CONTRÔLE INTERNE

Le cadre de management des risques de l'entreprise (COSO 2)

Présenté par Abderraouf YAICH

Le cadre de gestion des risques du COSO 2 Report (2004) s'appuie sur le cadre de contrôle interne (COSO 1, 1992), corrige et complète le concept de contrôle interne en élargissant la réflexion sur un thème plus global de gestion des risques. Ainsi, en englobant le contrôle interne, *the enterprise Risk Management - Integreted Framework* vise à répondre aux besoins des entreprises et organisations en contrôle interne tout en leur permettant d'évoluer vers un processus de management des risques plus développé.

Le postulat de base dans le concept de management des risques est la détermination du degré d'incertitude acceptable afin d'optimiser la création de valeur. En effet, l'incertitude est une donnée intrinsèque à la vie de toute entreprise. Elle est source de risques et d'opportunités susceptibles de créer ou de détruire de la valeur.

Le COSO 2 définit le risque comme étant **la possibilité qu'un événement survienne et nuise à l'atteinte d'objectifs alors qu'une opportunité est la possibilité qu'un événement survienne et contribue à l'atteinte d'objectifs**.

Les présidents de PWC et de l'IFACI précisent en préface à l'édition française du COSO 2 (page VIII) que «la prise en compte des opportunités et menaces doit irriguer l'organisation, de la fixation de sa stratégie jusqu'à la conduite quotidienne des opérations. La politique de management des risques doit être largement partagée pour éviter toute surexposition non souhaitée, et les dispositifs en place doivent faciliter un pilotage global des risques qui embrasse les complexités métiers, géographiques et juridiques de l'entité. Ici, comme ailleurs, les maître-mots sont **anticipation**, **réactivité** et **flexibilité**».

Section 1. Les concepts de management des risques

Le dispositif de management des risques s'intègre dans le processus de management global et intègre le contrôle interne. Le cadre COSO de management des risques définit les concepts d'incertitude de création de valeur, d'événements, de risques et d'opportunité pour introduire une définition du management des risques.

§ 1. Dispositif de management des risques et processus de management global

Le dispositif de management des risques est intégré au processus de management global de l'organisation mais toutes les actions accomplies par le management ne constituent pas un élément du dispositif de gestion des risques. Ainsi, les notions de jugement et d'appréciation servant à la prise de décision, qui sont une partie intégrante du processus de management global, ne relèvent pas du dispositif de management des risques.

Le COSO 2 précise : «qu'en règle générale, le dispositif de management des risques intègre des éléments du processus du management global qui permettent à la direction de prendre des décisions avisées. Toutefois, le fait que des bons choix ont été faits ne permet pas de conclure que le dispositif est efficace.

Par ailleurs, si les objectifs spécifiques, les modes de traitement des risques et les activités de contrôle sélectionnées relèvent de l'appréciation et du jugement de la direction, les choix doivent se traduire par

une diminution des risques à un niveau acceptable, correspondant à l'appétence de l'organisation pour le risque, et doivent donner une assurance raisonnable que les objectifs de celle-ci seront atteints».

§ 2. Objectifs du management des risques

Toute organisation détermine ses objectifs stratégiques dans le cadre de sa mission et de sa vision, conçoit une stratégie et décline les objectifs qui en découlent à tous les niveaux pertinents de l'entité. Le cadre de management des risques a pour objectif d'aider l'organisation à atteindre ses objectifs qu'il regroupe en 4 grandes catégories, à savoir :

- Les objectifs stratégiques ;
- Les objectifs opérationnels ;
- Les objectifs de reporting ;
- Les objectifs de conformité.

Tout en étant distincts, ces objectifs se recoupent, un objectif donné peut relever de plusieurs catégories.

Le COSO 2 admet «qu'une autre catégorie, la protection des actifs, est également utilisée par certaines organisations. Il s'agit de prévenir les pertes des actifs ou des ressources d'une entité du fait :

- de vols,
- d'improductivité,
- d'inefficience ;

ou de ce qui s'avère être simplement une mauvaise décision, comme :

- de vendre un produit à un prix trop bas,
- de ne pas être capable de conserver des collaborateurs clés,
- d'éviter la contrefaçon d'un brevet,
- ou de supporter des charges imprévues.

Ces objectifs sont essentiellement opérationnels, bien que certains aspects de la protection puissent être rattachés à d'autres catégories».

La catégorie d'objectifs relatifs au reporting financier est très large puisqu'elle englobe tous les rapports produits par une organisation, diffusés en interne comme en externe. Entrent ainsi dans cette catégorie d'objectifs :

- les rapports utilisés par le management,
- les rapports destinés à des tiers,
- les documents établis à des fins réglementaires ou pour d'autres parties prenantes.

De même, le périmètre de ces rapports dépasse le cadre des états financiers pour couvrir à la fois les données financières et les données non financières.

Le COSO 2 précise que si l'on peut attendre du dispositif de management des risques qu'il donne une assurance raisonnable que les objectifs sont atteints en ce qui concerne la fiabilité du reporting et de la conformité aux lois et réglementations, puisque l'atteinte de ce type d'objectifs fait partie du champ de contrôle de l'organisation et est intrinsèquement liée à la façon dont les activités sont gérées, l'atteinte des objectifs stratégiques peut, en revanche, échapper au contrôle de l'organisation.

Le COSO 2 souligne «qu'un dispositif de management des risques ne saurait prévenir des jugements erronés ou des mauvaises décisions, ni un événement extérieur imprévisible faisant échouer un projet. Il doit cependant renforcer la possibilité, pour la direction, de prendre de meilleures décisions. Par conséquent, pour les catégories d'objectifs stratégiques et opérationnelles, le dispositif de management des risques peut fournir une assurance raisonnable que la direction et le conseil d'administration, dans son rôle de contrôle et de supervision, sont informés régulièrement de la progression de l'organisation dans l'atteinte de ses objectifs».

§ 3. Incertitude, valeur, événements, risques et opportunités

La raison d'être de toute organisation est la création de valeur pour les parties prenantes.

Ceci constitue le postulat de base du management des risques de l'entreprise.

Le COSO 2 précise que «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'entité est prête à accepter dans son effort de création de valeur.

La notion d'incertitude se traduit aussi bien en termes de risques que d'opportunités, pouvant potentiellement détruire comme créer de la valeur».

La valeur est créée, préservée ou détruite par des décisions, tant au niveau de la stratégie que dans la

gestion quotidienne des activités. Il y a création de valeur quand les avantages procurés sont supérieurs à l'ensemble des coûts des ressources utilisées.

L'identification des risques et des opportunités est inhérente à toute prise de décision rationnelle. Elle implique la prise en compte des informations disponibles sur l'environnement interne et externe et entraîne le déploiement des ressources en fonction des besoins, de même qu'elle requiert un ajustement des activités à mesure que les circonstances évoluent.

Pour le COSO 2, la survenance d'un événement d'origine interne ou externe peut avoir des répercussions sur l'atteinte des objectifs. Les événements peuvent avoir un impact négatif, positif ou les deux simultanément.

Les événements ayant un potentiel d'impact négatif constituent des risques. **Un risque représente la possibilité qu'un événement survienne et nuise à l'atteinte d'objectifs.**

Les événements ayant un potentiel d'impact positif peuvent :

- compenser les impacts négatifs,

- ou constituer des opportunités.

Une opportunité est la possibilité qu'un événement survienne et contribue à l'atteinte d'objectifs.

§ 4. Définition du management des risques

Le COSO 2 définit le management des risques comme étant :

- 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 toutes les activités de l'organisation ;

- Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et, pour gérer les risques dans la limite de l'appétence de l'organisation pour le risque ;

- Il vise, enfin, à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.

Le dispositif de management des risques inclut l'identification des événements potentiels susceptibles d'affecter l'organisation et le maintien de son exposition aux risques en cohérence avec son appétence (globale) pour le risque.

§ 5. Le concept d'appétence pour le risque et le concept de tolérance au risque

Selon le cadre COSO, «l'appétence pour le risque est le niveau de risque global auquel l'organisation accepte de faire face, en cohérence avec ses objectifs de création de valeur. Il reflète sa conception en matière de management des risques et influence sa culture et son approche opérationnelle.

L'appétence pour le risque est directement liée à la stratégie de l'organisation. Chaque stratégie induit des risques différents. Le dispositif de management des risques aide la direction à choisir une stratégie en cohérence avec son niveau d'appétence pour le risque».

Les techniques de management des risques aident à améliorer les choix stratégiques, par un système itératif, et à les affiner en fonction des risques associés à chaque choix et à l'appétence pour le risque de l'entreprise.

«La tolérance au risque, quant à elle, se rapporte aux objectifs de l'organisation et se définit comme le niveau de variation que l'entité accepte quant à l'atteinte d'un objectif spécifique (par exemple pour un objectif de livraisons dans les délais de 98% au minimum, on peut tolérer un taux de 97%). La tolérance au risque, pour être un indicateur pertinent, doit toujours être mesurée dans la même unité que l'objectif.

Enfin, lorsqu'elle définit le seuil de tolérance au risque, la direction considère l'importance relative des objectifs et aligne la tolérance au risque avec l'appétence globale pour le risque».

§ 6. Avantages du management des risques

Selon le cadre de gestion des risques COSO, le dispositif de management des risques comprend les 7 bénéfices suivants :

1. Alignement de la stratégie de l'organisation avec son appétence pour le risque.

2. Renforcer les modes de traitement du risque : Le management des risques apporte la rigueur nécessaire pour identifier et choisir, parmi plusieurs possibilités, la meilleure méthode pour traiter un

risque : évitement, réduction, partage ou acceptation du risque.

3. Diminuer les incidents et les pertes opérationnelles : L'identification et l'analyse des risques permettent d'élaborer des réponses à même de diminuer les coûts ou les pertes associés.

4. Identifier et gérer les risques transverses : Le management des risques vise à gérer les risques à la fois de manière individuelle et dans leur globalité par la prise en compte des impacts corrélés.

5. Traiter, de manière intégrée, les risques multiples : Toute activité comporte une grande variété de risques ; de nombreux risques s'enchaînent ou sont intereliés. Le dispositif de management des risques offre la possibilité d'intégrer les solutions pour gérer ces risques, ce qui permet de traiter, de façon cohérente et complète, l'enchaînement des événements générateurs des risques.

6. Saisir les opportunités : L'identification large des risques aide à identifier les opportunités et à élargir les perspectives.

7. Améliorer l'utilisation du capital : Le management des risques aide la direction à évaluer efficacement les besoins en capital, à améliorer son utilisation et à éviter une déperdition des ressources.

Section 2. Les éléments du dispositif de management des risques

Le dispositif de management des risques du COSO 2 comprend 8 éléments :

- L'environnement interne ;
- La fixation des objectifs ;
- L'identification des événements ;
- L'évaluation des risques ;
- Le traitement des risques ;
- Les activités de contrôle ;
- Information et communication ;
- Le pilotage.

§ 1. L'environnement interne

L'environnement interne forme le style d'une organisation. Il révèle la sensibilisation aux risques des personnes qui composent l'entreprise.

L'environnement interne est le fondement structurel sur lequel s'appuient tous les autres éléments du dispositif de management des risques.

Dans ce sens, l'environnement interne exerce une influence sur :

- la façon dont les stratégies et les objectifs sont définis,
- la façon dont les activités sont structurées et les risques identifiés, évalués et gérés,
- la conception et le fonctionnement des activités de contrôle,
- les systèmes d'information et de communication,
- et le suivi des opérations.

Le cadre COSO précise que «l'impact d'un environnement interne inefficace peut être considérable et se traduire par des pertes financières, une altération de l'image de marque, voire par une faillite.

L'attitude et le souci de la direction générale, dans un dispositif de management des risques efficace, doivent être indiscutables et clairs, et doivent se manifester à travers l'ensemble de l'organisation. Il ne suffit pas de faire des déclarations pertinentes. **L'attitude prônant «faites ce que je dis mais pas ce que je fais» se traduira immanquablement par un environnement inefficace**».

L'environnement interne comprend notamment la culture du risque, l'appétence pour le risque, l'exemplarité des dirigeants (tone at the top), la culture d'intégrité et les valeurs éthiques, l'engagement de compétence, le modèle de structure organisationnelle, la délégation de pouvoirs et l'imputabilité (système de responsabilité et d'accountability) et la politique de ressources humaines.

Selon le cadre COSO, «la culture en matière de management des risques d'une organisation est un ensemble de croyances et d'attitudes partagées caractéristiques de la façon dont l'entité appréhende les risques dans toutes ses activités, depuis l'élaboration d'une stratégie jusqu'à la mise en œuvre au quotidien.

La culture du risque reflète les valeurs de l'organisation, influence la culture de l'entreprise et son approche opérationnelle. Elle affecte la manière dont les éléments du dispositif de management des risques sont

appliqués, notamment la façon d'identifier les risques, de les accepter ou non, puis de les gérer» (1).

«Lorsque la culture du risque est bien développée et bien comprise et qu'elle remporte l'adhésion du personnel, l'organisation peut effectivement identifier et gérer les risques» (2).

Quant au management, désignant les dirigeants exécutifs, la culture du risque transparaît à travers ses actions de gestion quotidienne, ses politiques, ses communications orales et écrites et ses prises de décision ; ce qui en fait un modèle pour le reste du personnel. Il est, par conséquent, primordial que le management soutienne la culture du risque non seulement à travers ses discours, mais également dans ses actions quotidiennes **(tone at the top)**.

Le principe du tone at the top s'applique aussi au conseil d'administration qui est un organe essentiel de l'environnement interne ayant une influence majeure sur cet environnement.

Le cadre COSO précise qu'un «conseil d'administration actif et impliqué doit posséder les compétences appropriées, notamment sur le plan technique, ainsi que la volonté nécessaire pour exercer l'intégralité de ses responsabilités. Il s'agit là d'un élément essentiel de l'efficacité de l'environnement interne de l'organisation vis-à-vis du management des risques. Comme, par ailleurs, le conseil d'administration doit être prêt à questionner et à poser au crible les activités du management, à proposer d'autres points de vue et à prendre des mesures en cas d'agissements répréhensibles, il doit être composé d'administrateurs indépendants vis-à-vis de la direction» (3).

L'intégrité et l'éthique sont, aussi, des éléments essentiels de l'environnement interne. Pour le cadre de management des risques COSO, «le comportement éthique et l'intégrité des dirigeants sont le fruit de la culture d'entreprise qui se matérialise par des normes d'éthique et des règles de conduite ainsi que dans la façon dont elles sont communiquées et rappelées. Le management expose ses souhaits en la matière par des messages officiels. La culture d'entreprise influence l'application des règles, leur contournement ou leur ignorance. La direction, à commencer par le P-DG, joue un rôle clé dans la détermination de cette culture d'entreprise.

En tant que personnalité dominante, le P-DG donne en effet le ton et montre l'exemple en matière d'éthique» (4).

Parmi les outils de consolidation de l'éthique, le cadre COSO considère :

(1) qu'un système de reporting doté des contrôles appropriés peut constituer un garde-fou contre la tentation de «maquiller» les performances ;

(2) la formalisation d'un code de conduite au sein d'une organisation est importante et constitue la base d'un programme éthique efficace ;

(3) il est important de prévoir des dispositifs permettant aux employés de faire remonter les informations en toute confiance (whistle-blowing) ;

(4) il faut également prévoir des sanctions à l'encontre de ceux qui enfreignent le code de conduite ou bloquent le dispositif permettant aux employés de dénoncer les violations qu'ils suspectent ainsi que de pénaliser «les employés qui omettraient volontairement de signaler ces violations» (5) ;

(5) enfin, la mise en œuvre et le respect du principe dit «tone at the top» en raison du fait que les messages véhiculés par les actes de la direction sont rapidement intégrés à la culture d'entreprise.

L'engagement de compétence est aussi un élément déterminant d'un environnement interne favorable au management des risques. De même qu'en raison du fait qu'un compromis entre les compétences souhaitées et les coûts est toujours nécessaire, ce compromis nécessite une adéquation entre le niveau de supervision et le niveau de compétence.

La structure organisationnelle qui représente l'infrastructure permettant de planifier, d'exécuter, de contrôler et de piloter les activités de l'entreprise est aussi un élément clé de l'environnement interne.

«Une structure organisationnelle pertinente nécessite de définir les principaux domaines d'autorité et de responsabilité et d'établir les lignes de reporting» (6).

---

(1) COSO 2, «Le management des risques de l'entreprise - Cadre de références techniques d'application», IFACI, PWC & LANDWELL, éditions d'organisation, page 40.
(2) COSO 2, op. cit., page 41.
(3) COSO 2, op. cit., page 43.
(4) COSO 2, op. cit., page 44.
(5) COSO 2, op. cit., page 46.
(6) COSO 2, op. cit., page 47.

Quant à la délégation des pouvoirs et de responsabilités, elle concerne, selon le cadre COSO, la manière dont les personnes et les équipes sont autorisées et incitées à prendre des initiatives pour faire face et résoudre les problèmes, ainsi que les limites de leurs pouvoirs.

Pour être un élément favorable à l'environnement interne, la délégation suppose :

- des circuits de reporting (obligation de rendre compte),

- des règles en matière d'autorisation,

- des normes décrivant les pratiques professionnelles à respecter,

- des responsables qui disposent des connaissances, des compétences et des moyens nécessaires à l'exercice de leur mission,

- les responsabilités déléguées ne doivent l'être que dans la limite des objectifs à réaliser,

- et, chacun des responsables soit conscient du lien existant entre ses actes et ceux des autres et que la priorité soit donnée par tous à la réalisation des objectifs de l'entreprise.

Mais la délégation génère aussi certains risques tels que les risques de décisions tardives ou indésirables.

Le cadre COSO précise qu'une «augmentation de la délégation exige implicitement un niveau de compétences plus élevé ainsi que des responsabilités accrues. Elle doit, également, s'accompagner de procédures efficaces permettant au management de contrôler les résultats.

Le fait que le personnel reconnaisse qu'il pourra être tenu pour responsable a une incidence considérable sur l'environnement interne» (1).

Dans ce sens, les mesures disciplinaires permettent de faire comprendre quels sont les manquements aux règles de comportement qui ne sont pas tolérés. **De même, un système d'évaluation permet au personnel de se fixer des objectifs d'amélioration**. Le cadre COSO conclut «qu'il est essentiel que le personnel soit préparé pour faire face aux nouveaux défis. Les études et la formation, qu'elles soient scolaires, autodidactes ou qu'elles proviennent de l'apprentissage sur le lieu de travail, doivent préparer les collaborateurs à s'adapter aux évolutions de l'environnement et à y faire face» (2).

§ 2. La fixation des objectifs

La détermination des objectifs appropriés pour toutes les activités de l'organisation est un facteur essentiel de réussite. C'est par rapport aux objectifs que l'organisation identifie les risques qui peuvent menacer, justement, l'atteinte de ces objectifs.

Selon le cadre de management des risques COSO, «en définissant des objectifs au niveau global de l'organisation et au niveau plus détaillé des activités, une entité peut identifier les facteurs clés de succès, à savoir les éléments indispensables à l'atteinte des objectifs. Ces facteurs clés de succès existent au niveau d'une organisation, d'une unité, d'une fonction, d'un département ou d'un individu.

En définissant des objectifs, le management peut identifier des critères de mesure de performances, en se focalisant sur les facteurs clés de succès» (3).

La direction définit les objectifs stratégiques, choisit la stratégie pour les atteindre et décline la stratégie en objectifs opérationnels, de reporting et de conformité.

Les objectifs doivent être clairs, intelligibles et mesurables. Lorsque les objectifs d'une organisation, particulièrement les objectifs stratégiques et opérationnels, manquent de clarté ou sont mal conçus, cela se traduit par un manque d'efficacité et une mauvaise affectation des ressources.

Chaque collaborateur doit acquérir une bonne compréhension des objectifs de l'organisation qui se rapportent à son périmètre d'activité.

Dans la sélection des objectifs, le cadre COSO soutient que l'entité doit prendre suffisamment de risques sans en prendre trop soit l'application du principe, en matière de prise de risque « **Ni pas assez, Ni trop** ».

Pour ce faire, la détermination de l'appétence pour le risque constitue le repère permettant de valider la stratégie et le niveau de risque associés à cette stratégie. En effet, toute stratégie visant à atteindre

---

(1) COSO 2, op. cit., page 49.
(2) COSO 2, op. cit., page 51.
(3) COSO 2, op. cit, page 55.

des objectifs de croissance et un rendement déterminé comporte son lot de risques.

Le cadre COSO souligne que «lorsque les objectifs correspondent à la pratique et aux performances existantes, le lien avec les activités est connu. En revanche, si les objectifs sont différents des pratiques habituelles, le management doit établir ce lien, faute de quoi il s'expose à des risques accrus (1).

§ 3. Identification des événements

L'identification des événements, qui sont source de risque ou d'opportunité, est à la base du management des risques.

Selon le cadre COSO, «un événement est un incident ou une occurrence, d'origine interne ou externe, qui affecte la mise en œuvre ou l'atteinte des objectifs. Les événements peuvent avoir un impact positif, négatif ou les deux» (2).

L'importance de l'identification de tous les événements importants justifie que le cadre de management des risques en fait un élément autonome qui doit être réalisé de façon indépendante des autres éléments de management des risques et de recommander d'éviter particulièrement de confondre l'identification des risques et leur évaluation.

Facteurs d'influence et catégories d'événements : Les événements qui ont un impact (négatif ou positif ou les deux) sur l'atteinte des objectifs dépendent de facteurs internes et externes. Il est important de connaître ces facteurs et de comprendre le type d'événements pouvant en découler, les interdépendances et les enchaînements de risques subséquents.

D'un point de vue méthodologique, il est aussi important de regrouper les événements en grandes catégories telles que :

- interne/externe,
- par catégorie d'objectifs, etc...

Le cadre COSO fournit un exemple de classification des catégories d'événements selon la distinction interne - externe :

Catégories d'événements	
Facteurs externes	**Facteurs internes**
Economiques • Disponibilité des capitaux • Emission, défaut de crédit • Concentration • Liquidité • Marchés financiers • Chômage • Concurrence • Fusions - acquisitions **Environnementaux - Naturels** • Emissions et déchets • Energie • Catastrophes naturelles • Développement durable **Politiques** • Changement de gouvernement • Législation • Politique publique • Réglementation **Sociaux** • Démographie • Comportement des consommateurs • Responsabilité sociale • Vie privée • Terrorisme **Technologiques** • Interruptions • Commerce électronique • Données externes • Nouvelles technologies	**Infrastructure** • Disponibilité des actifs • Capacité des actifs • Accès aux capitaux • Complexité **Personnel** • Compétence des employés • Activités frauduleuses • Santé et sécurité **Processus** • Capacité • Conception • Exécution • Fournisseurs / dépendance **Technologie** • Intégrité des données • Disponibilité des systèmes et des données • Choix des systèmes • Développement • Déploiement • Maintenance

Techniques d'identification des événements : Plusieurs techniques et outils peuvent être utilisés pour l'identification des événements.

L'identification des événements couvre à la fois le passé et le futur :

- Les techniques centrées sur les faits et tendances passés permettant de constituer une base de données d'événements et leurs conséquences réelles.

- Les techniques axées sur les risques futurs visant les tendances et conditions prévisibles et leurs conséquences prévisibles.

Le cadre COSO précise que «les organisations ayant un dispositif de management des risques avancé utilisent couramment une combinaison de techniques prenant en compte à la fois les événements passés et futurs» (3).

Le cadre COSO présente une multitude de techniques et d'outils d'identification d'événements :

---

(1) COSO 2, op. cit, page 55.
(2) COSO 2, op. cit, page 64.
(3) COSO 2, op. cit, page 67.

(1) Bibliothèque d'événements : Il s'agit d'un outil qui présente une liste détaillée d'événements potentiels communs à des entreprises d'un secteur donné ou un processus ou des activités donnés que l'on retrouve, avec une grande similitude, dans plusieurs secteurs. Ces bibliothèques se présentent souvent sous forme de logiciels.

(2) Analyse interne : Réalisée dans le cadre de la planification routinière ou lors de réunions de travail, l'analyse interne utilise, parfois, les informations provenant d'autres parties prenantes et peut faire appel à l'expertise de professionnels externes ou internes.

(3) Seuils de déclenchement ou de remontée des informations : La technique du seuil vise à alerter la direction sur les domaines préoccupants en comparant les transactions ou événements en cours à des critères prédéterminés.

(4) Groupes de travail et cercles de discussions : Cette technique permet d'identifier les événements grâce à des discussions structurées à l'intérieur d'un collectif de compétences avec un animateur (faciliteur) pour organiser le débat sur les événements pouvant nuire à l'atteinte des objectifs concernés par le débat ou offrant un potentiel d'opportunités.

(5) Analyse du déroulement des processus : Cette technique permet d'analyser les points forts et les faiblesses du processus et d'identifier les événements susceptibles d'être préjudiciables à l'atteinte des objectifs du processus (faiblesses du processus). Cette technique est cruciale pour les activités de laboratoire médical, par exemple.

(6) Indicateurs d'événements clés : En identifiant et en établissant les corrélations d'événements, une organisation devient à même de détecter l'existence de conditions pouvant germer un événement à risque à partir du suivi des informations sur les événements ou les faits générateurs d'événements corrélés.

(7) Base de données sur les pertes et incidents : La construction d'une base de données sur les pertes et incidents passés offre une source riche en informations pertinentes permettant d'identifier les causes et les évolutions d'un risque.

Une fois une cause identifiée, il est plus facile de lui apporter une solution globale au lieu de répondre à chaque événement de façon individualisée.

Les techniques et outils d'identification d'événements se trouvent à la base du management des risques, car ils permettent de percevoir le risque ou l'opportunité et, par conséquent, constituent le point de départ, après la fixation des objectifs, de toute la chaîne de management du risque.

Le cadre de management des risques COSO précise que «souvent, les événements ne surviennent pas isolément. Un événement peut en déclencher un autre et des événements peuvent survenir simultanément. Lorsqu'il identifie les événements, le management doit comprendre les liens unissant les événements entre eux. En évaluant ce lien, il est possible de mieux cibler les mesures de management des risques» (1).

§ 4. Evaluation des risques

Evaluer un risque consiste à en apprécier la gravité estimée sur la base de la combinaison :

Probabilité d'occurrence x impact

Un facteur de risque commun à un secteur d'activité ou à plusieurs entreprises peut avoir un impact différent et propre à chaque entité en raison des objectifs spécifiques de chaque entité et de ses choix passés. Selon le cadre de management COSO, «les événements futurs potentiels s'apprécient à la lumière des facteurs influençant le profil de risque de l'organisation comme sa taille, la complexité de ses activités et la réglementation applicable» (2).

Le cadre COSO considère l'élément «évaluation des risques» comme une suite d'actions continues et itératives à l'échelle de l'organisation».

Risque inhérent et risque résiduel : Le risque inhérent est défini par le cadre COSO comme étant «celui auquel une entité est exposée en l'absence de mesures correctives pour en modifier la probabilité d'occurrence ou l'impact» alors que «le risque résiduel est le risque auquel l'entité reste exposée après la prise en compte des solutions mises en œuvre par le management».

La démarche consiste à évaluer le risque inhérent dans un premier temps puis, une fois les réponses définies, l'évaluation porte sur les risques résiduels.

Probabilité d'occurrence et impact : La probabilité d'occurrence représente la possibilité qu'un événement

---

(1) COSO 2, op. cit, page 69.
(2) COSO 2, op. cit, page 74.

donné survienne alors que l'impact désigne les conséquences de la réalisation de l'événement.

Le cadre COSO précise que l'utilisation des données générées en interne basées sur l'expérience de l'organisation permet, généralement, une meilleure estimation de la probabilité d'occurrence et de l'impact du risque ; les données générées en interne étant moins sujettes à des biais liés à la subjectivité des personnes et donnent de meilleurs résultats que les données provenant de sources externes. Néanmoins, les données externes restent toujours utiles soit pour servir de point de référence soit pour renforcer l'analyse.

Limites des estimations relatives à l'occurrence et à l'impact du risque : Selon le cadre COSO, «le management formule souvent des jugements subjectifs concernant les incertitudes auxquelles l'entité est exposée et ce faisant, il doit être conscient des limites qui en découlent. Des recherches en psychologie montrent que les décideurs, à différents niveaux et notamment les chefs d'organisation, ont une confiance excessive dans leurs capacités d'estimation et ne sont pas conscients de leur niveau réel d'exposition aux incertitudes. Cette tendance à l'excès de confiance lors de l'estimation de l'incertitude peut être minimisée par une utilisation efficace de données empiriques générées en interne ou en externe. En l'absence de ce type de données, il est nécessaire d'avoir une conscience aiguë de ce biais pour en limiter les effets» (1).

Le comportement de toute personne est, en effet, selon la théorie des perspectives *(prospect theory)* différent à l'égard des perspectives qui suivent la réalisation de gains ou de pertes :

- Après des gains, la personne tend à éviter l'exposition au risque et cherche plutôt à consolider ses gains ;

- En revanche, en situation de pertes, la personne est prête à prendre des risques importants et adopte une grande tolérance au risque parce qu'elle s'imagine en mesure de rattraper ses pertes.

A ce biais cognitif, s'ajoute l'aversion à la dépossession *(divestiture aversion)* qui pousse le détenteur d'un actif à considérer, par une sorte d'attachement psychologique, que l'actif qu'il détient, qu'il soit en situation de plus-value ou de moins-value, vaut plus que ce que le marché propose. Ce deuxième biais émotionnel est dû à la difficulté de se séparer d'un bien auquel on s'est habitué.

Modes et techniques d'évaluation : Il existe deux modes d'évaluation : l'évaluation quantitative et l'évaluation qualitative.

Selon le cadre COSO, «la méthodologie d'évaluation des risques d'une organisation s'appuie sur un ensemble de techniques quantitatives et qualitatives.

Les techniques quantitatives sont habituellement plus précises et sont utilisées dans les activités plus complexes et sophistiquées afin d'apporter un complément aux techniques qualitatives.

La mise en œuvre des techniques d'évaluation quantitatives nécessite en règle générale un investissement et une rigueur plus importants, et requiert parfois l'utilisation de modèles mathématiques» (2) probabilistes et non probabilistes. Les entreprises recourent aussi à la technique du benchmarking qui consiste à se comparer avec les meilleures pratiques ainsi que de procéder à la comparaison de mesures et de résultats. Ces comparaisons permettent d'identifier les opportunités d'amélioration.

Les organisations se limitent à l'évaluation qualitative (faible, moyen, fort) quand :

- les risques ne se prêtent pas à une quantification, ou

- qu'il n'y a pas suffisamment de données fiables pour effectuer une quantification, ou

- lorsqu'il n'est pas possible d'obtenir ou d'analyser les données moyennant un coût raisonnable.

§ 5. Traitement des risques

Le cadre COSO retient quatre types de traitement des risques (l'évitement, la réduction, le partage et l'acceptation) :

- L'évitement : qui consiste à cesser ou à céder les activités génératrices du risque que l'organisation n'est pas prête à assumer. L'évitement suppose qu'aucune des réponses identifiées ne soit à même de réduire la probabilité d'occurrence et l'impact à des niveaux acceptables de risque résiduel.

- La réduction : qui consiste à prendre des mesures qui soient à même de réduire la probabilité d'occurrence ou l'impact ou les deux à la fois de sorte que le risque résiduel descende à un niveau correspondant à la tolérance au risque.

---

(1) COSO 2, op. cit, pages 77.
(2) COSO 2, Op. cit., pages 78-79.

- Le partage : qui consiste à transférer (externalisation ou sous-traitance, par exemple) ou à couvrir le risque, moyennant un coût compatible (achats de produits d'assurance ou opérations de couverture) pour diminuer sa probabilité d'occurrence ou son impact sur l'entreprise à un niveau correspondant à sa tolérance au risque.

- L'acceptation : lorsque le risque inhérent se situe déjà au niveau de la tolérance au risque, la solution consiste à n'engager aucun coût spécifique pour modifier la probabilité d'occurrence ou l'impact du risque tolérable.

Selon le cadre COSO, «le choix de traitements adéquats nécessite la prise en compte de facteurs tels que :

- L'effet des traitements potentiels sur la probabilité d'occurrence et l'impact des risques, et l'identification de ceux permettant de respecter la tolérance au risque de l'organisation.

- Le rapport coût/bénéfice des traitements potentiels.

- Les opportunités éventuelles, au-delà de la gestion du risque en question, permettant de contribuer à la réalisation des objectifs de l'organisation» (1).

Souvent, plusieurs traitements ou une combinaison de différents types de traitements sont nécessaires pour ramener le risque résiduel à un niveau correspondant au seuil de tolérance. De même, un traitement efficace d'un risque peut constituer une réponse appropriée à d'autres risques.

Pour choisir un traitement parmi différents traitements envisageables, il convient d'évaluer les conséquences de chaque traitement sur la probabilité d'occurrence et l'impact de façon séparée, car chaque traitement peut avoir des répercussions différentes sur la probabilité d'occurrence d'une part et sur l'impact d'autre part. Pour ce faire, il est utile de prendre en compte les événements et tendances historiques en plus des scénarios futurs possibles ainsi que d'analyser les coûts, comparativement aux bénéfices attendus, des différentes solutions de réponses aux risques possibles. Bien qu'il puisse dans certains cas s'avérer difficile de quantifier le coût, il convient, lorsque la quantification est possible, de considérer tous les coûts directs et indirects associés à chaque solution et, lorsqu'il est à la fois pertinent et possible, il convient de tenir également compte des manques à gagner découlant de l'utilisation des ressources.

L'évaluation des bénéfices attendus est, quant à elle, généralement plus subjective. Le cadre COSO précise que «dans de nombreux cas cependant, les bénéfices liés au traitement d'un risque peuvent être évalués au regard de ceux dégagés si l'objectif concerné est atteint» (2).

La sélection du traitement du risque à retenir doit prendre en compte les nouveaux risques susceptibles de découler du traitement du risque lui-même ainsi que des risques avérés dont on ne s'était pas aperçu au premier abord, ce qui conduit à un processus itératif.

Une fois le traitement d'un risque arrêté, il convient d'élaborer un plan de mise en œuvre.

§ 6. Activités de contrôle

Les activités de contrôle sont constituées des politiques et des procédures qui permettent de s'assurer que les traitements des risques fonctionnent et que les activités se déroulent sous contrôle. Les activités de contrôle dépendent notamment des politiques, méthodes et technologies mises en œuvre mais aussi de la qualité, de la qualification, des comportements et des compétences des personnes qui les exécutent.

Les activités de contrôle sont fonction des traitements des risques choisis et du risque résiduel accepté. Il doit y avoir une cohérence entre les objectifs, le traitement du risque et les activités de contrôle.

Il existe une multitude d'activités de contrôle utilisées avec ou sans combinaison, au nombre desquelles, on peut énumérer :

- Les contrôles préventifs ;

- Les contrôles détectifs ;

- Les contrôles manuels ;

- Les contrôles informatisés ;

- Les contrôles hiérarchiques ;

- La revue de la direction ;

- Le contrôle par le reporting ;

- La supervision directe d'une activité ou d'une fonction ;

- Les contrôles révélés par les résultats du traitement de l'information ;

---

(1) COSO 2, op. cit., page 85.

(2) COSO 2, op. cit., page 87.

- Les contrôles physiques ;

- Les contrôles à travers les indicateurs de performance ;

- La séparation des tâches ;

- Les contrôles du système d'information (contrôles généraux et contrôles applicatifs).

Les activités de contrôle reposent sur les politiques et les procédures qui permettent d'appliquer les politiques.

La qualité de mise en œuvre des activités de contrôle dépend des techniques, méthodes et moyens dédiés compte tenu de l'environnement, à la fois général et spécifique, du secteur d'activité, de la taille de l'entreprise et de sa dispersion géographique. **Mais de tous les éléments ayant une influence sur l'efficacité des activités de contrôle, la qualité morale et professionnelle des hommes est la plus déterminante**.

§ 7. Information et communication

La capacité d'identifier, de saisir, de traiter l'information pertinente est une composante clé de tout système de gestion du risque. Ceci mesure l'importance de mettre en place un système d'information (infrastructure, logiciels et utilisateurs qualifiés) efficace et performant permettant d'identifier, de saisir, de traiter et de communiquer les informations pertinentes dans un format et dans des délais permettant à chacun de s'acquitter de ses responsabilités.

L'entreprise doit aussi s'enquérir des informations externes et leur accorder l'importance qu'elles requièrent.

De même, pour être efficace, la circulation de l'information doit être multidirectionnelle c'est-à-dire ascendante, descendante et transversale.

L'exemplarité de la direction adresse un message fort au personnel et à tous les responsables indiquant que les risques et le traitement efficace des risques doivent être pris au sérieux. Le personnel et les responsables doivent disposer de moyens de communication leur permettant de faire remonter les informations importantes en toute circonstance.

La communication doit être non seulement efficace à l'intérieur de l'entreprise, elle doit aussi l'être avec les partenaires externes tels que les clients, les fournisseurs, les actionnaires, les autorités publiques, etc...

Les sources d'informations pertinentes : L'information pertinente peut être produite en interne ou être de source externe. Elle peut être formalisée ou informelle.

L'entreprise doit organiser son système de capture, de traitement et de production d'information interne comme elle doit également gérer de façon appropriée les informations relatives aux événements externes.

Les discussions internes peuvent être une source d'information et d'identification importante des risques. Une autre source importante d'information interne est la capture et le reporting sur les anomalies ainsi que les analyses des données et des résultats obtenus.

Les informations externes comprennent un large éventail de sources telles que la documentation, les systèmes de veille, le benchmark, la participation aux séminaires et manifestations publiques des associations et organismes professionnels et cabinets dispensant une formation qualifiante, les discussions et échanges avec les clients, les fournisseurs, les conseils, les statistiques, internet et médias, etc...

Système d'information : «La conception de l'architecture des systèmes d'information et l'acquisition des technologies sont des aspects importants de la stratégie d'une organisation et les choix réalisés en matière de technologies peuvent être un facteur déterminant pour la réalisation des objectifs. Les décisions sur le choix et le déploiement de la technologie reposent sur de nombreux facteurs, notamment sur des choix organisationnels, sur les besoins du marché et sur les exigences de compétitivité. Si les systèmes d'information sont essentiels au management des risques, les techniques de management des risques peuvent aider à prendre des décisions concernant la technologie.

Les systèmes d'information sont depuis longtemps conçus et utilisés pour soutenir la stratégie de l'organisation. Ce rôle devient essentiel, l'évolution des besoins commerciaux et le progrès des technologies créant de nouvelles opportunités stratégiques à saisir. Dans certains cas, les changements technologiques remettent en cause les avantages acquis par de précédentes réalisations, donnant lieu à une réorientation stratégique» (1).

«**Les évolutions des systèmes d'information ont amélioré la capacité de nombreuses organisations à**

(1) COSO 2, op. cit., page 106.

mesurer et suivre la performance et à présenter des informations analytiques à l'échelle de l'organisation. La complexité et l'intégration des systèmes se poursuivent et les organisations utilisent les nouvelles capacités technologiques au fur et à mesure de leur apparition. Toutefois, la dépendance accrue, sur le plan stratégique et opérationnel, envers les systèmes d'information donne naissance à de nouveaux risques qui doivent être pris en compte dans le dispositif de management des risques» (1).

L'efficacité en matière d'information consiste à ce que les bonnes informations parviennent de façon fiable et en temps opportun aux bonnes personnes et dans le bon format et le niveau de détail qui les rendent immédiatement exploitables. Il est ainsi primordial que le système d'information soit capable de fournir des informations pertinentes, en temps opportun et au bon endroit.

La qualité de l'information comporte cinq attributs :

(1) Un contenu approprié ;

(2) Une fourniture en temps opportun ;

(3) Une information actuelle ;

(4) L'exactitude ;

(5) Une information accessible.

Quant à la communication, elle doit véhiculer :

(1) L'importance et la pertinence d'un dispositif de management des risques efficace ;

(2) Les objectifs de l'organisation ;

(3) L'appétence pour le risque et la tolérance au risque de l'organisation ;

(4) Une terminologie commune sur les risques ;

(5) Les rôles et les responsabilités des collaborateurs dans l'exécution et le renforcement des éléments du dispositif de management des risques.

Les collaborateurs doivent également mesurer l'importance de faire converger leurs activités avec celles des autres en ce qui concerne particulièrement :

- L'identification des problèmes ;

- L'analyse de leurs causes ;

- et, la mise en œuvre des mesures correctives.

(1) COSO 2, op. cit., page 108.

Ils doivent également connaître les comportements jugés acceptables et les comportements jugés inacceptables.

La communication ascendante est généralement réalisée par les lignes de reporting habituelles. Néanmoins, les lignes de remontée de l'information habituelles peuvent devenir inopérantes.

Pour traiter un tel risque, des voies de communication distinctes et sécurisées permettant une remontée de l'information doivent être conçues et communiquées aux collaborateurs.

La communication doit être appropriée au sein de l'organisation et avec le monde extérieur. La qualité de la communication avec l'extérieur véhicule un message au sein même de l'organisation. De même, les dirigeants doivent être conscients que les actes sont plus parlants que les mots.

Enfin, dans ses relations commerciales, l'entreprise doit veiller **à ne pas s'exposer involontairement à trop de risques par l'intermédiaire de ses partenaires notamment les clients et les fournisseurs.**

§ 8. Le pilotage

La qualité et l'efficacité d'un système de management des risques sont fonction de la vigueur et de l'efficacité du pilotage du dispositif de management des risques dans son ensemble.

Le pilotage est réalisé de deux manières qui interagissent, se complètent et se combinent, à savoir :

- Le **pilotage** continu c'est-à-dire permanent et **courant** ;

- **L'évaluation spécifique** périodique.

Les différents outils de pilotage donnent lieu à un reporting sur les défaillances du dispositif de gestion des risques. Le pilotage est efficace lorsqu'il permet de résoudre les problèmes et assurer l'amélioration continue du système.

1. Le pilotage courant : Ce pilotage s'intègre dans les activités courantes et fait partie des activités habituelles. Il repose sur l'observation active qui permet de détecter les problèmes et d'identifier les disfonctionnements et d'entreprendre les actions correctrices de façon efficace.

Les sources de pilotage courant sont multiples et nombreuses. Parmi les sources permettant d'évaluer le système à partir des activités, on peut énumérer :

(1) Le pilotage à partir de la comptabilité et des opérations de décaissements et d'encaissements ;

(2) L'exploitation active des différents états de reporting ;

(3) Le suivi du reporting sur les anomalies ;

(4) Les tableaux de bord ;

(5) La communication avec les tiers et l'observation active des incidents avec les tiers ;

(6) Les résultats des contrôles administratifs et les relations avec les différentes administrations publiques ;

(7) Les recommandations de l'audit interne ;

(8) Les recommandations de l'audit externe ;

(9) Les recommandations des conseils externes ;

(10) La participation aux séminaires de formation et aux colloques professionnels ;

(11) Les discussions activités avec les opérationnels et les responsables.

Plus le dispositif de pilotage courant est efficace, plus le recours à l'évaluation spécifique peut être espacé. Mais, la combinaison d'opérations de pilotage courant avec des évaluations spécifiques périodiques sont de nature à renforcer et maintenir considérablement l'efficacité du dispositif de gestion des risques.

2. Les évaluations spécifiques : Une évaluation qui focalise sur des activités de gestion du risque permet d'émettre un regard neuf et de réfléchir sur l'efficacité du système de gestion des risques.

L'évaluation spécifique périodique concerne l'ensemble de l'organisation. Elle devra être plus fréquente pour les domaines à risque prioritaire ainsi que les traitements et les procédures associés.

L'évaluation spécifique peut se faire selon deux procédés :

(1) L'auto-évaluation des personnes en charge de l'activité. Elle est simple, peu coûteuse mais moins objective ;

(2) L'évaluation par les tiers qui peuvent être à l'intérieur de l'organisation ou des tiers externes :

- L'audit interne peut effectuer une évaluation spécifique à la demande de la direction générale ;

- Les auditeurs externes peuvent procéder, dans le cadre de leur mission, à une évaluation spécifique de l'efficacité du système ;

- Les organismes de certification du système de qualité, du système d'information, du système de contrôle interne, du système de gestion du risque ou de la fonction audit interne procèdent à une évaluation totale ou partielle du système de gestion des risques ;

- Les experts investis d'une mission d'évaluation spécifique du système de gestion du risque.

L'évaluateur doit acquérir une bonne compréhension des activités de l'entreprise et apprécier le fonctionnement réel du dispositif. L'évaluation peut déboucher sur une opération de documentation du processus d'évaluation.

Lorsque la direction est tenue de communiquer officiellement aux tiers sur l'efficacité du dispositif de gestion des risques, elle doit documenter le système d'évaluation et conserver une documentation à l'appui de ses déclarations.

3. Le reporting sur les défaillances du dispositif : Un système de gestion des risques bien organisé constitue en lui-même une des meilleures sources d'information sur ses propres défaillances.

Les défaillances doivent être capturées et faire l'objet d'un reporting adéquat.

Le reporting est normalement destiné aux responsables hiérarchiques en situation de prendre les mesures qui s'imposent.

Des voies alternatives au reporting aux supérieurs hiérarchiques doivent être mises en place pour permettre, en cas de blocage, la remontée du reporting sur les défaillances graves à la haute direction.

Des protocoles doivent être établis pour définir les niveaux hiérarchiques auxquels sont destinées les états de reporting par importance d'anomalies. Plus on descend dans la structure hiérarchique, plus les responsables doivent disposer d'une information détaillée sur les défaillances au sein de leurs unités.

4. Suivi de la résolution des anomalies et amélioration continue : Pour être efficace, un système de pilotage de la gestion du risque comporte le suivi des actions correctrices et assure l'amélioration continue du système de gestion du risque dans son ensemble.

Pour ce faire, l'efficacité du système de pilotage doit, elle-même, être l'objet d'évaluation courante et d'évaluation spécifique à intervalles réguliers.