

Prise de position de l'IIA

LES TROIS LIGNES DE MAÎTRISE POUR UNE GESTION DES RISQUES ET UN CONTRÔLE EFFICACES

JANVIER 2013



**The Institute of
Internal Auditors**

TABLE DES MATIÈRES

Introduction	1
La surveillance du système de gestion des risques et la définition de la stratégie par les organes de gouvernance	2
La première ligne de maîtrise : les managers	3
La deuxième ligne de maîtrise : les fonctions de gestion des risques et de conformité	4
La troisième ligne de maîtrise : l'audit interne	5
Auditeurs externes, régulateurs et autres organes externes	6
Coordination des trois lignes de maîtrise	6

PRISE DE POSITION DE L'IIA :

LES TROIS LIGNES DE MAÎTRISE POUR UNE GESTION DES RISQUES ET UN CONTRÔLE EFFICACES

INTRODUCTION

Il est assez courant que différentes équipes d'auditeurs internes, d'experts en gestion des risques, en conformité, en contrôle interne, en contrôle qualité et en investigation de fraude, ainsi que d'autres professionnels en matière de risques et de contrôle, coopèrent pour aider leur organisation à gérer ses risques. Chacun de ces spécialistes a un point de vue particulier et possède des compétences spécifiques qui peuvent être une contribution précieuse pour l'organisation concernée. Toutefois, les tâches afférentes à la gestion des risques et au contrôle sont de plus en plus souvent réparties entre plusieurs départements et divisions, et requièrent de ce fait une coordination rigoureuse afin de s'assurer que les processus de gestion des risques et de contrôle fonctionnent comme prévu.

Il ne suffit pas que les différentes fonctions de gestion des risques et de contrôle existent. Encore faut-il leur assigner des rôles précis et assurer une coordination effective et efficiente entre ces groupes de façon à éviter des redondances inutiles et des lacunes dans les contrôles. Leurs responsabilités doivent donc être clairement définies de telle sorte que chaque groupe puisse appréhender son périmètre de responsabilités et son positionnement dans le système global de gestion des risques et de contrôle de l'organisation.

Les enjeux sont de taille. L'absence d'approche cohérente et coordonnée peut conduire à une utilisation inefficace des ressources limitées affectées à la gestion des risques et au contrôle, et à une situation dans laquelle des risques significatifs ne sont pas identifiés ou sont mal gérés. Il peut arriver, dans le pire des cas, que la communication entre les divers groupes chargés de la gestion des risques et du contrôle se limite à un débat permanent sur leurs attributions respectives et leur rôle vis-à-vis d'une tâche donnée.

Ce problème peut se poser dans n'importe quelle organisation, y compris dans celles qui utilisent un référentiel formalisé de gestion des risques. En effet, si ces référentiels permettent une identification efficace des types de risques à maîtriser, ils ne s'attachent guère à préciser les modalités d'attribution et de coordination des tâches nécessaires à leur mise en œuvre.

Heureusement, des bonnes pratiques émergent et peuvent aider les organisations à déléguer et à coordonner les fonctions essentielles de gestion des risques selon une approche systématique. Le modèle des trois lignes de maîtrise fournit un moyen simple et efficace d'améliorer la communication en matière de gestion des risques et de contrôle en clarifiant les rôles et les activités essentiels. Ce modèle permet d'aborder les opérations sous un angle nouveau et contribue à assurer le succès permanent des initiatives relatives à la gestion des risques ; en outre, il convient à tout type d'organisation, quelle qu'en soit la taille ou la complexité. Même dans les organisations qui ne disposent pas d'un référentiel ou d'un système formalisé de gestion des risques, le modèle des trois lignes de maîtrise peut clarifier les enjeux des systèmes de gestion des risques et contribuer à leur efficacité.

UN PRÉ-REQUIS : LA SURVEILLANCE DU SYSTEME DE GESTION DES RISQUES ET LA DÉFINITION DE LA STRATÉGIE PAR LES ORGANES DE GOUVERNANCE

Dans le cadre du modèle des trois lignes de maîtrise :

- la première ligne de maîtrise correspond aux contrôles pilotés par le management,
- la deuxième ligne de maîtrise est celle des différentes fonctions instituées par le management pour assurer le suivi du contrôle des risques et de la conformité,
- la troisième ligne de maîtrise est celle de l'assurance indépendante fournie par l'audit interne.

Chacune de ces trois « lignes » joue un rôle distinct dans le cadre de la gouvernance de l'organisation.

LE MODÈLE DES TROIS LIGNES DE MAÎTRISE

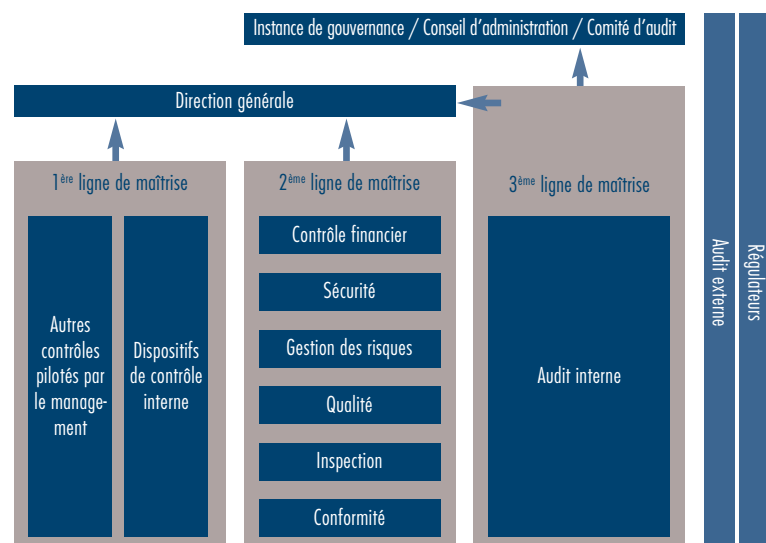


Schéma adapté à partir des lignes directrices ECIIA/FERMA sur la 8^e directive de l'UE relative au droit des sociétés, article 41.

Bien que les organes de gouvernance (Conseil / Comité d'audit et direction générale) se distinguent des trois lignes de maîtrise, toute approche globale des systèmes de gestion des risques implique, au préalable, la prise en compte des responsabilités de ces organes de gouvernance. Ce sont les principales parties prenantes auxquelles chacune des trois lignes de maîtrise apportent un appui. Ces organes de gouvernance sont les mieux placés pour faire en sorte que le modèle des trois lignes de maîtrise soit pris en compte dans les processus de gestion des risques et de contrôle de l'organisation.

Les organes de gouvernance ont collectivement la responsabilité et le devoir de rendre compte de :

- la définition des objectifs de l'organisation,
- la définition des stratégies à adopter pour atteindre ces objectifs et,
- la mise en place de la gouvernance et des processus permettant d'optimiser la gestion des risques associée à la réalisation de ces objectifs.

Le modèle des trois lignes de maîtrise sera d'autant plus efficace que les organes de gouvernance formuleront des directives soutenant activement son déploiement.

LA PREMIÈRE LIGNE DE MAÎTRISE : LES MANAGERS

Le modèle fondé sur les trois lignes de maîtrise établit une distinction entre trois groupes de fonctions impliquées dans la gestion efficace des risques :

- **les fonctions qui endossent et gèrent les risques.**
- **les fonctions qui assurent le suivi des risques.**
- **les fonctions qui fournissent une assurance indépendante.**

En tant que première ligne de maîtrise, les managers endossent et gèrent les risques. Ils ont également la responsabilité de la mise en œuvre des mesures correctives permettant de remédier aux déficiences des processus et des contrôles.

Les managers sont responsables de la mise en place des dispositifs de contrôle interne efficaces et de la mise en œuvre au quotidien des procédures de gestion des risques et de contrôle. Ils identifient, évaluent, contrôlent et maîtrisent les risques, pilotent l'élaboration et la mise en œuvre des règles et procédures internes et s'assurent que les activités sont compatibles avec les objectifs fixés. Dans le cadre d'un système de responsabilité en cascade, le management intermédiaire définit et met en place des procédures de contrôle détaillées et supervisent l'application de ces procédures par leurs collaborateurs.

Les managers constituent la première ligne de maîtrise parce que la conception des contrôles et leur intégration dans les systèmes et les processus s'effectuent sous leur supervision. Des contrôles managériaux et de supervision adéquats devraient être en place pour assurer la conformité ainsi que pour la mise en évidence des contrôles défectueux, des processus inadéquats et des événements inattendus.

LA DEUXIÈME LIGNE DE MAÎTRISE : LES FONCTIONS DE GESTION DES RISQUES ET DE CONFORMITÉ

Dans un monde parfait, une seule ligne de maîtrise serait peut-être suffisante pour assurer une gestion des risques efficace. Toutefois la réalité est souvent toute autre. Le management met en place différentes fonctions de gestion des risques et de conformité chargées de contribuer à la mise au point et/ou à la surveillance des contrôles relevant de la première ligne de maîtrise. Ces fonctions varient selon l'organisation et le secteur d'activité. La deuxième ligne de maîtrise comprend typiquement :

- Une fonction (et/ou un comité) de gestion des risques qui facilite et surveille la mise en œuvre de dispositifs efficaces de gestion des risques par le management et qui assiste les propriétaires des risques dans la définition du niveau cible d'exposition aux risques et la communication d'informations adéquates en matière de risques dans l'ensemble de l'organisation.
- Une fonction de conformité chargée de surveiller divers risques spécifiques tels que le non-respect des lois et réglementations en vigueur. A ce titre, cette fonction distincte est directement rattachée à la direction générale, voire dans certains secteurs d'activités, au Conseil.
- Il arrive souvent que plusieurs fonctions de conformité notamment en matière de santé et de sécurité, de chaîne d'approvisionnement, d'environnement ou de qualité, coexistent dans une même organisation.
- Une fonction de contrôle de gestion qui effectue le suivi des risques financiers et du reporting financier.

Le management instaure ces fonctions pour s'assurer que la première ligne de maîtrise est bien conçue, est effective et fonctionne comme prévu. Chacune de ces fonctions est, dans une certaine mesure, indépendante de la première ligne de maîtrise, mais il s'agit, par nature, de fonctions support du management. À ce titre, elles peuvent intervenir directement dans la modification et la mise au point des systèmes de contrôle interne et de gestion des risques. La deuxième ligne de maîtrise répond par conséquent à un objectif essentiel pour les organes de gouvernance. Cependant, elle n'a pas la capacité de produire des analyses réellement indépendantes concernant les dispositifs de gestion des risques et de contrôle interne.

Les responsabilités de ces fonctions varient, mais peuvent consister à :

- **Soutenir les orientations du management, à définir les rôles et les responsabilités et à fixer des objectifs relatifs à leur mise en œuvre.**
- **Elaborer des référentiels de gestion des risques.**
- **Identifier les enjeux connus et émergents.**
- **Expliciter les évolutions de l'appétence au risque de l'organisation.**
- **Aider le management à mettre au point des processus et des contrôles afin de gérer les risques et les enjeux.**
- **Émettre des lignes directrices et dispenser des formations sur les processus de gestion des risques.**
- **Faciliter et surveiller la mise en œuvre de processus efficaces de gestion des risques par le management.**
- **Alerter le management à propos des enjeux émergents et de l'évolution de la réglementation ou des scénarios de risques.**

- Surveiller l'adéquation et l'efficacité du contrôle interne, notamment en ce qui concerne l'exactitude et l'exhaustivité du reporting, la conformité à la législation et à la réglementation et la remédiation des défaillances en temps opportun.

LA TROISIÈME LIGNE DE MAÎTRISE : L'AUDIT INTERNE

Les auditeurs internes fournissent aux organes de gouvernance une assurance globale fondée sur un plus haut degré d'indépendance organisationnelle et d'objectivité. L'audit interne fournit une assurance sur l'efficacité de la gouvernance, de la gestion des risques et du contrôle interne, y compris sur l'atteinte des objectifs de gestion des risques et de contrôle par les première et deuxième lignes de maîtrise. L'assurance donnée par l'audit interne, qui est communiquée aux organes de gouvernance, couvre généralement les domaines suivants :

- Un large éventail d'objectifs, liés notamment à l'efficience et à l'efficacité des opérations, à la protection des actifs, à la fiabilité et à l'intégrité des processus de reporting et à la conformité aux lois, réglementations, normes, procédures et contrats.
- Toutes les composantes du référentiel de gestion des risques et de contrôle interne, qui incluent l'environnement de contrôle, l'identification des risques, leur évaluation et leur traitement, l'information et la communication, ainsi que le pilotage.
- L'ensemble de l'entité, des divisions, filiales, unités opérationnelles et fonctions — y compris les processus métier tels que les ventes, la production, le marketing, la sécurité, le service client et les opérations —, ainsi que les fonctions support (comme la comptabilité clients et la comptabilité fournisseurs, les ressources humaines, les achats, la paie, le budgeting, la gestion des infrastructures et des actifs, les stocks et les systèmes d'information).

La mise en place d'un audit interne faisant preuve de professionnalisme devrait figurer parmi les règles de gouvernance de toute organisation. Ce point est important non seulement pour les organisations de grande dimension ou de taille moyenne, mais également pour les entités de taille plus modeste, qui peuvent être confrontées à des environnements aussi complexes sans disposer d'une structure organisationnelle aussi formalisée et robuste pour s'assurer de l'efficacité de leurs processus de gouvernance et de gestion des risques.

L'audit interne contribue activement à l'efficacité du dispositif de gouvernance d'une organisation sous réserve que certaines conditions — de nature à favoriser son indépendance et son professionnalisme — soient remplies. Les bonnes pratiques en la matière consistent à mettre en place et à maintenir une fonction d'audit interne indépendante, dotée de ressources et de compétences adéquates et répondant notamment aux critères suivants :

- Appliquer les normes internationales généralement admises pour la pratique de l'audit interne.

La mise en place d'un audit interne faisant preuve de professionnalisme devrait figurer parmi les règles de gouvernance de toute organisation. Ce point est important non seulement pour les organisations de grande dimension ou de taille moyenne, mais également pour les entités de taille plus modeste, qui peuvent être confrontées à des environnements aussi complexes sans disposer d'une structure organisationnelle aussi formalisée et robuste pour s'assurer de l'efficacité de leurs processus de gouvernance et de gestion des risques.

- Être rattaché à un niveau suffisamment élevé dans l'organisation pour pouvoir assurer ses responsabilités de manière indépendante.
- Avoir une relation étroite et effective avec le Conseil ou l'organe de gouvernance équivalent.

AUDITEURS EXTERNES, RÉGULATEURS ET AUTRES ORGANES EXTERNES

Les auditeurs externes, les régulateurs et d'autres organes externes peuvent jouer un rôle important dans le dispositif global de gouvernance et de contrôle d'une organisation. Tel est le cas en particulier dans les secteurs d'activité réglementés, comme les services financiers ou l'assurance. Il arrive parfois que les régulateurs aient des exigences visant à renforcer les contrôles au sein des organisations et procèdent ponctuellement à des revues indépendantes et objectives afin d'évaluer en tout ou partie les première, deuxième ou troisième lignes de maîtrise à l'aune de ces exigences. Sous réserve d'une coordination efficace, les auditeurs externes, les régulateurs et d'autres groupes externes peuvent être considérés comme des lignes de maîtrise supplémentaires, qui fournissent une assurance aux parties prenantes de l'organisation, notamment à ses organes de gouvernance. Toutefois, compte tenu du périmètre et des objectifs spécifiques de leurs missions, les informations relatives aux risques recueillies par ces intervenants sont généralement moins complètes que celles relevant du périmètre d'activité des trois lignes de maîtrise internes à l'organisation.

COORDINATION DES TROIS LIGNES DE MAÎTRISE

Étant donné que chaque organisation est unique et qu'il y a de nombreuses spécificités selon les situations, il n'existe pas une « bonne » méthode en matière de coordination des trois lignes de maîtrise. Toutefois, lors de l'attribution de tâches spécifiques et de la coordination des diverses fonctions impliquées dans le processus de gestion des risques, il peut être utile de tenir compte du rôle fondamental de chacun de ces groupes.

PREMIÈRE LIGNE DE MAÎTRISE	DEUXIÈME LIGNE DE MAÎTRISE	TROISIÈME LIGNE DE MAÎTRISE
Propriétaires des risques / Managers	Gestion des risques et conformité	Assurance globale relative à l'efficacité de la gestion des risques
• Management	• Indépendance limitée • Rend compte principalement au management	• Audit interne • Plus grande indépendance • Rend compte aux organes de gouvernance (direction générale et Conseil)

Chacune des trois lignes devrait exister sous une forme ou sous une autre dans toute organisation, quelle qu'en soit la taille ou la complexité. Le système de gestion des risques est généralement plus performant lorsqu'il existe trois lignes de maîtrise distinctes et clairement définies. Toutefois, dans certains cas exceptionnels, en particulier dans les petites organisations, certaines lignes de maîtrise peuvent être regroupées. Par exemple, il arrive que l'audit interne soit chargé de mettre en place et/ou de diriger les activités de gestion des risques ou de conformité d'une organisation. Dans ce cas, l'audit interne devrait communiquer clairement l'impact de ce regroupement aux organes de gouvernance. Si plusieurs responsabilités sont assignées à une même personne ou un même département, il serait approprié d'envisager de dissocier ultérieurement les responsabilités de façon à mettre en place les trois lignes.

Quelles que soient les modalités de mise en œuvre du modèle des trois lignes de maîtrise les organes de gouvernance (direction générale et Conseil) devraient clairement souligner la nécessité d'un échange d'informations et d'une coordination entre les différents acteurs de la gestion des risques et des contrôles d'une organisation. Les *Normes internationales pour la pratique professionnelle de l'audit interne* requièrent expressément que les responsables de l'audit interne « partagent des informations et coordonnent les activités avec les autres prestataires internes et externes d'assurance et de conseil » afin « d'assurer une couverture adéquate et d'éviter les doubles emplois ».

PRATIQUES RECOMMANDÉES :

- Les processus de gestion des risques et de contrôle devraient être structurés selon le modèle des trois lignes de maîtrise.
- Chaque ligne de maîtrise devrait s'appuyer sur des procédures et des définitions de rôles appropriés.
- Il devrait y avoir une bonne coordination entre les différentes lignes de maîtrise pour favoriser l'efficacité et l'efficience.
- Les fonctions de gestion des risques et de contrôle impliquées dans les différentes lignes devraient procéder à un partage approprié de connaissances et d'informations afin d'aider l'ensemble des fonctions à assurer leurs responsabilités de manière efficace.
- Les lignes de maîtrise ne devraient pas être regroupées ni coordonnées si cela compromet leur efficacité.
- Lorsque des fonctions relevant de différentes lignes sont regroupées, les organes de gouvernance devraient être informés de la structure adoptée et de son impact. Pour les organisations qui n'ont pas mis en place d'activité d'audit interne, leurs organes de gouvernance (direction générale et Conseil) devraient être tenus de préciser comment une assurance adéquate concernant les dispositifs de gouvernance, de gestion des risques et de contrôle sera obtenue et d'en informer leurs parties prenantes.

Chacune des trois lignes devrait exister sous une forme ou sous une autre dans toute organisation, quelle qu'en soit la taille ou la complexité. Le système de gestion des risques est généralement plus performant lorsqu'il existe trois lignes de maîtrise distinctes et clairement définies.

À propos de l'IIA

Créé en 1941, l'Institute of Internal Auditors (IIA) est une association professionnelle internationale dont le siège social est situé à Altamonte Springs, Floride, États-Unis. L'IIA, qui est le représentant mondial de la profession d'audit interne, est une autorité reconnue, ainsi que le principal défenseur et formateur de la profession.

Prises de position

Les prises de position font partie du Cadre de Référence International des Pratiques Professionnelles (CRIPP) de l'audit interne, qui est le référentiel conceptuel regroupant les lignes directrices publiées par l'IIA. En tant qu'organe normalisateur reconnu à l'échelle mondiale, l'IIA publie à l'intention des professionnels de l'audit interne du monde entier des lignes directrices rassemblées dans le CRIPP sous la forme de dispositions obligatoires ou fortement recommandées. Les prises de position relèvent de la catégorie des dispositions fortement recommandées dont le respect n'est pas obligatoire, mais est vivement recommandé. Ces dispositions sont adoptées par l'IIA à l'issue de processus formalisés d'examen et d'approbation.

Les prises de position aident un large éventail de parties prenantes, y compris celles qui ne sont pas des professionnels de

l'audit interne, à comprendre les enjeux importants en matière de gouvernance, de risques ou de contrôle. Elles précisent également le rôle et les responsabilités de l'audit interne.

D'autres lignes directrices émises par l'IIA sont publiées sur notre site à l'adresse suivante: www.globaliia.org/standards-guidance.

Avertissement

L'IIA publie ce document à titre informatif et pédagogique. Ces lignes directrices ne sont pas censées apporter des réponses définitives aux situations spécifiques et sont donc uniquement destinées à servir de guide. L'IIA recommande de consulter systématiquement des experts indépendants sur les points concernant les situations spécifiques. L'IIA décline toute responsabilité dans le cas où quiconque s'appuierait exclusivement sur ces lignes directrices.

Copyright

Copyright © 2013 The Institute of Internal Auditors et l'IFACI pour sa traduction française. Toute demande d'autorisation de reproduction doit être adressée par courrier électronique à l'IIA à l'adresse guidance@theiia.org.



The Institute of Internal Auditors
247 Maitland Avenue
Altamonte Springs, Florida 32701 USA
T +1-407-937-1111
F +1-407-937-1101
Site web : www.globaliia.org



IFACI
98bis, boulevard Haussmann
75008 PARIS, France
T : +33-1.40.08.48.00
F : +33-1.40.08.48.20
Site web : www.ifaci.com