Institut Français des Administrateurs

LE SUIVI DE L'EFFICACITÉ DES SYSTÈMES DE CONTRÔLE INTERNE ET DE GESTION DES RISQUES

GUIDE MÉTHODOLOGIQUE

LES TRAVAUX DE L'IFA

NOVEMBRE 2010

Composition du groupe

Ces travaux ont été menés dans le cadre du groupe d'échanges réunissant des Présidents de Comités d'audit de l'IFA en partenariat avec l'Audit Committee Institute de KPMG.

Président du groupe

ALDO CARDOSO

Membres du groupe

CHRISTIAN AUBIN
ROBERT BACONNIER
PATRICIA BARBIZET
ERIC BOURDAIS DE CHARBONNIÈRE
FRANK DANDEARD
ALAIN GROSMANN
JEAN-BERNARD GUILLEBERT
FRANCOIS JACLOT
HELMAN LE PAS DE SECHEVAL
DANIEL LEBÈGUE
GERARD DE LA MARTINIÈRE
VICTOIRE DE MARGERIE
PATRICE MARTEAU
HELENE PLOIX
GEORGES RALLI
PIERRE RODOCANACHI

Rapporteurs du groupe

DIDIER DE MENONVILLE, Associé KPMG Audit

JEAN-MARC DISCOURS, Associé KPMG Audit

Avant propos

La mission de suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques : quels enjeux pour les comités d'audit ?

La transposition de la 8ème directive européenne en droit français en décembre 2008 a renforcé le rôle du comité d'audit. En effet, l'article L.823.19 précise que :

Le comité spécialisé assure le suivi des questions relatives à l'élaboration et au contrôle des informations comptables et financières.

Le comité est notamment chargé d'assurer le suivi :

- du processus d'élaboration de l'information financière,
- de l'efficacité des systèmes de contrôle interne et de gestion des risques.

Il appartient au conseil de déterminer le niveau de risque qu'il est prêt à accepter. Le management, quant à lui, est responsable de la conception, de la mise en œuvre et de la supervision des systèmes de contrôle interne et de gestion des risques. Dans ce cadre, les risques doivent être évalués de manière continue et les activités de contrôle doivent être conçues pour répondre aux risques propres de l'entité. Mais il faut également que la gouvernance définisse comment le management doit réagir en cas de défaillance et aussi comment les systèmes doivent être adaptés à la suite d'une défaillance.

Cette mission de suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques représente un challenge certain pour les comités d'audit.

Pour faire face à ce défi tant organisationnel que méthodologique, l'IFA a souhaité, en complément de son rapport « Les comités d'audit : 100 bonnes pratiques » publié en janvier 2008, élaborer un document complémentaire qui propose une approche méthodologique aux membres de comités d'audit pour mener à bien leur mission de suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques.

Cette nouvelle publication de l'IFA souhaite contribuer à l'enrichissement des pratiques dans les comités d'audit et ceci dans le respect du rapport du groupe de travail AMF sur le comité d'audit de juillet 2010 qui laisse à chaque conseil le soin de définir les modalités concrètes pour la détermination du rôle qu'il souhaite leur voir jouer.

Ce document qui a été réalisé avec le soutien de l'Audit Committee Institute de KPMG présente une approche globale qu'il conviendra d'adapter aux situations particulières ainsi qu'à la taille des groupes et des organisations en place.

Sommaire

✔ Au fil du guide méthodologique, ce symbole graphique signale la présence de bonnes pratiques.

1 Que faut-il entendre par « efficacité des systèmes de contrôle interne et de gestion des risques » ?

Si l'on se réfère à la définition que donne le « COSO 2 »[1] du dispositif de gestion des risques, il s'agit d'un « *processus mis en œuvre par le conseil*[2]*, les dirigeants et le personnel d'une organisation, exploité pour l'élaboration de la stratégie et transversal à l'entreprise* ». Qu'en est-il alors d'un dispositif **efficace** de gestion des risques ?

1.1 QUELS SONT LES OBJECTIFS DU DISPOSITIF DE GESTION DES RISQUES ET DU CONTRÔLE INTERNE ?

Gérer les risques est une partie essentielle de la mission légale de contrôle du conseil.

Les **objectifs d'un système de contrôle interne et de gestion des risques** et les principaux effets escomptés au sein de l'organisation sont de trois ordres :

1- Identifier les événements potentiels susceptibles d'affecter la réalisation des objectifs de l'organisation (positivement s'il s'agit d'opportunités, négativement s'il s'agit de risques). Ce premier objectif a pour but de définir les contours du « portefeuille de risques » de l'organisation ;

Un système est efficace dès lors qu'il répond aux objectifs pour lesquels il a été créé.

2- Maîtriser les risques en fonction du niveau de risque que l'organisation est prête à accepter et que le conseil d'administration a défini pour accroître sa valeur.

Etroitement lié à la définition de la stratégie de l'organisation, un dispositif adéquat de gestion des risques doit :

- permettre au management de prendre ses décisions de façon éclairée, en cohérence avec le degré d'appétence ou d'aversion au risque de

1 « Committee of Sponsoring Organizations of the Treadway Commission », référentiel de contrôle interne utilisé notamment dans la mise en place des dispositions relevant des lois Sarbanes-Oxley ou LSF. Le COSO 2 propose un cadre de référence pour la gestion des risques de l'entreprise (« Enterprise Risk Management Framework »).

2 Dans l'ensemble du document, la dénomination « conseil » se rapporte au conseil d'administration ou au conseil de surveillance, selon la structure des sociétés considérées.

l'organisation et en fonction de la criticité des risques auxquels elle est exposée (probabilité d'occurrence et impact potentiel),
- en assurer la parade, et,
- prévoir les actions à mener en cas de survenance du risque.

3- Fournir une assurance raisonnable quant à la réalisation des objectifs de l'organisation.

A ce titre, intégrés à l'activité de gestion des risques, les mécanismes de contrôle interne doivent viser plus particulièrement à assurer :

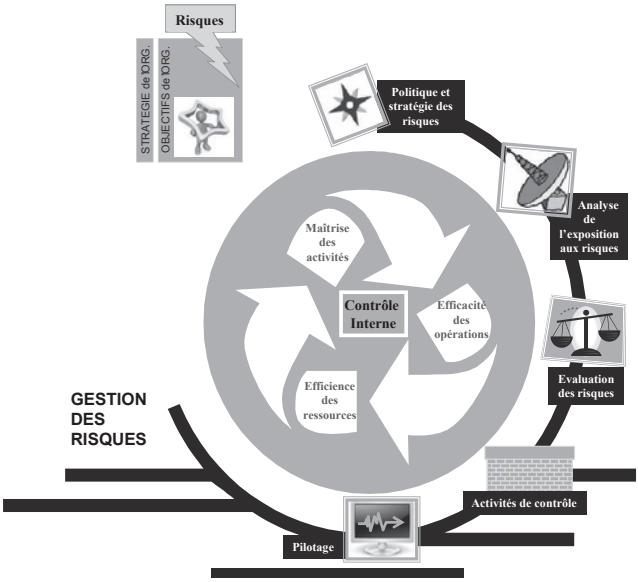
- la conformité aux lois et règlements,
- l'application des instructions et des orientations fixées par le management,
- le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde des actifs,
- la fiabilité des informations financières.

1.2 QUELLES CARACTÉRISTIQUES POUR UN SYSTÈME EFFICACE DE CONTRÔLE INTERNE ET DE GESTION DES RISQUES ?

Un système est efficace dès lors qu'il répond aux objectifs pour lesquels il a été conçu et mis en œuvre.

Ainsi, le système de gestion des risques et le processus de contrôle interne doivent fonctionner de manière imbriquée et coordonnée pour atteindre l'objectif de maîtrise des risques qui leur est assigné.

Système de contrôle interne et de gestion des risques



L'efficacité du système de gestion des risques et du contrôle interne passe par une bonne coordination des dispositifs autour d'activités-clés :

- cartographie et évaluation des risques

- définition et évaluation des activités de contrôle

- plans de remédiation

- pilotage et diffusion de l'information

- supervision continue

L'ensemble du dispositif doit être adapté aux caractéristiques propres de chaque entité. Néanmoins, quelle que soit l'organisation considérée, la mise en œuvre des 15 pratiques suivantes pourrait garantir l'efficacité du système.

■ Politique et stratégie :

1. L'appétence aux risques est définie par le conseil ;
2. les responsabilités en matière de gestion des risques (y compris les problématiques de délégation) sont clairement définies et diffusées au sein de l'entité ;

■ Analyse de l'exposition aux risques :

3. le recensement des événements potentiels susceptibles d'avoir un impact sur les objectifs de la société est réalisé de manière exhaustive et l'univers des risques est régulièrement mis à jour ;
4. les événements négatifs (internes ou externes) pouvant générer des risques sont analysés ;

■ Evaluation des risques :

5. les risques et leurs incidences potentielles sont évalués ;
6. les réponses aux risques sont élaborées ;
7. les risques résiduels sont analysés en lien avec le niveau de risque acceptable tel que défini par le conseil ;

■ Activités de contrôle :

8. les activités de contrôle sont mises en œuvre dans chaque processus de l'organisation ;
9. les activités de contrôle font l'objet d'une évaluation ou auto-évaluation ;
10. les activités de contrôle sont supervisées par des fonctions de surveillance ;
11. l'évaluation des activités de contrôle fait l'objet d'une revue indépendante ;

■ Pilotage :

12. des indicateurs-clés de performance relatifs au dispositif de gestion des risques sont définis et suivis ;
13. les plans de remédiation font l'objet d'un suivi documenté ;
14. les incidents avérés sont recensés et analysés ;
15. les objectifs et la stratégie du dispositif sont régulièrement mis à jour.

In fine, suivre l'efficacité d'un système revient à suivre le niveau de réalisation de ses objectifs. Cela suppose qu'il en existe une mesure, une évaluation.

2 Que doit mettre en œuvre le comité d'audit pour mener à bien cette mission ?

A la lumière des points de repère méthodologiques exposés ci-dessus, la seconde partie de ce document a pour ambition d'apporter un éclairage pragmatique sur la façon dont les comités d'audit pourraient exercer leur rôle compte tenu des exigences de l'ordonnance.

2.1 QUEL CADRE POUR LA MISSION DU COMITÉ D'AUDIT ?

✔ La **charte du comité d'audit** définit le cadre des responsabilités que le conseil confie au comité d'audit et formalise l'ensemble des missions du comité. En conséquence, il apparaît essentiel qu'elle soit amendée afin d'intégrer la nouvelle mission attribuée au comité en matière de suivi de l'efficacité du système de contrôle interne et de gestion des risques. Il sera nécessaire d'y décrire formellement la nature des travaux relevant de la responsabilité du comité au titre de sa mission et qu'il devra mettre en œuvre pour le compte du conseil.

Les diligences du comité relatives à la mission de suivi de l'efficacité et leur formalisation doivent être définies dans la charte du comité d'audit.

✔ Il paraît également essentiel que le conseil soit en mesure de définir le **périmètre des risques** qui feront l'objet du suivi par le comité d'audit (risques financiers, risques industriels, risques sociaux, risques environnementaux, etc.).

✔ Par ailleurs, il apparaît nécessaire que le comité d'audit définisse **un processus de communication et d'échange** avec le conseil (modalités, fréquence, etc.) propre à sa mission de suivi de l'efficacité du système de contrôle interne et de gestion des risques. Les informations transmises devront porter aussi bien sur les éléments financiers que non financiers.

✔ Il conviendrait également que le comité d'audit rende compte formellement au conseil de l'exécution de sa mission de suivi de l'efficacité du dispositif de gestion des risques et de contrôle, et ce en conformité avec les diligences définies par le conseil dans la charte du comité d'audit. Cette communication devrait notamment intégrer l'appréciation de l'importance des défaillances dont le comité d'audit a eu connaissance à travers ses travaux, ainsi que du caractère approprié des plans d'actions afférents.

2.2 QUELS ACTEURS LE COMITÉ D'AUDIT POURRA-T-IL SOLLICITER ?

Pour permettre au comité d'audit de suivre l'efficacité des mécanismes de contrôle interne et de gestion des risques de l'entreprise, il apparaît indispensable d'organiser une communication spécifique et documentée entre la direction, les fonctions de gestion des risques, l'audit interne et le comité d'audit, chacune de ces fonctions devant contribuer à apporter au comité les informations et assurances dont il a besoin pour s'acquitter de sa mission.

✔ Le comité d'audit pourra notamment s'appuyer sur :

- le « **risk manager** » qui est responsable du recensement et du suivi des risques du groupe en mettant en place notamment une cartographie des risques qui est déployée au niveau de chaque entité du groupe ;
- le **département de contrôle interne** qui a pour mission d'assurer l'application des instructions de la direction et de favoriser l'amélioration des performances. Il met en place une organisation, des méthodes et des procédures pour chacune des activités de l'entreprise, afin de garantir sa pérennité ;
- l'**audit interne** qui est entre autres chargé de revoir périodiquement les moyens dont disposent les opérationnels pour gérer et contrôler l'entreprise. Ses objectifs sont de vérifier que les structures sont claires et bien adaptées, que les procédures comportent les sécurités suffisantes, que les opérations ne présentent pas d'irrégularités et que les informations diffusées sont sincères.

✔ En outre, le comité d'audit pourra consulter des acteurs externes à l'entreprise, comme :

- les **commissaires aux comptes** qui se doivent d'alerter la direction et les organes de gouvernance sur les faiblesses significatives de contrôle interne affectant les procédures d'élaboration des comptes ;
- le cas échéant, **les experts indépendants** afin d'obtenir une évaluation tierce sur l'efficacité des systèmes de contrôle interne.

2.3 QUELLES DILIGENCES LE COMITÉ D'AUDIT POURRA-T-IL METTRE EN ŒUVRE ?

La mise en place du dispositif de gestion des risques et de contrôle interne relève de la responsabilité des dirigeants de l'entreprise, l'objectif étant de donner une assurance raisonnable que les objectifs de l'entreprise seront atteints.

L'enjeu pour le comité d'audit est d'avoir une vision d'ensemble du dispositif de gouvernance des risques et du contrôle interne. Il doit veiller à l'existence d'un système de contrôle interne et de gestion des risques et en apprécier le fonctionnement. Il doit notamment pouvoir apprécier les points suivants :

- l'adéquation entre l'approche retenue pour gérer les risques de l'entité et la stratégie de l'entité, ainsi que l'environnement légal, opérationnel et financier dans lequel elle évolue ;
- l'efficacité des contrôles pour les risques significatifs ;
- la mise en œuvre des plans d'actions, en cas de défaillances constatées.

Telles sont les implications concrètes du rôle élargi que lui a assigné la 8ème directive en lui confiant la surveillance du mécanisme de management des risques et plus spécifiquement le suivi de son efficacité.

Les départements de gestion des risques, de contrôle interne, d'audit interne et l'auditeur externe sont des interlocuteurs-clés pour le comité d'audit pour répondre aux exigences de sa mission.

Les diligences présentées ci-dessous ont vocation à être mises en œuvre par les groupes cotés. Elles pourront faire l'objet d'**une mise en œuvre simplifiée et/ou progressive dans les small et mid caps**.

2.3.1 Première mission : réaliser un diagnostic du dispositif de gouvernance des risques et du contrôle interne

Pour réaliser son diagnostic du dispositif de gouvernance des risques et du contrôle interne, le comité d'audit pourrait procéder à un examen de l'existence des éléments constitutifs du dispositif en considérant les trois niveaux suivants :

- 1er niveau du dispositif de gouvernance des risques : **les directions opérationnelles ;**
- 2ème niveau du dispositif de gouvernance des risques : **les fonctions de surveillance** (Direction contrôle interne, Risk manager, Direction qualité, Direction des assurances,...) ;
- 3ème niveau du dispositif de gouvernance des risques : **la fonction audit**.

1- Premier niveau du dispositif de gouvernance des risques : les directions opérationnelles

Les directions opérationnelles évaluent et gèrent les risques. Elles mettent en œuvre les activités de contrôle. Pour réaliser son diagnostic, le comité d'audit pourrait examiner l'existence des éléments suivants :

Niveau 1 – ÉLÉMENTS DE DIAGNOSTIC AU NIVEAU DES OPÉRATIONS

Politique et stratégie	
i. La stratégie et l'allocation des ressources sont définies au niveau de l'organisation ii. L'appétence aux risques est prise en compte dans la définition de la stratégie et de l'organisation iii. Les responsabilités en matière de gestion des risques (y compris les problématiques de délégation) sont clairement définies et diffusées au sein de l'entité	• Existence d'un dispositif de gestion des risques et de contrôle interne (prévention/traitement des risques) • Existence d'un manuel de procédures de contrôle interne permettant de relier objectifs, risques, contrôles • Existence d'un processus de communication de l'information sous une forme et un délai qui permettent à chacun d'exercer ses responsabilités
Analyse de l'exposition aux risques	
iv. Le recensement des événements potentiels susceptibles d'avoir un impact sur les objectifs de la société est réalisé de manière exhaustive et l'univers des risques est régulièrement mis à jour v. Les événements négatifs (internes ou externes) pouvant générer des risques sont analysés	• Existence d'un recensement des événements générateurs de risques • Existence d'une cartographie des risques (identification) • Existence d'une analyse des impacts (échelle)
Evaluation des risques	
vi. Les risques sont évalués vii. Les réponses aux risques sont élaborées viii. Les risques résiduels sont analysés en lien avec le niveau de risque acceptable tel que défini par le conseil de la société	• Existence d'une cartographie des risques (incluant une évaluation des risques) • Existence de plans de réponses aux risques
Activité de contrôle interne	
ix. Les activités de contrôle sont mises en oeuvre dans chaque processus de l'organisation x. Les activités de contrôle font l'objet d'une évaluation (auto-évaluation ou évaluation) xi. Les activités de contrôle sont supervisées par des fonctions de surveillance xii. L'évaluation des activités de contrôle fait l'objet d'une revue indépendante	• Existence d'un référentiel de contrôle interne • Existence d'un processus d'auto-évaluation/d'évaluation du contrôle interne
Pilotage	
xiii. Des indicateurs-clés de performance relatifs au dispositif de gestion des risques sont définis et suivis xiv. Les plans de remédiation font l'objet d'un suivi documenté xv. Les incidents avérés sont recensés et analysés xvi. Les objectifs et la stratégie du dispositif sont régulièrement mis à jour	• Existence d'indicateurs-clés • Existence de plans de remédiation • Existence d'un processus de recensement et d'analyse des incidents • Existence d'un processus régulier et planifié de mise à jour des objectifs et de la stratégie du dispositif de gestion des risques

2- Deuxième niveau du dispositif de gouvernance des risques : les fonctions de surveillance

Les fonctions de surveillance conçoivent les politiques et les procédures. Elles sont responsables de l'introduction de bonnes pratiques et du respect des procédures. Elles supervisent l'efficacité du dispositif.

Pour réaliser son diagnostic, le comité d'audit pourrait examiner l'existence des éléments suivants :

Niveau 2 – ÉLÉMENTS DE DIAGNOSTIC AU NIVEAU DE LA FONCTION DE SURVEILLANCE

- Existence d'un référentiel adapté (cadre de référence AMF, Coso, autre)
- Existence d'un code éthique
- Existence d'un comité des risques
- Existence d'une procédure de revue de la centralisation des risques
- Existence d'une procédure de revue de l'évaluation des risques
- Existence d'une procédure de revue des plans de réponses aux risques
- Existence d'un service de contrôle interne
- Existence d'un département d'audit interne
- Existence d'une procédure de revue par l'audit interne/externe de l'auto-évaluation/évaluation des activités de contrôle
- Existence d'un dispositif de suivi des indicateurs-clés de performance relatifs au dispositif de gestion des risques
- Existence d'une procédure de revue des plans de remédiation (intégrant échéanciers, responsables, etc.)
- Existence d'une procédure de revue de l'analyse des incidents
- Existence d'une procédure de revue de la mise à jour des objectifs

3- Troisième niveau du dispositif de gouvernance des risques : la fonction audit

Les auditeurs internes réalisent des missions d'audit sur les procédures de contrôle qui permettent d'obtenir un avis indépendant sur le fonctionnement du système de contrôle interne et de gestion des risques.

Les conclusions des travaux des auditeurs externes sur les faiblesses significatives de contrôle interne liées au processus d'élaboration de l'information financière constituent également un élément d'assurance indépendante.

Pour réaliser son diagnostic, le comité d'audit pourrait examiner l'existence des éléments suivants :

Niveau 3 – ÉLÉMENTS DE DIAGNOSTIC AU NIVEAU DE LA FONCTION AUDIT

- Existence d'une fonction d'audit interne
- Examen de l'organisation de l'audit interne (rattachement, couverture des pays, etc.)
- Examen du plan d'audit interne en matière de diligences sur le dispositif de gestion des risques et de contrôle interne
- Examen du périmètre d'intervention des auditeurs externes
- Recours à des experts indépendants pour l'évaluation des risques et des activités de contrôle
- Revue par l'audit interne/externe de l'auto-évaluation/évaluation des activités de contrôle

2.3.2 Deuxième mission : obtenir des assurances de la direction sur le fonctionnement du système de contrôle interne et de gestion des risques

Une fois le diagnostic de gouvernance des risques et du contrôle interne établi, il conviendrait que le comité d'audit obtienne de la direction l'assurance que le dispositif fonctionne de manière efficace et ceci de manière dynamique dans le temps.

Selon le mode de fonctionnement de l'entité, et en fonction de l'existence et de la profondeur des procédures mises en œuvre par les opérationnels, le comité d'audit pourrait être amené à déployer des approches différentes pour s'acquitter de ses missions en matière de suivi de l'efficacité des systèmes.

Examen d'ensemble du dispositif, appréciation du processus d'évaluation de l'efficacité et revue de la documentation sont les trois principaux leviers d'action des comités pour mener à bien leur mission de suivi.

1- L'entité a mis en place des indicateurs de risques

Les indicateurs de risques sont de plusieurs natures : des indicateurs de niveau du risque, des indicateurs de suivi de l'avancement des actions de maîtrise des risques et des indicateurs permettant le suivi de risques qui se sont effectivement avérés.

✔ Afin d'examiner le fonctionnement du dispositif de gestion des risques, il conviendrait que le comité d'audit obtienne de la direction :

- le suivi des indicateurs d'alerte (ex : dérives par rapport aux prévisions) ;
- le degré de réalisation des plans de réponse aux risques significatifs (ex : recours à l'assurance, surveillance accrue, réduction de sa criticité) ;
- La synthèse des cas de risques avérés significatifs (incidents, fraude, sinistres...).

✔ En interaction avec la fonction audit interne, il conviendrait que le comité d'audit confronte l'appréciation des risques des auditeurs à celle de la direction afin d'identifier et d'apprécier la portée des éventuelles divergences de vue.

2- L'entité a mis en place une procédure d'évaluation de l'efficacité des activités de contrôle

Les activités de contrôle sont documentées par les opérationnels. L'évaluation est réalisée par des services internes (direction du contrôle interne, direction de l'audit interne).

Le comité d'audit doit s'assurer de l'existence de l'évaluation de l'efficacité des activités de contrôle et de l'utilisation qui en est faite.

✔ Afin d'assurer le suivi de l'efficacité des activités de contrôle, il conviendrait que le comité d'audit obtienne de la direction :

- la documentation relative à la mise à jour régulière des risques et des contrôles associés ;
- pour les risques majeurs, la synthèse des résultats des tests d'efficacité des activités de contrôle.

3- L'entité n'a pas mis en place de procédure d'évaluation de l'efficacité des activités de contrôle, mais procède à une auto-évaluation

Limitée à des critères prédéfinis et menée le plus souvent sur un mode déclaratif, l'auto-évaluation n'a pas la même portée qu'une procédure d'évaluation. Outre l'absence de vérification indépendante, une auto-évaluation ne saurait suffire à l'appréciation de l'efficacité des activités de contrôle. En effet, elle ne répond généralement pas aux exigences d'examen documenté et éprouvé (par le test) des procédures, telles que requises pour une mission d'évaluation de l'efficacité.

✔ Afin d'assurer le suivi de l'efficacité des activités de contrôle, il conviendrait que le comité d'audit :

- obtienne de la direction la synthèse des résultats de l'auto-évaluation de l'efficacité des activités de contrôle ;
- demande à ce que les résultats de l'auto-évaluation fassent l'objet d'une revue indépendante. Cette revue aura pour objet de confronter l'auto-évaluation déclarative aux résultats de l'examen documenté et indépendant.

✔ Sur cette base, il conviendrait que le comité d'audit analyse l'écart éventuel entre les résultats de l'auto-évaluation et les résultats de l'évaluation indépendante.

4- L'entité n'a pas mis en place de procédure d'évaluation ou d'auto-évaluation de l'efficacité des activités de contrôle

✔ Dans ce cas, le comité d'audit pourrait solliciter la fonction audit (interne/externe) pour qu'elle procède à une revue des contrôles-clés au sein de l'entité. Cette revue indépendante devra alors avoir une portée suffisamment large pour couvrir les risques clés de l'entité.

2.3.3 Troisième mission : procéder à l'examen des défaillances significatives du système de contrôle interne et de gestion des risques

Afin d'apprécier l'importance des défaillances du système de contrôle interne et de gestion des risques, il conviendrait que le comité d'audit :

- obtienne de la Direction, pour les incidents avérés, la synthèse des impacts financiers et extra-financiers ;
- obtienne de la Direction, pour les défaillances significatives identifiées, une estimation de leur impact potentiel ;
- examine les plans d'actions afin d'apprécier leur caractère approprié.

Nous avons joint, en annexe, un exemple d'état de suivi de l'efficacité du système de contrôle interne et de gestion des risques, sous forme d'un **tableau de bord spécifique**, qui pourrait être examiné par le comité d'audit pour les **risques significatifs**.

2.4 QUELLE DOCUMENTATION LE COMITÉ D'AUDIT POURRA-T-IL OBTENIR ?

En synthèse, nous avons listé ci-dessous la documentation susceptible d'être mise à disposition du comité d'audit afin de lui permettre de mener à bien sa mission de suivi de l'efficacité du dispositif de gestion des risques et du contrôle interne :

- le tableau de bord de suivi de l'efficacité du dispositif (cf. Annexe),
- la cartographie des risques,
- la synthèse des résultats de l'auto-évaluation ou de l'évaluation,
- la synthèse des rapports de l'audit interne,
- la synthèse des commissaires aux comptes, relative aux faiblesses significatives de contrôle interne,
- la synthèse des plans d'actions de la société pour remédier aux faiblesses significatives.

La mission de suivi de l'efficacité nécessite que le comité d'audit fasse un examen critique des documents clés relatifs à la gestion des risques et au contrôle interne et s'assure de leur cohérence.

✔ Enfin, il conviendrait que le comité d'audit s'assure de la **cohérence** des informations collectées sur le dispositif de gestion des risques et du contrôle interne avec, notamment :

- les facteurs de risques communiqués dans le document de référence, et,
- le rapport du président sur le contrôle interne.

Perspectives

La mission de suivi de l'efficacité du système de contrôle interne et de gestion des risques rend le comité d'audit partie prenante d'un dispositif capital pour les organisations. En effet, si un système de contrôle interne et de gestion des risques efficace et pertinent peut améliorer la qualité des rapports financiers, il peut surtout contribuer à créer de la valeur ajoutée pour l'entreprise :

- en donnant une vision des coûts cachés au sein des différentes fonctions de l'entreprise ;
- en aidant à comparer les performances des contrôles des différentes activités ;
- en aidant à identifier les points d'amélioration des contrôles, les contrôles à supprimer et ceux à automatiser ;
- en aidant une organisation à trouver un équilibre entre la gestion des risques et ses objectifs de croissance et de profitabilité.

Annexe

EXEMPLE DE TABLEAU DE BORD POUR LE SUIVI DE L'EFFICACITÉ DU SYSTÈME DE CONTRÔLE INTERNE ET DE GESTION DES RISQUES

Dans cet exemple de tableau de bord, l'incidence potentielle de chaque risque (impact et probabilité d'occurrence) est évaluée sur une échelle de 1 à 5.

De même, l'efficacité des contrôles couvrant les risques bruts identifiés est évaluée sur une échelle à quatre niveaux (faible, moyenne, bonne, élevée).

Il en résulte un niveau de risque net (ou résiduel) également évalué sur une échelle de 1 à 5.

	Risque	Risque Brut		Responsabilité	Description des contrôles	Efficacité des contrôles	Risque net/résiduel		Action	Responsabilité	Date de l'examen
		Impact	Probabilité				Impact	Probabilité			
1	Stratégie d'acquisition inappropriée	5	4	Directeur financier	Recours à des conseillers externes pour les audits préalables	Faible	4	4	Élaboration d'un cadre de référence pour les fusions/acquisitions en phase avec la stratégie métier. Élargissement de la fonction recherche d'acquisitions	Directeur financier	Sept. 200X
2	Incapacité à satisfaire aux exigences réglementaires et légales (c.-à-d. Cartels)	4	4	Directeur général et directeurs de division	Auto-évaluation annuelle. Supervision par le département juridique	Moyenne	3	4	Renforcement des procédures afférentes à l'observation des dispositions réglementaires et légales	Directeur juridique	Juin 200X
3	Défaillances des systèmes informatiques après mise en œuvre	4	2	Directeur informatique	Procédures de gestion de projet	Bonne	3	2	Application stricte de la liste de vérification de l'adéquation aux besoins pour tous les projets	Directeur informatique	Juin 200X

	Risque	Risque Brut		Respon-sabilité	Description des contrôles	Efficacité des contrôles	Risque net/ résiduel		Action	Respon-sabilité	Date de l'examen
		Impact	Proba-bilité				Impact	Proba-bilité			
4	Incapacité de gérer l'incertitude économique et d'y réagir correctement	3	3	Directeur général, directeur financier, directeurs de divisions	Examen mensuel, par la direction, des prévisions économiques et comparaison avec la position financière prévisionnelle du groupe	Bonne	2	3	Création de modèles financiers en vue de modéliser des scénarios	Directeur général	Sept. 200X
5	Plans de continuité et anti-sinistre inadéquats, ne permettant pas de faire face à une défaillance majeure du réseau informatique	4	1	Directeur informatique	Examen semestriel (et au besoin actualisation) des plans de continuité et anti-sinistre, et tests correspondants	Élevée	3	1	Sauvegarde hors site des systèmes	Directeur informatique	Sept. 200X

Notes

Audit Committee Institute France de KPMG

L'Audit Committee Institute est un forum d'échanges dédié aux membres des comités d'audit. Il a été conçu pour apporter aux membres de comités d'audit des informations, outils et techniques les aidant à remplir la mission liée à leur fonction. L'Audit Committee Institute communique à travers le monde avec les responsables de comités d'audit depuis 1999.

L'Audit Committee Institute France propose à ses membres :

- Un site internet (www.audit-committee-institute.fr) conçu pour donner aux membres de comités d'audit un accès permanent aux meilleures pratiques et à des outils conçus pour améliorer le fonctionnement des comités d'audit
- Des rencontres sous forme de petit déjeuner/table ronde permettant aux membres de comités d'audit d'échanger sur des sujets d'actualité avec leurs pairs
- Des newsletters (Audit Committee News) qui traitent des sujets d'actualité technique et réglementaire et des développements récents sur des problématiques spécifiques aux comités d'audit
- Des publications sur le gouvernement d'entreprise telle que « La pratique des comités d'audit en France et dans le monde ».

Contacts :

Associés KPMG Audit, Responsables de l'Audit Committee Institute France

Didier de Ménonville - Tél : 01 55 68 72 82

Jean-Marc Discours - Tél : 01 55 68 68 83)

KPMG Audit

1, cours Valmy

92923 Paris La Défense Cedex

fr-auditcommittee@kpmg.fr

L'IFA EST LE RÉSEAU DE RÉFÉRENCE DES ADMINISTRATEURS

Présent sur l'ensemble du territoire français avec 7 délégations régionales, l'IFA est également membre actif de la Confédération européenne des associations d'administrateurs (ecoDa).

L'IFA a pour mission :

- de représenter l'ensemble des administrateurs et formaliser des propositions visant à améliorer les conditions dans lesquelles les administrateurs exercent leurs mandats dans les entreprises de tout type : cotées ou non, pme patrimoniales, mutualistes, publiques, associations, fondations,…
- de proposer des séminaires de formation destinés aux membres ou futurs membres de conseil d'administration,
- d'associer, dans une même organisation de place, tous ceux qui souhaitent contribuer à la promotion et au partage des bonnes pratiques du gouvernement d'entreprise en France.

LES MEMBRES FONDATEURS

AFG, BOYDEN FRANCE, CCIP, ERNST&YOUNG, NYSE EURONEXT et PARIS EUROPLACE

& LES MEMBRES ASSOCIÉS

AON GLOBAL RISK CONSULTING, BIGNON LEBRAY, CNCC, CONSEIL SUPERIEUR DE L'ORDRE DES EXPERTS COMPTABLES, DELOITTE, FIDAL, GEMA, GRANT THORNTON, HEWITT ASSOCIATES, KORN/FERRY INTERNATIONAL, KPMG AUDIT, LEADERS TRUST INTERNATIONAL, MAZARS, MICHAEL PAGE INTERNATIONAL, ONDRA-INVESTORSIGHT, PRICEWATERHOUSECOOPERS, RUSSELL REYNOLDS ASSOCIATES, SPENCER STUART.

ILS PARTICIPENT AVEC L'IFA À LA PROMOTION DES MEILLEURES PRATIQUES DE GOUVERNANCE ET À LA PROFESSIONNALISATION DES ADMINISTRATEURS.

IFA - 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

CDECORTIAT-IFA-5112010