

Management des risques et contrôle interne : L'apport du cadre référentiel COSO¹⁰⁸

Par : Youssef GHANDARI¹⁰⁹

Résumé :

Dans cet article, nous avons pu mettre en articulation le contrôle interne, le management du risque et les apports du référentiel COSO 1 et 2 en la matière. La démarche déductive que nous avons adoptée dans ce papier a montré que le contrôle interne a connu une évolution spectaculaire. Il est passé, dans un espace de quelques années, du stade de la bonne pratique selon des standards non contraignants à celui d'obligation légale pour de nombreuses sociétés à travers le monde. En outre, il est à souligner que le dispositif de Contrôle Interne et de management de risques ne peut fournir une garantie absolue quant à la réalisation des objectifs de l'entreprise. Il existe en effet des limites inhérentes aux dispositifs qui résultent de nombreux facteurs, notamment des incertitudes liées au monde extérieur, et des erreurs d'aspect technique ou humain.

¹⁰⁸ Committee of Sponsoring Organizations of the Treadway Commission.

¹⁰⁹ Enseignant-chercheur à l'ENCG de Settat - Université Hassan 1^{er}

Introduction

Dans le contexte économique actuel, caractérisé par la prédominance de l'économie du marché, la régulation et la gouvernance des entreprises restent les moyens les plus sensibles et nécessitent d'être mieux contrôlées pour éviter les dérives et les abus aboutissant à des scandales, ou à des faillites voire même des crises systémiques des économies en général et des marchés financiers en particulier.

L'histoire récente nous révèle des événements ayant bouleversé le monde de la finance et des affaires en générale : la faillite de Lehman Brothers en 2008 (691 Milliard \$ d'actifs), Washington Mutual en 2008 (327 milliard \$ d'actifs), Enron (64 Milliard \$), Worldcom (103,9 Milliard \$), Consec (61,1 Milliard \$), Aldephia (21,5 Milliard \$). Ces scandales retentissants mettent en cause le fonctionnement de tout un système, celui des sociétés cotées en bourse et de leur autorégulation dans un environnement ultralibéral de création de valeur actionnariale.

Depuis, le contrôle interne et le management des risques sont devenus un thème d'actualité pour lesquels différents pays, en particulier les plus développés, ont adapté leur législation afin de mettre en place des systèmes de surveillance pour détecter plus précocement les risques encourus par les organisations et prévenir les comportements frauduleux des dirigeants.¹¹⁰

L'augmentation des risques dans l'économie et la fréquence des défaillances d'entreprises ont mis en évidence la nécessité de disposer d'outils de pilotage et de contrôle de plus en plus efficaces ; la conduite des affaires impose désormais une véritable culture de contrôle qui permet en effet de renforcer la résistance et la dynamique d'une entreprise ou d'une organisation.

Tous les acteurs de la vie économique sont directement concernés, c'est pourquoi il apparaît fondamental de disposer d'un référentiel de concepts et d'une approche nouvelle de management des risques et du contrôle interne.

Parmi les référentiels reconnus sur le plan international, on citera COSO¹¹¹. Sa perception du contrôle Interne en tant que processus visant à fournir une assurance raisonnable quant à la réalisation des objectifs liés aux opérations, aux informations financières et à la conformité aux lois et réglementations en vigueur, a permis d'apprécier

¹¹⁰ Loi sarbanes Oxley (loi Sox) aux Etats-Unis et la Loi sur la sécurité financière (LSF) en France.

¹¹¹ Rédigé en 1992 par la commission du COSO sous l'appellation « Internal Control-Integrated Framework »

toute l'importance que revêt un dispositif de Contrôle Interne efficace. Cette affirmation s'est renforcée par le fait que pour répondre aux besoins d'informations rapides, l'entreprise doit constamment ajuster ses méthodes de fonctionnement, surtout dans un contexte de mondialisation et d'incertitude où la concurrence est de plus en plus rude.

En se plaçant dans cette optique, la présente recherche qui s'inspire du référentiel COSO 2¹¹², connu également sous : «Enterprise Risk Management (ERM) Integrated Framework », tend à mettre en lumière sa contribution à la pratique émergente de la gestion des risques d'entreprise et répond à la question de son prolongement à la cible « management des risques ».

Ce cadre de référence proposé par le COSO 2, adopte une vision orientée risques de l'entreprise. Il est donc intéressant avant d'explicitier l'apport de ce cadre référentiel d'aborder le concept du management des risques et son rôle incontournable dans la réussite du contrôle interne.

1- Le Management des risques :

1.1- Définition et rôle du management des risques :

Le risque est inhérent à l'entreprise. Il a toujours existé et constitue, d'après les économistes, son essence.¹¹³

Le risque est une notion importante notamment dans les domaines de l'industrie, de l'environnement, du droit, de la santé, de la finance et de l'assurance. Il apparaît clairement que les problèmes financiers qu'ont connus les grandes entreprises aux Etats-Unis notamment, ont secoué le monde des affaires.

L'incertitude est une donnée intrinsèque à la vie de toute organisation. L'un des principaux défis pour la direction est de définir le degré d'incertitude que l'organisation est prête à accepter dans son effort de création de valeur. Le management des risques permet à la direction d'identifier, d'évaluer et de gérer les risques liés à ces incertitudes. Il s'agit donc d'un élément déterminant de la création et de préservation de la valeur.

Le management des risques traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Il se définit comme suit :

¹¹² Publié par la commission COSO en 2014 est connu également sous COSO-ERM

¹¹³ Olivier Hassid, « La gestion du risque » Edition Dunod, P. 5

*« Le management des risques est un processus mis en œuvre par le Conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation, Il est conçu pour identifier les événements potentiels susceptibles affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation ».*¹¹⁴

Le management des risques contribuent à l'amélioration de la performance de l'entreprise en permettant de :

- Créer et préserver la valeur, les actifs et la réputation de la société par l'identification et l'analyse des principales menaces et opportunités potentielles de la société. Il vise ainsi à anticiper les risques au lieu de les subir.

- Sécuriser la prise de décision et les processus de la société pour favoriser l'atteinte des objectifs en permettant d'identifier les principaux événements et situations susceptibles d'affecter de manière significative la réalisation des objectifs de la société. La maîtrise de ces risques permet ainsi de favoriser l'atteinte des dits objectifs.

- Favoriser la cohérence des actions avec les valeurs de la société : De nombreux risques sont le reflet d'un manque de cohérence entre les valeurs de la société et les décisions et actions quotidiennes. Ces risques affectent principalement la crédibilité de la société.

- Mobiliser les collaborateurs de la société autour d'une vision commune des principaux risques et les sensibiliser aux risques inhérents à leur activité.

1-2- Politique générale du management des risques

La politique générale du management des risques doit contenir :

- L'appréciation du contexte et des risques majeurs de l'entreprise ;
- La définition des objectifs fixés par les dirigeants pour contenir les risques correspondant à leurs activités et à leurs projets ;
- Les limites de risques acceptables ;
- Un ensemble d'actions cohérentes sous-tendues par ces objectifs et ces limites.

Elle doit définir globalement, pour chaque activité et chaque niveau de l'entreprise, par

¹¹⁴ Définition donnée par le COSO II. The Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control-Integrated Framework*, 1994,
http://www.coso.org/publications/executive_summary_integrated_framework.htm

grand type de risque :

- Les principes directeurs de la gestion des risques : priorités entre objectifs (humain, économique, réglementaire, technique) et déclinaison du sens de chaque objectif pour l'entreprise ;
- L'organisation et la place dévolue à chaque acteur, tout particulièrement celle de la fonction « Risk manager » : c'est à ce stade que la question cruciale du rattachement de cette fonction est résolue ;
- Les limites globales et spécifiques par type de risques et/ou d'activité (risque maximum tolérable, et risque raisonnablement escomptable) ;
- Les règles d'allocation des fonds propres aux activités, élaborées en cohérence avec le niveau de risque quantifié de chaque activité ;
- Les principales orientations de réduction et de financement du risque et notamment les dispositifs de plan de continuité d'activité et de gestion de crise ;
- Les modalités de suivi de la qualité et l'audit de cette gestion de risques.

Cette politique générale des risques devrait comporter :

- un périmètre (activités couvertes) et une période de référence (un an en général)
- un langage commun (terminologie)
- des personnes identifiées responsables de l'application de la politique
- une démarche solide de mise en œuvre (simple et adaptable)
- un processus de suivi et de contrôle (reporting et audit)¹¹⁵

Le contenu de la politique générale du management des risques exige une vision stratégique et exhaustive de l'entreprise, de ses composantes et de ses relations internes et externes.

Il est pertinent pour les dirigeants d'analyser le profil de risque de l'entreprise et non seulement les types de risques pris indépendamment les uns les autres¹¹⁶ (interactions entre les risques).

Dans la pratique, on observe des scénarios différents de construction de la politique générale de gestion des risques :

- certaines entreprises déroulent leur projet en commençant par un groupe de travail au niveau du comité de direction et généralisent ensuite les échanges vers l'ensemble des responsables de l'entreprise ;

¹¹⁵ Catherine Veret et Richard Mekouar « Fonction : Risk Manager » Edition Dunod p. 63

¹¹⁶ Catherine Veret et Richard Mekouar « Fonction : Risk Manager » Edition Dunod p. 64 et 65

- d'autres choisissent une entité pilote ;
- d'autres enfin, combinent les deux approches.

1-3- Mise en place d'un dispositif du Management des risques

La construction d'un dispositif de Management des risques efficace passe par un diagnostic objectif du niveau d'appétence réel des dirigeants face aux risques.

Ce dispositif comprend 8 éléments qu'on peut résumer ainsi :

- Environnement interne : englobe la culture de l'organisation et particulièrement l'appétence du management pour le risque, l'intégrité et les valeurs éthiques ;
- Fixation des objectifs ;
- Identification des événements internes et externes susceptible d'affecter l'atteinte des objectifs d'une organisation ;
- Evaluation des risques en fonction de leur probabilité d'occurrence et de leur impact ;
- Traitement des risques : le management définit des solutions permettant de faire face aux risques (éviter, accepter, réduire ou partager) ;
- Activités de contrôle : des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques ;
- Information et communication verticalement et transversalement ;
- Pilotage : le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités¹¹⁷.

1-4- Communication de la politique des risques :

Il est important bien sûr que la politique et les objectifs de l'entreprise soient régulièrement communiqués au managers et l'ensemble du personnel.¹¹⁸

En termes de communication externe, la problématique est plus complexe :

- doit-on se limiter à la communication d'une démarche ou doit-on aller jusqu'à révéler ses vulnérabilités ?
- doit-on communiquer intégralement sur les moyens mis en œuvre, leurs coûts et leurs résultats ?
- doit-on donner tous les détails du financement des risques ?

Il n'y a pas une, mais plusieurs communications pour une même politique dépendant

¹¹⁷ COSO II (P. 7 et 8).

¹¹⁸ Catherine Veret et Richard Mekouar « Fonction : Risk Manager » Edition Dunod (p. 71)

avant tout de ceux à qui l'entreprise transmet l'information (les actionnaires ; les analystes ; les cabinets d'audit ; les organismes de rating ; les partenaires ; les journalistes ; le personnel interne).

Tout l'art est de rassurer, de donner des informations sincères, sans dévoiler celles qui pourraient constituer des armes pour les concurrents ou pour des acteurs mal intentionnés.

En fonction de leur stratégie générale, les dirigeants peuvent, ou ne peuvent pas, tout dire à leurs partenaires, clients, fournisseurs. Il leur est alors indispensable de ne pas dire de contre-vérités. En fait, il s'avère qu'il vaut mieux parler le même langage pour ne pas courir le risque d'être mal compris, et surtout de perdre toute crédibilité.

L'erreur serait de croire qu'une communication sur les risques n'est rien d'autre qu'une activité limitée à une bonne relation avec la presse. Elle est beaucoup plus profonde et a fortement évolué en se fondant, en particulier, sur les théories de la perception.

L'entreprise ne doit pas s'attacher seulement à l'analyse du risque objectif tel qu'il est défini par ses experts, mais aussi la perception de ce risque par les individus et les groupes qui constituent son environnement le plus large¹¹⁹.

Le Risk manager doit bien évidemment tenir une veille stratégique et technique, en visitant régulièrement les différents médias, en participant à différents colloques traitant des risques de son secteur et de son entreprise.

1.5- Limites et contraintes du dispositif du management des risques

Les limites de la mise en place d'un dispositif du management des risques peuvent être similaires aux contraintes d'implémentation de tout processus de gestion. Plus particulièrement, ces limites sont, dans le cas du risque, communes à toute fonction support. S'ajoute à ces limites organisationnelles, une contrainte d'ordre opérationnelle : celle de la mesure du risque.

a - Limites inhérentes à tout processus de gestion :

Un dispositif efficace de management des risques, qu'il soit ou non conçu et mis en œuvre de manière appropriée, ne donne au management et au Conseil d'administration qu'une assurance raisonnable quant à l'atteinte des objectifs fixés pour l'organisation.

En effet, l'atteinte des objectifs peut être affectée par les limites inhérentes à tout processus de gestion. Par exemple, le jugement humain peut pousser à prendre de mauvaises

¹¹⁹ Catherine Veret et Richard Mekouar « Fonction : Risk Manager » Edition Dunod (p.71)

décisions, des dysfonctionnements peuvent subvenir du fait de simples erreurs humaines. En outre, les contrôles peuvent être contournés en raison d'une entente entre plusieurs personnes, et le management a parfois la possibilité d'outrepasser les règles définies dans le dispositif de management des risques, y compris les décisions relatives au traitement des risques et aux activités de contrôle. Enfin, la nécessité de tenir compte du rapport coûts-bénéfices relatifs aux traitements envisagés pour chaque risque constitue également une limite.

b-Limites communes à toute fonction «support» :

Le Risk manager ne peut pas agir opérationnellement. Il ne peut que catalyser, accompagner globalement les transformations utiles pour une meilleure maîtrise des risques. En outre, il n'est pas propriétaire du processus de management des risques : Il en est juste le dépositaire privilégié. La vie de l'entreprise l'amène à intervenir sur des enjeux extrêmement variés (juridiques, financiers, techniques, humains, sanitaires, sécuritaires, environnementaux, sociopolitiques) : il n'est donc pas en mesure de prendre en charge à lui seul la diversité des enjeux.

c-Limites de la mesure :

Les instruments de mesure du risque sont multiples : contrôle, visites, observation, entretiens, sondages, enquêtes, analyse historique, retour d'expérience, audit et expertise.

Les limites de ces mesures, selon Olivier Hassid¹²⁰ seraient de 3 types :

Le premier problème est de type cognitif. Par cognitif, il faut entendre tout ce qui a trait au raisonnement et notamment ce qui a une incidence sur le traitement de l'information. Or, pour mesurer le risque, il faut du temps. En effet, il peut exister des délais importants entre le temps de traitement et d'exécution d'une solution. Une fois mesurée l'ampleur du risque, cette mesure peut déjà avoir perdu de sa pertinence. Cette observation est d'autant plus vraie que le concours d'experts peut avoir des effets négatifs dans le contexte de la décision.

En effet, ce concours peut conduire à des précautions excessives, qui se manifestent par des retards et par des conclusions qui préservent la valeur scientifique des travaux en restant ambiguës. A cela s'ajoute l'idée que les problèmes sont généralement pensés en fonction de cadres d'hypothèses stables, sans grand facteur de surprise. Personne, hormis des cinéastes et des écrivains, n'aurait en effet imaginé avant le 11 septembre 2001, qu'un avion de ligne puisse être utilisé comme une bombe contre des immeubles de grande hauteur.

Le deuxième problème est de nature éthique. Il existe des situations où les risques

¹²⁰ Olivier Hassid : La gestion des risques (P. 60/61) -Edition DUNOD

dépassent le somme des consentements individuels. De même dans la question de la traçabilité, il y a une idée de contrôle, de panoptique¹²¹ qui inquiète.

Le troisième problème est de nature organisationnelle. L'estimation du risque bute souvent sur le caractère réfractaire de nombreux salariés vis-à-vis d'une collaboration. En ce sens, il faut souligner par rapport à la question du retour d'expériences que si cette démarche est essentielle en matière de prévention des risques, elle est difficile car elle met en évidence des dysfonctionnements. En effet, le retour d'expériences peut faire apparaître qui a failli dans l'organisation.

Autrement dit le retour d'expérience est aussi un bon outil de contrôle, Dans ces conditions, les salariés ont plus tendance à cultiver le secret par méfiance qu'à collaborer, se mettant ainsi moins en danger par rapport à la direction.¹²²

2- Intégration du contrôle interne

Le contrôle interne fait partie intégrante du dispositif de management des risques. Ce cadre de référence intègre le contrôle interne, constituant ainsi une modélisation et un outil de management plus «solide».

Le contrôle interne est défini et décrit dans l'ouvrage intitulé Internal Control – Integrated Framework¹²³. Ce référentiel a fait ses preuves et constitue le fondement de règles, réglementations ou lois actuellement en vigueur et reste applicable comme référentiel de contrôle interne.

2-1- Le contrôle interne selon le référentiel COSO :

Le référentiel COSO (The Committee of Sponsoring Organizations of the Treadway Commission) est le cadre architectural du contrôle interne le plus fréquemment employé à l'échelle mondiale.

Le référentiel initial connu par COSO 1 a évolué depuis 2002 vers un second corpus dénommé COSO 2 (*cf* 3-).

¹²¹ Le panoptique est un type d'architecture carcérale imaginée par le philosophe utilitariste Jeremy Bentham à la fin du XVIII^e siècle. L'objectif de la structure panoptique est de permettre à un individu, logé dans une tour centrale, d'observer tous les prisonniers, enfermés dans des cellules individuelles autour de la tour, sans que ceux-ci ne puissent savoir s'ils sont observés. Ce dispositif devait ainsi créer un « sentiment d'omniscience invisible » chez les détenus.

¹²² Olivier Hassid : La gestion des risques (P. 60-61) -Edition DUNOD.

¹²³ Ouvrage traduit en français, par Pricewaterhouse Coopers et l'IFACI sous le titre «La pratique du contrôle interne, COSO report». Copyright en français IFACI.

a- Origine et buts du COSO :

Revenons au point de départ. En octobre 1985, une commission nationale, la Commission Treadway, est mise en place aux Etats-Unis sur le thème de la « fraude dans le reporting financier » Son rapport est publié en septembre 1987. Il constitue une base de recommandations pour prévenir et détecter ce type de fraude.

Le COSO regroupe aux USA les associations et instituts dans les domaines de la Comptabilité et de l'Audit Interne qui ont sponsorisés les travaux de cette Commission et qui sur la base de ses recommandations ont rédigé en 1992 le rapport COSO, intitulé « Internal Control-Integrated Framework ».

Le rapport vise à concrétiser la notion de contrôle interne dans l'idée :

- d'établir une définition commune servant les besoins des différentes parties.
- de fournir un standard avec lequel les entreprises peuvent apprécier leur système de contrôle interne et déterminer comment l'améliorer.

Il ne se limite donc pas à donner une simple définition de ce qu'est le contrôle interne, mais montre également comment un système de contrôle interne peut être aménagé, entretenu et évalué.

Le rapport COSO ne s'applique pas de manière contraignante. Il peut être librement utilisé par toute entreprise qui désire s'inspirer de ses recommandations. Il n'est donc pas limité aux seules sociétés américaines.

b- Définition du contrôle interne

COSO définit le contrôle interne comme un processus mis en œuvre par les dirigeants et le personnel d'une organisation destinée à assurer dans des limites raisonnables la réalisation des objectifs suivants:

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité par rapport aux lois et aux règlements en vigueur.

Cette définition du contrôle interne est large. Elle ne se limite pas à la préparation d'états financiers fiables mais inclut, également, la poursuite des objectifs commerciaux de base de l'entreprise et le respect des lois et réglementations auxquelles elle est assujettie. Ce qui devrait lui permettre d'améliorer sa rentabilité, de sauvegarder ses ressources et d'éviter tout dommage à sa réputation ou autre conséquence négative.

2-2- Le cadre COSO

Le cadre COSO repose sur les notions d'objectifs et de composants.

a- Les objectifs :

Le système de contrôle interne conçu selon le modèle COSO concourt à la réalisation des trois objectifs suivants :

- la réalisation et l'optimisation des opérations,
- la fiabilité des informations financières,
- et la conformité aux lois et règlements

On notera que ces objectifs correspondent en grande partie aux préoccupations des investisseurs.

b- Composantes du contrôle interne¹²⁴

Le concept de contrôle interne selon COSO repose sur cinq éléments principaux qui sont étroitement liés :

- L'environnement de contrôle (control environment) : il constitue la base des autres composantes du contrôle interne. L'environnement peut être défini comme étant l'attitude de la direction et du personnel face au contrôle interne.

Il comprend notamment l'intégrité, les valeurs éthiques et les compétences techniques au sein de l'entreprise mais aussi, plus globalement, la philosophie de la direction, son style de management et la culture d'entreprise qu'elle façonne. Cet élément est fondamental car il donne le ton de l'organisation et influence la conscience de contrôle des employés. Un environnement de contrôle défaillant peut en effet encourager des actes illicites de la part de collaborateurs.

Il peut être positivement influencé par des outils clarifiant les structures et procédures au sein de l'entreprise : organigramme, description des tâches, procédures écrites, audit interne.

- L'évaluation des risques (risk assesment) : L'entreprise doit être consciente des risques et les maîtriser. Elle doit instaurer des mécanismes permettant d'identifier et d'analyser les risques majeurs auxquels l'entreprise est exposée dans la réalisation de ses objectifs.

- Les activités de contrôle (control activities) : elles permettent de s'assurer que les mesures prises contre les risques identifiés et pour la réalisation des objectifs sont correctement appliquées. Souvent désignées comme système de contrôle interne, elles permettent plus

¹²⁴ COSO, The Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control-Integrated Framework*, 1994, [://www.coso.org/publications/executive_summary_integrated_framework.htm](http://www.coso.org/publications/executive_summary_integrated_framework.htm), , P 4 & 5

spécifiquement d'examiner si des mécanismes de contrôle adéquats ont été mis en place (« reliance tests ») et s'ils sont effectivement pris en compte (« compliance tests »). Au niveau des activités/transactions, cela se traduit par le fait de contrôler que chaque opération est autorisée/validée et enregistrée de manière exacte et exhaustive.

- **L'information et la communication** (information and communication) : les méthodes d'information et de communication permettent d'assurer que l'ensemble des collaborateurs au sein de l'entreprise dispose des informations nécessaires à la réalisation de leur tâche. Elles doivent aussi faire comprendre à chaque collaborateur son rôle dans l'ensemble du processus de contrôle interne et comment il interagit avec les autres. La communication doit enfin être assurée aussi bien à l'intérieur de l'entreprise que vers l'extérieur.

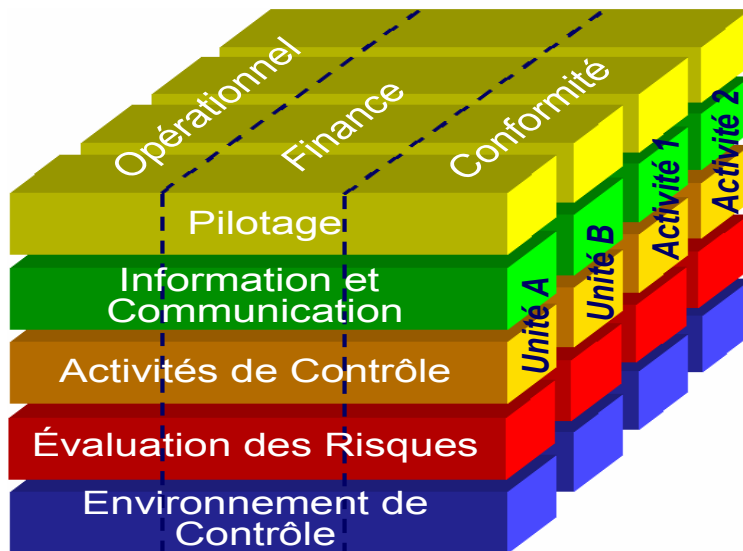
- **Le pilotage ou surveillance** (monitoring) : L'ensemble du processus doit faire l'objet d'un suivi et des modifications doivent y être apportées le cas échéant. Ainsi, le système peut réagir rapidement en fonction du contexte. L'audit interne joue ici un rôle important en tant qu'organe de surveillance.

c-Le cube COSO¹²⁵

Selon COSO, Il existe un lien direct entre les objectifs généraux, qui représentent ce qu'une organisation s'efforce de réaliser, et les composantes du contrôle interne, qui représentent les instruments nécessaires à leur réalisation. Ce lien peut être représenté schématiquement par une matrice à trois dimensions, de la forme d'un cube. Ainsi le référentiel COSO a donné naissance à un Cube dont les 3 faces visibles représentent les 3 objectifs, les 5 composants et les processus de l'entreprise. Ce Cube se découpe en 3 x 5 x p cubes élémentaires (p=nombre de processus de l'entreprise) qui donnent la base des évaluations à réaliser : Ci-après une représentation graphique de ce modèle conceptuel.¹²⁶

¹²⁵ COSO, The Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control-Integrated Framework*, 1994, [://www.coso.org/publications/executive_summary_integrated_framework.htm](http://www.coso.org/publications/executive_summary_integrated_framework.htm), P 17.

¹²⁶ Deloitte, « Mettre en œuvre le contrôle interne dans un contexte réglementaire mouvant : Où en sont les entreprises » par Eric Dugelay, 13 décembre 2007



2-3- Limites du contrôle interne :

Le contrôle interne est un élément fondamental au sein de l'entreprise. Il ne doit cependant pas être considéré comme une solution à tous les problèmes. Il serait erroné de croire qu'il peut assurer le succès de l'entreprise. En effet, un contrôle interne efficace ne peut qu'aider une entité à atteindre ses objectifs. Il peut permettre à la direction de mieux gérer l'entreprise, mais en aucun cas changer une direction mauvaise en une bonne direction.

Le contrôle interne ne peut pas garantir la fiabilité des états financiers et le respect des lois. Cette attente est également trop élevée, puisqu'il ne peut fournir qu'une assurance raisonnable (« reasonable assurance »), donc pas absolue, quant à la réalisation des objectifs de l'entreprise. En particulier, les contrôles peuvent être détournés par la collusion de deux ou plusieurs personnes et la direction a la possibilité de court-circuiter le système (« Management Overriding »)¹²⁷.

3-Articulation entre le management des risques et le contrôle interne : COSO 2

Les dispositifs du management des risques et de contrôle interne participent de manière complémentaire à la maîtrise des activités de la société :

- Le dispositif de management des risques vise à identifier et analyser les principaux risques de la société. Les risques, dépassant les limites acceptables fixées par la société, sont traités et le cas échéant, font l'objet de plans d'action. Ces derniers peuvent prévoir la mise en place de contrôles, un transfert des conséquences financières (mécanisme d'assurance ou

¹²⁷COSO, The Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control-Integrated Framework*, 1994, [://www.coso.org/publications/executive_summary_integrated_framework](http://www.coso.org/publications/executive_summary_integrated_framework)., P 6

équivalent) ou une adaptation de l'organisation. Les contrôles à mettre en place relèvent du dispositif de contrôle interne. Ainsi, ce dernier concourt au traitement des risques auxquels sont exposées les activités de la société ;

- De son côté, le dispositif de contrôle interne s'appuie sur le dispositif de management des risques pour identifier les principaux risques à maîtriser.

Le management des risques doit lui-même intégrer des contrôles, relevant du dispositif de contrôle interne, destinés à sécuriser son bon fonctionnement.

L'articulation et l'équilibre conjugué des deux dispositifs sont conditionnés par l'environnement de contrôle, qui constitue leur fondement commun, notamment: la culture du risque et du contrôle propres à la société, le style de management, les valeurs éthiques de la société.

La présente section vise à en réaliser une synthèse, notamment en se basant sur les concepts développés précédemment dans le COSO 1, "Internal Control – Integrated Framework".

3-1- Positionnement du COSO 2 par rapport au COSO 1

Le COSO 2 ou COSO-ERM (ERM= Enterprise Risk Management), publié par la commission COSO en 2004 est aujourd'hui le cadre de référence du management des risques. C'est un modèle global structuré, construit sur le socle du premier rapport COSO, vu sous l'angle de la gestion des risques.

Pour rappel, le COSO 1 propose un cadre de référence du contrôle interne. Il définit le contrôle interne comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- La réalisation et l'optimisation des opérations,
- La fiabilité des informations financières,
- La conformité aux lois et aux réglementations en vigueur.

Le COSO 2 propose un cadre de référence pour le management des risques de l'entreprise. Il définit ainsi la gestion des risques de l'entreprise¹²⁸ comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, exploité pour l'élaboration de la stratégie et transversal à l'entreprise, destiné à :

- Identifier les événements potentiels pouvant affecter l'organisation,

¹²⁸COSO II Report : Enterprise Risk Management Framework

- Maîtriser les risques afin qu'ils soient dans les limites du « *RiskAppetite* » de l'organisation (**appétence au risque**= le niveau de prise de risque accepté par l'organisation dans le but d'accroître sa valeur)»,
- Fournir une assurance raisonnable quant à la réalisation des objectifs de l'organisation.

Il apparaît que le COSO 2 inclut les éléments du COSO 1 et le complète par le concept de Management des risques. Le COSO 2 élargit le concept du contrôle interne au management des risques d'entreprise en assignant au contrôle interne « *un quatrième objectifs de maîtrise de risques liés à la stratégie de l'entreprise* ».

Autrement dit le référentiel COSO 2 (Management des risques d'entreprise) s'approprie les trois objectifs du contrôle interne du COSO 1 et les complète par un quatrième objectif de stratégie tout en ne limitant plus l'objectif de fiabilité des informations aux seules informations financières mais l'étend aussi aux informations tant internes qu'externes, financiers ou non financières.

3-2- Synthèse des modifications opérées sur le cube COSO

Le modèle du cube et son architecture à trois plans sont conservés :

- Processus (niveaux de l'organisation)
- Composants de contrôle interne (qui devient Eléments de gestion des risques)
- Objectifs de l'organisation

En revanche, les différents plans sont modifiés ou enrichis.

a. Axe "Niveaux de l'organisation" :

Apport d'un cadre plus strict de décomposition de la structure d'une organisation

Mise en évidence de la nécessité de prendre en compte l'ensemble de l'organisation pour que le COSO 2 soit appliqué avec succès.

Le COSO 2 s'applique à l'ensemble de l'entreprise, aussi bien au niveau le plus haut (« entité ») qu'au niveau opérationnel (« business unit »). Mais pour appliquer le COSO 2 avec succès, il faut prendre en compte l'ensemble du périmètre des activités d'une organisation. Le COSO 2 considère les activités à différents niveaux de l'organisation :

- Au niveau de l'organisation (« entity ») pour des activités telles que la planification stratégique ou l'allocation des ressources,
- Au niveau des unités de métier (« business unit ») pour des activités telles que le marketing, et les ressources humaines,

- Au niveau des processus métier (« business process ») pour des activités telles que la production, les achats,
Et aussi aux niveaux des projets ou initiatives qui n'ont pas encore de place définie dans la structure de l'organisation.

Par rapport au COSO 1, le COSO 2 apporte :

- un cadre plus strict de décomposition de la structure d'une organisation - par niveaux - que le COSO 1 (qui ne retient pas de structure de décomposition spécifique pour une organisation).
- la nécessité de prendre en compte l'ensemble de l'organisation pour être appliqué avec succès.

b. Axe "Objectifs" :

- Apport d'un nouvel objectif : « stratégique ».

Un objectif stratégique est un objectif « high-level », qui soutient et concourt à la mission/vision de l'organisation. Les objectifs stratégiques reflètent les choix du management quant à la recherche de création de valeur par l'organisation pour ses actionnaires.

Les trois autres types d'objectifs : opérationnel, reporting, et réglementaire, sont dépendants des objectifs stratégiques. Ils sont appelés les « related » objectifs. Par exemple, pour une organisation, il s'agira de définir :

Quelle est sa mission/vision,

Quels sont les objectifs stratégiques soutenant cette mission/vision,

Quelle est la stratégie à mettre en œuvre pour atteindre ces objectifs stratégiques,

Et en déduire les « related » objectifs qui soutiennent la stratégie mise en œuvre.

A la différence du COSO 1, la mise en œuvre de COSO 2 nécessite donc d'avoir une vision des objectifs stratégiques de l'entreprise en plus des « related » objectifs.

- Elargissement de la notion de reporting

Par rapport au COSO 1, cette notion couvre désormais :
non seulement le reporting financier, mais aussi la remontée d'informations non-financières,
non seulement la remontée d'informations externes mais aussi la remontée d'informations internes.

c. Axe "Composants de contrôle"

Enrichissement de l'axe « Composants de contrôle » qui devient « éléments de gestion des risques » et qui passe de cinq à huit catégories :

L'élément environnement interne est complété de la notion de « RiskAppetite »,

L'élément évaluation des risques est éclaté en quatre éléments dont les notions existaient déjà dans le COSO 1 mais sous forme moins détaillée : définition d'objectifs, Identification des événements, Evaluation des risques, Réponse aux risques, L'élément activités de contrôle reste inchangé,

L'élément « Information et Communication » est complété des notions de temps et de granularité de l'information,

L'élément pilotage reste inchangé.

Suite à ces modifications, la lecture de ce nouveau plan met en évidence un bloc homogène que l'on peut qualifier «de bloc d'éléments de risques » et qui contient les cinq éléments : définition d'objectifs, identification des événements, évaluation des risques, réponse au risque et activités de contrôle.

Ci-après une représentation graphique du modèle COSO 2 :



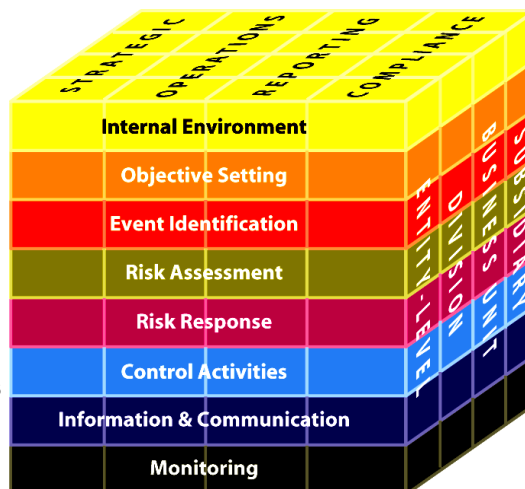
Management des risques de l'entreprise – COSO II

Objectifs

- Objectifs stratégiques
- Objectifs opérationnels
- Objectifs de reporting
- Objectifs de conformité

Éléments du dispositif

- Environnement interne
- Fixation des objectifs
- Identification des événements
- Evaluation des risques
- Traitement des risques
- Activités de contrôle
- Information et communication
- Pilotage



Conclusion :

A travers cet article, nous avons essayé de toucher de près les concepts du contrôle interne et management des risques et les apports du référentiel COSO 1 et 2 en la matière. Nous avons constaté que la notion de contrôle interne, très importante en pratique, a connu une évolution fulgurante. Elle est passée, en quelques années, du stade de la bonne pratique

selon des standards non contraignants à celui d'obligation légale pour toute une série de sociétés à travers le monde¹²⁹

Cependant, l'application ou le respect de ces obligations de la part des responsables d'entreprises reste encore insuffisant. Cela est dû à la fois au manque de contrôle de la part des Institutions de l'Etat sur la mise en œuvre de ces lois, mais aussi au peu d'importance que donnent certains responsables d'entreprises au contrôle Interne et le management des risques.

Le choix du modèle COSO comme cadre de référence à utiliser par les entreprises et organisations et qui vise à fournir une assurance raisonnable quant à la réalisation des objectifs liés aux opérations, aux informations financières et à la conformité aux lois et réglementations en vigueur, ainsi que le fait que le cadre COSO intègre cinq composantes (environnement de contrôle, évaluation des risques, activité de contrôle, information et communication, activités de pilotage), ont permis d'apprécier toute l'importance que revêt un dispositif de Contrôle Interne efficace. Cette affirmation s'est renforcée par le fait que pour répondre aux besoins d'informations rapides, l'entreprise doit constamment ajuster ses méthodes de fonctionnement, surtout dans un contexte de mondialisation et d'incertitude où la concurrence est de plus en plus rude.

Une entreprise est contrainte de cohabiter avec les risques. Et parce qu'ils sont de plus en plus immatériels, pouvoir les anticiper, les hiérarchiser pour en mesurer le pouvoir de nuisance s'avère vital. Sous la pression des nouvelles directives, législations et normes, le management des risques, qui a considérablement évolué ces vingt dernières années, tend dès lors à se professionnaliser. Parce qu'elle a un impact direct sur la performance de l'entreprise, elle requiert une approche globale et transversale. Reste maintenant à optimiser l'utilisation des outils de pilotage stratégique et les intégrer à la politique de l'entreprise.

Pour conclure, il est essentiel de souligner qu'un dispositif de Contrôle Interne et de management de risques aussi bien conçu et aussi bien appliqué soit-il, ne peut fournir une garantie absolue quant à la réalisation des objectifs de l'entreprise. Il existe en effet des limites inhérentes à tout système ou dispositif. Ces limites résultent de nombreux facteurs, notamment des incertitudes liées au monde extérieur, de l'exercice de la faculté de jugement

¹²⁹ Aux Etats-Unis d'Amérique par la Loi Sarbanes Oxley (loi sox) et en France par la Loi de Sécurité Financière (LSF).

ou de dysfonctionnements pouvant survenir en raison d'une défaillance humaine ou technique ou d'une simple erreur.

Bibliographie :

BARTHELEMY(Bernard), **COURREGES** (Philippe) « Gestion des risques : Méthode d'optimisation globale » 2^{ème} édition, Editions d'Organisation 2004

BERNARD (Frédéric), **GAYRAUD** (Rémi), **ROUSSEAU** (Laurent) « Contrôle interne » Edition 4, Maxima 2013

COLLIER (Paul M.) « Fundamentals of Risk Management for Accountants and Managers : Tools and Techniques », éditeur: Taylor & Francis 2009

CORDEL (Frédéric), **LEBEGUE** (Daniel) « Gestion des risques et contrôle interne : De la conformité à l'analyse décisionnelle », Vuibert 2013

CLEARY(Seán), **MALLERET** (Thierry) « Risques : Perception, évaluation, gestion » Maxima 2006

DARSA (Jean-David) « La gestion des risques en entreprise » Editeur: Gereso 2013

DELEUZE (Gilles), **IPPERTI** (Patrick) « L'analyse des risques : Concepts, outils, gestion, maîtrise », EMS Editions 2013

HASSID (Olivier) « La gestion des risques » 2^{ème} édition Dunod 2008

HASSID (Olivier), **MASRAFF** (Alexandre) « La sécurité en entreprise : Prévenir et gérer les risques », Maxima 2010

HASSID (Olivier) « Le management des risques et des crises » 3^{ème} édition Dunod 2011

HOPKIN (Paul) « Risk Management » Editeur : Kogan 2013

HULL (John), **MERLI** (Maxime), **GODLEWSKI** (Christophe) « Gestion des risques et institutions financières » Editeur : Pearson Education 2013

IFACI « Le management des risques de l'entreprise, Cadre de référence, techniques d'application » Editions d'organisation 2005

MASSELIN (Jean-Luc), **MADERS** (Henri-Pierre) « Contrôle interne des risques - Cibler - Evaluer - Organiser - Piloter – Maîtriser » Eyrolles 2014

KEREBEL Pascal, « Management des risques », Editions d'Organisation 2009

LE RAY (Jean) « Gérer les risques : Pourquoi ? Comment ? » Editeur : AFNOR 2010

PRICEWATERHOUSE COOPERS, IFACI, LANDWELL & ASSOCIES « Le management des risques de l'entreprise (Rapport COSO II) » Editions d'Organisation 2006.

RENARD (Jacques), « Théorie et pratique de l'Audit Interne », 8^{ème} édition, Eyrolles 2013

RENARD (Jacques), « Comprendre et mettre en œuvre le contrôle interne », Eyrolles 2013

VÉRET (Catherine), **MEKOUAR** (Richard) « *Fonction : Risk Manager* » Dunod 2005

FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS « *Cadre de référence de la gestion des risques* », 2003

AUTORITE DES MARCHES FINANCIERS (AMF) « *Les dispositifs de gestion des risques et de contrôle interne : Cadre de référence / AMF* », juillet 2010

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO) « *Internal Control-Integrated Framework* », 1994.