INTOSAI GOV 9130

Les Normes internationales des institutions supérieures de contrôle des finances publiques (ISSAI) sont publiées par l'Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI). Pour plus de renseignements visitez le site *www.issai.org*

INTOSAI

Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public – Informations complémentaires sur la gestion des risques des entité

INTOSAI Professional Standards Committee

PSC-Secretariat

Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Denmark

Tel.:+45 3392 8400 • Fax:+45 3311 0415 • E-mail: info@rigsrevisionen.dk

I N T O S A I

EXPERIENTIA MUTUA

OMNIBUS PRODEST

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

Sous-commission des normes de contrôle interne de
l'INTOSAI

F. VANSTAPEL
Premier Président de la Cour des comptes de Belgique

Rue de la Régence 2
B-1000 BRUXELLES
BELGIQUE

Tél : + 32 2 551 8111
Fax : + 32 2 551 8629
E-mail : international@ccrek.be

Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public – Informations complémentaires sur la gestion des risques des entités

Préambule

Les *Lignes directrices de l'INTOSAI sur les normes de contrôle interne* de 1992 ont été conçues comme un document vivant reflétant l'idée qu'il faut encourager l'utilisation de normes pour la conception, la mise en œuvre et l'évaluation du contrôle interne. Cette idée suppose un effort permanent d'actualisation.

Le 17e INCOSAI (Séoul, 2001) a pris acte de la nécessité grandissante de mettre à jour les lignes directrices de 1992 et a marqué son accord pour utiliser comme modèle le système intégré de contrôle interne élaboré par le Committee of Sponsoring Organizations of the Treadway

Commission (COSO – Comité des sponsors de la Commission Treadway). Par la suite, les lignes directrices actualisées ont été amplifiées pour intégrer également une dimension éthique ainsi qu'un chapitre supplémentaire consacré aux principes généraux du contrôle interne appliqués au traitement de l'information.

Les Lignes directrices sur les normes de contrôle interne actualisées ont été publiées en 2004 et devraient également être considérées comme un document vivant, qui sera encore développé et raffiné à l'avenir pour prendre en compte des évolutions telles que le modèle global de gestion des risques de l'entreprise (*Enterprise Risk Management framework - ERM*) du COSO1. C'est ainsi que la présente addition aux lignes directrices a pour but de refléter les conceptions actuelles en matière de gestion des risques, telles que définies dans le modèle ERM du COSO. Le présent document s'adressant en priorité à des lecteurs du secteur public, le terme d'"entité" a été utilisé au lieu de celui d'"entreprise", qui est plus particulièrement associé au secteur privé.

Les informations supplémentaires fournies ici sont le fruit de l'effort conjoint mené par les membres de la Sous-commission des normes de contrôle interne de l'INTOSAI. Cette actualisation a été coordonnée par un groupe de travail issu de la Sous-commission et constitué de représentants des ISC des Etats-Unis d'Amérique, de France, de Hongrie, de Lituanie, d'Oman, des Pays-Bas, de Roumanie, du Royaume-Uni, d'Ukraine et de Belgique (cette dernière assumant la présidence du groupe).

[1] Enterprise Risk Management - Integrated Framework (Le management des risques de l'entreprise – Cadre de référence - COSO - Septembre 2004)

Franki VANSTAPEL
Premier Président de la Cour des comptes de Belgique
Président de la Sous-commission des normes de contrôle interne de l'INTOSAI

Introduction

Selon le postulat de base du modèle de gestion des risques des entités du COSO, chaque organisation a pour but essentiel la création de valeur pour ses « stakeholders » ou parties prenantes. Dans le secteur public, les fonctionnaires sont censés servir l'intérêt public en toute équité et assurer une gestion correcte des ressources publiques. En pratique, les parties prenantes sont les citoyens et leurs représentants élus.

L'incertitude est une donnée intrinsèque à la vie de toute organisation. Aussi l'un des principaux défis pour la direction réside-t-il dans la détermination d'un degré d'incertitude acceptable afin d'optimiser la création de valeur. Par ailleurs, l'incertitude est source de risques et d'opportunités, susceptibles de créer ou de détruire de la valeur, ou, dans les termes propres au secteur public, de servir plus ou moins bien l'intérêt public. La gestion des risques vise non seulement à apporter une réponse efficace aux risques et aux opportunités associés aux incertitudes, renforçant ainsi la capacité de création de valeur de l'organisation, mais aussi à lui permettre de fournir des services plus efficaces de manière plus efficiente et économe, tout en tenant compte de valeurs telles que l'équité et la justice.

Les Lignes directrices de l'INTOSAI sur les normes de contrôle interne pour le secteur public conçoivent le contrôle interne comme un cadre conceptuel global permettant au management d'une entité de réaliser ses objectifs. Le modèle ERM du COSO et d'autres modèles similaires vont plus loin en affirmant que l'entité peut être amenée, en identifiant les risques et opportunités potentiels, à préciser ses objectifs et à élaborer des contrôles internes afin de minimiser les risques et de maximiser les opportunités.

La gestion des risques des entités ne suppose pas seulement d'élargir la définition des fonctions englobées dans la gouvernance d'entreprise, mais requiert également un changement dans la manière dont les organisations conçoivent la réalisation de leurs objectifs. Pour être efficace, la gestion des risques des entités représente, en effet, un processus continu pris en compte dans l'élaboration de la stratégie, mis en œuvre à chaque niveau et dans chaque unité de l'organisation et destiné à identifier les événements potentiels susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs.

Le présent document trace les grandes lignes d'un dispositif recommandé pour la mise en œuvre des principes de gestion des risques dans le secteur public et fournit une base en vue de son évaluation. Il n'a cependant pas pour vocation de remplacer ou de supplanter les Lignes directrices sur les normes de contrôle interne pour le secteur public, mais il vise plutôt à donner d'autres informations complémentaires que les Etats membres pourront utiliser conjointement avec ces normes, s'ils le jugent opportun. Il n'a pas davantage pour but de limiter ou d'entraver l'action des autorités dûment habilitées à élaborer une législation, à fixer des règles ou à mener une politique discrétionnaire au sein d'une organisation.

Enfin, il faut clairement souligner que la nature du présent document est de présenter des lignes directrices supplémentaires portant sur des normes de gouvernance d'entreprise. Ces directives ne fournissent ni politique, ni procédures, ni pratiques détaillées pour mettre en œuvre un système de meilleures pratiques en cette matière, et elles ne sont pas censées s'appliquer à toutes les organisations ni à tous les environnements réglementaires. Néanmoins, l'addendum apporte un complément au large cadre dans lequel les entités peuvent développer des systèmes leur permettant de maximiser les services qu'elles fournissent à leurs parties prenantes.

Quelle est la structure du présent document ?

La structure du supplément est similaire à celles des Lignes directrices de l'INTOSAI sur les normes de contrôle interne. Le premier chapitre définit le concept de gestion des risques des entités et délimite sa portée. Le second chapitre présente les composantes de la gestion des risques des entités et met en exergue les compléments aux normes de contrôle interne.

Chapitre 1:

Définition de la gestion des risques des entités

1.1 Définition

1.1.1 Selon le modèle global de gestion des risques des entités du COSO, la gestion des risques des entités traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Il se définit comme suit :

> "Le management des risques des entités 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 d 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." (COSO – Modèle ERM 2004)

1.1.2 Dans le secteur public, les termes de “création et préservation de la valeur” n’ont pas la même pertinence directe que dans le secteur privé. Cependant, cette définition est délibérément large, afin de couvrir autant de secteurs et de types d’organisation que possible. En l’occurrence, il suffirait de substituer les termes de “création et préservation de services” à ceux de “création et préservation de la valeur” pour que la définition s’applique intégralement aux entités du secteur public.

1.2 Identification de la mission

1.2.1 La gestion des risques des entités repose sur la mission ou la vision définie par l’organisation. Dans le cadre de cette mission, la direction devrait déterminer les objectifs stratégiques, concevoir les stratégies pour atteindre ces objectifs et décliner les objectifs secondaires qui en découlent à tous les niveaux de l’organisation.

1.3 Définition des objectifs

1.3.1 Selon les Lignes directrices de l’INTOSAI sur les normes de contrôle interne, on peut classer les objectifs dans les quatre catégories suivantes (bien que la plupart des objectifs relèvent de plus d’une catégorie) :

- **Stratégique** - objectifs stratégiques servant la mission de l’organisation
- **Opérationnel** – objectifs visant l’exécution d’opérations ordonnées, éthiques,

économiques, efficientes et efficaces, et la protection des ressources contre les pertes, les mauvais usages et les dommages

- **Rapportage** - objectifs liés à la fiabilité du rapportage et au respect des obligations de rendre compte
- **Conformité** - objectifs de conformité aux lois et aux réglementations en vigueur et de capacité d'action conforme à la politique gouvernementale

1.3.2 Les objectifs des deux premières catégories ne relèvent pas entièrement du contrôle de l'entité. Un système de gestion des risques pourra donc uniquement donner une assurance raisonnable que ces risques sont gérés de manière satisfaisante, mais il devrait également permettre à la direction de prendre conscience de la mesure dans laquelle ces objectifs sont réalisés en temps opportun. En revanche, l'organisation ayant le contrôle sur les objectifs relatifs à la faisabilité du rapportage et à la conformité, un processus de gestion des risques efficient donnera généralement à la direction une assurance quant à la réalisation de ces objectifs.

1.4 Identifications des événements - Risques et opportunités

1.4.1 Une fois les objectifs fixés, une organisation doit, dans le cadre de la gestion des risques, identifier les événements susceptibles d'affecter leur réalisation. Les événements peuvent avoir un impact négatif, positif, ou les deux à la fois. Les événements ayant un impact négatif sont des risques pouvant freiner la capacité de l'entité à réaliser ses objectifs. Ces risques peuvent être liés à des facteurs internes ou externes. Le tableau 1 ci-dessous présente bon nombre de risques

auxquels sont confrontées les organisations gouvernementales – il existe probablement d'autres risques s'appliquant à des entités particulières.

1.4.2 Les événements ayant un impact positif peuvent contrebalancer des impacts négatifs des risques ou constituer des opportunités. Par opportunité, on entend la possibilité qu'un événement, en survenant, augmente la capacité de l'entité à réaliser ses objectifs ou lui permette de les atteindre de manière plus efficiente. La direction devrait non seulement chercher à minimiser les risques mais aussi formuler des plans permettant de saisir les opportunités.

1.5 Communication et apprentissage

1.5.1 Déterminer l'"efficacité" de la gestion des risques d'une entité représente une partie fondamentale du processus. La direction doit vérifier si les éléments de la gestion des risques des entités sont en place et s'ils fonctionnent efficacement ; c'est-à-dire, exclure toute faiblesse majeure et s'assurer que tous les risques ont été ramenés à des paramètres acceptables dans les limites du degré d'aversion au risque propre à l'organisation. Lorsque le dispositif de management des risques s'avère être efficacement géré, la direction de l'organisation comprendra dans quelle mesure les objectifs relevant de ces quatre catégories correspondent à la mission et sont en passe d'être atteints. Une communication efficace, tant horizontale que verticale, dans l'ensemble de l'entité est essentielle pour faciliter ce processus.

1.6 Limites

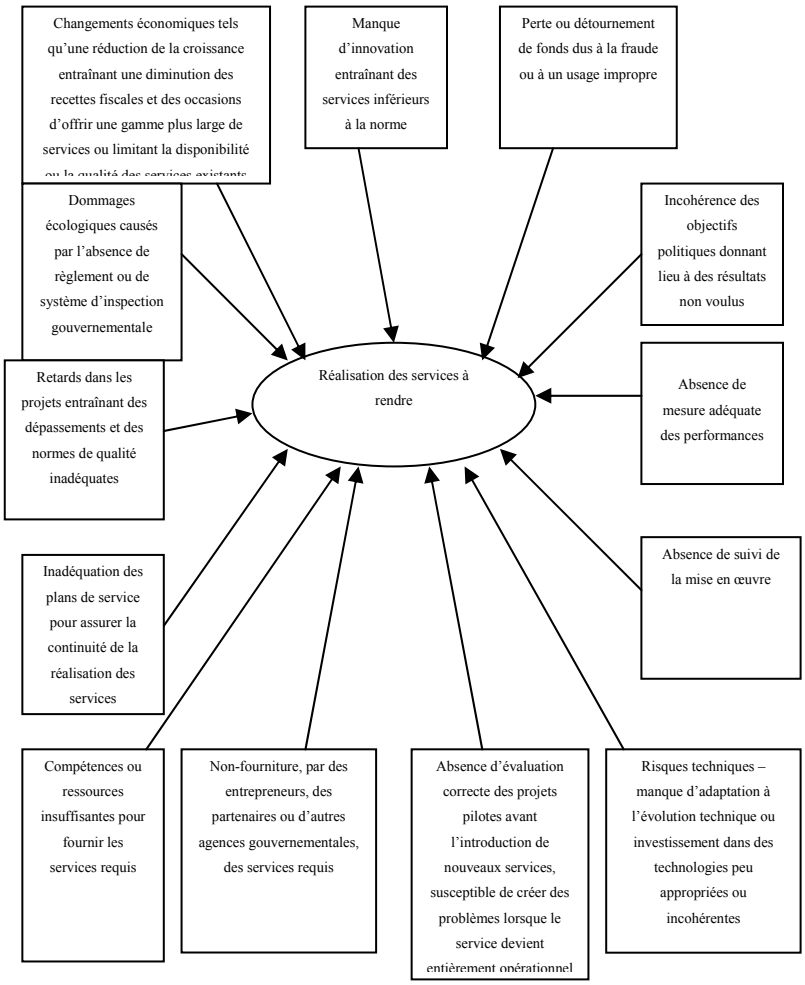
1.6.1 Aussi bien conçu et opérationnel que soit le système, la gestion des risques des entités ne peut donner à la direction une assurance absolue quant à l'atteinte des objectifs généraux de l'organisation. C'est pourquoi le présent supplément reconnaît plutôt que seul un niveau raisonnable d'assurance peut être obtenu.

1.6.2 L'assurance raisonnable correspond à un niveau satisfaisant de confiance dans la réalisation des objectifs ou dans l'information en temps voulu de la direction en cas d'atteinte improbable des objectifs. La détermination du niveau d'assurance requis pour garantir un niveau satisfaisant de confiance est une affaire de jugement. Cet exercice suppose que les responsables évaluent le degré d'aversion au risque de l'organisation ainsi que les événements susceptibles d'affecter la réalisation des objectifs.

1.6.3 L'assurance raisonnable reflète l'idée que l'incertitude et le risque sont liés au futur, que personne ne peut prédire avec certitude. La réalisation des objectifs peut en outre être compromise du fait de facteurs extérieurs, qui échappent au contrôle ou à l'influence de l'organisation, tels que des facteurs politiques. Dans le secteur public, des facteurs ne relevant pas du contrôle de l'entité peuvent même modifier des objectifs essentiels dans un délai très court. D'autres limites peuvent tenir aux éléments suivants : le jugement humain exercé pour prendre certaines décisions peut être défaillant, des dysfonctionnements peuvent survenir en raison d'erreurs humaines telles que de simples défaillances ou des erreurs, des décisions prises pour réagir au risque et établir des contrôles

doivent prendre en considération les coûts et profits inhérents à ces opérations, les contrôles peuvent être contournés à la suite d'une collusion entre deux ou plusieurs personnes, la direction peut passer outre au système de contrôle interne. Ces limitations empêchent la direction d'avoir l'assurance absolue que les objectifs seront réalisés. Le tableau 1 présente certains des risques typiques auxquels une organisation pourrait être confrontée. Il figure à titre d'illustration et n'entend pas être exhaustif.

Tableau 1: Risques caractéristiques auxquels les organisations publiques sont confrontées



1.7 Lien entre le contrôle interne et la gestion des risques des entités

1.7.1 A bien des égards, la gestion des risques des entités peut être considérée comme une évolution naturelle du modèle de contrôle interne. La plupart des organisations tendront à appliquer entièrement le modèle de contrôle interne avant de mettre en œuvre les concepts inhérents à la gestion des risques des entités, dont le contrôle interne fait intégralement partie. Le modèle de gestion des risques des entités comprend le contrôle interne, mais représente en outre une conceptualisation plus approfondie de la manière dont les décisions de gestion prises par une organisation devraient découler de sa mission principale et des objectifs dérivés ; de plus, il représente un outil susceptible d'aider la direction à déterminer la réponse correcte face à un événement particulier. Le modèle ERM va plus loin que les lignes directrices de l'INTOSAI sur les normes de contrôle interne dans plusieurs domaines, dont les suivants :

- Les catégories d'objectifs sont plus étendues et englobent également l'ensemble du rapportage, les informations non financières, les objectifs stratégiques ;
- La composante d'évaluation du risque est élargie et présente différents concepts de risques, tels que le degré d'aversion au risque, la tolérance du risque et la réponse au risque ;
- Le modèle insiste sur l'importance de nommer des administrateurs indépendants au sein du conseil et détaille leurs rôles et responsabilités.

Chapitre 2 – Composantes de la gestion des risques des entités

La gestion des risques des entités est constituée de huit composantes interdépendantes. Celles-ci résultent de la façon dont l'organisation est gérée et sont intégrées au processus de management. Il s'agit des composantes suivantes :

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

Pour appliquer les composantes de la gestion des risques des entités, une entité devrait prendre en compte l'ensemble du champ de ses activités à tous les niveaux de

l'organisation. La direction devrait également étudier les nouveaux projets et initiatives en appliquant le modèle de gestion des risques des entités.

Appliquer la gestion des risques des entités à l'ensemble de l'organisation

La direction doit avoir une vue d'ensemble du risque. En pratique, tous les responsables, quel que soit leur niveau, devront évaluer les événements susceptibles d'affecter leur domaine d'activité et en informer les hauts responsables. Cette évaluation peut être qualitative ou quantitative. La haute direction devrait utiliser ces évaluations couvrant tous les niveaux et domaines d'activité de l'entité pour aboutir à une évaluation du risque global au niveau de l'ensemble de l'organisation.

Importance des ressources humaines

La gestion des risques des entités est mise en œuvre et rendue efficace par la direction et les autres membres du personnel. Elle naît des personnes qui composent l'organisation, à travers ce qu'elles font et de ce qu'elles disent. De même, elle affecte leurs actions. Chaque employé est une personne disposant de compétences et de connaissances différentes. La gestion des risques des entités tend à créer les mécanismes qui permettront aux membres de l'organisation de comprendre le risque dans le contexte de ses objectifs.

Les membres du personnel devraient connaître leurs responsabilités et les limites de leur autorité. Il faudrait donc qu'existe un lien clair et direct entre les tâches d'une personne et la manière dont elle s'en acquitte. Les hauts responsables sont principalement chargés de la supervision. Mais ils doivent également définir la direction à prendre, approuver les stratégies et certaines transactions et

orientation, et ils ont donc un rôle vital à jouer pour faire respecter la culture de l'organisation.

2.1 Environnement/Contexte de risque

2.1.1 L'environnement/le contexte de risque reflète la culture d'une organisation puisqu'il détermine le niveau de sensibilisation au risque de l'ensemble du personnel. Il constitue le fondement de toutes les autres composantes de la gestion des risques des entités, en fournissant une discipline et une structure. Les facteurs de l'environnement interne englobent la philosophie de gestion des risques de l'entité, son degré d'aversion au risque, la supervision assurée par le conseil de direction, l'intégrité et les valeurs éthiques, ainsi que la compétence du personnel et la manière dont la direction délègue l'autorité et la responsabilité tout en assurant l'organisation et la formation du personnel.

2.1.2 La philosophie de gestion des risques d'une entité est constituée par l'ensemble de convictions et d'attitudes partagées qui déterminent comment cette entité considère le risque dans toutes ses activités, depuis la définition de la stratégie jusqu'aux activités opérationnelles journalières. Elle influe sur la culture et la manière d'opérer, notamment, pour identifier les risques, déterminer ceux qui seront acceptés et comment les gérer. La philosophie de gestion des risques d'une entité devrait être exprimée dans des déclarations de politique générale, des communications orales et écrites destinées aux parties prenantes et dans les prises de décision. Quel que soit le mode de communication, il est essentiel que la haute direction appuie cette philosophie, non seulement par sa politique de communication, mais aussi par ses actions quotidiennes.

2.1.3 Le degré d'aversion au risque d'une organisation correspond au niveau de risque qu'elle est prête à accepter pour atteindre ses objectifs. Il reflète la philosophie de gestion des risques et influe à son tour sur la culture de l'entité et sa manière d'opérer. Le degré d'aversion au risque peut être estimé de manière quantitative ou qualitative. Il doit être pris en compte pour définir la stratégie, dans ce sens qu'il devrait exister un parallèle entre le bénéfice escompté d'une stratégie et le degré d'aversion au risque, c'est-à-dire, la disposition à accepter ou à tolérer le risque.

2.1.4 Pour identifier l'environnement de risque et choisir le degré d'aversion au risque approprié, une organisation du secteur public doit, en outre, prendre en considération l'"entité élargie". Les opinions et les attentes des organisations qui la commanditent ou qu'elle supervise, qu'il s'agisse d'autres agences gouvernementales ou de corps législatifs, ainsi que les opinions des organisations partenaires peuvent indiquer clairement la direction à suivre pour déterminer une philosophie de gestion des risques et un degré d'aversion au risque adéquats.

2.1.5 La haute direction d'une entité constitue un élément crucial de l'environnement interne, qui exerce une influence déterminante sur ses éléments. C'est un truisme de dire que la culture d'une organisation peut être définie ou, au contraire, minée par l'état d'esprit de la direction. L'indépendance de la haute direction par rapport au pouvoir exécutif, l'expérience et l'envergure des membres, leur degré d'implication et de perspicacité, l'opportunité de leurs actions, tous ces éléments ont un rôle à jouer. Les autres dirigeants peuvent faire partie de la haute

direction, mais, pour assurer l'efficacité de l'environnement interne, il est recommandé d'inclure dans l'équipe de la haute direction quelques membres extérieurs indépendants. En effet, la haute direction doit être prête à demander des comptes aux cadres en les interrogeant et en examinant attentivement leurs activités, ainsi qu'à présenter des avis alternatifs.

2.1.6 L'intégrité et les valeurs éthiques de la direction influencent la mise en œuvre de la stratégie et des objectifs. La bonne réputation d'une entité est si précieuse que les normes de comportement ne peuvent se limiter au simple respect des normes légales minimales. Le comportement éthique et l'intégrité de la direction découlent de la culture d'entreprise, qui inclut des normes éthiques et comportementales ainsi que la manière de les communiquer et de les faire respecter. Le rôle de la haute direction est essentiel pour définir la culture d'entreprise. Si trop d'importance est accordée aux résultats à court terme par rapport à la réalisation de la mission globale, l'environnement interne qui en découle peut être inadéquat.

2.1.7 Un code de conduite formalisé est important et doit constituer la base de la promotion de valeurs éthiques appropriées. Il en va de même pour des canaux de remontée de l'information (ou des procédures formelles de dénonciation de dysfonctionnements) permettant aux employés de fournir des informations pertinentes au conseil. Toutefois, la présence d'un code de conduite écrit n'assure pas en soi le respect des procédures, même si tous les employés doivent déclarer être informés des comportements qu'on attend d'eux. L'existence de sanctions pour les employés qui

violent le code est tout aussi importante. Les messages transmis par la haute direction sont vite incorporés dans la culture d'entreprise, de telle sorte que les "bonnes réactions" à avoir quand on est confronté à des décisions de gestion complexes sont intégrées dans l'ensemble de l'entité.

2.1.8 La compétence reflète les connaissances et les aptitudes nécessaires à la réalisation des tâches fixées. Elle doit être renforcée par des pratiques en matière de ressources humaines concernant l'engagement et la promotion des personnes appropriées, leur désignation, la formation et les solutions à apporter aux prestations insuffisantes. La direction doit spécifier les niveaux de compétence requis pour des tâches particulières et les traduire sous la forme de descriptions de fonctions pour des postes spécifiques. Il est important d'admettre qu'un compromis peut exister entre la compétence et le coût.

2.1.9 La structure organisationnelle d'une entité fournit le cadre dans lequel elle planifie, exécute, contrôle et suit ses activités. La structure adoptée correspondra à ses besoins d'affaires. Certaines entités sont centralisées, d'autres décentralisées, certaines sont organisées selon l'emplacement géographique et d'autres, selon la fonction. Quelle que soit sa structure, une entité devrait être organisée de manière à lui permettre de gérer efficacement les risques et d'exécuter ses activités de manière à atteindre ses objectifs.

2.1.10 La délimitation des pouvoirs et des domaines de responsabilité concerne la mesure dans laquelle les individus et les équipes sont autorisés et encouragés à faire preuve d'initiative pour traiter

et résoudre des problèmes, mais également les limites de leur autorité. Les défis principaux consistent à assurer que l'ensemble du personnel comprenne les objectifs de l'entité ainsi que la manière dont ses actions contribuent à la réalisation de ces objectifs et à déléguer ces responsabilités uniquement dans la mesure requise par l'atteinte des objectifs. La responsabilité joue un rôle aussi important que l'autorité. L'environnement interne est fortement influencé par la mesure dans laquelle les individus sont conscients qu'ils auront à rendre compte. Ce qui précède s'applique à tous les niveaux, y compris au chef de la direction.

2.2 Fixation des objectifs

2.2.1 Les objectifs sont définis à un niveau stratégique et constituent la base sur laquelle se fondent les opérations de niveau inférieur, les rapports et les objectifs de conformité. Toute entité est confrontée à des risques divers d'origine externe et interne et la fixation d'objectifs constitue une condition préalable pour identifier efficacement les événements susceptibles d'en affecter la réalisation, en évaluer les risques et réagir par rapport à ces risques. Les objectifs doivent être établis pour que la direction soit en mesure d'identifier et d'évaluer les risques susceptibles d'influencer leur réalisation et qu'elle puisse prendre les initiatives nécessaires pour réduire ces risques. Les objectifs sont en ligne avec l'aversion au risque de l'entité, qui détermine les niveaux de tolérance du risque qu'elle appliquera.

2.2.2 La déclaration de mission de l'entité définit dans les grandes lignes les objectifs qu'elle cherche à atteindre. La direction définit les objectifs

stratégiques, formule la stratégie et fixe les opérations correspondantes. Les objectifs stratégiques sont des objectifs de haut niveau complétant et sous-tendant la mission. La stratégie mise en œuvre pour réaliser la mission et les objectifs correspondants est souvent plus dynamique que la mission et sera ajustée pour prendre en compte l'évolution des conditions.

2.2.3 Malgré la diversité des objectifs des différentes entités, certaines larges catégories peuvent s'appliquer. Tous les objectifs relèveront de l'une ou de plusieurs de ces catégories :

- *Objectifs opérationnels* – Cette catégorie d'objectifs se rapporte à l'efficience et à l'efficacité des opérations de l'entité et englobe les objectifs liés aux résultats et à la protection des ressources contre les pertes. Dans le contexte de la reddition publique de comptes, la définition de la « protection des ressources/de l'actif » peut être élargie comme suit : empêcher ou détecter et corriger le détournement des deniers publics. Les objectifs opérationnels doivent refléter l'environnement particulier dans lequel l'organisme est actif. Les objectifs opérationnels représentant le point focal des ressources à affecter, s'ils manquent de clarté ou sont mal conçus, ces ressources peuvent être mal affectées.

- *Objectifs de rapportage* – Ils sont liés à la fiabilité des rapports et peuvent inclure des données à la fois financières et non financières. Bien que ces objectifs s'appliquent également aux informations préparées à l'intention de tiers, ils visent

essentiellement à fournir à la direction des informations précises, complètes et en adéquation avec le but fixé. La direction éprouverait de grandes difficultés à prendre de bonnes décisions sans informations précises et exhaustives.

- *Objectifs de conformité* – Ces objectifs concernent la conformité aux lois et aux règlements. Il peut s'agir de règles relatives aux marchés, à l'environnement, au bien-être des travailleurs, etc. Certaines entités devront aussi se conformer à des objectifs de conformité internationaux.

2.2.4 La gestion des risques des entités fournit une assurance raisonnable quant à la réalisation des objectifs – opérationnels, de rapportage et de conformité – d'une organisation.

2.2.5 Le degré d'aversion au risque, déterminé par la direction et par le conseil d'administration, sert d'indicateur pour fixer une stratégie et évaluer l'importance relative importance des objectifs. En fait, le degré d'aversion au risque correspond au niveau de risque que l'organisation est prête à accepter pour créer de la valeur (sous la forme de services publics) pour ses parties prenantes. Généralement, plusieurs stratégies différentes peuvent être conçues pour atteindre le but poursuivi, chacune d'entre elles présentant des risques différents. La direction devrait choisir la stratégie et les objectifs associés qui correspondent le mieux au degré d'aversion au risque défini.

2.2.6 La tolérance au risque représente le degré de volatilité jugé acceptable dans la réalisation des

objectifs. Elle peut être mesurée à l'aide d'objectifs de performance. La mesure des objectifs de performance s'effectue souvent dans les mêmes unités que les objectifs qui s'y rapportent. En respectant les limites de la tolérance au risque, la direction obtient une meilleure assurance que l'entité ne dépasse pas son degré d'aversion au risque et qu'elle atteindra ses objectifs.

2.3 Identification des événements

2.3.1 La direction identifie des événements potentiels susceptibles, s'ils surviennent, d'affecter l'organisation. Il convient de distinguer les événements qui représentent des opportunités et ceux qui pourraient réduire la capacité de l'entité à mettre en œuvre sa stratégie avec succès et à atteindre ses objectifs (risques). Pour identifier ces événements, la direction prend en considération une série de facteurs internes et externes susceptibles de créer des risques et des opportunités, dans le contexte de l'ensemble de l'entité.

2.3.2 Les événements sont des incidents ou des faits d'origine interne ou externe qui affectent la mise en œuvre de la stratégie ou la réalisation des objectifs. Ils peuvent avoir un impact positif, négatif, ou les deux à la fois. Certains sont manifestes, d'autres obscurs, et ils peuvent avoir des effets insignifiants ou considérables. Toutefois, pour éviter que des événements n'échappent à l'attention, il vaut mieux procéder séparément à leur identification et à l'évaluation de la probabilité de leur survenance et de leur impact.

2.3.3 La direction doit comprendre les catégories fondamentales de facteurs internes et externes déterminant les événements. Les facteurs externes englobent, notamment, ceux découlant de changements survenus dans l'environnement politique, social et technologique et les problèmes économiques affectant l'organisation même ou ses fournisseurs. Les facteurs internes résultent de choix opérés par la direction quant à son mode de fonctionnement. Ceux-ci peuvent inclure l'infrastructure de l'entité, le nombre de sites sur lesquels l'activité est déployée, les capacités et les compétences du personnel ainsi que le fonctionnement des systèmes d'information professionnelle.

2.3.4 Les techniques d'identification des événements sont à la fois rétrospectives et prospectives. Celles qui se concentrent sur les événements du passé peuvent prendre en considération des éléments tels que les rapports et les comptes annuels, les historiques de défauts de paiement et les rapports internes. Les techniques axées sur les événements futurs peuvent s'intéresser à des facteurs tels que l'évolution démographique, les nouvelles conditions du marché et les changements prévus dans l'environnement politique. Le niveau de sophistication et d'automatisation de ces techniques est très variable et elles peuvent adopter une vision 'descendante' ou 'ascendante' des événements.

2.3.5 Il est rare que des événements se produisent isolément. Un événement peut en provoquer un autre et plusieurs événements peuvent survenir simultanément. Les directions devraient comprendre comment les événements sont interconnectés. En évaluant ces relations, il est

parfois possible de déterminer comment orienter au mieux les efforts de gestion des risques.

2.3.6 Il peut aussi être utile de regrouper les événements potentiels en différentes catégories. Concentrer les événements horizontalement dans toute l'organisation et verticalement dans les unités opérationnelles permet à la direction d'appréhender les relations entre les événements. Leur regroupement peut aussi fournir des indications quant aux réactions les plus efficaces en termes de coût. Chaque entité développera sa propre manière de regrouper les événements, mais elles pourront aussi se baser sur des outils standardisés tels que l'analyse du marché PEST[2].

2.4 Evaluation des risques

2.4.1 En évaluant les risques, une entité parvient à comprendre dans quelle mesure des événements potentiels ont une incidence sur la réalisation des objectifs. La direction devrait évaluer les événements selon deux perspectives – l'impact et la probabilité – en utilisant une combinaison de techniques quantitatives et qualitatives. Les impacts positifs et négatifs des événements

[2] L'analyse PEST est un instrument utile pour comprendre et évaluer l'incidence de facteurs externes sur la réalisation des objectifs de l'entité. PEST est un acronyme désignant les facteurs politiques, économiques, sociaux et technologiques.

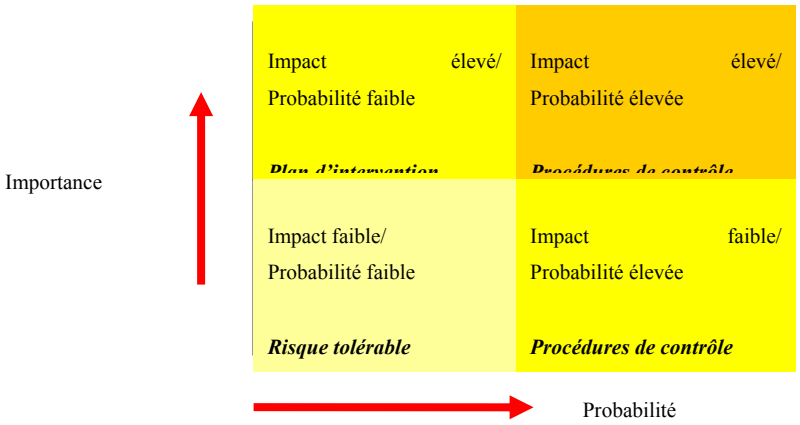
peuvent être établis soit individuellement, soit par catégorie couvrant l'ensemble de l'entité. L'évaluation doit porter à la fois sur les risques inhérents et sur les risques résiduels.

2.4.2 Si le terme d'"évaluation des risques" a parfois été utilisé pour désigner une activité unique, dans le contexte de la gestion des risques des entités, la composante d'évaluation des risques est plutôt conçue comme un jeu continu et itératif d'actions prises dans l'ensemble de l'entité. L'évaluation des risques a pour but d'identifier quels éléments sont assez importants et significatifs pour concentrer sur eux l'attention de la direction.

2.4.3 Les incertitudes relatives aux événements potentiels doivent être analysées sous l'angle de la probabilité et de l'impact. La probabilité représente la possibilité qu'un événement survienne au cours d'une période donnée, alors que l'impact désigne l'importance de l'effet que l'événement aura sur la capacité de l'entité à réaliser ses objectifs. La période durant laquelle la direction estime la probabilité devrait correspondre au délai fixé pour la stratégie concernée et ses objectifs. Les risques principaux sont ceux présentant une probabilité de survenance élevée et un impact important. Inversement, les risques les moins importants sont ceux dont la probabilité de survenance et l'impact sont peu élevés. La direction devrait concentrer ses efforts sur les risques présentant une probabilité et un impact élevés (voir le tableau 2 ci-après). Le résultat final du processus consistera en une note attribuée à chaque risque, en fonction, à la fois, de la probabilité et de l'impact. Certaines entités utilisent un système de notation de type "haut-

bas", d'autres, un système de "feux" dits rouge, orange et vert, et d'autres encore une mesure quantitative telle qu'un pourcentage.

Tableau 2: Matrice d'évaluation simple des risques et de réaction



2.4.4 La méthodologie d'évaluation des risques peut être quantitative ou qualitative et reposer sur des méthodes objectives ou subjectives. De plus, une entité n'est pas tenue d'utiliser les techniques d'évaluation classiques dans tous les domaines de son activité. Cependant, la direction doit être consciente des facteurs humains lorsqu'elle évalue les risques et doit s'assurer que tous les membres du personnel concernés comprennent la signification du système de notation utilisé pour cette évaluation. Si tel n'est pas le cas, la haute direction pourra difficilement déterminer l'importance respective des différents risques.

2.4.5 Une fois l'évaluation des risques terminée, les priorités de l'organisation en matière de risques

devraient apparaître. Si l'exposition au risque est inacceptable en fonction du degré d'aversion au risque défini par l'entité, le risque devrait être classé comme prioritaire ou "risque clé". Les risques clés doivent bénéficier d'une attention régulière au plus haut niveau de l'entité. Les priorités spécifiques en matière de risques évolueront avec le temps à mesure que l'entité se fixe d'autres objectifs, que l'environnement de risque est modifié et que des réponses sont apportées aux risques clés.

2.4.6 L'évaluation des risques esquissée ci-dessus se rapporte au 'risque inhérent'. Le risque inhérent est celui auquel une organisation est confrontée en l'absence de toute action du management susceptible d'influencer sa probabilité de survenance ou son impact. Le risque résiduel est celui qui reste après avoir pris en considération les mesures prises par la direction pour répondre au risque, comme le décrit le paragraphe suivant. L'avantage de cette méthode est qu'elle permet aux entités d'identifier les risques auquel le management consacre du temps qui pourrait être avantageusement utilisé pour résoudre d'autres problèmes (en raison, par exemple, d'une faible probabilité d'occurrence du risque inhérent).

2.5 Réponses à apporter aux risques

2.5.1 Ayant procédé à l'estimation du risque, la direction décide de quelle manière elle compte y répondre. La réponse au risque identifié peut consister à le transférer, à le traiter, à mettre fin à une activité ou encore, à le tolérer. Pour déterminer le type de réponse adéquat, la direction évalue son effet sur la probabilité et l'impact, prend en compte le rapport

coûts/bénéfices de chaque réponse, afin de choisir celle qui ramènera le risque résiduel au niveau de tolérance au risque souhaité. Elle devrait également identifier toutes les opportunités disponibles et permettre d'obtenir une vision globale de son exposition aux risques.

2.5.2 Les réponses à apporter aux risques peuvent se répartir dans les catégories suivantes :

- *Partage/Transfert du risque* – Cette réponse consiste à réduire la probabilité ou l'impact du risque en transférant ou encore en partageant une part de ce risque, par exemple en souscrivant une assurance conventionnelle ou en payant un tiers pour qu'il le traite d'une autre manière. Cette option est particulièrement utile pour réduire des risques financiers, des risques d'actif et ceux liés aux activités d'externalisation. Toutefois, la plupart des risques ne pourront pas être entièrement transférés. En particulier, il est généralement impossible de transférer le risque lié à la réputation même dans le cas où le service à fournir a été externalisé.

- *Réduction/Traitement du risque* – L'immense majorité des risques se résoudra de cette manière. Des mesures sont prises pour réduire la probabilité ou l'impact du risque, voire les deux. Ce type de réponse englobe généralement une myriade de décisions de gestion journalières, dont les procédures de contrôle décrites de manière plus détaillée à la section 2.6 ainsi que dans le document intitulé Modèle intégré de contrôle interne.

- *Evitement/Fin de l'activité* – Ce type de réponse consiste à supprimer les activités donnant lieu au risque. Les entités du secteur public seront rarement en mesure d'éviter de fournir un élément de leur programme de base, mais elles pourront néanmoins envisager l'évitement comme une méthode utile lorsqu'elles auront à déterminer si un nouveau mode de prestations de services est approprié ou s'il convient de poursuivre un projet spécifique.

- *Acceptation/Tolérance* – Aucune mesure n'est prise pour réduire la probabilité ou l'impact du risque. Cette réponse suppose qu'aucune méthode rentable n'a été identifiée pour réduire l'impact et la probabilité à un niveau acceptable ou que le risque inhérent se situe déjà au niveau des risques tolérables. Il est évidemment possible de compléter la tolérance au risque par des mesures d'intervention destinées à gérer les conséquences qu'entraînerait sa survenance.

2.5.3 Le modèle ERM insiste sur la nécessité, non seulement d'anticiper et de gérer les risques, mais aussi, selon la même approche, d'identifier les opportunités. La direction, confrontée à n'importe quelle situation, devrait envisager les opportunités ou les événements présentant un impact positif et pas seulement les risques ou les événements dont l'impact est négatif. A cet égard, deux aspects sont à prendre en considération : tout d'abord, il convient d'examiner si, parallèlement à la réduction des menaces, n'apparaît pas une opportunité dont on pourrait exploiter l'impact positif ; en second lieu, si des circonstances sont apparues qui

présentent des opportunités positives sans pour autant créer de menaces.

2.5.4 La direction devrait évaluer les effets des diverses manières d'aborder le risque et ensuite décider comment gérer celui-ci au mieux, en choisissant une réponse ou une combinaison de réponses susceptible de maintenir la probabilité et l'impact du risque dans les limites de la tolérance à celui-ci. La réponse retenue ne doit pas forcément être celle qui entraîne le moins de risque résiduel, mais si celui-ci dépassait encore le degré de tolérance au risque, la direction devrait soit réexaminer la réponse, soit revoir le niveau de risque acceptable.

2.5.5 L'évaluation des réponses alternatives au risque inhérent requiert la prise en compte de risques supplémentaires qui pourraient découler d'une réponse donnée. Dans ce cas, il serait utile que la haute direction envisage les réponses dans une perspective globale, ce qui lui donnerait une vue d'ensemble du profil général de réponse au risque et lui permettrait d'examiner si la nature et les types de risque résiduel subsistant correspondent à la mission globale et au degré d'aversion au risque de l'organisation.

2.5.6 Après avoir sélectionné la méthode de son choix pour faire face au risque, la direction doit développer un plan de mise en œuvre. Une partie essentielle de tout plan de mise en œuvre consiste à mettre en place des activités de contrôle afin de s'assurer que les mesures prises pour faire face au risque sont effectivement réalisées.

2.6 Activités de contrôle

2.6.1 Les activités de contrôle correspondent à l'ensemble des politiques et des procédures mises en place pour assurer que les mesures prises par la direction pour maîtriser les risques sont réalisées. Les activités de contrôle sont présentes à travers toute l'organisation, à tous les niveaux et dans toutes les fonctions. Comme les Lignes directrices sur les normes de contrôle interne pour le secteur public contiennent des informations détaillées sur la manière de mettre en place des contrôles efficaces, le présent addenda n'a pas d'autre but que de situer les contrôles internes dans le contexte de la gestion des risques des entités.

2.6.2 La gestion des risques des entités conçoit les activités de contrôle comme une partie essentielle du processus appliqué par une entité pour atteindre ses objectifs de gestion. Les activités de contrôle ne représentent pas un but en soi ni ce qui apparaît comme "ce qu'il convient de faire", mais elles servent plutôt de mécanismes permettant de gérer la réalisation des objectifs de gestion.

2.6.3 Les activités de contrôle sont généralement mise en place pour assurer la réalisation correcte des mesures prises pour faire face au risque, mais il arrive qu'à l'égard de certains objectifs, les activités de contrôle elles-mêmes constituent la réponse au risque. La sélection ou la révision des activités de contrôle doit inclure un examen de leur pertinence et de l'adéquation entre la réponse au risque et les objectifs poursuivis.

2.6.4 Chaque entité disposant d'une série d'objectifs et d'une approche de la mise en œuvre qui lui sont propres, les réponses à apporter aux risques et les activités de contrôle qui en découlent seront de nature variée. Même si deux entités avaient défini les mêmes objectifs et pris des décisions identiques quant à la manière de les réaliser, les activités de contrôle résultantes seraient probablement différentes, et ce parce que deux équipes de management différentes ont un degré d'aversion au risque et un niveau de tolérance du risque différents.

2.6.5 Toutefois, dans le contexte de la gestion des risques, toutes les procédures de contrôle entrent dans l'une des quatre catégories suivantes :

- Les **contrôles préventifs** ont pour but de limiter la possibilité de développement d'un risque et la réalisation d'un résultat non voulu. Plus l'impact du risque sur la réalisation des objectifs de l'entité est élevé, plus il devient important de mettre en place des contrôles préventifs adéquats.

- Les **contrôles directifs** visent à s'assurer qu'un résultat particulier sera atteint. Ce type de contrôle est particulièrement important quand il est essentiel d'éviter un événement indésirable (tel qu'une infraction à la sécurité) et il est donc souvent utilisé pour aider à réaliser des objectifs de conformité.

- Les **contrôles à des fins de détection** sont destinés à mettre en évidence si des résultats non voulus sont apparus "après coup". Cependant, la présence de contrôles de détection appropriés peut également réduire le

risque de survenance de résultats non voulus en créant un effet dissuasif.

- Les **contrôles correctifs** ont pour but de corriger les résultats non voulus qui sont apparus. Ils pourraient aussi servir de mesure d'intervention visant à préserver soit des fonds, soit des services contre les pertes et les dommages.

2.7 Information et communication

2.7.1 Les critères de qualité des données utilisées pour réaliser des objectifs de contrôle interne diffèrent peu de ceux qui s'appliquent aux données utilisées dans le cadre de la gestion des risques des entités. Comme les Lignes directrices sur les normes de contrôle interne pour le secteur public contiennent des informations détaillées sur les critères liés à l'information et à la communication, le présent addenda ne vise qu'à situer ces critères dans le contexte de la gestion des risques des entités.

Information

2.7.2 La gestion des risques des entités prévoit spécifiquement qu'une entité doit réunir un ensemble d'informations plus large que ce qui serait nécessaire pour réaliser les objectifs de contrôle interne : par exemple, pour se concentrer sur les objectifs stratégiques, il faut plus d'informations sur les produits ou les résultats. En outre, l'usage qui est fait de ces données est un peu différent. Les données historiques permettent de situer les réalisations effectives par rapport aux objectifs, aux plans et aux attentes et

peuvent donner un avertissement précoce au sujet d'événements potentiels qui requièrent l'attention de la direction. Les données actuelles lui permettent de se faire une idée en temps réel des risques existant au sein d'une unité/d'un processus opérationnel(le) et de déterminer dans quelle mesure ils diffèrent par rapport aux résultats attendus. L'entité peut ainsi déterminer si son action se situe dans les limites de tolérance des risques.

2.7.3 Les informations pertinentes doivent être identifiées, enregistrées et communiqués sous une forme et dans un délai qui permettent au personnel d'assumer ses responsabilités. Une communication efficace doit, en outre, circuler de manière descendante, transversale et ascendante dans l'organisation. Les plus hauts responsables de celle-ci doivent transmettre un message clair à tous les membres du personnel sur l'importance des responsabilités de chacun en matière de gestion de ces risques. Tous doivent comprendre le rôle qu'ils sont appelés à jouer dans le système de gestion des risques des entités, ainsi que la manière dont leurs propres activités s'articulent avec celles des autres membres du personnel. Ils doivent disposer de moyens pour communiquer des informations importantes au niveau approprié de la direction. La nécessité d'une communication efficace s'entend également des relations avec les parties prenantes à l'extérieur de l'organisation.

2.7.4 Il est essentiel de disposer des personnes adéquates détenant les informations pertinentes, en temps voulu et à l'endroit approprié pour assurer la gestion des risques des entités.

Communication

2.7.5 La communication est inhérente aux systèmes d'information. Elle a non seulement pour but de permettre aux membres du personnel concernés de s'acquitter de leurs responsabilités, mais elle doit également être envisagée dans un sens plus large, où elle diffuse la culture d'entreprise, répond aux attentes, couvre les responsabilités des individus et des groupes et assure d'autres tâches importantes.

2.7.6 La direction assure une communication interne spécifique et ciblée sur les comportements qu'elle souhaite voir adopter et sur les responsabilités du personnel. Il doit en résulter une déclaration claire sur la philosophie et l'approche de l'organisation en matière de gestion des risques. La communication relative aux processus et aux procédures devrait s'aligner sur la culture souhaitée et lui servir de fondement. La communication devrait sensibiliser aux sujets suivants :

- L'importance et la pertinence de la gestion des risques des entités
- Les objectifs de l'entité
- Le degré d'aversion et le degré de tolérance au risque de l'organisation
- Le recours à un langage commun en vue d'identifier et d'évaluer les risques
- Les rôles et responsabilités du personnel dans la mise en œuvre et le soutien apporté aux composantes de la gestion des risques.

2.7.7 Les employés doivent également disposer de méthodes pour communiquer des informations relatives aux risques à leur direction opérationnelle et dans l'ensemble de l'organisation. Souvent, les employés de première ligne qui doivent gérer quotidiennement des problèmes de fonctionnement essentiels sont les mieux placés pour reconnaître l'existence de difficultés dès qu'elles apparaissent. Faire rapport au sujet de telles informations suppose que l'existence de canaux de communication ouverts soit assurée, ainsi qu'une volonté claire d'être à l'écoute. Si la culture d'entreprise permet de "tuer le messager", les membres du personnel ne communiqueront pas les problèmes à leurs supérieurs et il se peut que des risques ne soient pas identifiés en temps voulu.

2.7.8 Dans la plupart des cas, les canaux d'information normaux sont appropriés pour transmettre des rapports à la hiérarchie. Toutefois, dans certaines circonstances, des canaux de communication alternatifs sont requis (comme, par exemple, une ligne d'assistance à la dénonciation de dysfonctionnements). En raison de son importance, la gestion efficace des risques des entités requiert l'existence d'un canal de communication alternatif permettant à tous les membres du personnel de joindre directement la haute direction sans crainte de répercussions.

2.7.9 Outre la communication interne, une communication adéquate doit être instaurée avec l'extérieur de l'organisation. Il est essentiel d'informer les interlocuteurs externes de la manière dont l'entité gère le risque afin de les assurer qu'elle répondra aux attentes et de gérer celles-ci. Ce point revêt une importance

particulière en ce qui concerne les risques qui affectent le public, lorsque celui-ci dépend de la capacité du gouvernement à gérer le risque pour lui. Lorsque la communication avec les interlocuteurs externes est envisagée avec sérieux et honnêteté, il en résulte des messages importants pour l'ensemble de l'entité, qui peuvent avoir un impact significatif sur la culture de l'organisation.

2.8 Pilotage

2.8.1 La gestion des risques des entités doit faire l'objet d'un suivi destiné à vérifier le fonctionnement de ses composantes au fil du temps. Ce suivi peut s'opérer au moyen d'activités de routine, par des évaluations ponctuelles ou encore en combinant les deux méthodes. Les lacunes du système de gestion des risques des entités doivent être signalées au niveau approprié de la direction et les problèmes graves feront l'objet d'un rapport destiné à la haute direction ou au conseil d'administration, afin de permettre à l'entité d'améliorer ses processus.

2.8.2 Les objectifs d'une organisation peuvent évoluer dans le temps. Il en est de même pour l'éventail des risques et leur importance relative. Les mesures destinées à répondre aux risques qui étaient efficaces dans le passé peuvent s'avérer inadéquates ou impossibles à mettre en œuvre et les activités de contrôle peuvent perdre de leur efficacité ou être entièrement abandonnées. La direction doit assurer le pilotage constant de l'efficacité du système de gestion des risques afin de vérifier s'il est toujours approprié et efficace.

2.8.3 Les évaluations de l'efficience de la gestion des risques varieront en ampleur et en fréquence en fonction de la portée des groupes de risques et de l'importance des mesures prises pour y faire face, ainsi que des contrôles destinés à les gérer. Lorsque la direction décide d'entreprendre une évaluation globale du cadre de gestion des risques, elle doit veiller à traiter tous les aspects du processus, y compris la définition de la stratégie. Toutefois, des activités de gestion ordinaire, telles que la mise à jour des registres de risques et les "contrôles périodiques" organisationnels ou fonctionnels constituent également un élément du pilotage du processus de gestion des risques.

Bibliographie

Australian Standard® for risk management (Standards Australia, 2004)

Le management des risques de l'entreprise – Cadre de référence (COSO, 2004)

Cadre de gestion intégrée du risque (Secrétariat du Conseil du Trésor du Canada, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM & ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)