1.2 Formation et ressources.....	48
Annexe I – Enquête auprès des entreprises du SBF 120	51
Annexe II – Lexique.....	65

Composition du groupe de travail

Co-Présidents du groupe de travail

- **Daniel Lebègue**
Président du Comité d'Audit de Technip et Scor, Président de l'IFA¹
- **Gérard Lancner**
Directeur Risk Management d'Yves Rocher
Président de l'AMRAE²

Membres du groupe de travail

- **Christian Aubin**
Christian Aubin & Associés
- **Robert Baconnier**
Président du Comité d'Audit de Sodexo, membre du Comité d'Audit de Siparex Associés, Président Délégué Général de l'ANSA
- **Emmanuel du Boullay**
Administrateur de sociétés, co-fondateur, Administrateur de l'IFA
- **Sylvain de Forges**
Directeur risques & marchés, Veolia Environnement ; membre du Conseil de Surveillance La Banque Postale et administrateur de la Monnaie de Paris
- **Alain Grosmann**
Président de la commission de déontologie de l'IFA,
Administrateur de sociétés

¹ IFA : Institut Français des Administrateurs

² AMRAE : Association du Management des Risques et des Assurances de l'Entreprise

- **Lionel d'Harcourt**
Directeur Associé Aon Global Risk Consulting
- **Bénédicte Huot de Luze**
Directeur Scientifique de l'AMRAE
- **Gérard de la Martinière**
Président du Comité d'Audit de Air Liquide, Schneider
- **Yves Nicolas**
Associé PricewaterhouseCoopers Audit, Directeur Général de l'activité audit, Président d'honneur du Département APE, Président de la Compagnie Régionale des Commissaires aux Comptes de Versailles
- **Jean-Philippe Riehl**
Directeur de la gestion des risques, Veolia Environnement ; Administrateur de l'AMRAE

Membre du groupe de travail, animateur rapporteur : PricewaterhouseCoopers & Landwell*

- **Xavier Maitrier**
Associé PricewaterhouseCoopers, directeur général de l'activité Conseil en Management, Comité Risques et contrôle interne de PwC / Landwell
- **Jean-Marc Truchi**
Associé PricewaterhouseCoopers, Conseil en Management, en charge du développement de l'offre « Gouvernance, risques et contrôle interne »
- **Sylvie Le Damany**
Avocat, associée Landwell & Associés, responsable du département litiges et pénal des affaires

* Landwell & Associés, cabinet d'avocats membre du réseau PricewaterhouseCoopers.

Objectifs et méthodologie du groupe de travail

En 2009, l'IFA et l'AMRAE, avec l'assistance de PwC et de Landwell, ont constitué un Groupe de travail visant à identifier, partager et diffuser les bonnes pratiques relatives au rôle du Conseil d'Administration et des administrateurs dans la maîtrise des risques de l'entreprise.

Les objectifs du groupe de travail ont été de :

- préciser les nouvelles obligations imposées aux administrateurs au titre de la maîtrise des risques de l'entreprise,
- rappeler les principes et les fondamentaux de la surveillance des risques de l'entreprise notamment en précisant les rôles et responsabilités attendus des différents acteurs clés de l'entreprise (organes de gouvernance, dirigeants et responsables d'activités),
- identifier les pratiques en vigueur dans les sociétés, notamment en matière d'organisation, de répartition des rôles et des responsabilités, de mise en œuvre des dispositifs de maîtrise des risques et d'implication des administrateurs dans le suivi des risques de l'entreprise,
- émettre des recommandations pratiques à l'attention des administrateurs.

La méthodologie suivie a été la suivante :

- l'examen de la législation actuelle et de la réglementation en France et à l'étranger en la matière,
- l'analyse des documents de référence de groupes cotés en France et à l'étranger,
- la réalisation d'une enquête sur base d'un questionnaire auprès de sociétés cotées en France, afin de préciser :
 - leur vision de la maîtrise des risques dans leur entreprise,
 - leur organisation en matière de suivi de ces risques et notamment le fonctionnement des organes en charge de ce suivi,
 - les évolutions qu'elles envisagent au cours des prochaines années,
- la tenue de réunions de travail avec les membres du Groupe et d'entretiens extérieurs.

Les bonnes pratiques proposées dans ce livre blanc ont vocation à être appliquées par les administrateurs de sociétés de toute nature quelle que soit leur activité ou leur mode d'organisation. Elles portent sur les thèmes suivants :

- les rôles et responsabilités des membres du Comité du Conseil en charge du suivi des risques de l'entreprise au regard de la réglementation en vigueur,
- les organisations à mettre en place,
- les modalités de fonctionnement du Comité du Conseil en charge du suivi des risques de l'entreprise et ses domaines de compétences.

Avant propos

L'une des missions imparties au Conseil d'administration, dans la législation et les codes de gouvernance de tous les pays, est de s'assurer que l'entreprise s'est dotée de dispositifs de contrôle interne et de gestion des risques solides et adaptés à la nature de l'activité de la société et à son projet stratégique. La loi française a spécifié à deux reprises en 2008 – loi du 3 juillet, ordonnance du 8 décembre – le rôle du Conseil et de son comité d'audit dans le champ du suivi et de la surveillance des risques.

Au moment où la crise mondiale a révélé, principalement dans le secteur financier, dans certains pays étrangers plus qu'en France, des déficiences, dans certains cas des défaillances graves dans les systèmes d'anticipation, d'identification et de gestion des risques, l'Institut Français des Administrateurs et l'Association du Management des Risques et d'Assurance d'Entreprises ont ressenti le besoin de réfléchir ensemble au rôle et aux moyens d'action du conseil et de ses comités spécialisés dans ce domaine.

Nous sommes en effet convaincus que ce dont nos entreprises ont besoin pour mieux maîtriser leurs risques dans un environnement de plus en plus complexe et incertain, ce n'est pas de réglementation supplémentaire mais d'un surcroît d'expertise, de bons outils et de méthodes de travail qui associent plus étroitement la direction générale, ses équipes en charge de la gestion et du contrôle des risques, les auditeurs externes et les membres du conseil d'administration.

Le travail mené en commun, avec l'appui du cabinet PricewaterhouseCoopers et de Landwell & Associés membre du réseau PricewaterhouseCoopers, nous a conduits à identifier certaines questions clés et à recommander quelques bonnes pratiques. Sans se substituer en aucune manière à la direction générale, qui a la responsabilité première de la gestion des risques de l'entreprise, le conseil d'administration doit avoir les moyens d'être bien informé et de rencontrer en tant que de besoin le directeur des risques de l'entreprise, de se doter d'une capacité d'expertise en la matière, d'organiser au mieux la répartition du travail entre ses comités spécialisés – comité d'audit, comité des risques le cas échéant.

Nous formons le vœu que ce guide pratique aide à la fois les administrateurs et les Directeurs de Risques dans les entreprises à exercer de manière aussi efficace que possible la difficile mission qui leur est impartie : contribuer au développement de l'entreprise tout en assurant une maîtrise raisonnable des risques qu'elle est appelée à prendre.

Gérard LANCNER
Président de l'AMRAE

Daniel LEBEGUE
Président de l'IFA

Executive Summary

La maîtrise des risques est l'affaire de tous.

Sous le contrôle de l'assemblée générale, le Conseil impulse la démarche de surveillance des risques dans l'entreprise. Il suit les risques les plus significatifs, apprécie l'exposition aux risques de l'entreprise au regard de la stratégie, et s'assure de l'efficacité des dispositifs de maîtrise des risques. Il suit plus particulièrement l'efficacité des dispositifs de contrôle mis en place par le management pour garantir la fiabilité et la conformité aux obligations légales des informations financières publiées.

Il appartient à la Direction Générale de définir, mettre en œuvre et s'assurer de l'efficacité des dispositifs de gestion des risques et de contrôle interne de la société.

L'ordonnance du 8 décembre 2008 prescrit la création d'un Comité d'Audit, donnant ainsi un cadre légal à la pratique, puisque une majorité des sociétés cotées a déjà un Comité d'Audit.

Ce Comité est chargé, sous la responsabilité exclusive et collective du Conseil d'Administration ou de Surveillance, d'assurer le suivi du processus d'élaboration de l'information financière. Il s'assure également du suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques, du contrôle légal des comptes annuels et le cas échéant des comptes consolidés par les commissaires aux comptes (CAC). Il rend compte régulièrement au Conseil de l'exercice de ses missions et l'informe sans délai des difficultés rencontrées.

Faut-il créer un Comité des Risques distinct du Comité d'Audit ? Si la création d'un Comité des Risques distinct du Comité d'Audit n'est pas obligatoire, elle peut être dictée par la complexité des risques à superviser par le Conseil, la nature des compétences à mobiliser et le secteur d'activité de l'entreprise. Pour autant, il convient d'organiser la répartition entre le Comité d'Audit et ce Comité, si le Conseil décide de le créer.

Le Comité en charge du suivi des risques comprend au moins un membre spécialiste de la gestion des risques ; des formations à la maîtrise des risques sont proposées aux administrateurs membres du Comité.

Le Comité en charge du suivi des risques rencontre au moins deux fois par an, et chaque fois que nécessaire, le Directeur des Risques.

Le positionnement de la Direction des Risques dans l'équipe de management de l'entreprise est à clarifier et à communiquer au sein de l'entreprise. Il doit lui permettre d'exercer sa fonction avec une certaine indépendance de vue et disposer des moyens nécessaires.

Le Comité en charge du suivi des risques dispose d'un budget suffisant pour diligenter des missions indépendantes et complémentaires à celles menées par le management de l'entreprise.

Le suivi des risques est mis régulièrement à l'ordre du jour des réunions du Conseil pour discussion et le cas échéant demande d'actions.

Partie I : Contexte réglementaire

Chapitre I - Des interventions successives du législateur français pour amener les entreprises à améliorer leur gouvernance, le contrôle interne et la gestion des risques

Sur un fond de scandales, de l'affaire ENRON (2002) à la crise financière et économique en 2008, le législateur est intervenu tant en France que dans de nombreux pays étrangers, et ce à plusieurs reprises, pour amener ou contraindre les entreprises à améliorer leur gouvernance, le contrôle interne et la gestion des risques.

I.1 Une évolution progressive des exigences réglementaires en France

Le législateur français, après avoir préféré la mise en place de lois pédagogiques prônant la mise en œuvre de bonnes pratiques, s'est orienté vers des lois plus contraignantes en matière de gouvernance et de gestion des risques visant à exiger :

- **une information plus complète et plus fréquente** sur des sujets déterminés (conventions réglementées, rapport environnemental et social, rémunérations des dirigeants, risques professionnels, contrôle interne, gestion des risques...),

- **une information plus normée** pour une meilleure compréhension des actionnaires et permettre à l'AMF d'analyser et comparer des documents de référence homogènes (cadre de référence de l'AMF sur le contrôle interne),
- **une information « obligée »** pour une responsabilisation des dirigeants et des administrateurs (*de l'incitation aux bonnes pratiques à l'apparition en France du concept **Comply or Explain** sur le Code de gouvernement d'entreprise (loi du 3 juillet 2008).*

Les grandes étapes réglementaires qui marquent cette évolution sont :

- la loi sur les Nouvelles Régulations Économiques (NRE) 2001,
- la loi américaine Sarbanes-Oxley 2002,
- la Loi de Sécurité Financière (LSF) 2003,
- la loi pour la confiance et la modernisation de l'économie 2005,
- la loi en faveur du travail, de l'emploi et du pouvoir d'achat (TEPA) 2007,
- la loi du 3 juillet 2008 (titre V : transposition de la Directive 2006/46 CE),
- l'ordonnance du 8 décembre 2008 transposant la 8e Directive 2006/43/CE.

En France, dès 2001, la loi sur les nouvelles régulations économiques dite NRE a exigé davantage de transparence sur certains sujets, notamment sur les conventions réglementées, les rémunérations des dirigeants et la prise en compte des conséquences sociales et environnementales des activités des entreprises.

Le législateur français a d'abord souhaité inciter les entreprises à mettre en place des bonnes pratiques (*Soft Laws*) issues de rapports divers sur la gouvernance (Vienot I et 2, Bouton, Barbier de Lasserre...).

Aux termes de la Loi de Sécurité Financière du 1er août 2003, il a ensuite exigé que les sociétés – sociétés anonymes dans un premier temps, puis les sociétés faisant appel public à l'épargne depuis la loi dite Breton du 26 juillet 2005, devenues les sociétés cotées (disparition de la notion de APE en 2009) – communiquent sur la gouvernance et leurs procédures de contrôle interne, au-delà des domaines financiers et comptables. Cette obligation s'est ajoutée à celles que connaissaient déjà les entreprises cotées, de communiquer aux actionnaires dans leur rapport annuel et dans le rapport environnemental et social sur un certain nombre de sujets.

La Loi de Sécurité Financière présentait ainsi un caractère pédagogique puisqu'elle incitait les entreprises à se doter des moyens nécessaires à l'« appréciation de la pertinence des contrôles internes » et à établir une « typologie des risques ».

En 2008, le législateur est intervenu plus directement pour obliger les entreprises cotées à communiquer sur la gestion des risques et donner de nouvelles responsabilités au Conseil d'Administration sur le suivi de l'efficacité des procédures de gestion des risques.

Ainsi, la **loi du 3 juillet 2008** portant diverses dispositions d'adaptation du droit des sociétés au droit communautaire (loi « DDAC ») a transposé en droit français la directive 2006/46/CE du 14 juin 2006 modifiant les 4ème et 7ème directives comptables en matière de gouvernement d'entreprise. Cette loi a renforcé les obligations de transparence des sociétés commerciales en matière de gouvernement d'entreprise et procédures de contrôle interne. Elle étend également l'objet du *rapport du Président* aux procédures de gestion des risques mises en place par la société. Ainsi, au-delà de communiquer sur les risques majeurs de l'entreprise et les procédures de contrôle interne, le Président va devoir communiquer sur les processus de gestion des risques mis en place au sein de l'entreprise. La loi impose en outre à l'entreprise d'appliquer un code de gouvernance et d'en préciser le référentiel. A défaut, les entreprises devront justifier l'absence de code de gouvernance (concept du « *Comply or Explain* »³). La majorité des sociétés cotées a déclaré fin 2008 à l'AMF qu'elle mettrait en œuvre le Code de gouvernance AFEP MEDEF.

L'**ordonnance du 8 décembre 2008** a transposé la directive 2006/43/CE du 17 mai 2006 dite 8ème directive sur le contrôle légal des comptes (JORF 0286 du 9 décembre 2008) et a été prise sur le fondement de l'article 32 de la loi du 3 juillet 2008 portant diverses dispositions d'adaptation du droit communautaire des sociétés. Elle prescrit la création d'un Comité d'Audit et donne par ailleurs un cadre légal à la pratique, puisque 72% des sociétés cotées avaient déjà un Comité d'audit.

Le Comité est alors chargé, sous la responsabilité exclusive et collective du Conseil d'Administration ou de Surveillance, d'assurer le suivi du processus d'élaboration de l'information financière. Il s'assure également du suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques, du contrôle légal des comptes annuels et le cas échéant des comptes consolidés par les CAC. Il veille également à l'indépendance des CAC, émet une recommandation sur ces derniers proposés à la désignation par l'AG (ou équivalent). Il rend compte régulièrement au Conseil de l'exercice de ses missions et l'informe sans délai des difficultés rencontrées.

Le Comité doit comporter au moins un administrateur indépendant présentant des compétences particulières en matière comptable ou financière.

Les entités visées par cette directive sont celles dont les titres sont admis à la négociation sur un marché réglementé, les établissements de crédit, les entreprises d'assurance et de réassurance, les mutuelles livre II et les institutions de prévoyance titre III livre IX.

Ces nouvelles dispositions suscitent un certain nombre de questions notamment sur ce que signifie « le suivi de l'efficacité des systèmes » et les nouvelles responsabilités qui en résultent pour le Conseil d'Administration.

³ « appliquer ou s'expliquer »

1.2 Une tendance en France à privilégier en priorité la mise en place de « bonnes pratiques » et le suivi de « référentiels » et de « recommandations », autrement dénommés « *Soft Laws* »

A cette série de mesures législatives et réglementaires visant à améliorer la gouvernance des entreprises, leur contrôle interne et leur gestion des risques, s'ajoutent les bonnes pratiques et recommandations, qualifiées de « *Soft Laws* » qui sont plus ou moins bien appliquées par les entreprises cotées et non cotées.

En matière de gouvernance, de contrôle interne et de gestion des risques, les principales références en matière de *Soft Laws* sont :

- les rapports VIENOT 1 et 2,
- le rapport BOUTON,
- les recommandations de l'AMF,
- les recommandations de IFA,
- les recommandations AFEP/MEDEF,
- le Code de gouvernement d'entreprise AFEP/MEDEF (consolidé en décembre 2008) sur les rémunérations des dirigeants mandataires sociaux (octobre 2008),
- les référentiels COSO 1 et COSO 2, AS/NZS 4360, ON49000, ISO 31000, Ferma, en matière de contrôle interne et de gestion des risques,
- le cadre de référence de l'AMF en matière de contrôle interne...

Les entreprises cotées ont, dans un premier temps, fondé leur démarche de contrôle interne sur le COSO⁴ recommandé par la loi Sarbanes-Oxley, pour s'orienter progressivement vers le Cadre de Référence de l'AMF présenté en janvier 2007 et constitué à partir des réflexions d'un groupe de place. Le périmètre du Cadre de Référence couvre à la fois le contrôle interne en général et le contrôle interne comptable et financier.

Le Cadre de Référence propose des principes généraux et des bonnes pratiques. Ces principes portent sur l'ensemble des processus de contrôle interne de la société et sont complétés par :

- un questionnaire relatif au contrôle interne comptable et financier,
- un questionnaire relatif à l'analyse et à la maîtrise des risques,
- un guide d'application pour les procédures de contrôle interne relatives à l'élaboration et au traitement de l'information financière et comptable publiée.

Ce référentiel est un « outil d'analyse et de conception du contrôle interne » ; ce n'est pas un outil d'évaluation.

⁴ COSO : Committee of Sponsoring Organizations

L'AMF recommande par ailleurs de mettre en perspective les procédures de contrôle interne avec les risques identifiés notamment ceux décrits dans le paragraphe « facteurs de risque » du document de référence, afin de permettre une meilleure compréhension de la manière dont l'entreprise gère ses risques.

En 2008, en partenariat avec MiddleNext, l'AMF a proposé une simplification du cadre de référence pour les Valeurs Moyennes et Petites (VaMPs) afin d'aider ces entreprises à initier une démarche de maîtrise des risques et de contrôle interne.

Chapitre 2 - L'évolution du rôle du Conseil d'Administration en matière de contrôle interne et de gestion des risques

1.1 Rappel sur les fonctions essentielles du Conseil d'Administration

Le Conseil d'Administration, selon l'article L. 225-35 du Code de commerce et ses alinéas 1^{er} et 3, « *détermine les orientations de l'activité de la société et veille à leur mise en œuvre. Sous réserve des pouvoirs expressément attribués aux assemblées d'actionnaires et dans la limite de l'objet social, il se saisit de toute question intéressant la bonne marche de la société et règle par ses délibérations les affaires qui la concernent. [...] « Le Conseil procède aux contrôles et vérifications qu'il juge opportuns [...] ».*

Ainsi, le Conseil décide des orientations stratégiques de la société et contrôle les actes de gestion courante. Il est en outre, l'organe compétent pour choisir, dans les conditions fixées par les statuts, le mode de direction de la société (C. com., art. L. 225-51-1).

Il a le pouvoir de nommer et de révoquer le Président du Conseil, le Directeur Général, les Directeurs Généraux délégués, et de fixer leur rémunération.

Depuis la loi du 3 juillet 2008, le Président doit obligatoirement faire approuver par le Conseil le rapport annuel qu'il établit pour les actionnaires en matière de gouvernance, de contrôle interne et de gestion des risques.

La loi n° 66-537 du 24 juillet 1966 a conçu le Conseil d'Administration comme un organe autonome et collégial. C'est collectivement que les administrateurs exercent les fonctions attribuées par la loi au Conseil. Ainsi, l'administrateur individuellement ne détient aucun pouvoir.

Cependant, le rôle de l'administrateur au sein du Conseil impose des droits et des obligations.

1.2 Les droits et obligations de l'administrateur, dont le rôle a été « professionnalisé »

L'administrateur s'assure qu'il détient toute l'information nécessaire à l'exercice de son mandat.

L'administrateur exercer son droit à l'information.

Chaque administrateur a le droit d'exiger « tous les documents nécessaires à l'accomplissement de sa mission » (Article L.225-35 du Code de commerce alinéa 3). L'administrateur peut (et donc doit), chaque fois que nécessaire, réclamer au Président, dans des délais appropriés, les informations indispensables à une intervention utile sur les sujets à l'ordre du jour du Conseil d'Administration. Le Président ou le Directeur Général est tenu de les lui communiquer.

En revanche, l'administrateur en tant que tel n'a pas à s'immiscer dans la gestion de l'entreprise. Il ne lui appartient pas de se substituer aux dirigeants exécutifs.

L'administrateur agit dans l'intérêt social et le privilège.

Lorsqu'un administrateur siège au Conseil, il défend l'intérêt social et non ses propres intérêts (ou ceux de la société qu'il défend dans le cas d'un représentant permanent).

L'administrateur prévient le Conseil dès lors qu'une décision à prendre est susceptible d'impliquer ses intérêts personnels ou ceux de l'entreprise qu'il représente. En cas de conflit d'intérêts, il doit être prêt à privilégier les intérêts de l'entreprise, en particulier ses intérêts à long terme, ou à se démettre.

L'administrateur participe et prépare les réunions du Conseil.

C'est le rôle le plus conséquent de l'administrateur.

Il est présent au sein du Conseil pour participer aux décisions relatives à l'administration de la société et ainsi contribuer aux décisions dans l'intérêt des actionnaires.

Il a pour rôle d'y développer les échanges et d'enrichir le débat. Il doit pour cela s'interroger sur la manière dont il peut aider le Conseil à prendre de meilleures décisions. Pour ce faire, l'administrateur prépare les Conseils et est au fait de toutes les questions portées à l'ordre du jour.

L'administrateur exerce un devoir permanent de vigilance, même en dehors des Conseils.

Les administrateurs exercent leur mandat avec vigilance et fermeté. Les administrateurs ne doivent pas « laisser faire », faire confiance aveuglément, ni sur l'application des lois et règlements, ni sur la stratégie, ni sur l'opportunité des décisions, ni sur les comptes. Ils doivent pouvoir agir en toute indépendance tant à l'égard du Président que du management de l'entreprise.

L'administrateur rend compte aux actionnaires.

A l'égard des actionnaires dont ils sont les mandataires, les administrateurs ont une obligation collective de rendre des comptes. Il leur appartient de veiller à ce que l'information des actionnaires soit complète.

L'administrateur respecte une obligation de discrétion.

La loi édicte, dans l'intérêt de la société, une obligation de discrétion sur les délibérations du Conseil d'Administration : « Les administrateurs, ainsi que toute personne appelée à assister aux réunions du Conseil d'Administration, sont tenus à la discrétion à l'égard des informations présentant un caractère confidentiel et données comme telles par le Président du Conseil d'Administration » (article L.225-37, al 5 du Code de Commerce).

L'administrateur s'assure que les Comités qui ont pour rôle de préparer la décision du Conseil, sont pleinement efficaces.

Le Conseil a un rôle essentiel dans la composition et le fonctionnement des Comités ad hoc qu'il constitue (Comité d'audit, des risques, des rémunérations, stratégique...). Ainsi, en matière de suivi de l'efficacité des systèmes de gestion des risques (ordonnance du 8 décembre 2008), le Conseil veille notamment à ce que les travaux réalisés au sein du comité en charge des risques soient étayés et réalisés en lien avec des « sachants » internes ou externes dans les domaines concernés.

Chapitre 3 - Les responsabilités de l'entreprise et de ses dirigeants en matière de contrôle interne et de gestion des risques

La judiciarisation renforcée de la vie économique se traduit par une mise en œuvre plus fréquente des responsabilités civile et pénale de l'entreprise, personne morale, et de ses dirigeants y compris des administrateurs.

Entreprendre a toujours été synonyme de prise de risques mais le contexte actuel réclame plus de transparence et de réactivité dans des organisations très souvent complexes.

1.1 Les dirigeants et les administrateurs voient leur rôle se transformer face aux risques

Ils doivent ainsi :

- se former, s'informer et agir,
- organiser la transmission de l'information au sein de l'entreprise,
- prendre des mesures adaptées de prévention des risques,
- rendre compte des procédures de contrôle interne mises en place,
- respecter des règles et expliquer les raisons du non respect de celles-ci (Comply or Explain),
- évaluer l'efficacité des procédures mises en place.

1.2 Qui est responsable en cas de défaillance du contrôle interne ou de la gestion des risques ?

Les responsabilités quant à la rédaction et au contenu du rapport du Président sur le contrôle interne et la gestion des risques

La loi du 3 juillet 2008 impose que ledit rapport soit approuvé par le Conseil et étend son périmètre à la gestion des risques.

S'il est démontré une faute caractérisée, un préjudice et un lien de causalité entre faute et préjudice, la responsabilité civile du Président et des administrateurs peut être engagée. De façon très exceptionnelle, leur responsabilité pénale pourrait également être mise en jeu sur le terrain du délit de communication d'informations fausses ou trompeuses, pour des sociétés dont les titres sont négociés sur un marché réglementé.

Les responsabilités quant à la qualité du contrôle interne et de la gestion des risques

C'est la Direction Générale qui est responsable de la qualité du contrôle interne et des processus de gestion des risques. Le Conseil pour sa part s'assure de l'existence et du suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques.

En cas de carence dans la mise en place des procédures de contrôle interne, ou de procédures inefficaces, la responsabilité civile collective des administrateurs, des membres du Conseil de Surveillance et de la Direction Générale peut être mise en cause.

Par ailleurs, aux termes de l'arrêt rendu par le Conseil d'Etat le 5 octobre 2007, en cas de fraude, une carence manifeste des dirigeants dans la mise en œuvre des dispositifs de contrôle interne peut être qualifiée d'acte anormal de gestion, avec les conséquences fiscales associées.

On observe ainsi une responsabilisation accrue des administrateurs en matière de suivi des risques. Ces derniers doivent se former, s'informer, agir et rendre compte des procédures mises en place. Ils doivent appliquer et/ou faire appliquer des règles, ou à défaut expliquer les raisons du non respect de celles-ci (concept du « Comply or Explain »). Ils doivent aussi s'assurer de l'efficacité des procédures mises en place par la Direction générale.

Les nouvelles fonctions du Comité d'Audit sous la responsabilité du Conseil au regard de l'ordonnance du 8 décembre 2009

Le Comité est chargé, sous la responsabilité exclusive et collective du Conseil d'Administration ou de Surveillance, d'assurer le suivi du processus d'élaboration de l'information financière. Il suit aussi l'efficacité des systèmes de contrôle interne et de gestion des risques, du contrôle légal des comptes annuels et le cas échéant des comptes consolidés par les CAC. La Direction Générale est en charge de la mise en place des procédures et processus de contrôle interne et de gestion des risques.

La responsabilité des membres du Comité d'Audit ne devrait pas être accrue. En revanche, leur rôle évolue. Ainsi, pour suivre l'efficacité des systèmes de contrôle interne et de gestion des risques, le Comité va devoir aller au-delà de la cartographie des risques. En effet, cette évolution va amener le Comité à demander une information plus formalisée et plus régulière en matière de gestion des risques, de la part des différents acteurs majeurs au sein de l'entreprise et plus particulièrement de la part de la Direction générale, des Directeurs des Risques, de l'audit interne et, le cas échéant, du contrôle interne.

La nécessité pour l'entreprise de gérer le risque de non conformité aux Lois et Règlements

La conformité aux lois et règlements est un des objectifs clés du contrôle interne.

Toutes les entreprises sont concernées et les sources de responsabilité sont nombreuses en raison d'une réglementation abondante qui se complexifie, et des actions judiciaires en accroissement. La DGCCRF, l'inspection du travail, les Douanes, l'administration fiscale, l'AMF... diligents de nombreuses enquêtes qui peuvent aboutir à des sanctions lourdes. Les entreprises et leur dirigeants en France comme l'étranger sont aussi exposés à des risques sensibles tels que les ententes, la corruption, le blanchiment, la présentation de comptes inexacts, le marchandage, plus généralement les fraudes diverses.

Ainsi, la gestion des risques de responsabilités civile, pénale et fiscale est devenue un véritable enjeu pour les Directions Générales. Les Conseils d'Administration et les investisseurs s'y intéressent de plus en plus. Un risque pénal mal géré peut être fortement dommageable pour la réputation de l'entreprise et son cours de bourse.

Le Conseil se doit alors de veiller à l'intégration des risques de non-conformité aux lois et règlements dans la cartographie globale des risques, et au suivi de l'efficacité des dispositifs mis en place pour la gestion desdits risques (Codes de conduite, procédures d'alerte, délégations de pouvoirs, formations...).

Partie II :

Principes et fondamentaux de la surveillance des risques de l'entreprise

Chapitre I - Liens entre surveillance, pilotage et gestion des risques

I.1 Les fondamentaux

La surveillance des risques est l'ensemble des politiques et moyens mis en œuvre par une entité pour détecter, limiter et contrôler les risques liés à ses activités. Elle peut contribuer aussi à l'identification et à la gestion des opportunités en mettant en évidence les événements et les facteurs tant internes qu'externes susceptibles d'avoir un impact favorable sur le développement de l'entreprise et la mise en œuvre de sa stratégie.

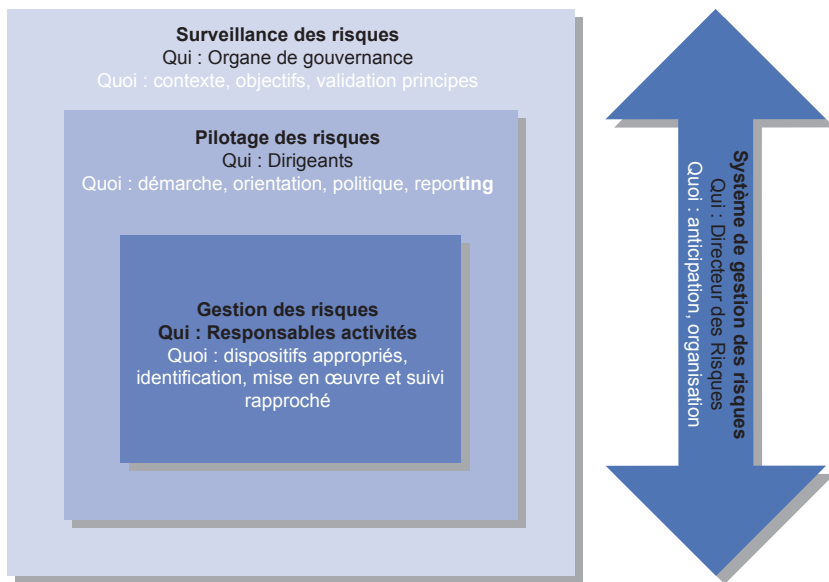
Le conseil donne l'impulsion à la démarche de maîtrise des risques et en suit la mise en œuvre, en vérifiant que le niveau de risques pris par l'entreprise est en ligne avec sa stratégie de développement, de rentabilité et sa politique de prise de risques.

Le pilotage des risques s'appuie sur l'analyse et la synthèse des principaux risques à l'échelle de l'entreprise. Il est mis en œuvre par les dirigeants de l'entreprise qui définissent la politique de gestion des risques ainsi que la démarche et le dispositif de contrôle nécessaires à son application effective. Le dispositif de pilotage des risques est mis en place par les dirigeants pour chaque entité de l'entreprise. Il s'intègre dans les modes de fonctionnement de l'entité, concourt à l'amélioration de sa performance, et contribue à l'atteinte de ses objectifs.

La gestion des risques est la traduction opérationnelle du dispositif de pilotage des risques : c'est la mise en œuvre des dispositifs d'identification, de hiérarchisation et de traitement des risques au niveau des activités par les responsables des directions, des grandes fonctions et l'ensemble des collaborateurs. Le management de chaque entité s'assure de l'application de la politique de l'entreprise en matière de maîtrise des risques liés à l'activité dont il a la charge et veille à ce que l'exposition à ces risques soit conforme à la politique de gestion des risques définie par les dirigeants.

La vision globale des risques relève de la Direction Générale de l'entreprise.

Le lien entre surveillance, pilotage et gestion des risques peut être illustré comme suit.



1.2 La maîtrise des risques, le contrôle interne et l'assurance : interactions et liens

La maîtrise ou le traitement des risques se traduit par des plans d'action pour réduire, transférer ou supprimer le risque. Ces plans d'actions peuvent comprendre des actions à entreprendre, des contrôles supplémentaires à mettre en place, et/ou la recherche de transfert financier ou de responsabilité. Les actions « permanentes ou récurrentes » relèvent en général du dispositif de contrôle interne, s'inscrivant ainsi dans les modes de fonctionnement de l'entreprise.

Au cours de ces dernières années, les entreprises ont principalement focalisé leurs projets sur l'amélioration du contrôle interne. Les démarches ont généralement été structurées par processus ou par grande fonction de l'entreprise. Ces projets ont renforcé l'intérêt du management et de l'ensemble des collaborateurs pour le contrôle de leur activité. Ils ont aussi mis en évidence la nécessité d'enrichir ces démarches en les rattachant aux objectifs et à la stratégie de l'entreprise, évoluant ainsi vers un cadre plus large de maîtrise globale des risques intégrée dans l'ensemble des composantes de l'entreprise. De fait, tous les acteurs de l'entreprise sont impliqués et ont un rôle à jouer dans la maîtrise des risques.

Chapitre 2 - Rôles et responsabilités des différents acteurs clés de l'entreprise

1.1 Principaux contributeurs à la surveillance des risques

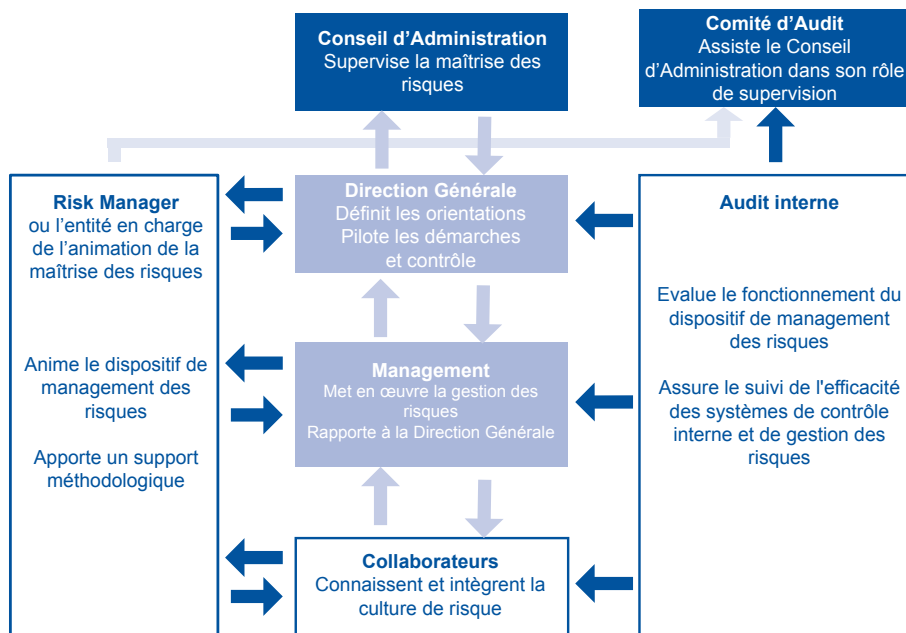
La globalisation et l'interdépendance croissante des économies ont conduit à un changement d'échelle du risque. Au cœur d'une chaîne de causalité de plus en plus complexe, avec une démultiplication des facteurs de risque où s'entremêlent des logiques économiques, politiques, industrielles, scientifiques, culturelles, médiatiques, sociales, managériales, l'anticipation doit désormais prendre en compte l'improbable voire dans certains cas l'impensable.

Les crises majeures récentes ont fait prendre conscience que dans le contexte réglementaire actuel, fortement judiciairisé et médiatisé, un risque mal maîtrisé peut anéantir une entreprise.

Si la prise de risques demeure une constante de l'activité entrepreneuriale, la maîtrise des risques est maintenant au cœur des débats de l'entreprise. La question n'est donc pas tant de chercher à éviter le risque, mais de savoir quel niveau de risque est acceptable pour l'entreprise.

La valeur d'une entreprise se mesure à la valeur de ses actifs nets, de ses dettes, de ses perspectives de développement et de résultats, de la qualité de son management, de son profil de risques... ; la «vraie» valeur de l'action est la résultante chiffrée de cet ensemble complexe.

La maîtrise des risques est au cœur de la stratégie des entreprises et repose sur une bonne gouvernance définissant pour chaque acteur clé son rôle et ses responsabilités.



Sous le contrôle de l'assemblée générale, le **Conseil** impulse la démarche de surveillance des risques dans l'entreprise. A partir des informations obtenues, il suit les risques les plus significatifs, et pour ces risques, apprécie l'exposition de l'entreprise, et sa cohérence avec la stratégie présentée par le management et s'assure de l'efficacité des dispositifs de maîtrise des risques. Il suit plus particulièrement l'efficacité des dispositifs de contrôle mis en place par le management pour garantir la fiabilité et la conformité aux obligations légales des informations financières publiées. En résumé, le Conseil se tient informé des risques encourus, apprécie la démarche mise en place par la Direction Générale pour les maîtriser et s'assure de l'efficacité du dispositif de maîtrise des risques.

Dans le cas des entreprises duales, le Conseil de Surveillance émet le Rapport sur les procédures de contrôle interne et de gestion des risques. Le Directoire est, pour sa part, responsable de l'arrêté des comptes. Le rôle de surveillance des risques est alors réparti entre les deux organes

Quelle que soit la structure de l'entreprise, le Conseil ne peut déléguer ses responsabilités mais peut se faire assister par un ou plusieurs comités ad-hoc.

Le **Comité**, chargé d'assister le Conseil dans son rôle de surveillance de l'efficacité de la maîtrise des risques, rend compte régulièrement au Conseil de l'exercice de ses fonctions et l'informe sans délai de tous les enjeux identifiés.

L'ordonnance du 8 décembre 2008 a renforcé le rôle du Conseil et le rend responsable du « suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques » et des actions prises en cas de défaillance. Le terme de « monitoring » utilisé dans la version anglaise de la 8ème Directive illustre la nécessité de disposer au niveau du Conseil d'un reporting spécifique sur les risques, les plans d'actions et les incidents majeurs.

Le Comité du Conseil s'assure ainsi de la mise en place d'un dispositif permettant de :

- disposer régulièrement d'une synthèse actualisée des risques sur l'ensemble du périmètre d'activité de l'entreprise : les métiers et les grandes fonctions, mais aussi sur les grands projets, les acquisitions de nouvelles structures, ..., et ce afin d'assurer l'exhaustivité du périmètre de l'analyse des risques,
- valider l'adéquation des dispositifs de maîtrise aux risques identifiés,
- vérifier leur bon fonctionnement.

La **Direction Générale** définit la politique de gestion des risques en cohérence avec la stratégie, ainsi que la démarche et le dispositif de pilotage nécessaires à son application effective.

La politique de gestion des risques arrête notamment :

- l'organisation générale d'identification, de hiérarchisation et de traitement des risques,
- l'exposition au risque (ou l'appétence pour le risque) c'est-à-dire les limites que l'entreprise s'interdit de dépasser,
- le mode et la périodicité du reporting de suivi de maîtrise des risques,
- les principes de responsabilisation des collaborateurs au regard des risques inhérents à leur fonction dans l'entreprise.

La Direction Générale s'appuie sur :

- une Direction des Risques pour la mise en œuvre de la démarche et l'animation du dispositif,
- le management pour la mise en place de la politique de maîtrise des risques, le déploiement de la démarche et le reporting,
- les collaborateurs pour l'application du dispositif de maîtrise des risques,
- l'audit interne ou des revues externes pour le contrôle et l'efficacité globale du dispositif.

Le **management** est responsable sur son périmètre de l'identification des principaux risques, de la mise en place des dispositifs de suivi et de la vérification de leur bon fonctionnement. Il rend compte à la Direction Générale des risques sur son périmètre d'activité et, le cas échéant, des actions mises en œuvre pour mieux les maîtriser. Il rend compte des vérifications relatives au bon fonctionnement des processus de gestion des risques en s'appuyant au besoin sur des indicateurs de pilotage et de suivi. Il veille à ce que l'exposition au risque reste conforme à la politique de gestion des risques.

Les **collaborateurs** mettent en œuvre les actions de gestion des risques et traduisent la culture de risque de l'entreprise dans la réalisation de leurs tâches quotidiennes.

La **Direction des Risques**

Organisation et principes directeurs :

La responsabilité de la Direction des Risques est de donner à la Direction Générale une assurance raisonnable quant à la maîtrise globale des risques de l'entreprise. Il s'agit en particulier de mettre en place un dispositif structuré, permanent et adaptable permettant de s'assurer que les principaux risques sont bien identifiés et hiérarchisés entre eux, analysés et pondérés à leur juste valeur, et que l'organisation et les moyens mis en œuvre pour y répondre sont suffisants et adaptés.

La Direction des Risques est responsable de la cohérence du processus global de gestion des risques. A ce titre, en liaison avec les directions opérationnelles et fonctionnelles de l'entreprise, elle anime les processus d'identification des événements susceptibles d'empêcher l'entreprise d'atteindre ses objectifs, d'évaluation des risques et le pilotage d'ensemble de la démarche. Elle établit la cartographie des risques majeurs du Groupe et synthétise les plans d'actions corrélatifs. Pour le reste, elle s'assure que des réponses appropriées sont données : mise en place de règles de conduite contribuant à un environnement interne cohérent et favorable à la maîtrise des risques ; adoption de réponses appropriées face aux risques identifiés ; pilotage des risques...

Une bonne démarche de gestion des risques nécessite tout d'abord de bien définir le périmètre de la gestion des risques qui présente des caractéristiques multidisciplinaires (risques financiers, juridiques, de marchés, d'image et de réputation ; mais aussi des risques et des enjeux environnementaux, voire des opportunités opérationnelles).

Cette démarche représente quatre enjeux majeurs :

1. **Faire travailler ensemble en mode projet des spécialistes** de différentes disciplines qui n'y sont pas toujours naturellement habitués. Clarifier les rôles et les responsabilités de chacun, pour ne pas déresponsabiliser les managers opérationnels, qui restent in fine responsables de la bonne maîtrise des risques sur leurs périmètres.
2. **Motiver les directions opérationnelles et fonctionnelles** : la cartographie des risques est un levier efficace qui permet :
 - une vision d'ensemble et hiérarchisée des principaux risques, dépassant les silos fonctionnels classiques,
 - la mise en œuvre et le suivi de plans d'action de minimisation des risques majeurs, proportionnés aux enjeux,
 - l'amélioration de l'efficacité opérationnelle des activités.

3. **Quantifier le risque**, chaque fois que c'est possible (variation du prix des carburants, risque énergie ou matières premières, risques émergents tels que Climat ou Carbone...), pour décider des actions à mener.
4. Enfin, **un enjeu de reporting interne et externe** : une communication claire sur les risques répond aussi à une demande croissante des parties prenantes (investisseurs et des agences de notation financière et extra-financière) pour plus de transparence et de prévisibilité des résultats, mais aussi pour partager les meilleures pratiques identifiées.

Feuille de route de la Direction des Risques :

La feuille de route de la Direction des Risques est de faire en sorte que les fonctions suivantes soient, en matière de gestion des risques, effectivement en place au sein de l'entreprise :

- connaître et anticiper : s'assurer qu'une veille permanente est en place sur les risques pour garantir qu'aucun d'eux n'est oublié ou sous-estimé, et aussi pour anticiper une évolution de la nature ou de l'intensité des risques,
- organiser : s'assurer que les principaux risques identifiés sont effectivement pris en compte au niveau le plus approprié de l'entreprise,
- contrôler : s'assurer que les organisations et moyens mis en place sont efficaces pour réduire les risques identifiés,
- informer : la mise en place d'un dispositif coordonné de gestion des risques est considérée par les indices non financiers et les agences de notation financière comme un élément important d'évaluation des entreprises. La communication de l'entreprise à l'égard des marchés financiers et de l'ensemble des parties prenantes, sur sa démarche de gestion des risques contribue à soutenir son développement et la prévisibilité de ses résultats.

L'audit interne a pour rôle d'évaluer le bon fonctionnement des processus de management des risques, de contrôle et de gouvernement d'entreprise et de contribuer à leur amélioration sur la base d'une approche systématique et méthodique. Cette évaluation porte sur l'ensemble des composantes du contrôle interne et en particulier sur la fiabilité et l'intégrité des informations financières, l'efficacité et l'efficience des opérations, la protection du patrimoine, le respect des lois, règlements et contrats.

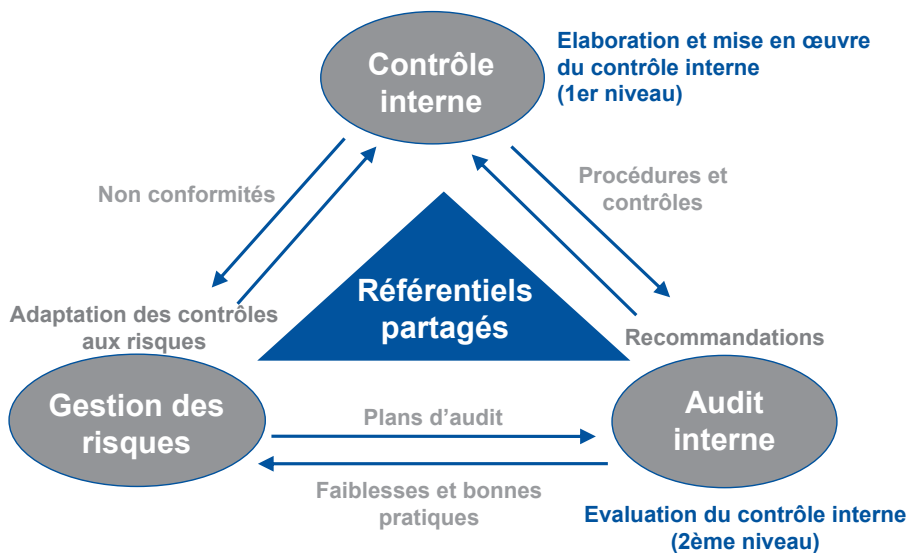
Selon les organisations, les groupes peuvent être dotés d'une **Direction du contrôle interne ou de structures de contrôle interne** en charge d'assurer la coordination des directions opérationnelles et fonctionnelles pour identifier, normaliser et fiabiliser les processus clés de l'entreprise. Elles orientent leur mission autour de trois axes :

- formaliser et mettre à jour les processus clés dans des procédures largement diffusées et déclinées,
- harmoniser les systèmes de gestion associés à leur mise en œuvre,
- veiller à l'adéquation des compétences avec les besoins de l'entreprise.

Le contrôle interne dépend, en amont, d'une gestion efficace de tous les processus de l'entreprise (commerciaux, techniques, ressources humaines, juridiques, économiques, ...) dont les directions opérationnelles et fonctionnelles ont la responsabilité. Il exige en aval un contrôle rigoureux de l'application des règles de l'entreprise, assuré par la direction de l'audit interne.

1.2 Les interactions entre les principaux dispositifs participant à la surveillance des risques

Le schéma ci-dessous résume la nature des échanges entre les différents dispositifs au titre de l'évaluation du processus de surveillance des risques, dont le contrôle interne fait partie.



Partie III :

Qu'attendent aujourd'hui les dirigeants des entreprises ?

L'Institut Français des Administrateurs (IFA) et l'Association du Management des Risques et des Assurances des Entreprises (AMRAE), avec l'assistance du cabinet d'audit et de conseil PricewaterhouseCoopers et du cabinet d'avocats Landwell, ont conduit une étude commune sur le rôle du conseil d'administration dans la gestion des risques et plus spécifiquement du comité d'audit, ou du comité des risques lorsqu'il en existe un.

Cette étude s'est appuyée sur une enquête menée auprès des entreprises du SBF 120. Elle est complétée par un état des lieux sur les pratiques 2008 en matière de gestion des risques en France et à l'étranger effectué par Aon en partenariat avec Euronext. Les résultats de l'enquête et les données de l'état des lieux sont présentés en annexe.

L'état des lieux met en évidence la structuration croissante de la gestion des risques et du contrôle interne, accompagnée d'une implication croissante des organes de gouvernance et de direction des entreprises. La mise en place des processus de gestion des risques et de contrôle interne émane le plus souvent d'une demande formulée par la Direction Générale et les Conseils d'Administration, directement ou par l'intermédiaire du Comité d'Audit.

L'enquête révèle aussi la multiplicité des acteurs impliqués dans la maîtrise des risques, parmi lesquels la Direction Générale, l'Audit Interne, le Comité d'Administration et le Comité d'Audit.

Les démarches d'analyse et d'identification des risques sont présentées de manière détaillée dans la majorité des rapports du Président. L'état des lieux montre néanmoins

des écarts de maturité pouvant s'expliquer par le type de capitalisation et le secteur de l'entreprise :

- les entreprises du CAC 40 se démarquent par rapport à l'échantillon analysé,
- le secteur des Energie/Matières premières/Utilités est plus mature que ceux des Technologies de l'information et des Loisirs/Médias,
- les sociétés de Services se distinguent par une nette progression de la maturité de leurs démarches.

L'enquête révèle néanmoins, que la maîtrise des risques n'est pas encore véritablement inscrite dans les modes de fonctionnement des entreprises, et reste encore une affaire de spécialistes : peu d'entre elles en tiennent compte dans la fixation des objectifs du management ou considèrent sa mise en œuvre comme étant du ressort de l'ensemble des collaborateurs.

Partie IV : Propositions de bonnes pratiques

Chapitre I - Rôles et Responsabilités des membres du Comité du Conseil au regard de la réglementation en vigueur

I.1 Les conséquences de la transposition de la 8ème directive européenne

La transposition de la directive « Audit » accroît-elle la responsabilité des membres des Comités d'Audit ?

S'il est clairement rappelé à juste titre par l'ordonnance du 8 décembre 2008 que le Comité d'audit agit sous la responsabilité exclusive et collective des membres de l'organe chargé de l'administration ou de l'organe de surveillance, il n'en demeure pas moins que le niveau d'exigence attendu par les membres du Conseil d'administration vis-à-vis des membres du comité d'audit va s'accroître. Le Comité d'audit ne doit plus uniquement donner un avis puisqu'il doit désormais assurer, pour le Conseil, le suivi de l'efficacité des systèmes de gestion des risques.

Le rôle du Comité des Risques doit-il se limiter au suivi des risques de nature comptable et financière ?

La loi stipule que le Président du Conseil doit rendre compte dans son rapport, des procédures de contrôle interne et de gestion des risques mises en place par la société.

Il doit notamment détailler les procédures relatives à l'élaboration et au traitement de l'information comptable et financière pour les comptes sociaux et, le cas échéant, pour les comptes consolidés.

Pour autant, le Rapport doit porter sur l'ensemble des objectifs de contrôle interne et couvrir donc potentiellement l'ensemble des procédures de gestion des risques de la société, dépassant le cadre de l'information financière.

Les administrateurs veillent par conséquent à ce que les travaux conduits par l'entreprise au titre de la gestion des risques, ainsi que les conclusions des travaux relatifs à ces procédures ne se limitent pas uniquement à celles relatives aux informations comptables et financières, et soient le reflet de tous les enjeux de l'entreprise.

Les risques comptables et financiers sont par nature suivis par le Comité d'Audit. Ce Comité peut aussi superviser les autres risques à la demande du Conseil.

Si le Conseil a décidé la création d'un Comité des Risques, le Comité d'Audit conserve la supervision des risques de nature comptable et financière ; pour les autres risques un partage des rôles devra être défini.

I.2 Périmètre d'intervention des administrateurs au titre du suivi des risques de l'entreprise

Quel rôle les administrateurs doivent-ils jouer dans la définition de la politique de gestion des risques de l'entreprise et de son appétence aux risques ?

L'appétence aux risques correspond au niveau de risque que l'entreprise est prête à accepter dans l'atteinte de ses objectifs. Elle est proposée par la Direction Générale et validée par le Conseil. Elle constitue le point d'équilibre entre les objectifs de développement et de rendement et les risques induits. En pratique, le Comité analyse les informations transmises par la Direction Générale et présente ses conclusions au Conseil.

Pour les entreprises dont le métier est fondé sur la prise de risques ou la souscription de risques, le Conseil a un rôle central d'arbitrage entre les orientations stratégiques et les risques que l'entreprise est prête à accepter.

D'une manière plus générale, le Conseil détermine les orientations de la société sur la base des informations transmises par la Direction Générale. Ainsi, lorsqu'il détermine les objectifs stratégiques de l'entreprise, le Conseil doit prendre en compte les risques identifiés pouvant compromettre leur réalisation, et si nécessaire fixer des limites chiffrées, par exemple sur les thèmes suivants :

- les niveaux d'investissement et d'endettement,
- les risques financiers notamment le risque de change, et le risque de taux et de contre-partie,
- les risques juridiques ou de conformité, par exemple si une implantation est envisagée dans un pays où le risque de corruption est élevé,
- les risques environnementaux...

Les dirigeants définissent la politique de gestion des risques, traduction opérationnelle de l'appétence au risque, ainsi que la démarche et le dispositif de pilotage nécessaires à son application effective.

Quels types de risques le Conseil doit-il suivre de manière particulière ?

Si le Conseil veille à ce que les risques soient correctement suivis par l'entreprise, il ne se substitue pas pour autant au management. Le Conseil doit s'assurer que les risques majeurs identifiés sont sous contrôle.

Il porte une attention particulière sur les risques pouvant avoir un impact majeur sur la réalisation de la stratégie de l'entreprise, l'atteinte de ses objectifs ou plus généralement sur sa pérennité, et sur les risques pouvant engager la responsabilité pénale de la personne morale. Il peut notamment s'agir des risques suivants : les risques sociaux, les risques pays, les risques d'image et de réputation, les risques financiers, les risques environnementaux, ...

Le Conseil suit l'évolution des risques présentés par la Direction Générale, et porte une attention particulière à l'identification des risques émergents tels que l'obsolescence technologique, qui ne sont parfois pas couverts.

Dans le cadre de la politique de gestion des risques, les administrateurs sont en mesure de s'exprimer sur les limites à respecter au titre de ces risques. Ce peut être le cas par exemple pour les décisions d'investissements dans certains pays jugés à risques pour l'entreprise.

Les administrateurs doivent-ils réclamer une mise à jour régulière de la synthèse des risques de l'entreprise ?

La synthèse des principaux risques est fondamentale pour que les dirigeants puissent identifier les axes d'actions prioritaires au titre de la couverture des risques, et décider de l'allocation des ressources disponibles.

Le rythme de mise à jour peut être calqué sur le calendrier de construction de la stratégie de l'entreprise dont les grandes étapes sont l'élaboration du planning stratégique et des budgets. L'objectif pour les dirigeants est de s'assurer de la cohérence entre les objectifs stratégiques, les risques potentiels et les moyens adossés à l'atteinte de ces objectifs. La surveillance des risques concourt ainsi à la performance opérationnelle et à la création de valeur.

En 2009, la crise a bouleversé l'environnement économique et financier, et a affecté la capacité de création de valeur et les équilibres financiers de nombreuses entreprises. Il est donc raisonnable d'envisager la mise à jour de la synthèse des principaux risques et de vérifier si la stratégie de couverture des risques est adaptée.

Si l'analyse des risques est propre à chaque entreprise, la crise a d'un point de vue général sensiblement modifié l'appréciation des risques et en a renforcé certains :

- des risques opérationnels à court terme, désormais prioritaires par rapport à des risques de nature stratégique, mais avec un impact potentiel à plus long terme. Les évolutions brutales des marchés multiplient les risques ayant un impact à court terme (ex : risque de défaillance d'un ou de plusieurs partenaires stratégiques, clients ou fournisseurs),
- des risques jugés non significatifs en période de croissance économique peuvent devenir particulièrement sensibles en période de crise ; tel peut être le cas de risques de rupture de financement à court terme de l'exploitation de certaines filiales ou de sites de production suite à une baisse brutale des ventes. Considéré aujourd'hui comme un risque difficile à couvrir, la direction peut décider de le gérer au niveau du groupe et non au niveau de l'entité ou du site de production concerné,
- des risques issus de la mondialisation de la crise, ainsi que des nouveaux désordres économiques, sociaux et politiques dans certaines régions du monde, peuvent affecter de manière significative le ratio Risques/Avantages des délocalisations et impacter la rentabilité et l'organisation du groupe. Jusqu'à présent ces risques étaient traités avec peu de précision par les entreprises du fait de leur faible probabilité d'occurrence. Il en résulte que les entreprises se trouvent souvent démunies pour y répondre s'ils n'ont pas été anticipés (à titre d'exemple, la diversité des sources d'approvisionnement pour faire face à la faillite de fournisseurs clés).

Si la prise de risques est une menace lorsqu'elle n'est pas maîtrisée, elle est également un attribut incontournable de management et constitue même un enjeu de survie et de développement dans l'environnement actuel de forte concurrence. Ainsi, seul un système de gestion des risques sur l'ensemble de l'organisation, avec une procédure régulière de mise à jour, permet à la direction de sécuriser la réussite de ses objectifs stratégiques en gérant l'équilibre entre l'exposition aux risques et la prise de risques.

Comment le Comité peut-il « suivre l'efficacité des systèmes de contrôle interne et de gestion des risques » ?

La version anglaise de la 8ème Directive utilise le terme « monitoring » pour le terme « suivi » utilisé dans la version française. L'objectif du Comité est donc de s'assurer :

- de l'organisation et de l'adéquation des moyens et des compétences mis en place pour identifier les principaux risques auxquels la société est exposée. De même un examen régulier des risques susceptibles d'avoir un impact majeur sur les objectifs de l'entreprise s'impose en tenant compte des caractéristiques de chaque société, par exemple : risques fiscaux, juridiques et pénaux, environnementaux, opérationnels, ... ,
- de l'adéquation des dispositifs de maîtrise des risques aux besoins de traitement des risques identifiés et de la vérification de leur correcte application : mise en place d'un processus de suivi des risques, définition de fonction des responsables opérationnels et du Directeur des Risques (ou équivalent), existence et mise en place de procédures adaptées de contrôle et de suivi des risques,
- de l'existence et de la revue régulière d'indicateurs de bon fonctionnement de ce dispositif de pilotage.

En pratique, pour suivre l'efficacité des systèmes de contrôle interne et de gestion des risques, le Comité peut notamment s'appuyer sur :

- les définitions de fonctions et d'objectifs des dirigeants et du management,
- les procédures de contrôle interne et de gestion des risques : revue de l'existence d'un manuel de procédures, analyse de l'adéquation des contrôles pour couvrir les risques, contrôles d'application de procédures effectués sous la responsabilité de la direction,
- les travaux de l'audit interne : l'examen de l'organisation et de la compétence de l'audit interne, la revue de la définition et de l'étendue des travaux au regard des risques significatifs et problématiques complexes, la prise de connaissance des conclusions des rapports d'audit interne et le suivi par la direction des recommandations pour couvrir des faiblesses constatées le cas échéant,
- les travaux et conclusions des auditeurs et des conseils externes qui peuvent être directement mandatés par le Comité d'Audit,

- les procédures pour couvrir des risques liés à des opérations non récurrentes ; telles que les opérations de croissance externe ou de cession, de restructuration, ...,
- l'application de codes de gouvernement d'entreprise comme celui de l'AFEP/MEDEF,
- l'existence et l'application de codes de bonne conduite et d'éthique.

Pour les PME et les VaMPs, le Conseil doit veiller à prévenir les situations d'auto-révision.

En l'absence de précisions apportées par l'ordonnance du 8 décembre 2008, il appartient aux entreprises de définir une démarche de suivi de l'efficacité de leurs systèmes de contrôle interne et de gestion des risques adaptés à leurs propres caractéristiques. L'appréciation de l'efficacité des systèmes de contrôle interne et de gestion des risques et de leurs défaillances potentielles sera évaluée à l'aune de ces critères.

Quels rôles doivent jouer les administrateurs lors de la revue du rapport du Président sur le contrôle interne et la gestion des risques ?

Les dispositions de la loi dite DDAC du 3 juillet 2008 imposent désormais que le rapport du Président soit approuvé par le Conseil. Selon le rapport 2008 de l'AMF sur le gouvernement d'entreprise et le contrôle interne (du 27 novembre 2008), les trois-quarts des sociétés étudiées ont traité ce sujet lors des réunions du Conseil et la moitié en ont discuté lors de réunions du Comité d'Audit. Ainsi il apparaît que le Conseil joue déjà un rôle dans la revue du rapport du Président dans un grand nombre d'entreprises.

Cette revue est donc devenue obligatoire et il est souhaitable que les administrateurs approuvent et s'approprient son contenu en veillant notamment à ce que :

- le contenu du rapport soit cohérent avec les autres documents d'information communiqués aux actionnaires et aux tiers : rapport de gestion et facteurs de risques décrits dans les notes aux états financiers,
- les éventuelles estimations comptables de fin de période (dont les provisions ou les ajustements de valeurs des actifs) soient en ligne avec l'appréciation des risques de l'entreprise,
- les démarches et les outils utilisés par l'entreprise pour élaborer les conclusions formulées dans le rapport soient adaptés aux enjeux de l'entreprise et correctement mis en œuvre au sein de l'organisation,
- le Conseil analyse les conclusions reprises dans le rapport en relation avec les résultats des travaux d'autres acteurs de l'entreprise avec lesquels il travaille (Direction générale, Directions opérationnelles de l'entreprise, Direction financière, Direction juridique, Direction de la stratégie, Direction de l'audit interne, Direction des Risques, Direction de la communication ...).

L'implication des administrateurs est par ailleurs continue, et ne se résume pas à la revue du rapport du Président.

En synthèse, le Comité d'Audit discute le projet de rapport avec le Président. Les autres administrateurs en prennent connaissance et sont en mesure de faire des observations. Tous les membres du Conseil sont réputés connaître le rapport avant sa publication et être en accord avec son contenu.

Qui doit participer à la rédaction du rapport du Président sur les procédures de contrôle interne et de gestion des risques ?

L'implication de chaque Direction de l'entreprise est un réel axe d'amélioration de la pertinence de ses conclusions. En effet, dans la mesure où la surveillance des risques et les dispositifs de contrôle interne sont intégrés aux modes de fonctionnement de l'entreprise et que le management veille à son bon fonctionnement, celui-ci semble le mieux à même d'en faire état. Dans le cadre d'un Groupe, les administrateurs veillent à ce que le Rapport prenne en compte les éléments consolidés, lorsqu'ils sont requis.

Il est en outre souhaitable d'associer à sa rédaction les principaux acteurs de l'entreprise en charge de la gestion des risques ou directement intéressés par les procédures de gestion des risques : lorsque ces fonctions existent, le Directeur des Risques, l'audit interne ou encore le contrôle interne. L'AMF recommande en effet que le rapport du Président sur le contrôle interne et la gestion des risques fasse apparaître le lien entre le recensement des risques et les procédures de gestion des risques.

Les contributions des acteurs en charge de sa conception et de la vérification de sa bonne application sont par conséquent indispensables à la pertinence des éléments contenus dans le rapport sur les procédures de contrôle interne et de gestion des risques.

Les administrateurs veillent enfin à ce que tous les acteurs mentionnés aient effectivement participé à la rédaction du Rapport, et que les points identifiés avec eux notamment lors des échanges réguliers sur la situation des risques de l'entreprise prévus à l'ordre du jour du Conseil, sont bien inscrits dans le Rapport.

Quelles sont les défaillances du contrôle interne à communiquer dans le rapport du Président ?

Au titre de son obligation d'information permanente, la société doit informer le marché des faits nouveaux importants de nature à affecter de façon significative la valeur en bourse de l'entreprise. Ces faits peuvent comprendre des défaillances ou insuffisances graves du dispositif de contrôle interne, lorsque l'on sait qu'elles vont avoir un impact significatif sur l'entreprise, au titre de la réalisation de la stratégie, de l'image, ou de la pérennité de l'activité. Certaines entreprises précisent dans le rapport de leur Président sur le contrôle interne les principaux plans d'actions qu'elles ont décidé de mettre en œuvre et leurs échéances prévues.

Se pose ainsi une question importante : le suivi de l'efficacité des systèmes de gestion des risques et de contrôle interne vise-t-il à s'assurer de leur correcte conception et de leur bon fonctionnement opérationnel ou doit-il permettre de prévenir, d'identifier et de gérer les éventuelles défaillances significatives et le cas échéant, les communiquer au marché ?

Il semble que « l'esprit » de la loi française soit plutôt de veiller à ce que les systèmes mis en place préservent les intérêts de l'entreprise et de ses actionnaires ; elle se distingue en ce sens de la loi Sarbanes-Oxley qui impose l'adoption de démarches évaluatives et la confirmation aux actionnaires et au marché du bon fonctionnement du dispositif de contrôle interne.

Comment revoir la communication de l'entreprise en matière de risques ?

La communication en matière de risques exige la plus grande vigilance dans la mesure où une communication inadéquate sur un risque peut compromettre la façon de le gérer et porter préjudice à l'entreprise.

Le Conseil veille donc à ce que l'information publiée sur les risques ne mette pas en péril les moyens de gérer leur couverture, sans cependant dissimuler la véritable situation de la société. Au-delà de l'exposé de la nature des risques rencontrés et des mesures prises en vue de leur couverture, la société communique sur les systèmes de gestion des risques existants.

Chapitre 2 - Quelle organisation mettre en place ?

Comment définir les rôles et responsabilités des administrateurs, du management et du Comité au titre du suivi et de la gestion des risques de l'entreprise ?

Le Conseil impulse la démarche de surveillance des risques dans l'entreprise. A partir des informations obtenues, il suit les risques les plus significatifs, et pour ces risques, apprécie l'exposition de l'entreprise et sa cohérence avec la stratégie présentée par le management, et s'assure du suivi de l'efficacité des dispositifs de maîtrise des risques.

Le Conseil peut créer un Comité pour l'assister dans sa fonction de suivi et d'appréciation des risques. Ce Comité peut rencontrer chaque fois que nécessaire et au moins deux fois par an le Directeur des Risques à l'occasion d'un point sur les risques de l'entreprise. Il rend régulièrement compte au Conseil de l'exercice de ses fonctions et l'informe sans délais de toute difficulté rencontrée.

Le management quant à lui est responsable au sein de son périmètre de l'identification des principaux risques, de la mise en place des dispositifs de suivi, et de la vérification de leur bon fonctionnement. Il rend compte à la Direction Générale des risques identifiés sur son périmètre d'activité et, le cas échéant, des actions mise en œuvre pour les maîtriser. De la même manière qu'il rend compte de sa performance, il rend compte des vérifications relatives au bon fonctionnement des processus de gestion des risques en s'appuyant au besoin sur des indicateurs de pilotage et de suivi.

Il s'assure notamment de l'application de la politique de l'entreprise en matière de maîtrise des risques, et veille à ce que l'exposition aux risques soit conforme à la politique de gestion des risques validée.

Le Conseil s'assure à ce propos, que le Comité en charge du suivi des risques est doté des budgets suffisants pour diligenter au besoin des missions indépendantes et complémentaires à celles menées par le management.

Les rôles et les responsabilités des différents acteurs de la surveillance des risques sont décrits dans la politique de gestion des risques de l'entreprise.

Faut-il créer un Comité des Risques distinct du Comité d'Audit ?

Force est de constater que le rôle du Comité d'Audit s'est élargi en matière de gestion des risques et de contrôle interne et il paraît difficile d'isoler les risques ayant uniquement un impact comptable et financier dans le portefeuille de risques de l'entreprise. Ainsi, dans l'hypothèse où le Comité d'Audit aurait en charge le suivi des risques financiers et un Comité spécifique (Comité des Risques) aurait en charge le suivi des « autres risques », la synthèse des risques devrait résulter de la consolidation des travaux des deux Comités.

La multiplication des Comités émanant du Conseil exige par ailleurs une définition rigoureuse à la fois des rôles et responsabilités, des objectifs et des missions de chacun, et ce afin d'éviter les zones de recouvrement et les lacunes potentielles.

La création d'un Comité dédié au suivi de la gestion des risques de l'entreprise a une réelle justification dans les secteurs où le métier de l'entreprise est de souscrire des risques : dans la mesure où ils constituent la matière première de l'entreprise, la création d'un Comité du Conseil spécifique peut être pertinente.

De la même manière si le Comité d'Audit ne parvient pas à dégager le temps nécessaire à une analyse rigoureuse des systèmes de contrôle interne et de gestion des risques, les administrateurs peuvent demander la création d'un Comité des Risques qui leur permettra de disposer des résultats d'un travail plus approfondi et d'une mise à jour plus régulière du suivi des risques de l'entreprise.

Enfin, si la création d'un Comité des Risques distinct du Comité d'Audit n'est pas obligatoire, elle peut être dictée par la complexité des risques à superviser par le Conseil, la nature des compétences à mobiliser et le secteur d'activité de l'entreprise. Pour autant, il conviendra alors d'organiser précisément la répartition des rôles entre le Comité d'Audit et ce Comité, si le Conseil décide de le créer.

Comment assurer le bon fonctionnement et la bonne complémentarité des différents Comités du Conseil ?

Les Comités spécifiques émanant du Conseil d'Administration sont aujourd'hui en effet nombreux : Comité des Rémunérations, Comité des Nominations, Comité d'Audit, Comité des Risques, ..., les administrateurs doivent veiller à ce que leurs missions soient correctement définies, complémentaires et cohérentes avec leurs rôles et attributions.

Le Conseil peut ainsi encourager l'organisation de réunions communes et favoriser la participation croisée de certains membres, siégeant à la fois au Comité d'Audit et au Comité des Risques, lorsqu'il existe.

Le bon fonctionnement des Comités repose notamment sur un certain nombre de principes :

- L'inscription des missions de chacun d'entre eux dans des Règlements Intérieurs permet de s'assurer que les Comités ont des rôles complémentaires et que leurs membres maîtrisent leur périmètre d'action et donc de responsabilités. Il est utile aussi que le Règlement Intérieur définisse le niveau de reporting attendu par les administrateurs,
- Les administrateurs veillent à ce que le calendrier des Comités et celui du Conseil soient compatibles afin que les Comités aient le temps de synthétiser leurs travaux,
- Le Président du Conseil facilite les échanges de points de vue et veille à la liberté de parole et d'opinion et ainsi crée les conditions d'un fonctionnement optimal.

Comment veiller à ce que les Comités émanant du Conseil ne « dépossèdent » pas ce dernier de ses responsabilités ?

En droit français, la responsabilité des membres du Conseil est collective. Les travaux des Comités font l'objet de compte-rendus détaillés destinés à préparer les délibérations et les décisions du Conseil et non de s'y substituer. Le Président du Conseil s'assure qu'en pratique, ce principe est d'application rigoureuse et constante. Concrètement les sujets spécifiques concernant les comités sont discutés en Conseil selon un agenda classique :

- présentation synthétique,
- avis du comité,
- débat,
- synthèse et conclusions.

Le Conseil fixe les objectifs et les missions de chacun des Comités, définit le contenu et la fréquence des reportings et évalue périodiquement la qualité des travaux effectués. Le Conseil est alors collégialement responsable vis-à-vis des tiers des décisions qu'il prend. Les Comités informent les administrateurs du calendrier et de l'ordre du jour des réunions ; un administrateur peut décider d'y assister.

Le Président du Conseil peut par ailleurs s'assurer au moins une fois par an, que les administrateurs non membres du Comité d'Audit ou du Comité des Risques estiment que l'information qui leur est transmise est suffisante, et ne se sentent pas déposséder des risques dont ils assurent la supervision.

Chapitre 3 - Modalités de fonctionnement du Comité du Conseil et domaines de compétences

1.1 Fonctionnement opérationnel

Le Comité doit-il établir un Règlement Intérieur définissant son organisation, son rôle et ses attributions ?

La rédaction d'un Règlement Intérieur adopté par le Conseil apparaît en effet souvent utile aux membres d'un Comité. Ce Règlement Intérieur instaure un cadre de référence qui fixe le rôle et les modalités de fonctionnement du Comité et évite aussi que les comités ne débordent de leur agenda et traitent des sujets ne relevant pas de leur compétence. Il permet à ses membres de mieux s'acquitter de leurs obligations.

Parmi les thèmes à couvrir au regard du suivi de l'efficacité de la gestion des risques, figurent les éléments suivants :

- relations avec la Direction Générale, les Directions des Risques du Contrôle interne et les autres Comités du Conseil,
- diligences quant au suivi de l'efficacité des systèmes de gestion des risques et de contrôle interne avec notamment :
 - revue régulière de la synthèse des risques de l'entreprise et examen critique des incidents majeurs survenus sur la période,
 - revue de l'adéquation des dispositifs de maîtrise aux besoins de traitement des risques identifiés et vérification de leur correcte application,
 - examen des procédures relatives à la détection de la fraude et au dispositif d'alerte éthique,
 - examen des informations relatives au contrôle interne et à la gestion des risques dans le Rapport du Président.
- fonctionnement :
 - composition et fréquence des réunions,
 - rapport d'activité.

Le règlement peut utilement prévoir que les membres du Comité bénéficient d'une veille législative et réglementaire.

Comment sont fixés les objectifs du Comité ?

De manière générale, les objectifs du Comité sont fixés dans son Règlement Intérieur et sont précisés par le Conseil à intervalles réguliers (par exemple chaque année). Ces objectifs prennent en compte la répartition des rôles et attributions entre les différents Comités. Ils seront naturellement enrichis de ceux que se fixera le Comité de sa propre initiative en fonction des événements affectant la vie de l'entreprise.

De quels moyens d'information doit disposer le Conseil en matière de suivi des risques de l'entreprise ?

Le Conseil s'assure qu'il dispose de toute l'information suffisante pour apprécier le bon fonctionnement du dispositif de gestion des risques. A ce titre il obtient du management de l'entreprise :

- les tableaux de bord utilisés par la Direction générale pour piloter les risques. Si le Conseil ne procède pas à des analyses aussi détaillées en matière de gestion des risques, il est important qu'il s'approprie ces outils, et ce pour affiner sa perception de l'efficacité des systèmes de maîtrise des risques,
- une information régulière sur les incidents survenus au sein des différentes activités de l'entreprise, et ceci notamment dans le cas d'un groupe ayant des implantations à l'étranger ou des segments d'activités distincts. L'analyse des incidents permet aux administrateurs d'apprécier l'efficacité des dispositifs d'identification des risques mais aussi celle des mécanismes de couverture des risques mis en œuvre par le management,
- les synthèses et les travaux menés par les Directions des Risques et du Contrôle interne,
- l'appréciation des propriétaires des grands risques de l'entreprise voire du Directeur des Risques ; le Conseil met régulièrement à son ordre du jour des échanges sur la situation des grands risques de l'entreprise, l'objectif étant de créer une relation régulière et de confiance entre le management de l'entreprise et le Comité. En l'absence de Directeur des Risques, le Conseil identifie la ou les personnes en charge de la maîtrise des risques au sein de l'entreprise, et l'invite à échanger avec le Comité,
- les résultats de la conduite de missions spécifiques par l'audit interne ou un conseil externe mandaté indifféremment par le management ou le Comité portant sur l'évaluation du bon fonctionnement opérationnel des dispositifs de maîtrise des risques et de contrôle interne. En effet, si elle n'est pas requise par la loi, l'évaluation régulière de ces dispositifs, en couvrant à la fois les risques majeurs de l'entreprise et les principales composantes de son organisation, est indispen-

sable afin de s'assurer de leur bon fonctionnement opérationnel et du correct dimensionnement des moyens dédiés à la gestion des risques de l'entreprise.

Les administrateurs fixent un calendrier de remontées périodiques de ces synthèses. Par analogie avec la production des comptes qui tend à devenir trimestrielle, une fréquence identique semble raisonnable à condition toutefois que le temps imparti à la revue des risques soit suffisant lors des réunions du Comité. Ce calendrier peut être modifié par la situation interne de l'entreprise et la conjoncture économique.

Le Conseil devra en particulier suivre l'existence et l'efficacité des systèmes de traitement des situations de crise et en particulier des dispositifs spécifiques d'information et de communication qui devront répondre aux objectifs suivants :

- identifier au plus tôt la survenance d'une crise grâce au dispositif de pilotage des risques,
- gérer la communication, agir rapidement afin d'assurer une bonne gestion de la crise,
- tirer rapidement les enseignements de la crise et ajuster, si besoin les dispositifs existants de gestion des risques.

Comment le Comité peut-il « justifier régulièrement de la réalisation de ses missions auprès du Conseil d'Administration et l'informer des difficultés sans délai » ?

Une attention particulière est à porter sur la formalisation des travaux et des conclusions. Bien plus qu'une formalité, la documentation constitue le moyen de justifier que le Comité a bien rempli sa mission vis-à-vis du Conseil. La formalisation est d'autant plus importante que ses diligences reposent en partie sur les travaux d'acteurs majeurs au sein de l'entreprise en matière de contrôle interne et de gestion des risques (audit interne, Directeur des Risques, contrôleurs internes).

La périodicité et la forme des comptes rendus d'activité sont définis par le Conseil dans le Règlement Intérieur du Comité. Ils peuvent notamment comprendre :

- des procès verbaux de ses réunions,
- des rapports sur les conclusions des missions réglementées et sur les travaux spécifiques demandés par le Conseil, décrivant les diligences réalisées, les conclusions, les mesures additionnelles proposées, le cas échéant, pour couvrir les anomalies identifiées,
- un suivi des plans d'actions décidés par le conseil sur les anomalies relevées,
- l'examen des tableaux de bord de suivi des principaux risques élaborés par la Direction Générale.

S'agissant des rapports écrits mettant en exergue des anomalies ou des dysfonctionnements, il est primordial qu'il y ait une information rapide du Conseil et surtout que des mesures appropriées soient prises au plus vite. Le Comité informe le Conseil voire provoque une réunion spéciale. À défaut il expose le Conseil et les membres du Comité eux-mêmes à des actions en responsabilité. La connaissance comme l'ignorance, au même titre que le défaut de diligence peuvent générer des responsabilités civiles voire pénales dans des cas exceptionnels, dont l'étendue variera en fonction de la gravité de la faute commise. En pratique, dans la mesure où le Conseil est un organe non permanent, l'information est dirigée vers son Président.

Comment s'assurer que les systèmes de rémunération en vigueur dans l'entreprise n'encouragent pas une prise de risques trop importante ?

Certaines situations récentes ont mis en lumière l'existence de systèmes de rémunération ayant conduit à survaloriser la rentabilité à court terme de l'entreprise au détriment de ses objectifs à moyen ou long terme. La logique du management peut parfois diverger de celle de certains administrateurs.

Il convient donc d'apprécier l'adéquation entre les systèmes de rémunération en vigueur, notamment ceux des mandataires sociaux et des principaux dirigeants de l'entreprise, avec le respect du niveau de risques cibles proposé par la Direction Générale et approuvé par le Conseil.

Les administrateurs veillent à ce que la prise de risque soit correctement maîtrisée en appréciant certains critères comme par exemple :

- la « mise en danger » des capacités de développement de l'entreprise sur le moyen / long terme dans le but d'atteindre des objectifs immédiats de rentabilité,
- des décisions de fusion ou d'acquisition n'apparaissant pas comme source de création de valeur ou relative ou encore propices à la pérennité de l'entreprise.

Dans le même esprit, les administrateurs pourront proposer que les rémunérations des dirigeants et du management incluent une part variable pondérée par :

- la bonne anticipation des risques et un pilotage satisfaisant des risques,
- le niveau de risque généré par la décision du dirigeant ou du manager.

En résumé, le système de rémunération ne doit pas être fondé sur un seul critère, mais sur un panier de critères représentant la performance et la maîtrise de risques. Il est d'ailleurs de bonnes pratiques de disposer d'un comité de rémunération en charge de ce sujet.

1.2 Formation et ressources

Quelles sont les compétences dont doit disposer le Comité ?

La supervision de la gestion des risques de l'entreprise réclame à l'évidence de disposer au sein du Comité, de compétences complémentaires dont les principales caractéristiques sont :

- la connaissance de l'activité de l'entreprise et de son marché,
- l'expertise sur les métiers clés de l'entreprise,
- des connaissances générales sur l'organisation, les processus et les systèmes des entreprises,
- une culture internationale,
- la connaissance des démarches de gestion des risques,
- les connaissances en matières comptables et financières dans l'hypothèse où le suivi de l'efficacité de la gestion des risques est confié au Comité d'Audit.

La présence au sein des Conseils et des Comités d'Audit ou des Risques, d'administrateurs disposant de compétences et d'expériences en matière de gestion des risques est par conséquent recommandée.

Les évolutions des marchés peuvent amener l'entreprise à se focaliser sur des objectifs plus opérationnels que stratégiques et de ce fait influencer le positionnement relatif des risques dans la cartographie, en donnant plus de poids aux incertitudes ayant un impact à court terme (ex : risque de défaillance d'un ou de plusieurs partenaires stratégiques, clients ou fournisseurs). Les situations de crise favorisent également l'apparition de nouveaux risques significatifs dans la cartographie des groupes, risques qui, dans des périodes plus stables n'auraient sans doute pas été retenus parmi les risques majeurs et auraient été gérés au niveau des entités des filiales ou des sites (ex : risque de financement à court terme de l'exploitation de certaines filiales ou sites de production suite à une baisse brutale des ventes). Les risques à suivre prioritairement sont alors de nature plus opérationnelle que stratégique.

Les administrateurs doivent avoir la capacité de se prononcer sur la pertinence des dispositifs de maîtrise proposés par le management voire de les compléter avec l'apport d'un regard externe et des éléments de « *benchmark* ».

L'identification et le suivi des risques présentés dans la cartographie nécessitent donc des compétences dépassant la sphère comptable et financière. Les administrateurs doivent être en mesure de s'approprier le sujet et être à même, si besoin est, de convaincre voire d'imposer au management de l'entreprise qu'il soit traité. Cette démarche est individuelle et relève de la responsabilité de chacun des administrateurs. Ils veillent à ce que le Pré-

sident du Conseil traduise l'expression pleine et entière de ses membres. Ce dernier suscite la discussion entre les administrateurs afin de traiter des sujets d'actualité mais aussi d'enrichir progressivement la qualité des travaux du Conseil au titre de la gestion des risques de l'entreprise.

Les membres du Comité doivent-ils bénéficier d'un programme de formation adapté ?

La mise en place d'une démarche de surveillance des risques ainsi que la création d'un Comité dédié au suivi de leurs systèmes de gestion modifient souvent les relations entre les différents acteurs de l'entreprise et impliquent, par conséquent, une adaptation de son organisation.

Les membres du Comité, au même titre que le management et les collaborateurs, sont formés aux méthodes de pilotage des risques. Cette formation, par un partage des concepts clés, facilite la diffusion des bonnes pratiques et favorise une compréhension commune des enjeux.

Des formations « techniques », liées aux types de risques identifiés, peuvent en outre compléter les connaissances acquises lors des échanges avec les responsables des grandes Directions de l'entreprise et aider les membres du Comité à évaluer la pertinence des informations qui leur sont présentées.



Annexe I :

Enquête auprès des entreprises du SBF 120

L'Institut Français des Administrateurs (IFA) et l'Association du Management des Risques et des Assurances des Entreprises (AMRAE), avec l'assistance du cabinet d'audit et de conseil PricewaterhouseCoopers et du cabinet d'avocats Landwell, ont conduit une étude commune sur le rôle du Conseil d'Administration dans la gestion des risques et plus spécifiquement du Comité d'Audit, ou du Comité des Risques lorsqu'il en existe un.

L'objectif de l'étude était de :

- faire un état des lieux de la manière dont ces entreprises abordent la maîtrise des risques,
- comprendre leurs modes de fonctionnement ainsi que la répartition des rôles et responsabilités,
- dégager les grandes tendances.

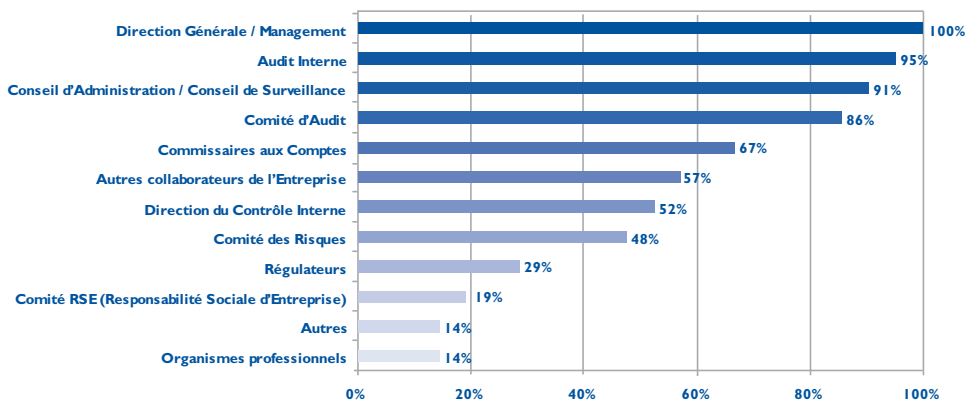
Cette étude s'appuie sur une enquête menée auprès des entreprises du SBF 120, complétée par un état des lieux sur les pratiques 2008 en matière de gestion des risques en France et à l'étranger effectué par Aon.

AI.1 -

Vision de la surveillance des risques au sein de l'entreprise

L'état des lieux met en évidence la structuration progressive de la gestion des risques et du contrôle interne dans les entreprises, qui s'accompagne d'une implication croissante des organes de gouvernance et de direction. La mise en place des processus de gestion des risques et de contrôle interne émane le plus souvent d'une demande formulée par la Direction Générale (62% des sociétés ayant répondu au questionnaire Aon – NYSE Euronext) et les Conseils d'Administration, directement ou par l'intermédiaire du Comité d'Audit (respectivement 19% et 14% des émetteurs ayant répondu à ce même questionnaire).

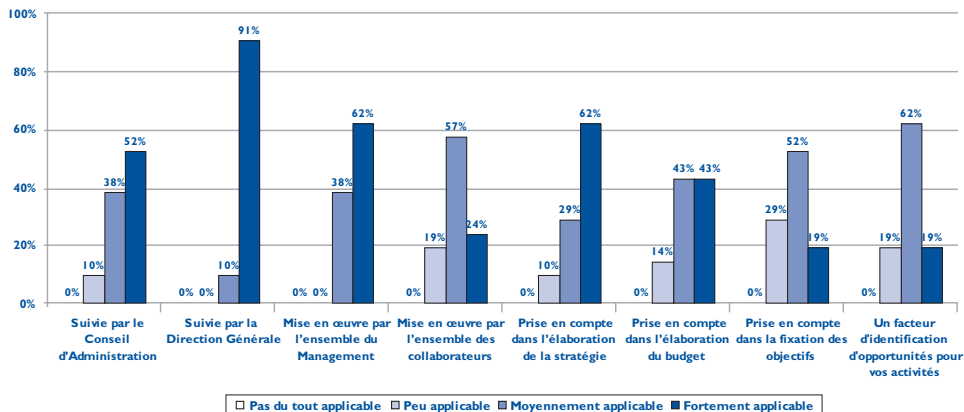
Les acteurs impliqués dans la maîtrise des risques



De nombreux acteurs sont impliqués dans la maîtrise des risques au sein des entreprises interrogées, parmi les principaux :

- la Direction Générale
- l'Audit Interne
- le Comité d'Administration
- le Comité d'Audit

La maîtrise des risques est :



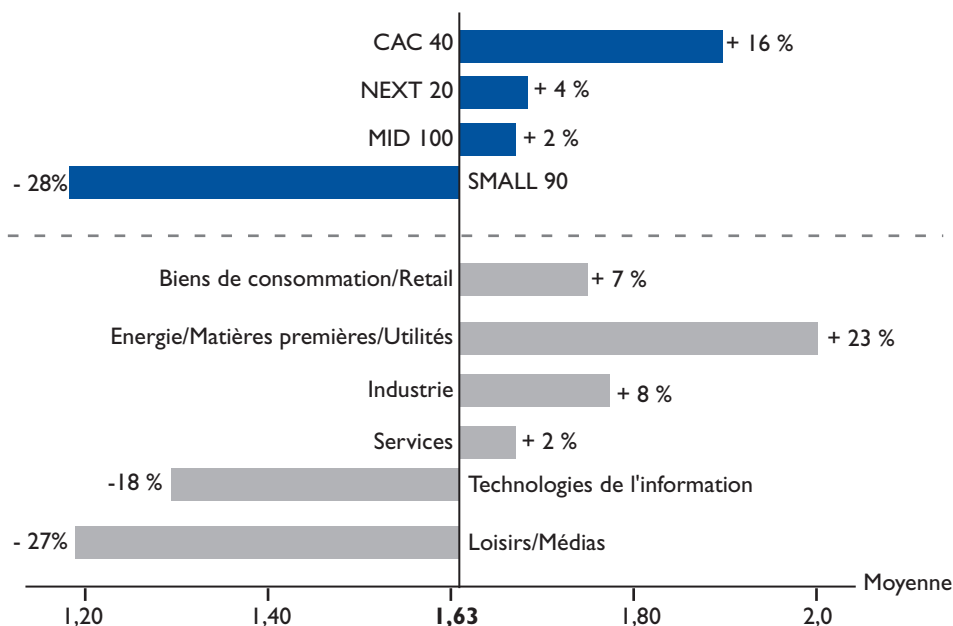
La maîtrise des risques est suivie par la Direction Générale et le Conseil d'Administration selon respectivement 90% et 52% des entreprises sondées ; elle est prise en compte dans l'élaboration de la stratégie pour 62% d'entre elles. Elle est par ailleurs, mise en œuvre par l'ensemble du management d'après 62% des sondés.

L'enquête révèle néanmoins, que la maîtrise des risques n'est pas encore complètement inscrite dans les modes de fonctionnement des entreprises puisque 19% seulement d'entre elles déclarent prendre en compte la maîtrise des risques dans la fixation de leurs objectifs et seuls 24% considèrent sa mise en œuvre comme étant du ressort de l'ensemble des collaborateurs.

L'état des lieux met en évidence une présentation détaillée des démarches d'analyse et d'identification des risques dans 77% des rapports du Président examinés dans le cadre de l'étude Aon – NYSE Euronext. Bien que le pourcentage soit relativement élevé, l'état des lieux montre des écarts de maturité pouvant être expliqués par le type de capitalisation et le secteur de l'entreprise :

- les entreprises du CAC 40 se démarquent par rapport à l'échantillon analysé,
- le secteur des Energie/Matières premières/Utilités est plus mature que ceux des Technologies de l'information et des Loisirs/Médias,
- les sociétés de Services se distinguent par une nette progression de la maturité de leurs démarches.

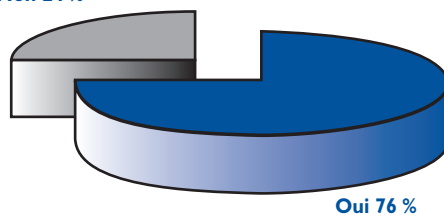
Identification et analyse des principaux risques : écarts à la moyenne par indice et par secteur.



76% des entreprises interrogées disposent d'un Comité du Conseil spécifiquement dédié au suivi des risques.

Votre entreprise dispose-t-elle d'un comité du Conseil spécifiquement en charge du suivi des risques ?

Non 24 %



AI.2 -

Les entreprises ne disposant pas de Comité du Conseil spécifiquement en charge du suivi des risques

24% des entreprises interrogées ne disposent pas de Comité du Conseil spécifiquement en charge du suivi des risques. Pour ces entreprises, le suivi des risques relève essentiellement de la Direction générale. La gestion des risques est animée soit transversalement par une direction métier ou fonctionnelle qui donne l'impulsion, soit par chaque direction ou activité sur son propre périmètre d'intervention. La Direction générale joue alors un rôle central couvrant à la fois des aspects de supervision et des aspects très opérationnels tels que :

- la définition de la politique et du dispositif de maîtrise des risques,
- le suivi régulier ou établissement de la synthèse (cartographie) des risques de l'entreprise,
- l'établissement des plans d'action devant permettre d'améliorer les dispositifs de maîtrise en place,
- l'analyse des risques sur les projets ou les investissements majeurs,
- le suivi des indicateurs de pilotage du dispositif de maîtrise des risques.

En l'absence d'un Comité du Conseil spécifiquement en charge du suivi des risques, le Conseil s'assure a minima que la Direction générale implique les acteurs clés de l'entreprise dans la gestion des risques et dispose de l'ensemble des informations et du temps nécessaires au pilotage des risques.

Ces entreprises souhaitent cependant faire progresser leurs modes de fonctionnement notamment sur les thèmes suivants :

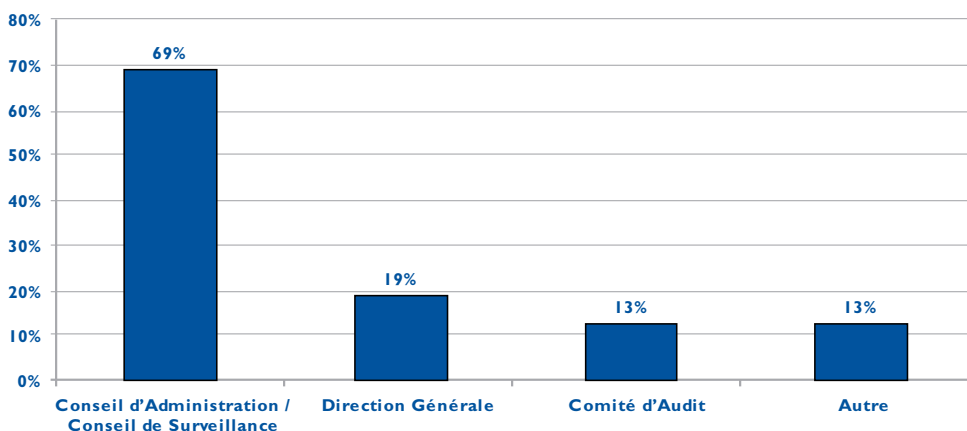
- améliorer la qualité des informations relatives à l'identification et à la maîtrise des risques au sein de l'entreprise,
- prévoir des réunions spécifiques dédiées à la gestion des risques dans le planning annuel des organes de Direction de l'entreprise,
- instituer au sein de l'équipe dirigeante, une fonction transverse de gestion des risques,
- consacrer plus de moyens à la formation à la gestion des risques pour les membres de la Direction.

Pour ces entreprises, la création d'un Comité du Conseil spécifiquement dédié au suivi des risques fait également partie des axes d'évolution identifiés mais n'est pas généralement jugée prioritaire.

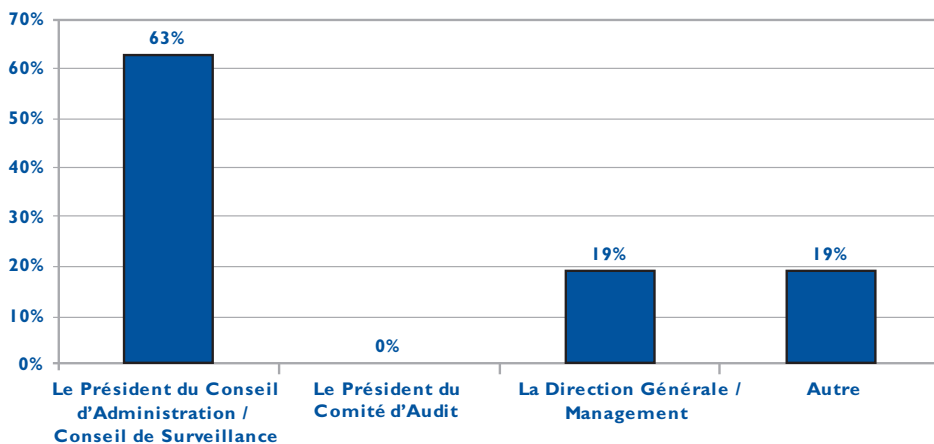
AI.3 - Les entreprises disposant d'un Comité du Conseil spécifiquement en charge du suivi des risques

Parmi les 76% d'entreprises disposant d'un Comité du Conseil spécifiquement en charge du suivi des risques, il s'agit à 88% du Comité d'Audit. L'enquête révèle que ce Comité est rattaché, dans 69% des cas, au Conseil, qui en nomme les membres selon 63% des entreprises interrogées.

A quel organe est rattaché le Comité en charge du suivi des risques ?



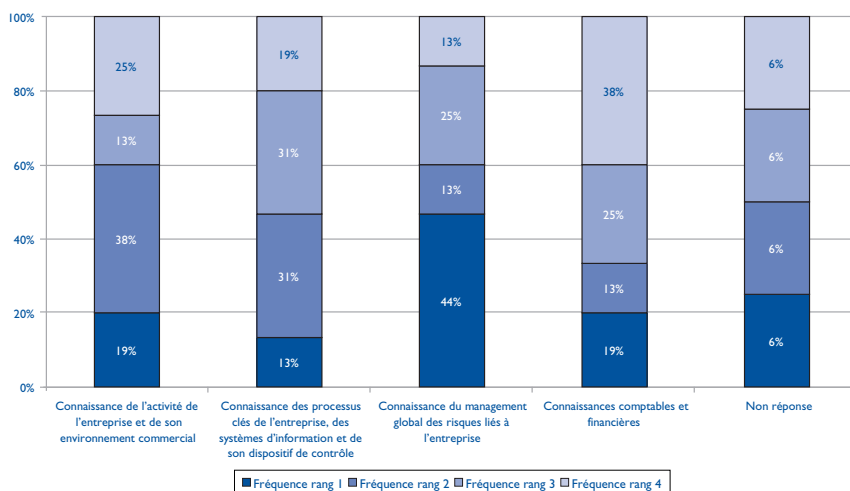
Qui nomme les membres du Comité en charge du suivi des risques?



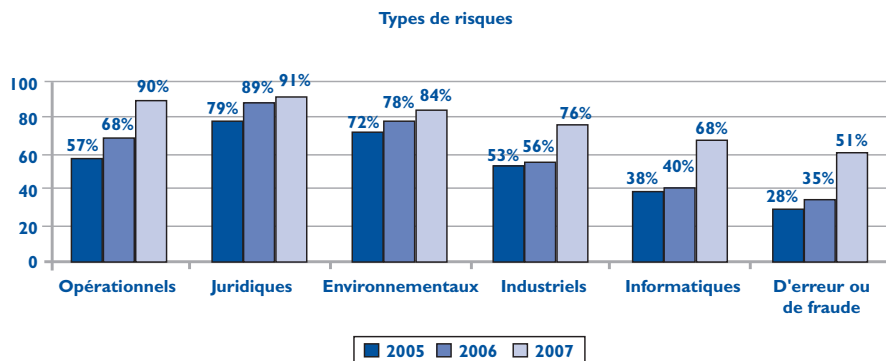
La durée du mandat confié au Comité varie entre 3 et 5 ans dans 45% des cas et est supérieure à 5 ans pour 34% des sondés.

La connaissance du management global des risques liés à l'entreprise se présente comme la première compétence dont doivent disposer les membres du Comité (44%), suivie d'une connaissance de l'activité de l'entreprise et de son environnement commercial (38%).

Quelles sont les compétences principales dont doivent disposer les membres du Comité ?



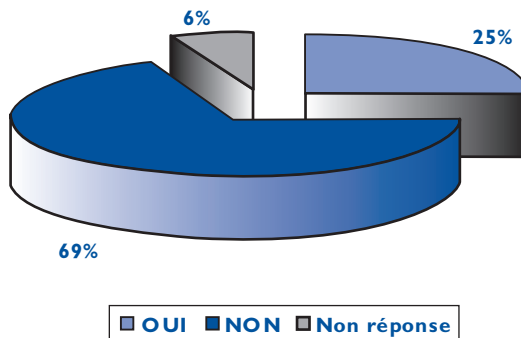
Cette tendance traduit l'importance de la connaissance des métiers de l'entreprise dans la maîtrise des risques. Elle illustre aussi l'élargissement du périmètre des risques (juridiques, opérationnels, environnementaux...), dépassant les strictes sphères comptables et financières et confirmant ainsi la tendance, observée depuis 2005.



AI.4 - Formation et ressources

Selon 70% des entreprises interrogées, les membres du Comité ne bénéficient pas d'un programme de formation particulier sur la maîtrise des risques.

Les membres du Comité bénéficient-ils d'un programme de formation continue afin de les aider dans l'accomplissement de leur mission ?



L'existence et le volume de formation est un indicateur du degré de maturité de l'entreprise en matière de gestion des risques. Le manque de formation peut révéler aussi le caractère souvent récent de la culture du risque au sein de l'entreprise.

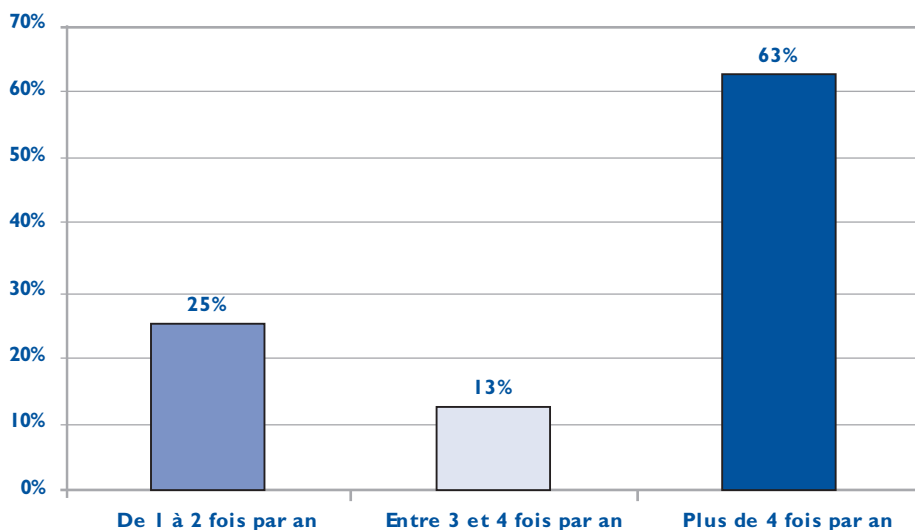
⁷ Source PricewaterhouseCoopers

AI.5 - Fonctionnement opérationnel

Pour 94% des entreprises sondées qui disposent d'un Comité spécifique, les rôles et responsabilités du comité sont formalisées au sein d'une Charte ou d'un document de référence, approuvé pour 67% d'entre elles par le Conseil d'Administration .

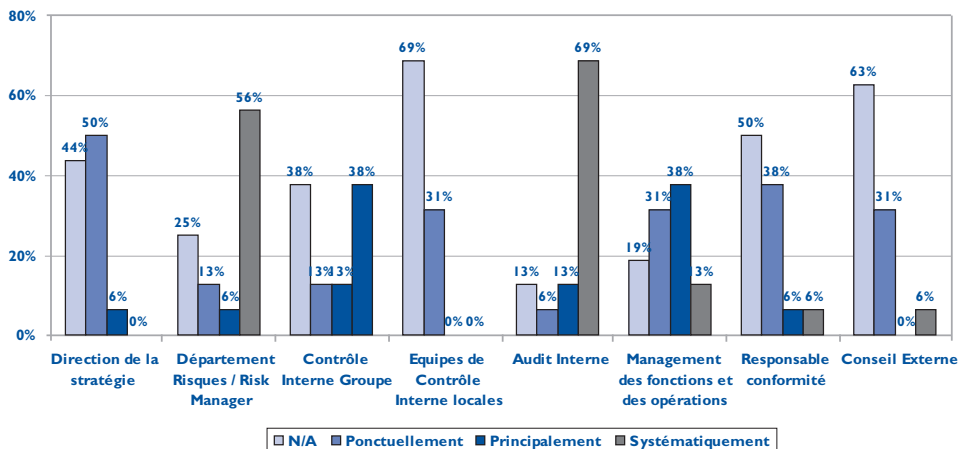
Pour 63% d'entre elles, ce Comité se réunit plus de 4 fois par an.

A quelle fréquence se réunit le Comité en charge du suivi des risques ?



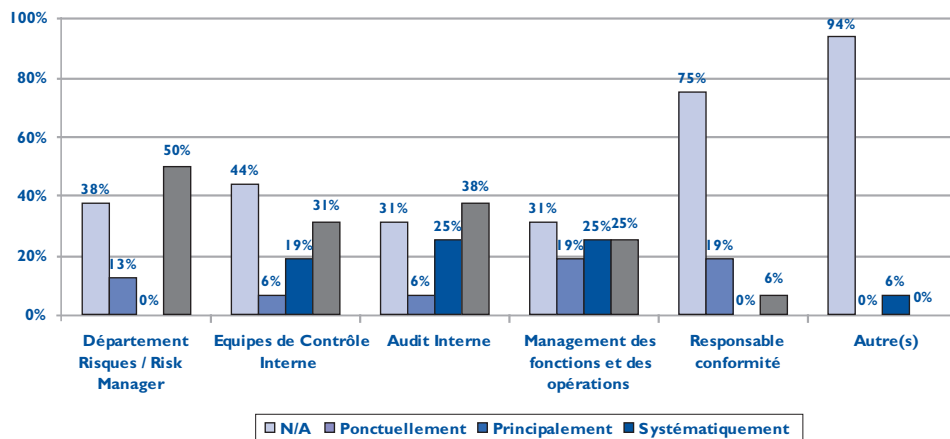
Le Comité s'appuie essentiellement sur les travaux de l'audit interne (70%), du département des risques (56%) ainsi que sur ceux du contrôle interne (38%) pour apprécier le degré de maîtrise des risques.

Sur les travaux de qui le Comité s'appuie-t-il pour apprécier la maîtrise des risques au sein de l'organisation ?



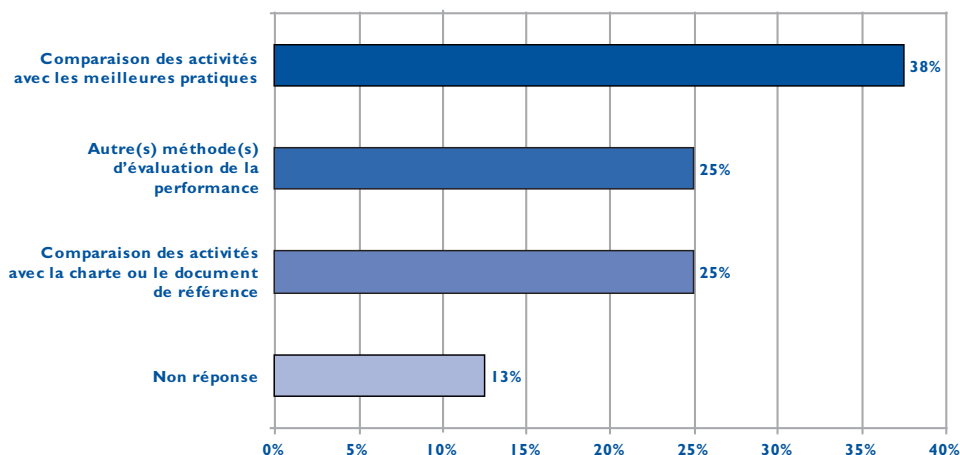
L'audit interne (38%) et le département des risques (50%) sont généralement en charge du suivi des recommandations émises par le Comité.

Qui est en charge du suivi des recommandations émises par le Comité ?



Les travaux du Comité font l'objet d'une évaluation périodique pour 50% des entreprises interrogées. 38% d'entre elles appliquent une méthode d'évaluation comparative avec les meilleures pratiques.

Quelle(s) est (sont) la méthode d'évaluation de la performance appliquée ?



Cette question de l'évaluation ouvre le débat relatif à la responsabilité individuelle ou collective des membres du Comité.

Annexe II : Lexique

Les fondamentaux de la surveillance des risques de l'entreprise

La surveillance des risques est l'ensemble des politiques et moyens mis en œuvre par une entité pour détecter, limiter et contrôler les risques liés à ses activités.

Le pilotage des risques s'appuie sur l'analyse et la synthèse des principaux risques à l'échelle de l'entreprise. Il s'intègre dans les modes de fonctionnement des métiers et des activités, il concourt à la performance de l'entité, et l'aide à atteindre ses objectifs.

La gestion des risques est la traduction opérationnelle du dispositif de pilotage des risques : il s'agit de la mise en œuvre des dispositifs d'identification, de hiérarchisation et de traitement des risques au niveau des activités.

Principaux contributeurs à la surveillance des risques

Le Conseil, sous le contrôle de l'assemblée générale, impulse la démarche de surveillance des risques dans l'entreprise. Il suit les risques les plus significatifs, apprécie la démarche mise en place par la Direction Générale pour les maîtriser et s'assure de l'efficacité du dispositif de maîtrise des risques.

La Direction Générale définit la politique de gestion des risques en cohérence avec la stratégie présentée au Conseil, ainsi que la démarche et le dispositif de pilotage nécessaires à son application effective. Elle s'appuie sur :

- une direction des risques pour la mise en œuvre de la démarche et l'animation du dispositif,
- le management pour la mise en place de la politique de maîtrise des risques, le déploiement de la démarche et le reporting,
- les collaborateurs pour l'application du dispositif de maîtrise des risques,
- l'audit interne ou des revues externes pour le contrôle et l'efficacité globale du dispositif.

La Direction des Risques donne à la Direction générale une assurance raisonnable quant à la maîtrise globale des risques de l'entreprise. Il s'agit en particulier de mettre en place un dispositif structuré, permanent et adaptable permettant de s'assurer que les principaux risques sont bien identifiés et hiérarchisés entre eux ; analysés et pondérés à leur juste valeur ; et que l'organisation et les moyens mis en œuvre pour y répondre sont suffisants et adaptés.

Le management est responsable sur son périmètre de l'identification des principaux risques, de la mise en place des dispositifs de suivi et de la vérification de leur bon fonctionnement. Il rend compte à la Direction Générale des risques identifiés sur son périmètre d'activité et, le cas échéants, des actions mises en œuvre pour les maîtriser.

Cadre et outils de la surveillance des risques

L'appétence au risque correspond au niveau de risque que l'entreprise est prête à accepter dans l'atteinte de ses objectifs. Elle est proposée par la Direction Générale et validée par le Conseil. Elle constitue le point d'équilibre entre les objectifs de développement et de rendement et les risques induits.

La politique de gestion des risques est la traduction opérationnelle de l'appétence au risque. Elle arrête notamment :

- l'organisation générale d'identification, de hiérarchisation et de traitement des risques,
- l'appétence pour le risque, c'est-à-dire les limites que l'entreprise s'interdit de dépasser,
- le mode et la périodicité des reportings de suivi de maîtrise des risques,
- les principes de responsabilisation des collaborateurs au regard des risques inhérents à leur fonction dans l'entreprise.

La cartographie des risques est la représentation synthétique et globale des risques hiérarchisés selon les critères de l'entreprise. Elle est l'outil fondamental des dirigeants pour identifier les axes d'actions prioritaires au titre de la couverture des risques, et décider de l'allocation des ressources disponibles.

Le dispositif de maîtrise regroupe les actions visant à réduire, transférer ou supprimer un risque. Les plans d'actions peuvent comprendre des actions à entreprendre, des contrôles supplémentaires à mettre en place, et/ou la recherche de transfert financier ou de responsabilité. Les actions « permanentes ou récurrentes » relèvent en général du dispositif de contrôle interne, s'inscrivant ainsi dans les modes de fonctionnement de l'entreprise. Les actions « ponctuelles ou limitées dans le temps » disparaissent à leur complète réalisation.

Un indicateur de pilotage est un moyen d'information choisi et mis en place par le management. Il donne des renseignements sur l'efficacité des dispositifs de maîtrise des risques en place. Il permet aux managers d'anticiper l'évolution de la criticité d'un risque et de mettre en place les plans d'action afin de contenir l'exposition au risque sur son périmètre d'activité. Un indicateur de pilotage peut être par exemple le nombre d'incidents de production, de litiges clients, d'accidents du travail,

Institut Français des Administrateurs

7, rue Balzac
75382 PARIS cedex 08
Tél : 01 55 65 81 32
contact@ifa-asso.com

www.ifa-asso.com

Association pour le Management des Risques et des Assurances de l'Entreprise

9/ 11, avenue F. Roosevelt
75008 PARIS
Tél : 01 42 89 33 16
Fax : 01 42 89 33 14

www.amrae.fr

PricewaterhouseCoopers

63, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 58 59
Fax : 01 56 57 58 60

www.pwc.fr

Landwell & Associés

61, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 56 57
Fax : 01 56 57 56 58

www.landwell.fr

Institut Français des Administrateurs

7, rue Balzac
75382 PARIS cedex 08
Tel : 01 55 65 81 32
contact@ifa-asso.com

www.ifa-asso.com

Association pour le Management des Risques et des Assurances de l'Entreprise

9/ 11, avenue F. Roosevelt
75008 PARIS
Tél : 01 42 89 33 16
Fax : 01 42 89 33 14

www.amrae.fr

PricewaterhouseCoopers

63, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 58 59
Fax : 01 56 57 58 60

www.pwc.fr

Landwell & Associés

61, rue de Villiers
92200 Neuilly-sur-Seine
Tél : 01 56 57 56 57
Fax : 01 56 57 56 58

www.landwell.fr