

INTOSAI



*Lignes directrices
sur les normes de
contrôle interne à
promouvoir dans le
secteur public*

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

INTOSAI



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>

Table des matières

| | |
|---|----|
| Préambule | 1 |
| Introduction | 3 |
| 1 Contrôle interne | 7 |
| 1.1 Définition | 7 |
| 1.2 Limites du contrôle interne | 14 |
| 2 Composantes du contrôle interne | 16 |
| 2.1 Environnement de contrôle | 20 |
| 2.2 Evaluation des risques | 25 |
| 2.3 Activités de contrôle | 31 |
| 2.4 Information et communication | 41 |
| 2.5 Pilotage | 46 |
| 3 Rôles et responsabilités | 50 |
| Annexe 1 Exemples | 57 |
| Annexe 2 Glossaire | 65 |



Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public

Préambule

Les lignes directrices 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 17^e 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, il a été établi que les lignes directrices actualisées devaient intégrer également une dimension éthique ainsi qu'un chapitre supplémentaire consacré aux principes généraux du contrôle interne appliqué au traitement de l'information. Les nouvelles lignes directrices tiennent compte de ces recommandations et doivent faciliter la compréhension des nouveaux concepts en matière de contrôle interne.

Malgré cet effort d'actualisation, ce serait une erreur de voir dans ces lignes directrices un référentiel figé: elles restent un document vivant, dont la mise en œuvre exige que l'on prenne en compte les évolutions qui surviendront inmanquablement, tels que les développements en matière d'*Enterprise Risk Management* émanant du COSO¹.

La présente mise à jour est le fruit d'efforts conjoints menés par les membres de la Commission des normes de contrôle interne de

¹ COSO, *Enterprise Risk Management Integrated Framework*, www.coso.org, 2004.



l'INTOSAI. Cette actualisation a été coordonnée par un groupe de travail issu de la Commission et constitué de représentants des ISC de Bolivie, des Etats-Unis d'Amérique, de France, de Hongrie, de Lituanie, des Pays-Bas, de Roumanie, du Royaume-Uni et de Belgique, cette dernière assumant la présidence du groupe.

Le comité directeur de l'INTOSAI a approuvé le plan d'action qui lui a été soumis en vue de l'actualisation des lignes directrices lors de sa 50^e réunion (Vienne, octobre 2002). Il a ensuite été informé de l'état d'avancement des travaux lors de sa 51^e réunion (Budapest, octobre 2003). Le projet a été examiné et globalement approuvé lors de la réunion de la Commission qui s'est tenue à Bruxelles en février 2004. A l'issue de cette réunion, il a été envoyé à tous les membres de l'INTOSAI pour récolter leurs dernières observations.

Les commentaires reçus ont été analysés et les modifications qui semblaient appropriées ont été apportées.

Je voudrais remercier tous les membres du Comité des normes de contrôle interne pour leur dévouement et leur coopération dans l'accomplissement de ce projet. Un merci tout particulier est adressé aux membres du groupe de travail.

Les Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public seront présentées pour approbation lors du XVIII^e INCOSAI à Budapest en 2004.

Franki VANSTAPEL

Premier Président de la Cour des comptes de Belgique

Président du Comité des normes de contrôle interne de l'INTOSAI



Introduction

En 2001, l'INCOSAI a décidé d'actualiser les lignes directrices de l'INTOSAI de 1992 sur les normes de contrôle interne afin d'y intégrer l'ensemble des dernières évolutions pertinentes intervenues dans l'intervalle et d'y incorporer les conceptions développées par le COSO dans son rapport intitulé *Internal Control – Integrated Framework* (système intégré de contrôle interne).

En transposant le modèle COSO dans son projet de lignes directrices, la Commission avait pour but non seulement d'actualiser le concept de contrôle interne, mais aussi d'essayer de contribuer à une compréhension uniforme du contrôle interne au sein des ISC. Il va de soi que le présent document intègre les caractéristiques du secteur public, ce qui a conduit la Commission à introduire quelques thèmes complémentaires ainsi que des adaptations ponctuelles.

Par rapport à la définition du COSO et aux lignes directrices de 1992, l'aspect éthique des opérations a été ajouté. La prise en compte de cette dimension nouvelle dans les objectifs du contrôle interne se justifie par l'attention accrue portée, depuis les années quatre-vingt-dix, au comportement éthique ainsi qu'à la prévention et à la détection de la fraude et de la corruption dans le secteur public². Les fonctionnaires sont censés servir l'intérêt public en toute équité et assurer une gestion correcte des ressources publiques. Les citoyens sont censés être traités en toute impartialité sur la base des principes de légalité et de justice. L'éthique publique constitue une condition sine qua non de la confiance publique, dont elle constitue le fondement, et la clef de voûte d'une bonne gouvernance.

Les moyens mis à la disposition du secteur public proviennent généralement de fonds publics, ce qui explique que leur utilisation dans l'intérêt du public exige une attention particulière. D'où aussi l'importance spécifique que revêt la préservation de ces ressources.

De surcroît, la comptabilité budgétaire sur base de caisse constitue toujours une pratique largement répandue dans le secteur public alors qu'elle ne fournit pas une assurance suffisante quant à l'acquisition, à l'utilisation et à l'affectation desdites ressources. En conséquence, les organisations du secteur public ne disposent donc pas toujours d'un

² XVI^e INCOSAI, Montevideo, Uruguay, 1998.

inventaire actualisé de l'ensemble de leurs actifs, ce qui les rend plus vulnérables.

C'est pourquoi il a été estimé que la protection des ressources constituait un objectif important du contrôle interne.

Tout comme en 1992, le contrôle interne ne s'arrêtait pas à l'optique traditionnelle du contrôle financier et du contrôle administratif qui en découle, mais incluait déjà le concept plus général de contrôle intégré à la gestion, le présent document pousse la réflexion plus loin, en soulignant l'importance des informations non financières.

Les systèmes d'information étant désormais largement utilisés dans toutes les organisations publiques, l'importance des activités de contrôle qui portent sur les technologies de l'information (IT) a crû de même. C'est ce qui a justifié l'insertion d'un chapitre distinct dans les présentes lignes directrices. Les contrôles des technologies informatiques concernent chacune des composantes du processus de contrôle interne d'une organisation, à savoir: l'environnement de contrôle, l'évaluation des risques, les activités de contrôle, l'information et la communication, ainsi que le suivi et le pilotage du système (aussi appelé monitoring). Toutefois, pour des raisons de présentation, ils seront présentés globalement dans la section consacrée aux activités de contrôle.

L'objectif de la Commission a été tout d'abord de mettre en place des balises pour établir et maintenir un contrôle interne efficace dans le secteur public. Dans cette perspective, les responsables publics constituent la cible première des présentes lignes directrices. Ils peuvent les prendre pour base dans le cadre de la mise en place et de la mise en œuvre du contrôle interne dans leurs organisations respectives.

L'évaluation du contrôle interne constituant une norme généralement admise en matière d'audit public³, les lignes directrices constituent un outil mis à la disposition des auditeurs. Incluant le modèle COSO, les lignes directrices relatives aux normes de contrôle interne ont donc vocation à être utilisées non seulement par les responsables publics⁴, qui peuvent s'en servir comme d'un exemple de cadre solide pour le contrôle interne de leur organisation, mais aussi par les auditeurs qui

³ Normes de contrôle de l'INTOSAI.

⁴ Le personnel d'exécution n'est pas mentionné spécifiquement comme groupe cible. Quoique concerné par le contrôle interne et effectuant des actions qui jouent un rôle important dans la réalisation du contrôle, il n'est, contrairement à la direction,



peuvent les utiliser comme outil d'évaluation du contrôle interne. Toutefois, les présentes lignes directrices n'entendent pas se substituer aux normes de contrôle de l'INTOSAI ou à toutes autres normes pertinentes.

Le présent document définit donc à la fois un cadre de référence pour le contrôle interne dans le secteur public et un référentiel possible pour l'évaluation du contrôle interne. L'approche qu'il présente a vocation à s'appliquer à l'ensemble des aspects du fonctionnement d'une organisation. Toutefois, le but des présentes lignes directrices n'est nullement de limiter le pouvoir des autorités légitimes ou d'interférer avec elles en matière d'élaboration des législations, des réglementations ou des stratégies applicables à l'organisation, qui par nature relèvent de leur intervention discrétionnaire.

Le contrôle interne dans les organismes du secteur public doit se comprendre dans le cadre de leurs caractéristiques spécifiques, c'est-à-dire en prenant en compte le caractère social ou politique de certains de leurs objectifs, le fait qu'ils aient recours aux fonds publics, l'incidence du cycle budgétaire, la complexité de l'évaluation de leur performance (qui nécessite un équilibre entre, d'une part, des valeurs traditionnelles, telles que la légalité, l'intégrité et la transparence, et, d'autre part, des valeurs plus modernes du management, telles que l'efficacité et l'efficacités), et la traduction de l'éventail de ces contraintes en termes de responsabilité publique.

Enfin, il faut clairement souligner que la nature du présent document est de présenter des lignes directrices portant sur des normes. Ces directives ne fournissent ni politiques, ni procédures, ni pratiques pour mettre en œuvre le contrôle interne mais fournissent plutôt un large cadre dans lequel les organisations peuvent développer de tels contrôles détaillés. La Commission n'est évidemment pas habilitée à imposer des normes.

Quelle est la structure du présent document ?

Le premier chapitre définit le concept de contrôle interne et délimite sa portée. Il attire également l'attention sur les limites du contrôle interne.

finaleme nt pas responsable de toutes les activités d'une organisation qui concernent le système de contrôle interne. Le chapitre 3 des présentes lignes directrices définit les rôles et les responsabilités individuelles.



Le second chapitre présente et examine les composantes du contrôle interne. Un troisième et dernier chapitre est consacré aux rôles et aux responsabilités.

Dans chaque partie, les principes essentiels sont d'abord présentés succinctement dans un encadré bleuté. Des informations plus détaillées y font suite. Il est également fait référence à des exemples concrets, repris dans les annexes. Le document compte également en annexe un glossaire reprenant les termes techniques les plus importants.



1 *Contrôle interne*

1.1 Définition

Le contrôle interne est un processus intégré mis en œuvre par les responsables et le personnel d'une organisation et destiné à traiter les risques et à fournir une assurance raisonnable quant à la réalisation, dans le cadre de la mission de l'organisation, des objectifs généraux suivants:

- exécution d'opérations ordonnées, éthiques, économiques, efficaces et efficaces;
- respect des obligations de rendre compte;
- conformité aux lois et réglementations en vigueur;
- protection des ressources contre les pertes, les mauvais usages et les dommages.

Le contrôle interne est un processus intégré et dynamique qui s'adapte constamment aux changements auxquels une organisation est confrontée. Le management et le personnel, à tous les niveaux, doivent être impliqués dans ce processus afin de traiter les risques et fournir une assurance raisonnable quant à la réalisation des missions de l'organisation et des objectifs généraux.

Un processus intégré

Le contrôle interne n'est pas un événement isolé ou une circonstance unique, mais un ensemble d'actions qui touchent à toutes les activités d'une organisation. Ces actions sont présentes de manière continue dans toutes les opérations d'une organisation. Elles sont perceptibles à tous les niveaux et inhérentes à la façon dont l'organisation est gérée. Le contrôle interne ainsi défini est, par conséquent, différent de la description qu'en font certains observateurs, qui le perçoivent comme une activité supplémentaire d'une organisation ou comme un fardeau nécessaire. Le système de contrôle interne fait partie intégrante des activités d'une organisation et est particulièrement efficace lorsqu'il est intégré dans l'infrastructure et la culture de l'organisation.



Le contrôle interne doit être intégré et non superposé. Ce faisant, il devient une partie intégrante des processus de gestion de base en matière de planification, d'exécution et de vérification.

L'intégration du contrôle interne a aussi une incidence importante en matière de maîtrise des coûts. Ajouter de nouvelles procédures de contrôle à celles qui existent déjà engendre des coûts supplémentaires. En revanche, si l'on part de l'examen des opérations existantes et de leur contribution à l'efficacité du contrôle interne et si on intègre des procédures de contrôle aux activités opérationnelles de base, l'organisation peut souvent éviter des procédures et des coûts inutiles.

Mis en œuvre, exécuté et suivi par les responsables et les autres membres du personnel

Le contrôle interne n'existe pas sans les personnes qui le font fonctionner. Il naît des personnes qui composent l'organisation, au travers de ce qu'elles font et de ce qu'elles disent. En conséquence, le fait que le contrôle interne soit suivi d'effets est tributaire des personnes. Elles doivent connaître leur rôle et leurs responsabilités ainsi que les limites de leur autorité. En raison de l'importance de ces considérations, un chapitre distinct (3) leur est consacré.

Quand on parle des personnes qui composent l'organisation, on vise à la fois les responsables et les autres membres du personnel. Si le management exerce en priorité un rôle de supervision, il arrête aussi les objectifs de l'organisation et assume une responsabilité globale sur le système de contrôle interne. Comme celui-ci contribue, de par les mécanismes qu'il suppose, à une meilleure compréhension des risques qui menacent la réalisation des objectifs de l'organisation, il appartient à la direction de mettre en place les activités de contrôle interne, d'assurer leur suivi et de les évaluer. La mise en oeuvre du contrôle interne exige que les responsables donnent une impulsion décisive et qu'ils accomplissent un effort de communication intensif en direction des autres membres du personnel. En ce sens, le contrôle interne constitue un outil de management, directement orienté vers la réalisation des objectifs de l'organisation. A ce titre, la direction est un maillon important du contrôle interne. Maillon important mais non unique: ce sont tous les membres du personnel de l'organisation qui jouent un rôle important dans sa concrétisation.



De la même façon, le contrôle interne est nécessairement tributaire de la nature humaine. Aussi, les lignes directrices en matière de contrôle interne tiennent-elles compte du fait que, d'une personne à l'autre, il peut y avoir des divergences dans la manière dont les choses sont comprises, communiquées ou exécutées: chaque individu apporte l'expérience et les compétences techniques qui lui sont propres, de même qu'il a ses propres besoins et priorités. Ces réalités influencent le contrôle interne et sont influencées par lui.

Quant à la réalisation des missions de l'organisation

Toute organisation vise prioritairement à réaliser sa mission. Toute entité a une finalité – le secteur public a généralement pour objet de fournir un service et un résultat bénéfique pour l'intérêt général.

Destiné à traiter les risques

Quelle que soit la mission de l'organisation, sa réalisation entraînera pour l'organisation d'être confrontée à toutes sortes de risques. La tâche du management sera d'identifier et maîtriser ces risques afin de maximiser la probabilité de réalisation de la mission. Si le contrôle interne peut aider à traiter ces risques, l'assurance quant à la réalisation de la mission et des objectifs généraux ne pourra être que raisonnable.

Destiné à fournir une assurance raisonnable

Le contrôle interne, aussi bien conçu et appliqué soit-il, ne peut offrir à la direction une assurance absolue quant à la réalisation des objectifs généraux. Les lignes directrices reconnaissent en effet que seul un niveau raisonnable d'assurance est atteignable.

La notion d'assurance raisonnable correspond à un degré de confiance satisfaisant pour un niveau de coûts, de bénéfices et de risques donné. La détermination de ce degré d'assurance raisonnable est une affaire de jugement. Cet exercice suppose que les responsables identifient les risques inhérents à leurs opérations, définissent les niveaux de risques acceptables en fonction de divers scénarios et évaluent le risque tant en termes qualitatifs que quantitatifs.



L'assurance raisonnable reflète l'idée que l'incertitude et le risque sont liés au futur, que nul 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.

D'autres limites peuvent tenir à des facteurs ou événements tels que: le jugement humain exercé pour prendre certaines décisions peut être défaillant, des dysfonctionnements peuvent survenir en raison de simples défaillances ou d'erreurs, des 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. De plus, les compromis pris dans le système de contrôle interne reflètent le fait que les contrôles ont un coût. Ces limitations empêchent la direction d'avoir l'assurance absolue que les objectifs seront réalisés.

Outre ces facteurs d'incertitude, l'idée d'assurance «raisonnable» renvoie au fait que le coût du contrôle interne ne doit pas dépasser le bénéfice qui en découle. Les décisions prises pour gérer les risques et mettre en place des contrôles doivent tenir compte des coûts et bénéfices qui en découlent. L'évaluation de ce coût intègre à la fois l'évaluation financière des ressources consommées pour la réalisation d'un objectif spécifique et l'évaluation économique des coûts d'opportunité résultant du retard pris dans les opérations, de la baisse de la qualité des services ou de la productivité ou d'une atteinte au moral des agents. Le bénéfice se mesure quant à lui par l'évaluation de la proportion dans laquelle un risque d'échec dans la réalisation d'un objectif déclaré se trouve réduit grâce au contrôle interne. Ainsi, on pourra dire que le contrôle interne produit un bénéfice si la probabilité de détecter les fraudes, le gaspillage, les abus ou erreurs, de faire obstacle à une activité inappropriée s'en trouve accrue, ou si l'exigence de respect de la réglementation est mieux assurée.

La conception de contrôles internes qui offrent un bon rapport coût-bénéfice tout en réduisant les risques à un niveau acceptable implique que le management comprenne clairement les objectifs généraux à atteindre. Il arrive que les responsables de l'administration publique conçoivent des systèmes de contrôle interne dans lesquels un secteur précis de leur domaine de compétence fait l'objet de contrôles excessifs qui affectent négativement d'autres activités. Dans pareil cas en effet, les agents peuvent être tentés de contourner des procédures fastidieuses, l'absence d'efficacité dans les opérations peut être à l'origine de retards, des procédures excessives peuvent étouffer la créativité du personnel et



sa capacité à résoudre des problèmes, ou se traduire par une dégradation dans la ponctualité, le coût ou la qualité des services fournis aux bénéficiaires. C'est ainsi que les bénéfices tirés des contrôles excessifs dans un domaine peuvent se trouver anéantis par l'accroissement des coûts que ces mêmes contrôles provoquent dans d'autres secteurs d'activités.

Des considérations qualitatives doivent toutefois également être prises en considération. Il peut par exemple être important d'avoir des contrôles appropriés de transactions financières d'un degré de risque plus ou moins élevé tels que les salaires, les dépenses de voyage et de réception. Les coûts des contrôles appropriés peuvent sembler disproportionnés si l'on considère les montants en jeu au regard de l'ensemble des dépenses publiques, mais ils peuvent être cruciaux pour maintenir la confiance dans les autorités et ses organisations.

Réalisation des objectifs

Le contrôle interne est conçu en vue de la réalisation d'une série d'objectifs généraux distincts mais interdépendants. Ces objectifs généraux sont réalisés par le biais de nombreux sous-objectifs, fonctions, processus et activités spécifiques.

Les objectifs généraux sont les suivants:

- *Exécution d'opérations ordonnées, éthiques, économiques, efficaces et efficaces*

Les opérations effectuées par l'organisation doivent être ordonnées, éthiques, économiques, efficaces et efficaces. Elles doivent être cohérentes par rapport à sa mission.

Ordonné, c'est-à-dire d'une manière bien organisée ou méthodique.

Ethique a trait aux principes moraux. Un comportement éthique et la prévention et la détection de la fraude et de la corruption dans le secteur public ont pris une acuité plus grande depuis les années quatre-vingt-dix. On attend généralement du personnel de l'Etat qu'ils servent équitablement l'intérêt public et gèrent correctement les ressources publiques. Les citoyens doivent bénéficier d'un traitement impartial dans le respect de la loi et de la justice. L'éthique publique constitue, dès lors, une condition préalable de la confiance publique, dont elle constitue le fondement, et une clef de voûte d'une bonne gouvernance.



Economique signifie ne pas être inutile ou dispendieux. Cela implique l'acquisition en nombre juste des ressources, d'une bonne qualité, fournies au moment et au lieu voulus et au moindre coût

Efficient se rapporte à la relation entre les ressources utilisées et les extrants produits pour atteindre les objectifs fixés. Cela implique la minimalisation des intrants employés pour atteindre une quantité et une qualité données d'extrants ou une maximalisation des extrants avec une quantité et une qualité données d'intrants.

Efficace se rapporte à la réalisation des objectifs ou à la mesure dans laquelle les résultats d'une activité correspondent à son objectif ou aux effets escomptés de cette activité.

- *Respect des obligations de rendre compte*

Rendre compte correspond à l'exigence que les organismes de service public et les personnes qui les composent rendent compte et répondent de leurs décisions et de leurs actes, en ce compris leur gestion des fonds publics qui leur sont confiés, leur loyauté et tous les aspects de leur performance.

Le respect de ce principe passe par le développement, le maintien et la mise à disposition d'informations, financières et non financières, fiables et pertinentes et au moyen d'une publication correcte de ces informations dans des rapports établis en temps opportun à l'intention de l'ensemble des parties prenantes, tant en interne qu'en externe.

Les informations non financières visées ci-dessus peuvent avoir trait par exemple aux critères d'économie, d'efficacité et d'efficacité des politiques et des opérations (informations relatives à la performance) ainsi qu'au contrôle interne et à son efficacité.

- *Conformité aux lois et réglementations en vigueur*

Les organisations sont tenues d'observer un grand nombre de lois et de réglementations. Dans les organisations publiques, des lois et des réglementations régissent les recettes et les dépenses publiques, et en déterminent les modalités. Dans cette perspective, on devra tenir compte par exemple, de la loi budgétaire, des traités internationaux, des lois sur la bonne administration, du droit et des normes comptables, du droit de l'environnement, des textes qui gouvernent les droits fondamentaux et les libertés publiques, de la législation relative à l'impôt sur les revenus et les lois réprimant la fraude et la corruption.



-
- *Protection des ressources contre les pertes, les mauvais usages et les dommages dus au gaspillage, aux abus, à la mauvaise gestion, aux erreurs, à la fraude et aux irrégularités*

Quoique le quatrième objectif général puisse être considéré comme une sous-catégorie du premier (opérations ordonnées, éthiques, économiques, efficaces et efficaces), il y a lieu de souligner l'importance de la protection des ressources dans le secteur public, et ce en raison du fait que, de manière générale, ces ressources proviennent de fonds publics et que leur utilisation dans l'intérêt public requiert une attention particulière. En outre, la comptabilité budgétaire sur base de caisse, toujours largement répandue dans le secteur public, n'offre pas d'assurance suffisante quant à l'acquisition, à l'utilisation et à l'affectation des actifs. En conséquence, les organisations du secteur public ne disposent pas toujours d'un inventaire actualisé et exhaustif de leurs actifs, ce qui les rend plus vulnérables. Dès lors, des contrôles doivent être intégrés dans chacune des activités se rapportant à la gestion des ressources de l'organisation, de leur acquisition jusqu'à leur utilisation ultime.

Des ressources tels que les informations, les documents probants et les pièces comptables sont cruciales pour permettre la transparence et la reddition de comptes quant aux opérations publiques et doivent de ce fait être préservées. Elles risquent cependant également d'être volées, soumises à un mauvais usage ou détruites. Depuis l'arrivée des systèmes informatiques, la protection de tels actifs et informations revêt même une importance de plus en plus grande. En l'absence de mesures de protection appropriées, les informations sensibles stockées sur des supports informatiques peuvent être détruites ou copiées, diffusées ou utilisées abusivement.

1.2 Limites du contrôle interne⁵

Le contrôle interne ne peut, à lui seul, garantir la réalisation des objectifs généraux définis plus haut.

Un système de contrôle interne efficace, aussi bien conçu et appliqué soit-il, ne peut fournir à la direction qu'une assurance raisonnable — et non absolue — quant à la réalisation des objectifs d'une organisation ou à sa pérennité. Le contrôle interne peut fournir des informations au management pour son évaluation du degré de réalisation des objectifs qui lui sont fixés mais non transformer un mauvais manager en un bon manager. Au demeurant, le management n'a aucun contrôle sur les changements qui pourraient intervenir dans la politique ou les programmes du gouvernement, ou dans le contexte démographique ou économique de son action. De tels changements peuvent imposer aux managers de revoir les contrôles et d'ajuster le niveau de risque acceptable.

Le propre d'un système de contrôle interne efficace réduit la probabilité de ne pas atteindre les objectifs. Il n'en élimine pas pour autant le risque toujours présent que le contrôle interne soit mal conçu ou ne fonctionne pas comme prévu.

En effet, dans la mesure où le contrôle interne repose sur le *facteur humain*, il est susceptible de pâtir d'erreurs de conception, de jugement ou d'interprétation, de malentendus, de négligence, de la fatigue ou de la distraction, voire de manœuvres telles que collusion, abus ou transgression.

Une autre limite tient au fait que la conception d'un système de contrôle interne doit tenir compte de *contraintes financières*. Les bénéfices tirés des contrôles doivent, par conséquent, être évalués par rapport à leur coût. La volonté de faire fonctionner un système de contrôle interne qui éliminerait tout risque de perte n'est pas réaliste et sa mise en œuvre serait probablement plus coûteuse que ne le justifierait le bénéfice qui en découlerait dans les faits. Pour déterminer si un contrôle particulier doit être mis en place, on doit prendre en compte non seulement la probabilité de survenance du risque correspondant et son incidence potentielle sur l'organisation mais aussi les coûts afférents à la mise en place de ce nouveau contrôle.

⁵ Il y a lieu de souligner les limites de l'efficacité du contrôle interne afin d'éviter de créer des attentes exagérées qui tiendraient à une perception erronée de sa portée.



Les *changements organisationnels* et *l'attitude du management* peuvent avoir un impact réel sur l'efficacité du contrôle interne et sur le personnel qui le met en oeuvre. C'est pourquoi il est nécessaire que la direction vérifie et actualise continuellement les contrôles, communique les changements au personnel et montre l'exemple en se conformant elle-même à ces contrôles.

2 Composantes du contrôle interne

Le contrôle interne est constitué de cinq composantes interdépendantes :

- Environnement de contrôle
- Evaluation des risques
- Activités de contrôle
- Information et communication
- Pilotage

Le contrôle interne est conçu pour fournir une assurance raisonnable quant à la réalisation des objectifs généraux de l'organisation. Dès lors, la fixation d'objectifs clairs constitue une condition préalable à la conception d'un processus de contrôle interne efficace

L'*environnement de contrôle* constitue le fondement de l'ensemble du système de contrôle interne. Il constitue la discipline et la structure aussi bien que le milieu qui influence la qualité globale du contrôle interne. En retour, il influe largement la manière dont la stratégie et les objectifs sont déterminés et dont les activités de contrôle sont structurées.

Une fois que des objectifs clairs ont été fixés et qu'un environnement de contrôle efficace a été créé, il est nécessaire de procéder à une *évaluation des risques* auxquels l'organisation est confrontée pour réaliser sa mission et atteindre ses objectifs, afin de définir une réponse adaptée à ces risques.

La principale stratégie pour minimiser les risques réside dans la mise en place d'*activités de contrôle interne*. Ces activités de contrôle peuvent être orientées vers la prévention et/ou la détection. Les mesures correctives constituent un complément nécessaire des activités de contrôle interne en vue de la réalisation des objectifs. Le coût des activités de contrôle et des mesures correctives doit avoir une contrepartie et créer de la valeur. Autrement dit, leur coût ne doit pas dépasser le bénéfice qui en découle (rapport coût-efficacité).



Une *information et une communication* efficaces sont cruciales pour qu'une organisation puisse mener et contrôler ses opérations. Les responsables de l'organisation doivent avoir accès, en temps opportun, à une communication pertinente, exhaustive et fiable concernant les événements internes aussi bien qu'externes. De manière générale, l'organisation a besoin d'information à tous les niveaux afin d'atteindre ses objectifs.

Enfin, puisque le contrôle interne est un processus dynamique qui doit être adapté constamment pour tenir compte des risques et des changements auxquels une organisation est confrontée, il est indispensable que le système de contrôle interne fasse l'objet d'un *suivi et d'un pilotage* pour garantir que le contrôle interne reste en phase avec des objectifs, un environnement, des moyens et des risques susceptibles d'avoir évolué.

Ces composantes définissent une méthode de référence pour la conception d'un système de contrôle interne dans une administration publique et fournissent une base d'évaluation possible du contrôle interne. Ces composantes s'appliquent à tous les aspects du fonctionnement d'une organisation.

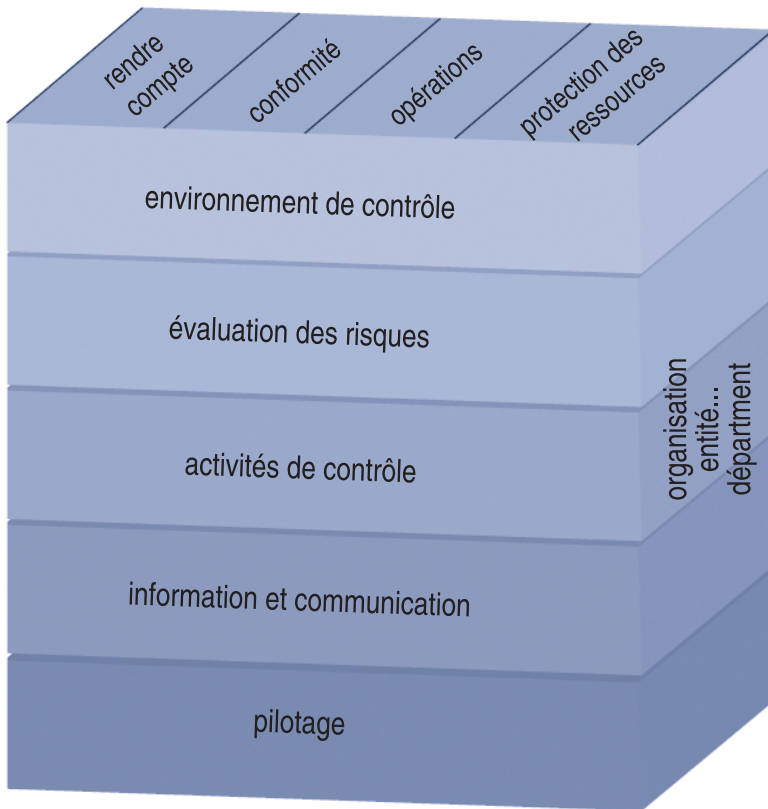
Les présentes lignes directrices fournissent un cadre général. Lors de leur mise en oeuvre, le management est responsable de l'élaboration de politiques, procédures et pratiques détaillées et adaptées aux activités de l'organisation et doit s'assurer qu'elles font partie intégrante de ces dernières.

Lien entre les objectifs et les composantes du contrôle interne

Il existe un lien direct entre les objectifs généraux, qui représentent ce qu'une organisation s'efforce de réaliser, et les composantes du contrôle interne, qui représentent les instruments nécessaires à leur réalisation. Ce lien peut être représenté schématiquement par une matrice à trois dimensions, de la forme d'un cube.

Les colonnes verticales représentent les quatre objectifs généraux – rendre compte (et faire rapport), conformité (aux lois et réglementations), opérations (ordonnées, éthiques, économiques, efficaces) et protection des ressources –, les rangs horizontaux, les cinq composantes, et la troisième dimension de la matrice correspond aux différentes divisions de l'organisation et à ses départements.





Chaque rang de composantes croise les quatre objectifs généraux et s'y applique. Par exemple, les informations financières et non financières provenant de sources internes et externes, qui relèvent de la composante «information et communication», sont indispensables pour gérer les opérations, pour rendre compte et pour assurer la conformité aux lois en vigueur.

De même, les cinq composantes sont pertinentes pour chacun des quatre objectifs généraux. Si l'on s'attache par exemple à l'objectif d'efficacité et d'efficience des opérations, il est clair que les cinq composantes interviennent et jouent un rôle dans sa réalisation.

Le contrôle interne s'applique aussi bien à l'organisation tout entière qu'à ses départements pris isolément. Ce lien est représenté par la troisième dimension, qui représente l'organisation entière, les entités et

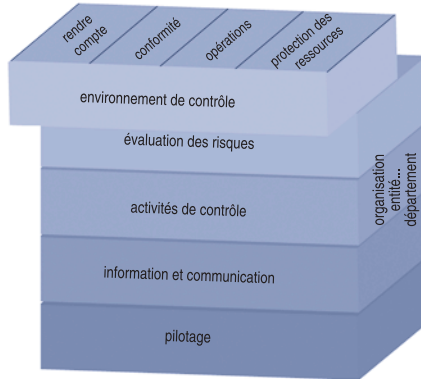


les départements. Il est ainsi possible de se focaliser sur n'importe quelle cellule de la matrice prise en particulier.

Si le système de contrôle interne ainsi défini est pertinent et applicable à toutes les organisations, la manière dont la direction le met en oeuvre varie largement en fonction de la nature de l'organisation et dépend d'un certain nombre de facteurs qui lui sont spécifiques. Ces facteurs comprennent, notamment, la structure de l'organisation, le profil de risque, l'environnement opérationnel, la taille, la complexité, les activités et le degré de réglementation. Au vu de la situation spécifique de l'organisation, les responsables opéreront une série de choix en ce qui concerne la complexité des processus et des méthodologies mises en oeuvre pour appliquer les composantes du système de contrôle interne.

Les pages qui suivent présentent de manière concise chacune des composantes précitées, en l'assortissant de commentaires.

2.1 Environnement de contrôle



L'environnement de contrôle reflète la culture d'une organisation puisqu'il détermine le niveau de sensibilisation de son personnel au besoin de contrôle. Il constitue le fondement de toutes les autres composantes du contrôle interne, en fournissant une discipline et une structure.

Les facteurs constitutifs de l'environnement de contrôle sont :

- (1) l'intégrité tant personnelle que professionnelle et les valeurs éthiques des responsables et du personnel, en ce compris un état d'esprit constructif à l'égard du contrôle interne, en tout temps et à travers toute l'organisation;
- (2) l'engagement à un niveau de compétence;
- (3) le style de management (en l'occurrence, la philosophie des responsables et leur manière d'opérer);
- (4) la structure de l'organisation;
- (5) les politiques et pratiques en matière de ressources humaines.

L'intégrité tant personnelle que professionnelle et les valeurs éthiques des responsables et du personnel

L'intégrité tant personnelle que professionnelle et les valeurs éthiques des responsables et du personnel déterminent leurs priorités et leurs jugements de valeur, qui se traduisent par un code de conduite. Ces qualités doivent se concrétiser par une attitude d'adhésion à l'égard du contrôle interne, en tout temps et dans l'ensemble de l'organisation.

Toute personne active dans l'organisation — tant les responsables que le personnel — doit prouver son intégrité personnelle et professionnelle, et de son respect l'éthique; tous doivent en permanence observer les codes de conduite en vigueur, par exemple, en s'obligeant, d'une



part, à déclarer les intérêts financiers personnels qu'ils peuvent avoir, les fonctions qu'ils pourraient exercer en dehors de l'organisation ou les dons qu'ils reçoivent (s'ils proviennent, par exemple, des élus ou de hauts fonctionnaires) et, d'autre part, à signaler tout conflit d'intérêts.

De même, les organisations publiques elles-mêmes doivent garder et démontrer leur intégrité et respecter des valeurs éthiques, et doivent permettre au public de percevoir ces qualités au travers de la formulation de leur mission et de leurs valeurs. En outre, leurs activités doivent être éthiques, ordonnées, économiques, efficaces et efficaces, et être cohérentes avec leur mission.

L'engagement à un niveau de compétence

L'engagement à un niveau de compétence se définit, notamment, au regard du niveau de connaissance et d'aptitudes nécessaires pour garantir à la fois que les tâches sont accomplies de manière ordonnée, éthique, économique, efficace et efficace, et que les responsabilités individuelles liées au contrôle interne sont bien comprises.

Les responsables et le personnel doivent veiller à garder un niveau de compétence qui leur permette de comprendre toute l'importance d'élaborer, de mettre en oeuvre, et de maintenir un bon contrôle interne et de s'acquitter de leurs tâches en vue de réaliser les objectifs généraux du contrôle interne et la mission de l'organisation. Chacun, au sein d'une organisation, participe au contrôle interne à son niveau et dans les limites des responsabilités qui sont les siennes.

Les responsables et leur personnel doivent, dès lors, entretenir et démontrer un niveau de compétence propre à évaluer les risques et assurer un travail efficace et efficient, et faire preuve d'une compréhension des contrôles internes suffisante pour leur permettre de s'acquitter efficacement de leurs responsabilités.

Au travers d'actions de formation, par exemple, on peut arriver à accroître la sensibilité des fonctionnaires aux objectifs du contrôle interne et, en particulier, à l'objectif d'opérations éthiques. Par ce biais, on pourra les aider à comprendre les objectifs du contrôle interne et à développer leur aptitude à traiter des problèmes d'ordre éthique.

Le style de management

Le style de management (c'est-à-dire la philosophie des responsables et leur manière d'opérer) reflète les éléments suivants:

- l'attitude permanente d'adhésion au contrôle interne, l'indépendance, la compétence et la volonté de montrer l'exemple;
- un code de conduite défini par les responsables ainsi qu'une assistance et des évaluations de performance qui tiennent compte des objectifs du contrôle interne et, en particulier, de celui qui a pour finalité la réalisation d'opérations éthiques.

L'état d'esprit défini par la haute direction se reflète dans tous les aspects des actions menées par la direction. L'engagement, l'implication et le soutien des hauts responsables politiques et des parlementaires pour asseoir ce style de management favorisent une attitude positive et sont déterminants pour le maintien d'une attitude constructive et d'adhésion au contrôle interne dans l'organisation.

Si la haute direction croit à l'importance du contrôle interne, les membres de l'organisation y seront sensibilisés et réagiront en respectant consciencieusement les contrôles établis. Par exemple, la création d'un service d'audit interne, faisant partie intégrante du système de contrôle interne, est un signal fort, par lequel le management montre l'importance du contrôle interne.

Si, au contraire, le personnel de l'organisation a le sentiment que le contrôle n'est pas une préoccupation majeure de la haute direction et est soutenu de manière formelle plutôt que réelle, il est pratiquement certain que les objectifs de contrôle de l'organisation ne seront pas effectivement atteints.

Par conséquent, il est extrêmement important que la direction fasse la démonstration et insiste sur ce qu'est une conduite éthique si elle veut atteindre les objectifs de contrôle interne et, tout particulièrement, l'objectif d'«opérations éthiques». Dans l'exercice de sa fonction, la direction doit donner l'exemple au travers de ses propres actions et sa conduite doit être le modèle de ce qu'il est bon de faire plutôt que l'image de ce qui n'est qu'acceptable ou simplement commode. Les politiques, les procédures et les pratiques de la direction doivent, tout particulièrement, promouvoir des façons de faire qui répondent à l'ensemble des critères énoncés: ordre, éthique, économie, efficacité et efficacité.



Nombreux sont, toutefois, les éléments qui ont une incidence sur l'intégrité des responsables et de leur personnel. Dès lors, il convient de rappeler au personnel, à intervalles réguliers, ses obligations dans le cadre d'un code de conduite fonctionnel, émanant de la haute direction. Conseiller et évaluer les performances ont aussi leur rôle à jouer. Ainsi, les évaluations globales doivent être basées sur l'appréciation de plusieurs facteurs clés, incluant le rôle des agents dans la réalisation du contrôle interne.

Structure de l'organisation

La structure de l'organisation d'une organisation prévoit les éléments suivants:

- délimitation de pouvoirs et domaines de responsabilité;
- délégations de pouvoirs et obligation de rendre compte;
- canaux d'information appropriés.

La structure organisationnelle définit les principaux domaines d'autorité et de responsabilité d'une organisation. Les délégations de pouvoirs et l'obligation de rendre compte ont trait à la manière dont cette autorité et ces responsabilités sont déléguées dans l'ensemble de l'organisation. Qui dit habilitation ou obligation de rendre compte dit établissement de rapports. Il est, dès lors, nécessaire que des canaux d'information appropriés soient définis. Dans des circonstances exceptionnelles, il doit être possible d'ajouter d'autres canaux d'information à ceux qui existent, notamment dans les cas où le management est lui-même impliqué dans des irrégularités.

La structure organisationnelle peut inclure un service d'audit interne qui doit être indépendant du management et faire rapport directement au plus haut niveau d'autorité de l'organisation.

La structure organisationnelle fait l'objet de développements complémentaires dans le chapitre 3, relatif aux rôles et aux responsabilités.

Politiques et pratiques en matière de ressources humaines

Les politiques et pratiques de gestion des ressources humaines englobent le recrutement, la dotation en personnel, la gestion des carrières, la formation (formelle et professionnelle) et les études accomplies, les



évaluations et les conseils au personnel, les promotions et la rémunération, ainsi que les mesures correctives.

Le personnel constitue un aspect important du contrôle interne. Il est nécessaire de s'entourer de personnes compétentes et dignes de confiance pour assurer un contrôle efficace. C'est ce qui fait que les méthodes de recrutement, de formation, d'évaluation, de rémunération, et de promotion jouent un rôle important dans l'environnement de contrôle. Les décisions en matière de recrutement et de dotation en personnel doivent par conséquent donner l'assurance que le personnel possède l'intégrité, la formation adéquate et l'expérience requise pour accomplir ses fonctions et que la formation formelle, professionnelle et éthique est assurée. La présence de managers et d'agents qui comprennent bien les contrôles internes et qui sont prêts à prendre des responsabilités dans ce cadre est indispensable si l'on veut disposer d'un contrôle interne efficace.

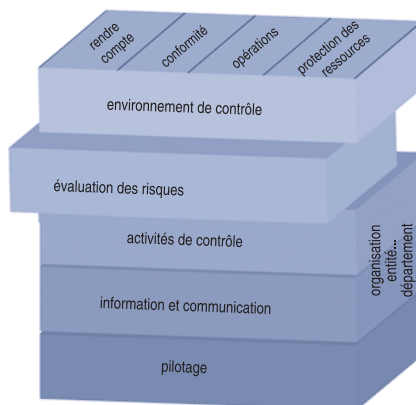
La gestion des ressources humaines joue également un rôle essentiel dans la promotion d'un environnement éthique en favorisant le professionnalisme et en faisant respecter les règles de transparence au quotidien. Ceci doit être particulièrement visible en matière de recrutement, d'évaluation du travail et des processus de promotion, qui doivent être basés sur le mérite. Assurer la transparence des processus de sélection par la publication des règles de recrutement et des vacances d'emplois contribue également à la mise en œuvre d'une gestion éthique des ressources humaines.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.



2.2 Evaluation des risques



L'évaluation des risques est le processus qui consiste à identifier et à analyser les risques pertinents susceptibles d'affecter la réalisation des objectifs de l'organisation, et à déterminer la réponse à y apporter.

Elle implique les éléments suivants :

- (1) Identification des risques
 - liée aux objectifs de l'organisation;
 - exhaustive;
 - qui prend en compte les risques dus à des facteurs externes et internes, à la fois au niveau de l'organisation et à celui des activités;
- (2) Analyse des risques
 - par l'évaluation de l'impact possible du risque;
 - par l'évaluation de la probabilité de survenance du risque;
- (3) Evaluation du degré d'aversion au risque de l'organisation
- (4) Mise au point des réponses à y apporter:
 - Quatre catégories de réponses doivent être envisagées : transfert, tolérance, traitement ou suppression; parmi celles-ci, le traitement des risques est ce qui s'inscrit le mieux dans le cadre des présentes lignes directrices parce que le principal mécanisme permettant de traiter des risques réside précisément dans l'existence de contrôles internes efficaces;
 - Les contrôles appropriés mis en œuvre peuvent être orientés vers la détection ou la prévention.

Compte tenu de l'évolution permanente des données politiques, économiques, industrielles, réglementaires et opérationnelles, l'évaluation

des risques doit constituer un processus continu et itératif. Cela implique d'identifier et d'analyser les changements, les opportunités et les risques qui en découlent (cycle d'évaluation des risques) et de modifier les contrôles internes pour l'adapter aux changements intervenus dans les risques.

Ainsi qu'il est souligné dans la définition, le contrôle interne ne peut fournir qu'une assurance raisonnable quant à la réalisation des objectifs de l'organisation. En tant que composante du contrôle interne, l'évaluation des risques joue un rôle crucial dans la sélection des activités de contrôle appropriées à entreprendre. Elle se définit comme le processus qui consiste à la fois à identifier et évaluer les risques pertinents susceptibles d'affecter la réalisation des objectifs de l'organisation, et à déterminer ensuite la réponse à y apporter.

En conséquence, la définition des objectifs de l'organisation doit précéder l'évaluation des risques. La séquence normale est donc la suivante: vient tout d'abord l'étape de détermination des objectifs qui permet ensuite aux responsables d'identifier les risques qui sont susceptibles d'avoir un impact sur leur réalisation et de prendre, dans un troisième temps, les mesures nécessaires à la gestion de ces risques. Cela implique un processus continu d'évaluation des risques et de gestion de leur impact en tenant compte du rapport coût-efficacité et à l'aide d'un personnel possédant les compétences requises pour identifier et apprécier les risques potentiels. Comme les activités de contrôle interne constituent un moyen pour traiter les risques, elles sont conçues pour contenir l'incertitude des résultats qui a été identifiée.

Les services publics sont appelés à gérer les risques susceptibles d'avoir un impact sur les services rendus et la réalisation des résultats souhaités.

Identification des risques

L'approche stratégique de l'évaluation des risques repose sur une démarche qui consiste à identifier les risques au regard des objectifs clés de l'organisation. Les risques ainsi identifiés sont alors analysés et évalués, et résultent en un nombre restreint de risques majeurs.

L'identification des risques majeurs ne détermine pas uniquement les priorités en termes d'affectation des ressources allouées à l'évaluation



des risques, mais aussi la répartition des responsabilités en vue de la gestion de ces risques.

Les performances d'un organisme peuvent être menacées par des facteurs aussi bien externes qu'internes, dont l'impact peut se mesurer tant à l'échelle de l'organisation qu'au niveau d'une activité donnée. L'évaluation des risques doit prendre en compte tous les risques susceptibles de survenir (y compris le risque de fraude et de corruption). Il faut par conséquent que l'identification des risques soit exhaustive. L'identification des risques doit constituer un processus continu et itératif et est souvent intégrée au processus de planification. Il est souvent utile de partir d'une «feuille blanche» plutôt que de se borner à examiner l'évolution des risques par rapport à la précédente étude. L'avantage de ce type d'approche est qu'elle facilite l'identification des changements intervenus dans le profil de risque⁶ d'une organisation du fait de l'évolution des données économiques et réglementaires, de la modification des conditions de fonctionnement internes et externes ou encore de l'émergence d'objectifs nouveaux ou modifiés.

Il est nécessaire de se doter d'outils appropriés pour identifier les risques. Deux des outils les plus communément utilisés sont la commande d'une analyse des risques et l'auto-évaluation des risques.⁷

⁶ Une vue d'ensemble ou la matrice des risques majeurs auxquels une organisation ou un service est confronté qui inclut le degré d'impact (ex.: haut, moyen, bas) et la probabilité de survenance de l'événement.

⁷ *Mise en place d'une analyse des risques*

Il s'agit d'une procédure du sommet à la base (*top-down*). Une équipe est mise sur pied pour examiner l'ensemble des opérations et des activités de l'organisation à la lumière de ses objectifs et pour identifier les risques qui en découlent. L'équipe mène une série d'entretiens avec les membres importants du personnel à tous les niveaux de l'organisation afin de dresser un profil de risque pour toutes les activités et d'identifier ainsi les domaines, les activités et les fonctions stratégiques susceptibles d'être particulièrement vulnérables aux risques (tels que le risque de fraude et de corruption).

Auto-évaluation des risques

Il s'agit d'une approche de la base au sommet (*bottom-up*). Chaque niveau et partie de l'organisation est invité à revoir ses activités et à faire remonter vers le haut son diagnostic des risques. Cette démarche peut revêtir la forme d'une procédure documentaire (avec un cadre de diagnostic établi par le biais de questionnaires) ou via une approche avec groupe de travail.

Ces deux approches ne s'excluent pas et il est souhaitable d'exploiter les données combinées obtenues ainsi dans le cadre du processus d'évaluation des risques pour faciliter l'identification des risques à la fois au niveau de l'organisme et des activités.

Evaluation des risques

Afin de décider comment gérer les risques, il est essentiel de ne pas se borner à constater le principe de l'existence d'un certain type de risque mais il s'agit aussi d'évaluer son impact éventuel et sa probabilité de survenance. La méthodologie de l'analyse des risques peut varier, surtout parce que de nombreux risques sont difficiles à quantifier (par exemple, risques portant sur la réputation de l'organisation), tandis que d'autres se prêtent facilement à une analyse chiffrée (particulièrement les risques financiers). Pour ce qui est des premiers, seule une approche intégrant une large part de subjectivité est possible. En ce sens, l'évaluation des risques relève plus d'un art que d'une science. Toutefois, l'utilisation de critères systématiques d'estimation des risques atténuera la subjectivité du processus en fournissant un cadre pour les jugements à poser.

L'un des principaux buts de l'évaluation des risques consiste à attirer l'attention de la direction sur les domaines de risque qui appellent des mesures et sur leur degré de priorité. A cet effet, il sera habituellement nécessaire de développer un cadre pour classer l'ensemble des risques, par exemple, comme élevé, moyen ou bas. Il est généralement préférable de réduire au minimum le nombre de ces catégories, un affinement excessif pouvant déboucher sur la séparation purement artificielle de niveaux de risque qui, dans la réalité, ne peuvent être séparés aussi clairement.

Semblable évaluation permet de classer les risques de manière à fixer des priorités de gestion et à présenter à la direction des informations utiles à la prise de décision quant aux risques qui doivent être gérés (par exemple, ceux présentant à la fois un impact potentiel majeur et une probabilité élevée de survenance du risque).

Estimation du degré d'aversion au risque de l'organisation

L'un des principaux déterminants de la stratégie de réponse aux risques réside dans le degré d'aversion au risque de l'organisation. Le degré d'aversion au risque d'une organisation correspond au niveau de risque qu'elle est prête à courir avant d'estimer qu'il est nécessaire d'intervenir. Les décisions de réponse au risque doivent être prises parallèlement à l'identification de ce degré de risque tolérable.

Il est nécessaire de prendre en considération à la fois les risques inhérents et résiduels pour déterminer le degré d'aversion au risque. 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 que le management ait pris des mesures pour répondre au risque.

Le degré d'aversion au risque d'une organisation dépendra de sa perception de l'importance des risques. Par exemple, le niveau maximal de perte financière tolérable peut varier en fonction d'un certain nombre d'éléments, dont l'importance du budget susceptible d'être affecté, l'origine de la perte ou les risques associés au même événement, comme le risque qu'il s'accompagne d'une publicité défavorable à l'organisation. L'identification du degré d'aversion est d'ordre subjectif mais elle n'en représente pas moins une étape importante dans la formulation de la stratégie globale en matière de risques.

Réponses à apporter aux risques

Les actions décrites ci-dessus permettront de dresser un profil de risque pour l'organisation. Une fois celui-ci élaboré, l'organisation peut se mettre en devoir de définir les réponses appropriées.

Les mesures de réponse au risque peuvent être subdivisées en quatre catégories. Dans certains cas, le risque peut être *transféré ou toléré, ou nécessiter de mettre un terme à une activité*⁸. Néanmoins, dans la plupart des cas, le risque devra être *traité* et l'organisme devra mettre en œuvre et maintenir un système de contrôle interne efficace afin de le maintenir à un niveau acceptable.

⁸ La meilleure réponse à certains risques peut consister à les *transférer*. Ce transfert peut revêtir la forme d'une assurance conventionnelle, ce qui revient à rémunérer un tiers pour qu'il assume le risque autrement, ou par le biais de clauses contractuelles.

La capacité à remédier à certains risques peut être limitée ou le coût d'une action quelconque disproportionné par rapport au bénéfice potentiel retiré. En pareils cas, la solution peut consister à *tolérer* ces risques.

Certains risques ne pourront être traités ou limités à des niveaux acceptables qu'en *mettant un terme* à l'activité. Dans le secteur public, le choix de mettre un terme à des activités est souvent bien plus limité que dans le secteur privé. En effet, un certain nombre d'activités sont menées dans le secteur public précisément parce que les risques qui y sont liés sont si importants qu'il n'existe pas d'autre moyen de réaliser le produit ou le résultat requis par l'intérêt public.

Le traitement n'a pas nécessairement pour objectif d'éliminer totalement le risque, mais plutôt de le maîtriser. Les procédures mises en place par une organisation en vue de gérer le risque sont appelées activités de contrôle interne. L'évaluation des risques joue un rôle crucial dans la sélection des activités de contrôle appropriées à entreprendre.

Il n'est pas inutile de répéter à ce stade qu'il n'est pas possible d'éliminer tous les risques et que les contrôles internes ne peuvent fournir qu'une assurance raisonnable que les objectifs de l'organisation sont en voie d'être atteints. Toutefois, les organismes qui identifient et maîtrisent activement les risques seront probablement mieux préparés à réagir rapidement en cas de problème et à faire face au changement en général.

Dans le cadre de l'élaboration d'un système de contrôle interne, il est important de veiller à ce que l'activité de contrôle mise en place soit proportionnée au risque. Mis à part les risques dont les conséquences seraient extrêmement préjudiciables à l'organisation, il suffit normalement de mettre au point un contrôle qui offre une assurance raisonnable de limiter les pertes à un niveau jugé acceptable au regard de l'aversion au risque de l'organisation. A chaque contrôle est associé un coût et l'activité de contrôle doit être rentable par rapport au risque qu'elle traite.

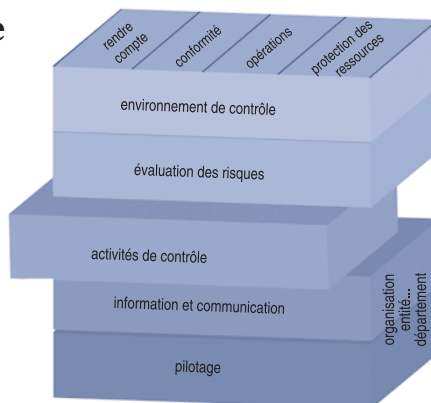
Les données politiques, économiques, industrielles, réglementaires et opérationnelles étant en constante évolution, l'environnement de toute organisation en matière de risque change continuellement et la hiérarchie des objectifs et le poids corrélatif des risques évoluent également. C'est pourquoi il est fondamental que l'évaluation des risques suive un processus itératif et continu de manière à détecter les changements (cycle d'évaluation des risques) et à prendre des mesures correctrices nécessaires. Les profils de risques et les contrôles y afférents doivent être révisés et réexaminés régulièrement pour s'assurer que le profil de risque reste pertinent, que les réponses aux risques restent adéquatement ciblées et proportionnées, et que les contrôles qui visent à atténuer les risques restent efficaces quand les risques eux-mêmes évoluent dans le temps.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.



2.3 Activités de contrôle



Les activités de contrôle correspondent à l'ensemble des politiques et des procédures mises en place pour maîtriser les risques et réaliser les objectifs de l'organisation.

Pour être efficaces, les activités de contrôle doivent être appropriées; fonctionner de manière cohérente, conformément aux plans, tout au long de la période; respecter un équilibre entre coût et bénéfices; être exhaustives, raisonnables et directement liées aux objectifs du contrôle.

Les activités de contrôle sont présentes à travers toute l'organisation, à tous les niveaux et dans toutes les fonctions. Elles englobent toute une série d'activités orientées vers la détection et la prévention, aussi diverses que:

- (1) Des procédures d'autorisation et d'approbation;
- (2) La séparation des fonctions (entre autorisation, traitement, enregistrement, vérification);
- (3) Les contrôles portant sur l'accès aux ressources et aux documents;
- (4) Les vérifications;
- (5) Les réconciliations;
- (6) Les analyses de performance opérationnelle;
- (7) Les analyses d'opérations, de processus et d'activités;
- (8) La supervision (affectation, analyse et approbation, directives et formation).

Les organisations doivent atteindre un équilibre adéquat entre les activités de contrôle orientées vers la détection et celles qui visent la prévention.

Des actions correctives sont un complément indispensable aux activités de contrôle en vue de la réalisation des objectifs.



Les activités de contrôle peuvent se définir comme l'ensemble des politiques et des procédures mises en place pour maîtriser les risques et réaliser les objectifs de l'organisation.

Pour être efficaces, les activités de contrôle doivent répondre à plusieurs critères:

- être appropriées (c'est-à-dire le bon contrôle, au bon endroit et dans une juste proportion par rapport au risque encouru);
- fonctionner conformément aux plans et de manière cohérente tout au long de la période (c'est-à-dire qu'elles doivent être scrupuleusement respectées par tous les agents concernés et qu'elles ne doivent pas être transgressées quand les principaux responsables sont absents ou la charge de travail élevée);
- respecter un équilibre entre coût et bénéfices (c'est-à-dire que le coût de mise en oeuvre du contrôle ne doit pas dépasser les bénéfices qui en sont tirés);
- être exhaustives, raisonnables et directement liées aux objectifs du contrôle.

Les activités de contrôle comprennent un large éventail de politiques et de procédures aussi diverses que:

1. Procédures d'autorisation et d'approbation

Les transactions et autres événements ne peuvent être respectivement autorisés et exécutés que par les personnes qui y sont spécialement habilitées. L'autorisation constitue le principal moyen de garantir que seuls ont lieu des transactions et des événements valides, conformes aux intentions de la direction. Les procédures d'autorisation, qui doivent être documentées et clairement communiquées aux responsables et aux agents, doivent prévoir les conditions et les termes à respecter pour que l'autorisation soit accordée. Le fait de se conformer aux termes d'une autorisation signifie que les agents s'acquittent de leurs fonctions conformément aux lignes directrices et dans les limites tracées par la direction ou par la législation.

2. Séparation des tâches (autorisation, traitement, enregistrement, analyse)

En vue de réduire les risques d'erreurs, de gaspillage ou d'actes illégaux ainsi que le risque de ne pas détecter ces problèmes, aucun individu ou équipe ne doit pouvoir contrôler toutes les étapes clés d'une transaction ou d'un événement. Il faut au contraire veiller à ce que les fonctions et les responsabilités soient systématiquement réparties entre plusieurs



personnes afin de garantir l'efficacité des contrôles et l'existence d'un équilibre des pouvoirs. Parmi ces fonctions clés, on peut retenir l'autorisation et l'enregistrement des transactions, leur traitement, ainsi que l'analyse ou le contrôle des mêmes transactions.

Toutefois la collusion peut réduire voire annihiler l'efficacité de cette technique de contrôle interne. Ne pas disposer de suffisamment de personnel peut empêcher un organisme de petite taille de mettre pleinement en oeuvre cette technique. Dans ces cas, la direction doit être consciente des risques et les compenser par la mise en place d'autres contrôles. La rotation des agents peut contribuer à garantir qu'aucune personne ne traite tous les aspects importants des transactions et des événements pendant une période inconsiderément longue. En outre, et en vue de réduire les risques, l'instauration d'une rotation temporaire des tâches peut être réalisée en encourageant ou même en exigeant de prendre des congés annuels.

3. Contrôle de l'accès aux ressources et aux documents

L'accès aux ressources et aux documents doit être limité aux personnes habilitées, qui ont à répondre de leur garde ou de leur utilisation. Pour rendre compte de la garde, on peut s'appuyer sur l'existence de reçus, inventaires ou tout autre note portant sur cette garde et reprenant le transfert de garde. La restriction de l'accès aux ressources à quelques personnes réduit le risque d'utilisation non autorisée voire de perte pour l'administration et contribue à mettre en oeuvre les lignes directrices de la direction. Le degré nécessaire de restriction variera suivant la vulnérabilité de la ressource à protéger et le niveau perçu du risque de perte ou d'usage impropre, qui doivent être tous deux périodiquement évalués. Pour déterminer la vulnérabilité d'un actif donné, son coût ainsi que la facilité avec laquelle on pourrait le transporter ou l'échanger doivent être étudiés.

4. Vérifications

Les transactions et les événements importants doivent être vérifiés avant et après leur traitement. Par exemple, lorsque des biens sont livrés, le nombre fourni doit être comparé au nombre commandé. Par la suite, le nombre de biens facturés est comparé au nombre effectivement reçu. Le stock peut aussi être contrôlé au moyen de sondages.

5. Réconciliations

Les enregistrements sont comparés régulièrement aux documents appropriés: par exemple, les pièces comptables relatives aux comptes en banque sont comparées aux relevés bancaires correspondants.



6. Analyses de performance opérationnelle

La performance opérationnelle est analysée régulièrement sur la base d'un ensemble de normes permettant de mesurer l'efficacité et l'efficience. S'il ressort du suivi des performances que les réalisations réelles ne rencontrent pas les normes ou objectifs fixés, les processus et activités établis pour atteindre les objectifs doivent être revus pour déterminer quelles améliorations sont nécessaires.

7. Analyses des opérations, des processus et des activités

Les opérations, les processus et les activités doivent être périodiquement analysés pour s'assurer qu'ils sont en accord avec les réglementations, politiques, procédures et autres exigences actuelles. Ce type d'analyse des opérations réalisées effectivement par une organisation est à distinguer clairement du suivi du contrôle interne, lequel est examiné séparément à la section 2.5.

8. Supervision (affectation, analyse et approbation, lignes directrices et formation)

La réalisation des objectifs du contrôle interne suppose également que les superviseurs soient qualifiés. Pour confier un travail à un agent, le vérifier et l'approuver, il est nécessaire de :

- communiquer clairement à chaque membre du personnel les fonctions, les responsabilités et les obligations de rendre compte qui lui sont assignés;
- vérifier systématiquement, au degré qui convient, le travail de chaque membre du personnel;
- approuver le travail à des moments clés pour s'assurer qu'il se déroule comme prévu.

Le fait pour un superviseur de déléguer une partie de ses missions ne l'exonère pas de ses responsabilités et devoirs. Les superviseurs donnent aussi à leurs agents les directives et la formation nécessaires pour réduire au minimum les erreurs, le gaspillage et les actes illégaux et pour veiller à ce que les directives de la direction soient bien comprises et appliquées.

Cette liste n'est pas exhaustive, mais énumère les activités de contrôle les plus courantes orientées vers la prévention et la détection les plus courantes. Les activités de contrôle numérotées de (1) à (3) sont orientées vers la prévention, de (4) à (6), elles sont davantage orientées vers la détection, tandis que celles visées aux points (7) et (8) visent les deux à



la fois. Les organismes doivent atteindre un équilibre adéquat entre les activités de contrôle orientées vers la détection et celles orientées vers la prévention, une combinaison de contrôles étant souvent utilisée à cet égard afin de compenser les inconvénients de chaque contrôle spécifique.

Une fois qu'une activité de contrôle est mise en place, il reste à acquérir des assurances quant à son efficacité. En conséquence, des actions correctives constituent un complément indispensable aux activités de contrôle. En outre, il doit être clair que les activités de contrôle ne constituent qu'un élément du contrôle interne et qu'elles forment un tout avec les quatre autres composantes.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.

2.3.1 Activités de contrôle relatives à la technologie de l'information

Les systèmes d'information impliquent des types d'activités de contrôle spécifiques. Ils se répartissent en deux grandes catégories:

(1) Contrôles globaux

Les contrôles globaux sont constitués à la fois par la structure et par les politiques et procédures applicables à l'ensemble ou un segment important des systèmes d'information d'une organisation et qui contribuent à assurer leur fonctionnement correct. Ils créent l'environnement dans lequel les systèmes applicatifs et les contrôles fonctionnent.

Les principales catégories de contrôles globaux sont: (1) la planification et la gestion du programme de sécurité à l'échelle de l'organisation; (2) les contrôles d'accès; (3) les contrôles portant sur le développement, la maintenance et la modification des applications; (4) le contrôle des logiciels d'exploitation; (5) la séparation des fonctions; (6) les contrôles visant à assurer la continuité du service.

(2) Contrôles applicatifs

Les contrôles applicatifs sont constitués par la structure, les politiques et les procédures applicables à des systèmes d'applications individuels distincts et concernent directement les applications informatisées individuelles. Ces contrôles sont généralement conçus pour prévenir, détecter et corriger les erreurs et les irrégularités affectant le flux des données qui transitent par les systèmes d'information.

Les contrôles globaux et applicatifs sont interdépendants et les deux sont nécessaires pour assurer un traitement exhaustif et correct des données. Les technologies de l'information changeant rapidement, les contrôles dont elles font l'objet doivent eux aussi évoluer constamment pour rester efficaces.

Avec les progrès de la technologie de l'information, les organisations sont devenues de plus en plus dépendantes de systèmes d'information automatisés pour réaliser leurs opérations et pour traiter, conserver et



transmettre des données essentielles. En conséquence, la fiabilité et la sécurité des données informatisées et des systèmes qui traitent, conservent et transmettent ces données sont devenues une préoccupation majeure pour la direction et les auditeurs. Bien que les systèmes d'information impliquent des types spécifiques d'activités de contrôle, la technologie de l'information ne doit pas être envisagée comme un problème isolé de contrôle. Elle fera partie intégrante de la plupart des activités de contrôle.

L'utilisation de systèmes automatisés pour traiter l'information induit de nouveaux risques que l'organisation doit prendre en compte. Ces risques sont liés, notamment, au traitement uniforme des transactions, au déclenchement automatisé de certaines transactions par les systèmes d'information, à la probabilité accrue de survenance d'erreurs non détectées, au degré de traçabilité des opérations, à la nature du matériel et des logiciels utilisés et aux modalités d'enregistrement des transactions inhabituelles ou qui ne suivent pas les routines informatiques habituelles. Par exemple, un risque inhérent au traitement uniforme des transactions réside dans le fait que toute erreur découlant d'une erreur de programmation se produira de la même manière dans des transactions similaires. Grâce à des contrôles efficaces des technologies de l'information, la direction peut acquérir une assurance raisonnable que l'information traitée par ses systèmes répond aux objectifs de contrôle souhaités, tels qu'assurer l'exhaustivité, la ponctualité et la validité des données ainsi que leur l'intégrité.

Les contrôles de la technologie de l'information se répartissent en deux grandes catégories: les contrôles globaux et les contrôles applicatifs.

Contrôles globaux

Les contrôles globaux sont constitués par la structure, la politique et les procédures applicables à l'ensemble ou à un segment important des systèmes d'information d'une organisation – tels que les serveurs, les mini-ordinateurs, le réseau, et l'architecture client-serveur – et qui contribuent à assurer leur fonctionnement correct. Ils créent l'environnement dans lequel les applications et les contrôles fonctionnent.

Les principales catégories de contrôles globaux sont les suivantes:

- (1) *La planification et la gestion du programme de sécurité à l'échelle de l'organisation:* elles fournissent un cadre et un cycle permanent d'activité pour la gestion des risques, le développement de politiques

de sécurité, l'attribution de responsabilités, et la vérification de l'adéquation des contrôles informatisés de l'organisation.

- (2) Les *contrôles d'accès*: ils limitent ou détectent l'accès aux actifs informatiques (données, programmes, équipements et infrastructures), préservant ainsi ces ressources contre toute modification, perte ou divulgation non autorisées. Les contrôles d'accès comprennent à la fois des contrôles physiques et logiques.
- (3) Les *contrôles du développement, de la maintenance et de la modification des applications*: ils empêchent l'introduction non autorisée de programmes nouveaux ou de modifications aux programmes existants.
- (4) Les *contrôles des logiciels*: ils limitent et surveillent l'accès aux programmes puissants et aux fichiers sensibles qui contrôlent le matériel informatique et, sécurisent les applications utilisées dans le système.
- (5) La *séparation des fonctions*: elle implique que les politiques, les procédures et une structure organisationnelle existent pour empêcher qu'une même personne ne puisse contrôler tous les aspects cruciaux d'opérations informatisées et ne procède à des opérations non autorisées ou n'accède sans autorisation aux actifs ou aux enregistrements.
- (6) Les contrôles de la *continuité du service*: ils garantissent qu'en cas de survenance d'un événement inattendu, les opérations de base seront poursuivies sans interruption ou seront reprises promptement, et que les données critiques et vulnérables seront protégées.

Contrôles applicatifs

Les contrôles applicatifs (spécifiques aux applications) sont constitués par la structure, les politiques et les procédures liées à des systèmes d'application individuels distincts – telles que le traitement des dettes fournisseurs, du stock, la gestion des salaires, les procédures de subventions ou de prêts – et sont conçus pour couvrir le traitement des données dans le cadre d'applications informatiques spécifiques.

Ces contrôles sont généralement conçus pour prévenir, détecter et corriger les erreurs et les irrégularités affectant le flux des données qui transitent par les systèmes d'information.

Les contrôles applicatifs et la manière dont les informations transitent par les systèmes d'information peuvent être répartis en trois phases d'un cycle de traitement:



-
- Intrans: les données introduites sont autorisées puis converties dans un format automatisé et introduites dans l'application de manière correcte, exhaustive et en temps voulu.
 - Traitement: les données sont traitées de manière adéquate par l'ordinateur et les fichiers sont correctement mis à jour.
 - Extrans: les fichiers et les rapports générés par l'application concernent des transactions ou des événements qui ont effectivement eu lieu et donnent une image fidèle des résultats du traitement; les rapports sont contrôlés et distribués aux utilisateurs habilités.

Les contrôles applicatifs peuvent également être regroupés en fonction des types d'objectifs de contrôle auxquels ils se rapportent, tels que l'autorisation, l'exhaustivité, l'exactitude et la validité des transactions et des informations. Les contrôles de l'autorisation concernent la validité des transactions et contribuent à garantir qu'elles correspondent à des événements qui ont effectivement eu lieu au cours d'une période donnée. Les contrôles de l'exhaustivité ont trait à la question de savoir si les transactions valides sont toutes enregistrées et correctement classées. Les contrôles de l'exactitude consistent à vérifier si les transactions sont enregistrées correctement et si tous les éléments d'information sont exacts. Toute défaillance des contrôles de l'intégrité du traitement et des fichiers de données pourrait anéantir les effets de tous les contrôles relatifs aux applications précités et permettre que surviennent des transactions non autorisées, ou contribuer à la création de données incomplètes et inexactes.

Les contrôles applicatifs comportent à la fois des techniques de contrôle programmées, telles que l'édition automatisée de rapports, et le suivi manuels d'extrans générés par l'ordinateur comme l'analyse de rapports identifiant des informations rejetées ou inhabituelles).

Interdépendance des contrôles globaux du système d'information et des contrôles applicatifs

L'efficacité des contrôles globaux est déterminante pour l'efficacité des contrôles applicatifs. La faiblesse des contrôles globaux a pour effet de réduire sévèrement la fiabilité des contrôles liés aux applications individuelles. L'absence de contrôles globaux efficaces peut rendre inopérants les contrôles des applications, qui sont alors susceptibles d'être court-circuités, contournés ou modifiés de manière incontrôlée. Ainsi, des contrôles d'édition destinés à empêcher des utilisateurs

d'introduire un nombre d'heures de travail anormal (par exemple, plus de 24 heures de travail en une journée) dans le système de gestion des salaires peuvent en soi constituer un contrôle efficace au niveau d'une application. Mais il est exclu de s'y fier s'il s'avère que les contrôles globaux sont susceptibles de laisser passer des modifications non autorisées du programme de nature à soustraire certaines transactions à ce contrôle des intrants.

Même si les objectifs de base du contrôle ne changent pas, les changements rapides qui affectent les technologies de l'information imposent que les contrôles évoluent de même pour rester efficaces. Des changements tels que la dépendance accrue au travail en réseau, l'arrivée d'ordinateurs puissants qui permettent que la responsabilité du traitement des données soit décentralisée jusqu'aux utilisateurs finaux, le développement du commerce électronique et d'internet ne manqueront sans doute pas d'avoir une incidence tant sur la nature que sur la mise en oeuvre des activités de contrôle propres aux technologies de l'information.

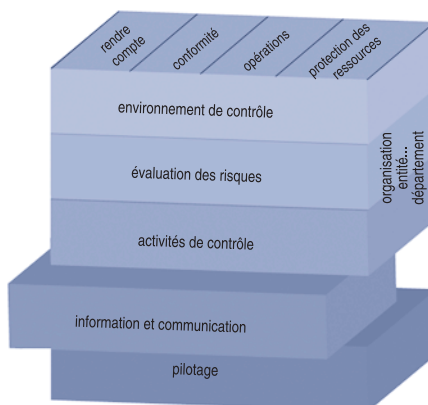
Pour obtenir des conseils complémentaires en ce qui concerne les activités de contrôle applicables aux technologies de l'information, il peut être renvoyé à l'*Information Systems Audit and Control Association* (ISACA ou Association de l'audit et du contrôle des systèmes d'information), au *Control Objectives for Information and related Technology* (COBIT ou Gouvernance, contrôle et audit de l'information et des technologies associées) et aux manières de procéder de la Commission pour le contrôle informatique de l'INTOSAI.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.



2.4 Information et communication



L'information et la communication sont essentielles à la réalisation de l'ensemble des objectifs du contrôle interne.

Information

La première des conditions à l'obtention d'une information susceptible d'être jugée fiable et pertinente réside dans l'enregistrement rapide et le classement convenable des transactions et des événements. L'information pertinente doit être identifiée, recueillie et communiquée sous une forme et dans des délais qui permettent au personnel de procéder aux activités de contrôle interne dont il a la charge et d'assumer ses autres responsabilités (transmettre la bonne information au bon moment aux bonnes personnes). Dès lors, le système de contrôle interne en tant que tel et l'ensemble des transactions et des événements importants que l'organisation peut avoir à gérer doivent faire l'objet d'une documentation complète.

Les systèmes d'information produisent des rapports contenant des informations opérationnelles, financières et non financières, ainsi que des informations liées au respect des obligations légales et réglementaires qui permettent de gérer et de contrôler les activités. Ils traitent non seulement les données produites en interne, mais également l'information liée aux événements externes, aux activités et aux conditions nécessaires à la prise de décisions et à l'établissement de rapports.

La capacité des responsables à prendre les décisions appropriées est conditionnée par la qualité de l'information; il s'agit donc qu'elle soit adéquate, disponible en temps opportun, à jour, exacte et accessible.



L'information et la communication sont essentielles à la réalisation de l'ensemble des objectifs du contrôle interne. Par exemple, l'un de ces objectifs consistant à remplir les obligations de rendre compte publiquement, une manière de l'atteindre peut être d'élaborer et de tenir à jour des informations, financières et non financières, fiables et pertinentes et de les rendre publiques loyalement au travers de rapports publiés en temps opportun. De même, l'information et la communication sur la performance de l'organisation aideront à évaluer le caractère ordonné et éthique, l'économie, l'efficacité et l'efficacité des opérations. Enfin, dans de nombreux cas, ce sont des dispositions légales et réglementaires qui exigent la production de certaines informations ou certaines actions de communication.

L'information est nécessaire à tous les niveaux d'une organisation afin d'assurer un contrôle interne efficace et de réaliser les objectifs de l'organisation, ce qui veut dire que pour que chacun puisse procéder aux activités de contrôle interne dont il a la charge et assumer ses autres responsabilités, un ensemble d'informations pertinentes, fiables et appropriées doivent être identifiées, recueillies et diffusées sous une forme et dans des délais convenables, sachant que la première condition de l'existence d'une information fiable et pertinente tient dans un enregistrement rapide et un classement adéquat des données relatives aux transactions et événements.

Ces derniers doivent en effet être enregistrés sans délai lors de leur survenance afin que l'information conserve sa pertinence et sa valeur pour la direction dans le cadre de ses activités de contrôle des opérations et de prise de décision. Ce principe vaut pour l'ensemble du processus ou cycle de vie d'une transaction ou d'un événement, c'est-à-dire dès qu'ils sont initiés et autorisés jusqu'à ce qu'ils soient consignés dans des rapports de synthèse et classés, en passant par toutes les étapes du traitement. Le même principe implique aussi la mise à jour rapide de toute documentation pour qu'elle garde sa pertinence.

Un autre facteur indispensable pour que la direction soit assurée de disposer d'informations fiables réside dans le classement correct des informations relatives aux transactions et événements. Cela suppose que les informations qui ont vocation à servir de base à la préparation des rapports, des programmes et des états financiers soient organisées, ordonnées par catégorie et présentées suivant un modèle prédéfini.

Les systèmes d'information produisent des rapports contenant des informations opérationnelles, financières et non financières, ainsi que des



informations liées au respect des obligations légales et réglementaires. Toutes sont utiles à la gestion et au contrôle de l'activité. Les systèmes traitent non seulement les données, tant quantitatives que qualitatives, qui sont produites en interne, mais également l'information, liée aux événements, aux activités et aux conditions externes, nécessaire à la prise de décisions et à l'établissement de rapports en pleine connaissance de cause.

La capacité des responsables à prendre les décisions appropriées est tributaire de la qualité de l'information; celle-ci doit donc satisfaire aux critères suivants:

- adéquation (l'information nécessaire est-elle présente ?);
- délai (est-elle disponible en temps voulu ?);
- à jour (est-ce la dernière information en date disponible ?);
- exactitude (est-elle correcte ?);
- accessibilité (peut-elle être obtenue aisément par les parties intéressées ?).

En vue de garantir la qualité de l'information et des rapports, de s'acquitter des activités de contrôle interne et des responsabilités et d'accroître l'efficacité et l'efficience du suivi, le système de contrôle interne en tant que tel et l'ensemble des transactions et des événements importants doivent faire l'objet d'une documentation exhaustive et claire (par exemple, par le biais d'organigrammes et de descriptifs). La documentation existante devra pouvoir être consultée à tout moment.

La documentation du système de contrôle interne doit comprendre l'identification de la structure et des politiques d'une organisation et de ses catégories d'opérations, ainsi que ses objectifs et procédures de contrôle. Toute organisation doit disposer de documents écrits reprenant les composantes du processus de contrôle interne, notamment ses objectifs et ses activités de contrôle.

L'ampleur de la documentation relative au contrôle interne d'une organisation varie, toutefois, en fonction de la taille de l'organisation, de sa complexité et d'autres facteurs du même type.

Communication

Une communication efficace doit circuler de manière ascendante, transversale et descendante dans l'organisation, dans toutes ses composantes et dans l'ensemble de sa structure.



Les plus hauts responsables de l'organisation doivent transmettre un message clair à tous les membres du personnel sur l'importance des responsabilités de chacun en matière de contrôle interne. Tous doivent comprendre le rôle qu'ils sont appelés à jouer dans le système de contrôle interne, ainsi que la manière dont leurs propres activités s'articulent avec celles des autres membres du personnel.

La nécessité d'une communication efficace s'entend également des relations avec l'extérieur de l'organisation.

A la base de la communication se trouve l'information. C'est pourquoi la communication doit répondre aux attentes de groupes et d'individus en leur permettant de s'acquitter efficacement de leurs responsabilités. Une communication efficace doit circuler de manière ascendante, transversale et descendante dans l'organisation, dans toutes ses composantes et dans l'ensemble de sa structure.

L'un des canaux de communication essentiels est celui qui relie la direction à son personnel. La direction doit être tenue au courant de la performance, de l'évolution, des risques et du fonctionnement du contrôle interne, ainsi que de tous les autres événements et problèmes pertinents. Par le même canal, la direction signale à son personnel les informations dont elle a besoin, lui renvoie son appréciation sur ses activités et lui fait connaître ses consignes. Elle doit également assurer une communication spécifique et ciblée sur les comportements qu'elle souhaite le voir adopter. Il doit en résulter une déclaration claire sur la philosophie et l'approche de l'organisation en matière de contrôle interne, ainsi que des délégations de pouvoir explicites.

La communication doit sensibiliser le personnel à l'importance et à l'utilité d'un contrôle interne efficace, faire connaître le degré d'aversion au risque de l'organisation et son degré de tolérance au risque et rendre le personnel conscient de son rôle et de ses responsabilités dans la mise en œuvre et le support à apporter aux composantes du contrôle interne.

Outre la communication interne, la direction doit assurer l'existence de moyens de communication adéquats avec les interlocuteurs externes et recueillir des informations de ces interlocuteurs, étant donné que la communication externe peut fournir une information susceptible d'avoir un impact sur la réalisation, par l'organisation, de ses objectifs.

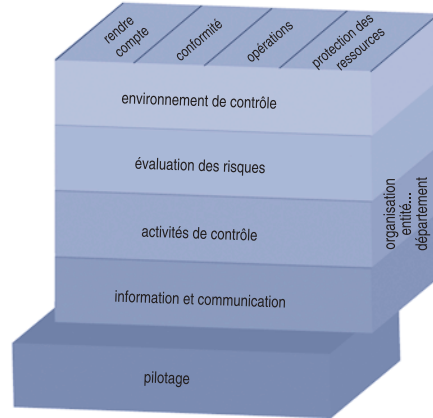


En se basant sur les données provenant de la communication à la fois interne et externe, le management doit prendre les actions nécessaires et entreprendre à temps des opérations de suivi.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.

2.5 Pilotage



Les systèmes de contrôle interne doivent faire l'objet d'un suivi destiné à en vérifier la qualité 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.

(1) Pilotage permanent

Le pilotage ou le suivi permanent du contrôle interne s'inscrit dans le cadre des activités d'exploitation courantes et récurrentes d'une organisation et comprend des contrôles réguliers effectués par la direction et le personnel d'encadrement, ainsi que d'autres actions effectuées par le personnel dans le cadre même des tâches qu'il a à accomplir.

Les activités de pilotage permanent portent sur chacune des composantes du contrôle interne et tend à empêcher que les systèmes de contrôle interne fonctionnent de manière contraire aux règles, à l'éthique ou aux critères d'économie, d'efficacité et d'efficacité.

(2) Evaluations ponctuelles

Les évaluations ponctuelles varieront en étendue et en fréquence essentiellement en fonction de l'évaluation des risques et de l'efficacité des procédures de pilotage permanent.

Les évaluations ponctuelles spécifiques portent sur l'efficacité du système de contrôle interne et garantissent que le contrôle interne atteint les résultats attendus sur la base de méthodes et procédures



prédéfinies. Les faiblesses du contrôle interne doivent être signalées au niveau approprié de direction.

Les procédures de suivi doivent garantir que les conclusions d'audit et les recommandations qui en résultent sont mises en œuvre de manière appropriée et sans retard.

Le suivi du contrôle interne garantit que les contrôles fonctionnent comme prévu et qu'ils sont mis à jour en fonction de l'évolution de l'environnement dans lequel opère l'organisation. Le suivi doit aussi évaluer si, dans la réalisation de la mission de l'organisation, les objectifs généraux, repris dans la définition du contrôle interne, ont été atteints. Pour cela, il convient de mettre en place un ensemble d'activités permanentes de pilotage, des évaluations ponctuelles ou de combiner les deux méthodes, afin d'assurer que le contrôle interne continue à s'appliquer à tous les niveaux et dans toute l'organisation et qu'il produit les résultats escomptés. Le suivi des activités de contrôle interne doit être clairement distingué de l'analyse des opérations d'une organisation, qui constitue, quant à elle, une activité de contrôle interne. Cette catégorie a été examinée au point 2.3.

Le pilotage permanent du contrôle interne s'inscrit dans le cadre des opérations courantes et récurrentes d'une organisation. Il s'opère en continu et en temps réel, réagit en direct à l'évolution de la situation et se trouve comme tissé dans les opérations de l'organisation. Dès lors, il est plus efficace que les évaluations ponctuelles et les actions correctives sont potentiellement moins coûteuses. Les évaluations ponctuelles étant effectuées a posteriori, les opérations courantes de surveillance permettront souvent une détection plus rapide des problèmes.

Les évaluations ponctuelles doivent varier en étendue et en fréquence essentiellement en fonction de l'évaluation des risques et de l'efficacité des procédures de pilotage permanent. A cet égard, l'organisation doit prendre en compte la nature et l'importance des changements occasionnés, tant par les événements internes qu'externes, ainsi que les risques correspondants, les compétences et l'expérience du personnel chargé de la mise en œuvre des contrôles, de même que les résultats du pilotage permanent. Les évaluations ponctuelles du contrôle peuvent aussi s'avérer utiles du fait qu'elles se focalisent sur l'efficacité des contrôles à un moment précis. Les évaluations ponctuelles peuvent revêtir la forme d'auto-évaluations, comme l'analyse de la conception du contrôle

ou la réalisation de tests portant directement sur le contrôle interne. Les évaluations ponctuelles peuvent aussi être réalisées par les ISC ou par des auditeurs externes ou internes.

En général, la combinaison du suivi permanent et des évaluations ponctuelles permettra d'assurer que le système de contrôle interne conserve son efficacité dans le temps.

Toutes les faiblesses décelées dans le cadre du suivi permanent ou à la suite d'évaluations ponctuelles doivent être signalées aux personnes habilitées à prendre les mesures nécessaires. Le terme «faiblesse» définit un état susceptible d'avoir une incidence sur la capacité d'une organisation à réaliser ses objectifs généraux. Une faiblesse peut, dès lors, correspondre à une carence perçue, potentielle ou avérée, ou à une opportunité de renforcer le contrôle interne afin d'accroître la probabilité d'atteindre les objectifs généraux de l'organisation.

Il est crucial de communiquer les informations nécessaires relatives aux faiblesses du contrôle interne aux personnes concernées. Dans cette perspective, il est nécessaire d'établir des règles définissant quelles sont les informations nécessaires à un niveau donné pour permettre la prise effective de décisions. De telles règles sont fondées sur le principe général qu'un responsable doit être au courant de ce qui a une incidence sur les actions ou le comportement des personnes placées sous sa responsabilité, de même qu'il doit être en possession de toute information liée à la réalisation de ses objectifs spécifiques.

Les informations produites par l'organisation dans le cadre de ses activités circulent généralement le long des circuits habituels de communication, et parviennent donc au moins jusqu'à la personne responsable de la fonction concernée et à son supérieur hiérarchique direct. Toutefois, des voies de communication alternatives doivent être prévues pour permettre la transmission des informations sensibles, telles que celles qui portent sur des agissements incorrects ou illégaux.

Le suivi et le pilotage du contrôle interne doivent comprendre des politiques et des procédures garantissant que les conclusions des audits et des autres formes d'évaluation sont mises en œuvre de la manière appropriée et sans retard. Les responsables doivent (1) évaluer rapidement les conclusions des audits et des autres formes d'évaluation, y compris quand les auditeurs ou les autres personnes mandatées pour évaluer les activités de l'organisme diagnostiquent des faiblesses et



émettent des recommandations, (2) déterminer les mesures appropriées à prendre pour donner suite aux conclusions et aux recommandations résultant des audits et des analyses et (3) prendre, dans des délais prédéfinis, toutes les mesures visant à corriger les défauts portés à leur attention ou à résoudre le problème qui en découlait.

Le processus de résolution commence dès que les résultats d'audit ou de toute autre analyse sont communiqués à la direction et ne s'achève qu'après l'adoption d'une mesure qui (1) porte remède aux faiblesses identifiées, (2) apporte des améliorations ou (3) démontre que les conclusions et les recommandations de l'évaluation ne justifient pas que la direction prenne des mesures.

Exemples

Nous renvoyons le lecteur aux annexes pour des exemples intégrés concernant chacun des objectifs et des composantes du contrôle interne.

3 *Rôles et responsabilités*

Chacun, au sein d'une organisation, a une part de responsabilité dans le contrôle interne.

Le management est directement responsable de l'ensemble des activités de l'organisation, ce qui inclut la conception, la mise en oeuvre, le fonctionnement adéquat, le maintien et la documentation du système de contrôle interne. Les responsabilités de chacun au sein du management varient selon la fonction qu'il occupe dans l'organisation et les caractéristiques de l'organisation elle-même.

Les auditeurs internes examinent et contribuent à l'efficacité continue du système de contrôle interne via leurs évaluations et recommandations et de ce fait jouent un rôle important dans l'efficacité du contrôle interne. Ils n'assument toutefois pas la responsabilité de base, qui revient à la direction, de la conception, la mise en oeuvre, le maintien et la documentation du contrôle interne.

Les membres du personnel contribuent eux aussi au contrôle interne. Le contrôle interne relève, explicitement ou implicitement, de la responsabilité de chacun. Tous les membres du personnel jouent un rôle dans la réalisation du contrôle interne et sont tenus de communiquer tout problème qu'ils viendraient à constater dans la conduite des opérations, de même que toute violation du code de conduite ou à la politique interne de l'organisation.



Certaines parties externes jouent aussi un rôle important dans le processus de contrôle interne. Ils peuvent contribuer à la réalisation des objectifs de l'organisation ou fournir des informations utiles au contrôle interne. Ils ne sont toutefois pas responsables de la conception, la mise en oeuvre, le fonctionnement adéquat, la maintenance ou la documentation du système de contrôle interne de l'organisation.

Les institutions supérieures de contrôle (ISC) encouragent et favorisent la mise en place d'un système de contrôle interne efficace dans l'administration. L'évaluation du contrôle interne est essentielle pour les audits de conformité, financiers et de performance réalisés par les ISC. Elles communiquent leurs conclusions et leurs recommandations aux parties intéressées.

Les auditeurs externes sont en charge de l'audit de certaines administrations dans certains pays. Ils sont appelés, de même que les associations professionnelles qui les représentent, à formuler des conseils et des recommandations au sujet du contrôle interne.

Le pouvoir législatif et réglementaire établissent des règles et des lignes directrices en matière de contrôle interne. Ils doivent contribuer à une compréhension commune du contrôle interne.

Les autres tiers sont en interaction avec l'organisation (usagers, fournisseurs, etc.) et fournissent des informations quant à la réalisation de ses objectifs.

Le contrôle interne est avant tout le fait des parties prenantes internes de l'organisation, ce qui inclut à la fois les responsables, les auditeurs internes et les autres membres du personnel. Toutefois, les actions de parties prenantes externes peuvent aussi avoir une influence sur le système de contrôle interne.



Les managers

L'ensemble du personnel de l'organisation joue un rôle important dans la mise en oeuvre du système de contrôle interne. C'est, toutefois, à la direction qu'incombe la responsabilité globale de la conception, de la mise en oeuvre, du bon fonctionnement et de la maintenance du système de contrôle interne, ainsi que de sa documentation. Ce que nous dénommons ici «management» peut inclure le conseil d'administration et le comité d'audit, dont les rôles et les compositions varient d'un pays à l'autre et qui, d'un pays à l'autre, sont soumis à des législations différentes.

Les auditeurs internes

Il n'est pas rare que la direction mette en place une unité d'audit interne qu'elle conçoit comme faisant partie intégrante de son système de contrôle interne et qu'elle utilise dans le cadre du suivi et du pilotage de l'efficacité du système de contrôle interne. Les auditeurs internes fournissent de manière régulière de l'information sur le fonctionnement du contrôle interne en se concentrant, avec une attention particulière, sur l'évaluation de la conception et des opérations du contrôle interne. Ils communiquent de l'information sur les forces et les faiblesses du contrôle interne et formulent des recommandations en vue de son amélioration. Leur indépendance et leur objectivité doivent toutefois être garanties.

Par conséquent, l'audit interne devrait être une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide une organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise et en faisant des propositions pour renforcer leur efficacité.

Pour autant, et même si les auditeurs internes jouent un rôle précieux en termes de formation et de conseil en matière de contrôle interne, ils ne sauraient remplacer à eux seuls une structure de contrôle interne solide.

Pour que la fonction d'audit interne soit efficace, il est essentiel que l'équipe d'audit interne soit indépendante de la direction, travaille de manière impartiale, correcte et honnête et qu'elle rende compte



directement au niveau hiérarchique le plus élevé de l'organisation. De la sorte, les auditeurs internes peuvent présenter des avis impartiaux sur l'évaluation du système de contrôle interne et présenter objectivement des propositions visant à corriger les défauts qu'ils auront découverts. Pour ce qui est des directives professionnelles, les auditeurs internes doivent utiliser le référentiel de pratiques professionnelles de l'Institut des auditeurs internes (*Professional Practices Framework* (PPF) – *Institute of Internal Auditors* (IIA) ou Institut français de l'audit et du contrôle internes (IFACI) affilié à l'IIA) qui inclut la définition de l'activité d'audit interne, le code de déontologie, les normes et des conseils pratiques. En outre, les auditeurs internes doivent suivre le code de déontologie de l'INTOSAI.

Outre son rôle de suivi des contrôles internes d'une organisation, une équipe d'audit interne qualifiée peut contribuer à l'efficacité des activités d'audit externe en apportant une assistance directe à l'auditeur externe. La nature, l'étendue ou la durée des procédures d'audit externe pourront ainsi faire l'objet d'aménagements si l'auditeur externe peut s'appuyer sur le travail de l'auditeur interne.

Les membres du personnel

Le reste du personnel, quel que soit son niveau, influe également sur le contrôle interne. Ce sont souvent ceux qui sont placés en première ligne qui appliquent et supervisent certains contrôles, les analysent et prennent les mesures correctives nécessaires si les contrôles sont mal mis en œuvre; par ailleurs, ils sont bien placés pour identifier dans le cours de leurs activités quotidiennes des problèmes qui appellent des réponses qui sont de l'ordre du contrôle interne.

Les parties externes

Le second groupe majeur de partenaires du contrôle interne est constitué par des tiers extérieurs, tels que les auditeurs externes (notamment les ISC), le pouvoir législatif et réglementaire, ainsi que d'autres tiers. Tous peuvent contribuer à la réalisation des objectifs de l'organisation ou fournir des informations utiles à la mise en œuvre du contrôle interne. Cependant, ils n'ont aucune responsabilité dans la conception, la mise en œuvre, le fonctionnement adéquat, la maintenance ou la documentation du système de contrôle interne de l'organisation.



ISC et auditeurs externes

Les missions des parties externes, et plus particulièrement celles des auditeurs externes et des ISC, comprennent l'évaluation du fonctionnement du système de contrôle interne et la transmission de leurs conclusions au management de l'organisation audité. L'examen du système de contrôle interne par les parties externes est toutefois déterminé en fonction de leur mandat.

L'évaluation des procédures de contrôle interne par les auditeurs passe par les étapes suivantes :

- déterminer l'importance du risque et le degré de sensibilité au risque du programme dont les contrôles sont évalués;
- évaluer le risque d'utilisation abusive des ressources, de non-réalisation des objectifs en matière d'éthique, d'économie, d'efficacité et d'efficacités, de non-respect des obligations de rendre compte et de non-conformité aux lois et règlements;
- identifier et comprendre les contrôles pertinents;
- faire le point sur ce que l'on sait déjà de l'efficacité du contrôle;
- apprécier le caractère adéquat de la conception du contrôle;
- déterminer par des tests si les contrôles sont efficaces;
- rendre compte de l'appréciation qu'ils portent sur le contrôle interne et discuter les mesures correctives nécessaires.

L'ISC a également tout intérêt à veiller à ce que des services d'audit interne solides existent là où ils sont nécessaires. Ces services d'audit constituent un élément important du contrôle interne, car elles sont un vecteur permanent d'amélioration de la manière dont les activités d'une organisation sont conduites. Dans certains pays, cependant, les services d'audit interne peuvent souffrir d'un manque d'indépendance, être faibles, quand ils ne sont pas purement et simplement inexistant. Dans ces cas, l'ISC doit, autant que possible, proposer aide et accompagnement en vue de leur mise en place et de leur développement, et contribuer à garantir l'indépendance des activités de l'auditeur interne. Cette assistance pourrait passer par des détachements ou des prêts de personnel, l'organisation de conférences, la mise en commun de supports de formation et l'élaboration de méthodologies et de programmes de travail. Cela doit toutefois être réalisé sans menacer l'indépendance de l'ISC ou de l'auditeur externe.

Il est également nécessaire que l'ISC puisse développer de bonnes relations de travail avec les services d'audit interne en vue de permettre



un échange d'expériences et de connaissances et l'émergence de synergies et de complémentarités dans le travail. Le fait d'intégrer, le cas échéant, les observations de l'audit interne dans le rapport de l'audit externe et de reconnaître l'importance de sa contribution peut favoriser l'instauration d'une telle relation. L'ISC doit concevoir des procédures d'évaluation du travail du service d'audit interne pour savoir dans quelle mesure il est possible de s'en servir. La présence d'un service d'audit interne solide peut réduire l'ampleur du travail de vérification à opérer par l'ISC et ainsi limiter les doubles emplois inutiles. Cela suppose que l'ISC puisse accéder aux rapports de l'audit interne, à ses documents de travail et aux informations relatives aux conclusions de l'audit.

Les ISC doivent aussi jouer un rôle moteur pour l'ensemble du secteur public en mettant en place un système de contrôle interne pour leur propre organisation, conforme aux principes des présentes lignes directrices.

Non seulement les ISC mais aussi les auditeurs externes jouent un rôle important en contribuant à la réalisation des objectifs du contrôle interne, en particulier en ce qui concerne le respect des obligations de rendre compte et la protection des ressources. Les audits externes des rapports et informations financières font en effet partie intégrante de l'obligation de rendre compte et de la bonne gouvernance. Les audits externes constituent encore un mécanisme de base que les parties prenantes externes utilisent pour suivre la performance, à côté des informations non financières.

Le pouvoir législatif et réglementaire

Enfin, la contribution du pouvoir législatif et réglementaire au contrôle interne peut contribuer à favoriser une compréhension commune de la définition du contrôle interne et des objectifs à atteindre. Ils peuvent aussi édicter les politiques auxquelles les acteurs internes et externes sont tenus de se conformer dans l'exercice de leurs rôles et responsabilités respectifs en matière de contrôle interne.

Annexe 1 Exemples



Exemple de pratique mise en place en vue du respect de l'obligation de rendre compte (1) : un service chargé d'assurer la sécurité du transport par voies fluviales et maritimes a été mis en place par différents départements responsables respectivement du pilotage, du balisage, de l'inspection de la qualité des eaux, de la promotion de l'utilisation des voies navigables, des investissements dans les infrastructures (ponts, digues, canaux et écluses) et de la maintenance de celles-ci.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|--|---|--|--|--|
| <p>Pour chaque département, il est désigné un responsable opérationnel tenu de faire rapport au directeur général du département. Les cadres opérationnels possèdent les aptitudes requises et sont habilités à prendre certaines décisions. Tous ont également signé un code de bonne conduite.</p> | <p>Les risques possibles sont les collisions entre navires, la perte de déchets toxiques ou de carburant et la rupture de digues. Au cas où la réalisation de l'un de ces risques serait imputable à la négligence des pouvoirs publics, leur responsabilité serait engagée dans des proportions énormes.</p> | <p>Les activités de contrôle suivantes peuvent être organisées : faire piloter les navires par des pilotes compétents, placer des bouées, des balises et des repères, mettre en place un dispositif de surveillance aérienne, prélever des échantillons d'eau.</p> | <p>L'information et la communication dans cette situation peuvent être les suivantes : signaler les collisions afin d'avertir les autres navires, informer les navires sur les conditions météorologiques, publier le nom des pollueurs et les sanctions auxquelles ils s'exposent, ainsi que les mesures engagées en vue de réparer les dommages qu'ils ont causés.</p> | <p>Un suivi du nombre de collisions, des infractions au droit de l'environnement, des résultats des prélèvements et une comparaison avec d'autres pays et avec des données historiques peuvent contribuer à surveiller l'efficacité et l'efficacité du pilotage des navires, du placement de balises et de repères, des inspections et du contrôle de la qualité des eaux.</p> |





Exemple de pratique mise en place en vue du respect de l'obligation de rendre compte (2) : le responsable du département des sports a annoncé, l'année dernière, que l'objectif était d'augmenter la pratique sportive de 15 % dans les prochaines années.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|--|---|--|--|---|
| <p>Le responsable jouissant d'une bonne réputation, le comité exécutif lui a fait confiance et n'a pas jugé utile d'organiser les réunions de suivi qu'il est ordinairement d'usage de tenir pour contrôler les progrès réalisés par le responsable.</p> <p>(La situation susmentionnée ne constitue pas un exemple de bonne pratique !)</p> | <p>Ne pas préciser les objectifs peut entraîner le risque de ne pas les atteindre. Un autre risque est que le rapport ne soit pas prêt en temps voulu, le responsable préférant attendre pour l'établir d'être en mesure d'annoncer qu'il a atteint son objectif de 15 % de croissance. Enfin, rien n'a été spécifié quant aux modalités de calcul de la croissance de la pratique sportive, de sorte que le responsable peut à sa guise choisir de déclarer que le nombre de pratiquants, d'heures de pratique ou de centres ou clubs sportifs a augmenté de 15 %. La qualité des informations publiées s'en trouve significativement altérée.</p> | <p>Ce risque peut être réduit en prévoyant des canaux d'information appropriés et un modèle de rapport définissant les informations à fournir.</p> | <p>Ce rapport doit être remis à temps et respecter le modèle préalablement défini. Il doit préciser les objectifs de croissance, les modalités de mesure des objectifs et les raisons pour lesquelles elles ont été définies ainsi. Toutes les pièces justificatives doivent être disponibles.</p> | <p>Une forme de suivi pourrait consister à vérifier si le rapport est satisfaisant ou non, à faire l'inventaire des informations qui y figurent et de celles qui manquent encore.</p> |

Exemple de pratique tendant à assurer la conformité des opérations aux lois et réglementations en vigueur : le ministère de la Défense souhaite acquérir de nouveaux avions de chasse par le biais d'un marché public et publie toutes les clauses et procédures afférentes à cet appel d'offres. Toutes les offres reçues restent fermées jusqu'à l'expiration du délai d'introduction des offres. Ce n'est qu'à ce moment qu'elles sont ouvertes, en présence des responsables compétents et de fonctionnaires. Ces offres seront les seules à être examinées et comparées pour décider laquelle est la meilleure.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|---|--|---|---|---|
| <p>L'équipe qui gèrera la passation de ce marché est composée de personnes compétentes qui ont signé un document par lequel elles certifient n'avoir aucun lien financier ou relationnel avec aucun des soumissionnaires. Les responsables et fonctionnaires ont également signé ce document.</p> | <p>L'un des risques liés aux appels d'offres publics et aux marchés publics est le délit d'initiés. L'un des soumissionnaires peut avoir connaissance préalablement des offres de ses concurrents et, fort de cette information, introduire une offre gagnante, faussant le choix des décideurs qui se trouvent orientés vers une proposition qui n'est en fait pas la meilleure. Un autre risque serait que les décideurs fassent le mauvais choix, ce qui les obligerait à passer un nouveau marché public pour compenser le fait que le premier n'ait pas répondu aux attentes. En outre, il pourrait aussi arriver que d'autres soumissionnaires, s'estimant victimes d'une inégalité de traitement, introduisent une réclamation.</p> | <p>Afin de réduire les risques, des procédures doivent être élaborées et appliquées conformément aux lois et règlements pertinents régissant les marchés publics.</p> | <p>Les procédures relatives à la publication de toutes les clauses de cet appel d'offres public, l'évaluation des offres reçues et l'annonce du soumissionnaire retenu doivent être décrites par écrit, en prenant soin de détailler toutes les étapes à respecter. Lors de la phase d'évaluation, toutes les raisons pour lesquelles l'offre d'un soumissionnaire donné a ou n'a pas été sélectionnée doivent être consignées par écrit.</p> | <p>L'audit interne peut procéder à des analyses sur dossier et assurer un suivi des réclamations.</p> |





Exemple d'actions ordonnées, éthiques, économiques, efficaces et efficaces (1) : le ministère de la Culture souhaite accroître la fréquentation des musées. Dans cette optique, il propose la construction de nouveaux musées, l'octroi à chaque citoyen d'un « chèque-culture » et l'abaissement du prix des billets d'entrée. Pour s'assurer que ces actions respectent les critères d'économie, d'efficacité et d'efficacité, les responsables doivent déterminer si les objectifs qu'ils ont formulés sont susceptibles d'être atteints grâce à ces propositions et évaluer le coût de chacune d'entre elles.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|--|--|---|---|---|
| <p>Le ministère doit vérifier que sa structure organisationnelle permet d'assurer la supervision de la conception et de la construction des nouveaux bâtiments proposés, et d'organiser la programmation et le fonctionnement des nouveaux musées.</p> | <p>L'un des risques potentiels est que la fréquentation des musées n'augmente pas. De même, il est à craindre que certaines des propositions ne donnent pas les résultats attendus et dépassent les limites de leur budget. Par exemple, si la diminution du prix des billets d'entrée n'a pas une incidence positive sur la fréquentation des musées, cette initiative se traduira par une baisse des recettes de l'Etat. Autre exemple : construire de nouveaux musées sans respecter un planning approprié ni prendre en compte les impératifs de luminosité, de température ou de sécurité, peut entraîner un certain nombre d'ajustements onéreux pendant ou après la construction.</p> | <p>Les activités de contrôle liées aux risques susmentionnés peuvent consister en un contrôle budgétaire comparant les données réelles aux données budgétées, dans la formulation d'observations sur l'état d'avancement des travaux de construction et de demandes de justification en cas de dépassement de budget.</p> | <p>L'information et la communication relatives au présent cas peuvent consister en une documentation sur les réunions organisées avec les architectes, les services de lutte contre l'incendie (concernant les règles de sécurité), les artistes et des tierces personnes. Elles peuvent aussi inclure différents rapports sur le suivi de l'exécution du budget et l'avancement des travaux de construction.</p> | <p>L'analyse des justifications de dépassement de budget et des charges d'intérêt liées à des retards dans les travaux ou les paiements fait partie des activités de suivi à mettre en place dans pareille situation.</p> |

Exemple d'activités ordonnées, éthiques, économiques, efficaces et efficaces (2) : le gouvernement entend développer l'agriculture et améliorer la qualité de la vie à la campagne. Il débloque des fonds destinés à l'octroi de subventions afin d'encourager la construction d'installations d'irrigation et le forage de puits.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|--|--|--|--|---|
| <p>Le gouvernement doit identifier le département sur lequel il pourra compter pour mettre en oeuvre et mener à bien la politique d'aides publiques, et créer les conditions appropriées pour réaliser ce projet à temps et avec efficacité.</p> | <p>Le risque réside dans le fait que des associations peu scrupuleuses prétendent à l'octroi d'une subvention, l'obtention et n'utilisent pas les fonds alloués dans le but prévu.</p> | <p>Les activités de contrôle peuvent être les suivantes :</p> <ul style="list-style-type: none"> - vérifier les compétences des associations sollicitant l'octroi d'une subvention. - vérifier sur place l'état d'avancement des travaux de construction et analyser les rapports qui s'y rapportent. - contrôler les dépenses exposées par les associations en passant en revue les factures qu'elles produisent et différer le paiement de tout ou partie de la subvention jusqu'au complet achèvement de cette vérification. | <ul style="list-style-type: none"> - Rapports sur l'état d'avancement des travaux détaillant le coût et le nombre de puits forés, ainsi que le nombre d'hectares irrigués. - Demande de production de (copies de) factures justifiant les dépenses subventionnées. | <p>Le pilotage peut consister dans le suivi du forage des puits et de la construction d'installations d'irrigation, et leur comparaison avec des projets similaires.</p> <p>Une autre méthode peut résider dans le suivi des revenus produits par la culture des terres nouvellement irriguées.</p> |





Exemple de pratique visant à protéger les ressources (1) : le ministère de la Défense possède quelques entrepôts, magasins militaires et dépôts de carburant. L'état-major militaire a pour politique que ces fournitures soient strictement réservées à un usage militaire et de n'en autoriser en aucun cas une utilisation privée.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|---|--|---|--|--|
| Une politique efficace de gestion des ressources humaines consisterait à recruter et à fidéliser le personnel le plus qualifié pour faire fonctionner et gérer les entrepôts. | Le risque est réel que des personnes cherchent à voler des armes pour les utiliser à mauvais escient ou les vendre. De même, d'autres fournitures, tel que le carburant, risquent d'être volées. | Les activités de contrôle destinées à répondre à ces risques peuvent consister à ériger des clôtures ou des murs autour des magasins et des dépôts. On peut compléter le dispositif en plaçant des maîtres-chiens armés à l'entrée. La vérification régulière du stock et une procédure qui prévoit que les livraisons ne peuvent avoir lieu qu'avec l'accord d'un officier de rang supérieur contribueront également à la protection des actifs. | Etablissement de rapports si des clôtures viennent à être endommagées ou si l'inventaire révèle des écarts par rapport à l'état théorique du stock. Les autorisations et les procédures relatives aux approvisionnements sont des sources d'information et de communication utiles dans le cadre de la réalisation de l'objectif de protection des ressources. | Le pilotage et le suivi peuvent passer par l'inspection des clôtures, l'organisation d'inventaires imprévisibles, le suivi des stocks, voire par l'organisation d'un test secret de la sécurité. |

Exemple de pratique visant à protéger les ressources (2): De grandes quantités d'informations sensibles sont stockées sur des supports informatisés confiés à la garde d'une agence qui relève du ministère de la Justice. Toutefois, l'importance des contrôles informatiques est négligée et, par conséquent, le contrôle interne des systèmes d'information présente de nombreuses déficiences.

| Environnement de contrôle | Evaluation des risques | Activités de contrôle | Information & Communication | Pilotage |
|--|---|---|---|---|
| <p>La direction doit prendre nettement position pour encourager le développement des compétences et d'un comportement approprié dans le domaine de l'informatique, et veiller à ce que le personnel reçoive une formation adéquate. De manière générale, la politique de ressources humaines joue un rôle essentiel dans l'instauration d'un environnement de contrôle positif pour les questions informatiques.</p> | <p>Au niveau des contrôles globaux, l'agence n'a pas:</p> <ul style="list-style-type: none"> - limité l'accès des utilisateurs aux seuls domaines strictement nécessaires à l'accomplissement de leurs tâches; - mis au point des contrôles adéquats des systèmes logiciels afin de protéger les programmes et les données sensibles; - conservé la trace des changements de logiciel; - séparé les fonctions incompatibles; - veillé à la continuité du service; - protégé son réseau contre le trafic non autorisé. <p>Au niveau des contrôles applicatifs, l'agence ne s'est pas préoccupée du système des autorisations d'accès.</p> <p>(Ceci ne constitue pas un exemple de bonne pratique!)</p> | <p>Le service peut prendre les mesures suivantes:</p> <ul style="list-style-type: none"> - mettre en œuvre des contrôles d'accès logiques (par exemple, mots de passe) et physiques (par exemple, verrous, badges d'identification, alarmes). - définir un mécanisme visant à interdire l'accès au système d'exploitation aux simples utilisateurs de l'application; - limiter l'accès à l'environnement de production au personnel chargé de développer les applications; - utiliser les journaux d'audit pour enregistrer tous les accès ou simples tentatives d'accès et autres commandes afin de détecter les atteintes aux systèmes de sécurité. - élaborer un plan de sauvegarde et un plan d'urgence pour garantir la disponibilité de ressources essentielles et contribuer à la continuité des opérations. - installer des pare-feu informatiques et surveiller le serveur de manière à sécuriser le réseau. | <p>Commander un audit des systèmes d'information, faire un exercice de simulation de désastre et surveiller l'activité du serveur peuvent contribuer au suivi et au pilotage de l'environnement informatique.</p> | <p>L'analyse des justifications de dépassement de budget et des charges d'intérêt liées à des retards dans les travaux ou les paiements fait partie des activités de suivi à mettre en place dans pareille situation.</p> |



Annexe 2 Glossaire



Le présent glossaire est destiné à faciliter une compréhension commune des principaux termes utilisés dans les présentes directives en ce qui concerne les définitions et la pratique du contrôle interne.

En plus des définitions que nous avons introduites dans le présent document, nous nous référons à des définitions existantes, extraites des sources suivantes :

- *Code de déontologie et normes de contrôle*, INTOSAI, 2001 (Normes de contrôle de l'INTOSAI)
- *Internal Control – Integrated Framework*, COSO, 1992 (COSO 1992)
- *Glossaire*, Office des publications officielles des Communautés européennes, P. Everard et D. Wolter, 1989 (Glossaire)
- *Auditing And Assurance Services, An Integrated Approach*, A. A. Arens, R. J. Elder et M. S. Beasley, Prentice Hall international edition, neuvième édition, 2003 (Arens, Elder & Beasley)
- *Projet d'exposé du COSO Enterprise Risk Management Framework*, COSO, 2003 (COSO ERM)
- *Handbook Of International Auditing, Assurance, And Ethics Pronouncements*, IFAC, 2003 (IFAC)
- *Transparency International Source Book 2000* (Transparency International)
- XVI^e INCOSAI, Montevideo, Uruguay, 1998, *Exposé principal relatif au thème 1A (Prévention et détection de la fraude et de la corruption)*, février 1997 (XVI^e INCOSAI, Uruguay, 1998)
- *Referentiel de pratiques professionnelles*, Institut des Auditeurs internes (*Professional Practices Framework (PPF)*) – Institute of Internal Auditors (IIA) ou Institut Français de l'Audit et du Contrôle Internes (IFACI) affilié à l'IIA)

A

Accès logique

Le fait de pouvoir accéder aux données informatiques. L'accès peut être limité à la «lecture seule»; des droits d'accès plus étendus comportent l'autorisation de modifier les données, de créer de nouveaux fichiers et d'effacer les fichiers existants. (voir aussi accès physique)

Accès physique

S'emploie en matière de contrôle d'accès pour désigner le fait de pouvoir accéder aux locaux et entités physiques. (voir accès logique)

Activité de contrôle

Les activités de contrôle sont les politiques et les procédures mises en place pour maîtriser les risques et réaliser les objectifs de l'organisation. Les procédures

mises en place par une organisation pour maîtriser les risques sont appelées activités de contrôle interne. Les activités de contrôle interne constituent une réponse au risque du fait qu'elles sont conçues pour réduire l'incertitude du résultat préalablement identifiée.

Activités

Voir Opérations

Application

Programme informatique conçu pour faciliter un certain type de travail et par exemple apporter une assistance dans l'exécution de fonctions spécifiques, telles que le paiement des salaires, le suivi des stocks, la comptabilité et les activités de support. En fonction de l'activité pour laquelle elle est conçue, une application peut traiter du texte, des chiffres, des éléments graphiques ou une combinaison de ces éléments.

Assurance (garantie) raisonnable

- Correspond à un niveau satisfaisant de confiance au regard de considérations liées aux coûts, aux bénéfices et aux risques.
- Le concept selon lequel le contrôle interne, même s'il est très bien conçu et appliqué avec la plus grande rigueur, ne peut pas garantir la réalisation des objectifs qu'une organisation s'est fixés, en raison des limites inhérentes à tout système de contrôle interne. (COSO 1992)

Audit (Contrôle)

- Examen des activités et des opérations d'une entité en vue de s'assurer qu'elles sont exécutées ou fonctionnent conformément à des objectifs, à des budgets, à des règles et à des normes. L'objet de cet examen est de relever, à intervalles réguliers, les écarts qui pourraient nécessiter l'application de mesures correctives. (Glossaire)

Audit externe (Contrôle externe)

Contrôle exercé par un organisme externe et indépendant de l'entité contrôlée, ayant, d'une part, pour objet de donner une opinion sur les comptes et les états financiers, la régularité et la légalité des opérations et/ou sur la gestion financière et, d'autre part, d'établir des rapports correspondants. (Glossaire)

Audit interne

- Moyens fonctionnels par lesquels les gestionnaires d'une unité acquièrent au sein même de cette unité la certitude que les circuits comptables et financiers dont ils sont responsables fonctionnent d'une manière qui réduit au maximum les risques de fraudes, d'erreurs, de non-rentabilité ou de gaspillage. Les caractéristiques sont très proches de celles de l'audit externe, à cette différence près que l'audit interne permet de se conformer aux directives des chefs de services concernés. (Normes de contrôle de l'INTOSAI)



- Activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. (IIA – IFACI)
 - Activité d'évaluation qu'une organisation met en place en tant que service interne à l'organisation. Ses activités comportent, notamment, l'examen, l'évaluation et le suivi de la pertinence et de l'efficacité des systèmes comptables et de contrôle interne. (IFAC)
- (voir aussi Auditeur(s) interne(s) et Service d'audit interne)

Auditeurs internes

Ils examinent et contribuent à l'efficacité continue du système de contrôle interne à travers leurs évaluations et recommandations, mais ils n'assument pas la responsabilité de base de sa conception, sa mise en œuvre, son maintien et sa documentation

Aversion au risque

- Le niveau de risque que l'organisation est disposée à courir avant d'estimer qu'une action s'impose.
- Le niveau de risque, apprécié de manière globale, qu'une société ou une autre entité est disposée à accepter dans la mise en œuvre de sa mission ou de sa vision. (COSO ERM)

B

Budget

Expression quantitative et financière d'un programme d'actions dont la réalisation est envisagée pour une période donnée. Le budget est établi en vue de planifier les opérations futures et de contrôler a posteriori les résultats obtenus. (Glossaire)

C

Collusion

Effort concerté entre plusieurs employés en vue de détourner des avoirs, des stocks ou d'autres actifs appartenant à l'organisation. (Arens, Elder & Beasley)

Comité d'audit

Comité émanant du conseil d'administration dont le rôle consiste habituellement à suivre le rapportage financier et les processus mis en œuvre par l'organisme

pour gérer les risques opérationnels et financiers et pour assurer la conformité avec les exigences légales, éthiques et réglementaires importantes en vigueur. Quelques-unes des missions typiques attribuées au comité d'audit consistent à assister le Conseil d'administration dans la supervision (a) de l'intégrité des états financiers publiés par l'organisation, (b) de la conformité de l'organisation aux exigences légales et réglementaires, (c) des compétences et de l'indépendance des auditeurs externes, (d) de la performance de la fonction d'audit interne de l'organisation et de celle des auditeurs externes et (e) de la rémunération des cadres (en l'absence d'un comité de rémunération «remuneration committee»).

Composante du contrôle interne

Un des cinq éléments du contrôle interne. Les composantes du contrôle interne sont l'environnement de contrôle interne, l'évaluation des risques, les activités de contrôle, l'information et la communication, et le pilotage. (COSO 1992)

Conception

1. Intention. Lorsque ce mot est utilisé dans la définition du contrôle interne, il signifie que le système de contrôle interne a été conçu pour fournir une assurance raisonnable quant à la réalisation des objectifs; lorsque cette intention est réalisée, il est possible de conclure à l'efficacité du système.
2. La façon dont le système devrait fonctionner, par opposition à la façon dont il fonctionne dans la réalité. (COSO 1992)

Conformité

Le respect des lois et de la réglementation auxquelles l'entreprise est soumise. (COSO 1992)

Contrôle

- 1. Employé en tant que sujet d'une phrase, ex.: existence d'un contrôle: une politique ou une procédure qui fait partie du contrôle interne. Un contrôle peut exister au sein de n'importe laquelle des cinq composantes. 2. Employé en tant qu'objet d'une phrase, ex.: assurer le contrôle: le résultat de l'application des politiques et procédures destinées à assurer le contrôle; ce résultat peut se traduire ou ne pas se traduire par un contrôle interne efficace. 3. Employé en tant que verbe dans une phrase, ex.: contrôler: régler; créer ou mettre en œuvre une politique ayant trait au contrôle. (COSO 1992)
- Toute mesure prise par le management, le Conseil et d'autres parties afin de gérer les risques et d'accroître la probabilité que les buts et objectifs fixés seront atteints. Les managers planifient, organisent et dirigent la mise en œuvre de mesures suffisantes pour donner une assurance raisonnable que les buts et objectifs seront atteints. (IIA – IFACI) (Voir aussi Audit)

Contrôle à des fins de détection

Contrôle destiné à mettre en évidence un événement ou un résultat non voulu (à comparer au contrôle préventif). (COSO 1992)



Contrôle budgétaire

Contrôle par lequel une autorité, qui a accordé un budget à une entité, s'assure que ce budget a été exécuté conformément aux prévisions, aux autorisations et aux règlements. (Glossaire)

Contrôle d'accès

En matière de technologies de l'information, contrôles conçus pour protéger les ressources informatiques contre toute modification, perte ou divulgation non autorisée.

Contrôle de la continuité du service

Ce type de contrôle consiste à garantir qu'en cas de survenance d'un événement inattendu, les opérations fondamentales se poursuivront sans interruption ou reprendront promptement, et que les données critiques et vulnérables sont protégées.

Contrôle interne

Le contrôle interne est un processus intégré mis en œuvre par les responsables et le personnel d'une organisation et destiné à traiter les risques et à fournir une assurance raisonnable quant à la réalisation, dans le cadre de la mission de l'organisation, des objectifs généraux suivants: exécution d'opérations ordonnées, éthiques, économiques, efficaces et respect des obligations de rendre compte, conformité aux lois et réglementations en vigueur et protection des ressources contre les pertes, les mauvais usages et les dommages.

Contrôle préventif (Contrôle orienté vers la prévention)

Contrôle destiné à prévenir un événement ou un résultat non voulu (par opposition à Contrôle à des fins de détection). (COSO 1992)

Contrôles applicatifs

- Structure, politiques et procédures portant sur des systèmes d'applications individuels distincts et conçus pour contrôler le traitement des données dans le cadre d'applications informatiques spécifiques.
- Procédures programmées dans les logiciels d'application, ainsi que les procédures manuelles et associées, qui contribuent à garantir l'exhaustivité et l'exactitude des opérations de traitement des données. On peut citer comme exemples les bordereaux de contrôle de saisie édités par le système, les contrôles de la séquence numérique et les procédures manuelles de suivi des éléments figurant dans des états d'anomalies. (COSO 1992)

Contrôles édités par le système

Contrôles automatisés intégrés aux phases initiales du processus de saisie pour détecter les entrées erronées. Par exemple, un contrôle de ce type peut rejeter les caractères alphanumériques introduits dans des champs numériques. Les contrôles édités programmés sont aussi applicables, par exemple, lorsque des données relatives à des transactions sont intégrées dans le cycle de traitement et qu'elles proviennent d'une autre application.

Contrôles globaux

- Les contrôles globaux sont constitués par la structure, les politiques et les procédures applicables à l'ensemble des systèmes d'information d'une organisation ou à un segment important de ceux-ci, et qui contribuent à assurer leur fonctionnement correct. Ils créent l'environnement dans lequel les systèmes d'application et les contrôles fonctionnent.
- Politiques et procédures qui contribuent à assurer le fonctionnement correct et continu des systèmes informatiques. Ces contrôles peuvent porter sur la gestion des technologies de l'information, l'infrastructure des systèmes d'information, la gestion de la sécurité ou encore sur l'acquisition, le développement et la maintenance des logiciels. Les contrôles globaux servent de support au fonctionnement des contrôles applicatifs automatisés. Les expressions «contrôles globaux informatisés» et «contrôles de la technologie de l'information» sont parfois utilisées pour évoquer les contrôles globaux. (COSO ERM)

Contrôles informatiques

1. Contrôles réalisés par le système informatique, à savoir les contrôles programmés dans le logiciel informatique (par opposition aux contrôles manuels).
2. Contrôles sur le traitement informatique des données, comprenant à la fois les contrôles globaux et les contrôles applicatifs (tant programmés que manuels). (COSO 1992)

Contrôles manuels

Contrôles réalisés manuellement et non par le système informatique (par opposition aux «contrôles informatiques»). (COSO 1992)

Contrôles des systèmes d'exploitation

Contrôles de l'ensemble des programmes informatiques et des sous-programmes y afférents, destinés à faire fonctionner et contrôler les activités de traitement de l'équipement informatique.

Corps législatif

Assemblée qui a le pouvoir de légiférer; le Parlement, par exemple. (Normes de contrôle de l'INTOSAI)

Corruption

- Toute forme d'utilisation non éthique de l'autorité publique pour s'assurer un avantage personnel ou privé (XVI^e INCOSAI, Uruguay, 1998).
- Détournement à des fins privées du pouvoir confié. (Transparency International)

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

Comité des organisations parrainantes de la Commission Treadway, qui regroupe plusieurs organisations comptables. Il a publié en 1992 une étude importante consacrée au contrôle interne intitulée *Internal Control – Integrated*



Framework (Système intégré de contrôle interne). L'étude est souvent appelée COSO Report ou «rapport COSO».

Cycle d'évaluation des risques

Un processus itératif et continu destiné à identifier et analyser les changements dans les conditions, les opportunités et les risques, et à prendre des mesures correctrices nécessaires, particulièrement en adaptant le contrôle interne aux modifications survenues dans les risques. Les profils de risques et les contrôles y afférents doivent être révisés et réexaminés régulièrement pour s'assurer que le profil de risque reste pertinent, que les réponses aux risques restent adéquatement ciblées et proportionnées, et que les contrôles qui visent à atténuer les risques restent efficaces quand les risques eux-mêmes évoluent dans le temps.

D

Diagramme de circulation (flowchart ou flow-charting)

- Diagramme illustrant un flux de procédures, d'informations et de documents. Cette technique permet de décrire de manière synthétique des circuits ou des procédures complexes. (Glossaire)
- Représentation sous forme de diagramme des documents et pièces justificatives du client et de l'ordre dans lequel ils sont traités. (Arens, Elder & Beasley)

Direction (Management)

Comprend les cadres et autres personnes qui assument des fonctions de direction supérieures. La direction ne comprend les directeurs et le comité d'audit que dans les cas où ils remplissent de telles fonctions. (IFAC)

Documentation

La documentation du dispositif de contrôle interne est la preuve matérielle et écrite des composantes du processus de contrôle interne, incluant la description de la structure et des politiques d'une organisation, détaillant ses catégories opérationnelles, et spécifiant ses objectifs ainsi que ses activités de contrôle. Ces données doivent figurer dans des documents tels que des directives de la direction, des règlements administratifs, des manuels de procédures et des manuels comptables.

Données

Faits et éléments d'information susceptibles d'être communiqués et traités.

E

Economie

- Minimiser le coût des ressources utilisées pour une activité donnée tout en veillant à la qualité des résultats. (Normes de contrôle de l'INTOSAI).

-
- Acquisition de ressources financières, humaines et matérielles appropriées, tant sur le plan de la qualité que sur celui de la quantité, aux moments opportuns et au moindre coût. (Glossaire)

Economique

Ni inutile ni dispendieux, cela implique d'acquérir le nombre juste de ressources, de qualité appropriée, fournies au bon moment et au bon endroit et au moindre coût.

Efficace

Se rapporte à la réalisation des objectifs ou à la mesure dans laquelle les résultats d'une activité correspondent à son objectif ou aux effets escomptés de cette activité.

Efficacité

- Mesure dans laquelle les objectifs ont été atteints et rapport entre les effets escomptés et les effets réels d'une activité donnée. (normes de contrôle de l'INTOSAI)
- Mesure dans laquelle les objectifs sont atteints, selon un rapport coût/bénéfice favorable (Glossaire)

Efficiace

- Rapport entre la production de biens, de services ou d'autres résultats, et les ressources utilisées pour les produire. (Normes de contrôle de l'INTOSAI)
- Utilisation des ressources financières, humaines et matérielles de façon à atteindre la maximalisation des extrants pour un niveau donné de ressources ou la minimisation des intrants pour une quantité et une qualité données d'extrants. (Glossaire)

Efficient

Se réfère à la relation entre les ressources utilisées et les extrants produits pour atteindre les objectifs fixés et implique la minimisation des intrants employés pour atteindre une quantité et une qualité données d'extrants ou une maximalisation des extrants avec une quantité et une qualité données d'intrants.

Entité (ou Organisation ou Organisme)

Toute organisation créée pour un besoin spécifique, quelle que soit sa taille. Une entité peut être, par exemple, une entreprise commerciale, une association sans but lucratif, un ministère ou un établissement d'enseignement. Les autres termes utilisés en tant que synonymes sont «organisation», «organisme» et «département». (adapté de COSO 1992)

Environnement de contrôle

L'environnement de contrôle reflète la culture d'une organisation puisqu'il détermine le niveau de sensibilisation de son personnel au besoin de contrôle. Il constitue le fondement de toutes les autres composantes du contrôle interne, en fournissant une discipline et une structure.



Ethique

Se rapporte aux principes moraux.

Evaluation des risques

- L'évaluation des risques est le processus consistant à identifier et à analyser les risques liés à la réalisation des objectifs de l'entité et à déterminer les actions correctives appropriées. (*Risk assessment*)
- Se rapporte à l'estimation de l'importance d'un risque et de sa probabilité de survenance. (*Risk evaluation*)

Extrant (output)

En technologie de l'information, désigne les données/informations produites à l'issue d'un traitement sur ordinateur. Un affichage graphique sur un terminal ou une copie papier sont des extrants.

F

Faiblesse

Défaillance perçue, potentielle ou réelle du contrôle interne ou un domaine dans lequel le contrôle interne pourrait être renforcé afin d'accroître les possibilités de réalisation des objectifs de l'entité. (COSO 1992)

Fraude

Interaction illégale entre deux entités, par laquelle l'une des parties trompe intentionnellement l'autre par le biais d'une fausse représentation dans le but d'obtenir un avantage illicite et injustifié. Elle inclut des actes de tromperie, de supercherie, de dissimulation ou d'abus de confiance accomplis pour obtenir un avantage injuste ou malhonnête. (XVI^e INCOSAI, Uruguay, 1998)

I

Incertitude

Impossibilité de connaître à l'avance la probabilité ou l'incidence exactes d'événements futurs. (COSO ERM)

Indépendance

- Liberté d'agir sans aucune interférence externe, conférée à une institution de contrôle et à ses contrôleurs, en conformité avec un mandat de contrôle. (Glossaire)
- Liberté dont dispose l'ISC pour s'acquitter de son mandat de contrôle sans être soumise à des pressions d'aucune sorte. (Normes de contrôle de l'INTOSAI)
- Le fait de n'être exposé à aucune situation susceptible d'altérer l'objectivité, en réalité ou en apparence. Cette situation doit être gérée au niveau de l'auditeur

individuel et de la mission, ainsi qu'au niveau de la fonction et de l'organisation. (IIA – IFACI)

- Capacité de l'auditeur à maintenir un point de vue impartial dans l'exercice de ses fonctions (indépendance de fait). (Arens, Elder & Beasley)
- Capacité de l'auditeur à maintenir un point de vue impartial aux yeux d'autrui (indépendance d'apparence). (Arens, Elder & Beasley)

Informatique de l'utilisateur final (End user computing)

Se réfère à l'utilisation d'un traitement de données non centralisé (c'est-à-dire ne relevant pas du département «technologies de l'information») et appliquant des procédures automatisées développées par des utilisateurs finaux, généralement à l'aide de progiciels (par exemple, tableur et banque de données). Les processus développés et exploités par les utilisateurs finaux peuvent être complexes et devenir une source extrêmement importante d'informations pour la direction. Il n'est pas sûr qu'ils soient testés et documentés comme il se doit.

Institut des Auditeurs Internes (IAI)

L'IAI est une organisation qui établit des normes d'éthique et de pratique, organise des formations et encourage le professionnalisme de ses membres.

Institution de contrôle

Entité publique qui, quelle que soit la forme sous laquelle elle est désignée, constituée ou organisée, exerce, conformément à la loi, les fonctions de contrôle externe. (Glossaire)

Institution supérieure de contrôle des finances publiques (ISC)

- Organisme public qui, quelles que soient les dispositions qui régissent sa création, son organisation et la désignation de ses membres, remplit un mandat officiel de contrôle au plus haut niveau de l'Etat considéré. (Normes de contrôle de l'INTOSAI)
- Organe officiel d'un Etat qui, quel que soit son mode de désignation, de constitution ou d'organisation, exerce, en vertu de la loi, la plus haute fonction de contrôle des finances publiques de cet Etat. (IFAC)

Intégrité

Etat d'une personne qui est de bonne moralité; l'honnêteté, l'incorruptibilité et la probité; le souhait de bien faire, d'exprimer et de respecter un ensemble de valeurs et d'attentes. (COSO 1992)

Intervention de la direction

Les actions de la direction pour annuler ou déroger à des politiques ou des procédures prescrites, pour des raisons légitimes; l'intervention de la direction est généralement nécessaire dans le cas de transactions ou d'événements non récurrents ou inhabituels, qui seraient traités de façon inappropriée par le système (par opposition à «outrepasser»). (COSO 1992)



INTOSAI

Voir Organisation Internationale des Institutions Supérieures de Contrôle.

Intrant (input)

Voir saisie

L

Limites inhérentes

Les limites qui sont inhérentes à tout système de contrôle interne. Ces limitations résultent de l'imperfection du jugement humain, des contraintes en matière de ressources qui rendent nécessaire une étude du ratio coût/bénéfice lorsque la mise en place d'un contrôle est envisagé, de l'impossibilité d'enrayer totalement tout risque de dysfonction, et de la possibilité qui existe pour la direction d'outrepasser des contrôles ou pour toute personne d'agir en collusion avec une autre. (COSO 1992)

O

Objectivité

Attitude intellectuelle impartiale qui permet une indépendance d'esprit et de jugement et implique que les ISC et les auditeurs internes et externes ne subordonnent pas leur propre jugement à celui d'autres personnes. Leurs appréciations doivent être fondées sur les faits ou preuves indiscutables et s'appuyer sur des travaux incontestables exempts de tout préjugé. (IIA – IFACI)

Obligation de rendre compte

- Processus par lequel les organismes des services publics et les personnes qui les composent doivent répondre de leurs décisions et actions, notamment de leur gestion des fonds publics et de tous les aspects liés à la performance.
- Obligation imposée à une personne ou à une entité contrôlée de démontrer qu'elle a géré ou contrôlé les fonds qui lui ont été confiés conformément aux conditions dans lesquelles les fonds lui ont été fournis. (Glossaire)
- Obligation des personnes ou des unités – y compris des entreprises publiques – gérant ou utilisant des fonds publics, d'assumer la responsabilité de l'utilisation de ces fonds, au niveau de l'exécution du budget, de la gestion et de la mise en oeuvre des programmes, et d'en rendre compte à ceux qui leur ont confié ces missions. (Normes de contrôle de l'INTOSAI)

Opérations (ou activités)

- Lorsque ce mot est employé avec «objectifs» ou «contrôles», il se rapporte à l'efficacité et à l'efficience des activités d'une organisation, y compris en termes d'objectifs de performances et de rentabilité, et de la protection des ressources. (COSO 1992)

-
- De manière générale, désigne les fonctions, processus et activités qui permettent la réalisation des objectifs d'une organisation.

Optimisation des ressources

Voir Economie, Efficacité et Efficience.

Ordinateur central (ou macro-ordinateur, ou serveur)

Ordinateur de haut niveau conçu pour l'exécution des tâches informatiques les plus poussées. Les ordinateurs centraux sont souvent utilisés par des utilisateurs multiples qui y sont connectés par l'intermédiaire de terminaux.

Ordonné

D'une manière bien organisée ou méthodique.

Organisation internationale des institutions supérieures de contrôle des finances publiques (INTOSAI)

Organisation internationale indépendante dont l'objectif est de promouvoir l'échange entre institutions supérieures de contrôle d'idées et d'expériences dans le domaine des finances publiques. (Normes de contrôle de l'INTOSAI)

Outrepasser

Les actions des dirigeants pour annuler ou déroger à des politiques ou des procédures prescrites, à des fins illégitimes, dans le but soit d'en tirer profit personnellement soit d'améliorer la présentation de la situation financière de l'organisation ou de dissimuler la non-conformité à la législation ou à la réglementation (par opposition à «intervention de la direction»). (COSO 1992)

P

Parties prenantes (stakeholders)

Parties touchées par les activités d'une entité, tels que les actionnaires, les collectivités au sein desquelles l'entité opère intervient, les employés, les clients et les fournisseurs. (COSO ERM)

Pilotage (ou suivi ou monitoring)

Le pilotage est une composante du contrôle interne et constitue le processus qui évalue la qualité du fonctionnement du système de contrôle interne dans le temps.

Politique

Directives émises par la direction sur ce qui doit être fait pour mettre en oeuvre le contrôle. Une politique sert de base aux procédures permettant la mise en oeuvre du contrôle. (COSO 1992)

Procédure

Une action qui met en oeuvre une politique. (COSO 1992)



Processus de gestion

L'ensemble d'actions entreprises par la direction pour gérer l'organisation. Le système de contrôle interne fait partie du processus de gestion et y est intégré. (COSO 1992)

Profil de risque

Une vue d'ensemble ou la matrice des risques majeurs auxquels une organisation ou un service est confronté qui inclut le degré d'impact (ex.: haut, moyen, bas) et la probabilité de survenance de l'événement.

Programme de sécurité

Programme destiné à planifier et à gérer la sécurité pour l'ensemble de l'organisation; il constitue le fondement de la structure de contrôle de la sécurité de l'organisation et traduit l'engagement des hauts responsables au regard de la maîtrise des risques susceptibles d'affecter la sécurité. Le programme doit prévoir un cadre et un cycle continu d'activités pour évaluer les risques, élaborer et mettre en oeuvre des procédures de sécurité efficaces, et suivre l'efficacité de ces procédures.

R

Réseau

En technologie de l'information, désigne un groupe d'ordinateurs et d'appareils complémentaires reliés entre eux par des installations de communication. Un réseau peut être constitué grâce à des connexions permanentes, telles que des câbles, ou à l'aide de connexions temporaires réalisées par téléphone ou d'autres moyens de communication. Un réseau peut être peu étendu – il s'agira alors d'un réseau local composé d'un petit nombre d'ordinateurs, d'imprimantes et d'autres appareils – comme il peut être composé de nombreux ordinateurs, de tailles diverses, et répartis sur une grande étendue géographique.

Risque

La possibilité qu'un événement survienne et affecte négativement la réalisation des objectifs. (COSO ERM)

Risque inhérent

Le risque encouru par une organisation en l'absence de toute action que la direction pourrait prendre pour réduire la probabilité de survenance du risque ou son impact. (COSO ERM)

Risque résiduel

Le risque qui reste après que le management ait pris des mesures pour répondre au risque.

S

Saisie (Intrant, Input)

Toute entrée de données ou le processus d'entrée de données dans un ordinateur.

Secteur public

Désigne à la fois les administrations nationales, régionales (ex: Etat, administrations provinciales, collectivités territoriales), locales (ex: ville, agglomération), et les autres organismes assimilés (ex: agences publiques, organismes publics, parastataux, services municipaux, commissions et entreprises). (IFAC)

Séparation des fonctions

Pour réduire le risque d'erreur, de gaspillage ou d'actes illicites ainsi que le risque de ne pas détecter de tels problèmes, aucun individu ou équipe ne doit pouvoir contrôler l'ensemble des étapes essentielles (autorisation, traitement, enregistrement, vérification) d'une transaction ou d'un événement.

Service d'audit interne

- Service (ou activité) au sein d'une entité, chargé par sa direction d'effectuer des contrôles et d'évaluer les systèmes et les procédures de l'entité afin de minimiser les probabilités de fraudes, d'erreurs ou de pratiques inefficaces. L'audit interne doit être indépendant au sein de l'organisation et rendre compte directement à la direction. (Glossaire)
- Service, division, équipe de consultants ou tout autre praticien qui fournit une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. L'activité d'audit interne aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. (IIA – IFACI)

Système (Processus ou Architecture) de contrôle interne

Synonyme de «contrôle interne», appliqué à une entité. (COSO 1992)

Système d'exploitation

Logiciel destiné principalement à coordonner et contrôler le matériel et les ressources informatiques, l'accès aux fichiers et aux documents, et à contrôler et synchroniser les applications.

Systèmes d'information informatisés

L'environnement d'une entité sera caractérisé par l'existence de systèmes d'information informatisés (SII) lorsqu'un ordinateur, quels que soient son type et sa taille, est impliqué dans le traitement, par cette entité, d'informations (financières) ayant une incidence sur l'audit, que les opérations traitées par cet ordinateur soient effectuées en interne ou exécutées par un tiers. (IFAC)

T

Tolérance au risque

Se rapporte au degré de volatilité jugé acceptable dans la réalisation des objectifs. (COSO ERM)



Traitement (processing)

En technologie de l'information, désigne l'exécution d'instructions programmées par l'unité centrale de traitement par ordinateur.

V**Valeurs éthiques**

Valeurs qui permettent au décisionnaire de déterminer le comportement le plus approprié; ces valeurs sont fondées sur ce qui est « bien » et ne se limitent pas à ce qui est admissible sur le plan légal. (COSO 1992)

* L'usage veut que l'on précise les références complètes de chacun des ouvrages cités dans une bibliographie. S'agit-il du document présenté sur internet à la page <http://www.transparency.org/sourcebook/>? Si oui, l'auteur est Jeremy Pope, le titre complet: *TI Source Book 2000 – Confronting Corruption: The Elements of a National Integrity System* et l'éditeur: «Transparency International» à Berlin. Il en a été dérivé une version en français, plus spécifiquement focalisée sur les enjeux de la lutte contre la corruption en Afrique: *Combattre la Corruption – Enjeux et perspectives (Adapté du TI Source Book 2000, par les partenaires de Transparency International en Afrique)*, Paris: Karthala, 2002 – (source: recherche sur Google ce 17/06/2004; les premiers résultats convergent tous vers ce site).

