

Partie 6

Contrôle interne

Dieter WIDMER, expert-comptable dipl., associé, membre de la Direction générale, KPMG

Hans-Ulrich PFYFFER, expert-comptable dipl., certified internal auditor (CIA), associé, responsable des Internal Audit Services (IAS), KPMG

Sommaire de la partie 6

I. Remarques préliminaires

1. Résumé de la situation
2. Obligations du conseil d'administration et de la direction
3. Le contrôle interne en tant que moyen pour atteindre les objectifs de l'entreprise
4. Le contrôle interne en tant qu'instrument au service des propriétaires
5. Recommandations du Code suisse de bonne pratique pour le gouvernement d'entreprise
6. La révision interne en tant qu'organe de surveillance du contrôle interne
7. But et structure de la présente partie

II. Nouvelles exigences des Etats-Unis et conséquences pour la Suisse

III. Qu'est-ce que le contrôle interne?

1. Définition du contrôle interne
2. Délimitation par rapport à la révision interne
3. Délimitation par rapport à la révision externe
4. Délimitation par rapport aux autres fonctions de contrôle

IV. Modèles de contrôle

1. COSO Framework
 - 1.1 Environnement de pilotage et de contrôle
 - 1.2 Evaluation des risques
 - 1.3 Activités de pilotage et de contrôle
 - 1.4 Information et communication
 - 1.5 Surveillance
2. COSO ERM Framework
3. CoCo Framework
4. Système de gestion de la qualité
5. Mise en place d'un modèle de contrôle

V. Tâches et responsabilités

1. Conseil d'administration
2. Direction
3. Cadres et collaborateurs
4. Révision interne
5. Révision externe
6. Collaboration entre les différentes fonctions de contrôle

VI. Mesures de contrôle

1. Mesures de contrôle
 - 1.1 Contrôles préventifs et détectifs
 - 1.2 Contrôles automatiques, programmés et manuels
 - 1.3 Contrôles par la direction
2. Risques de contrôle

VII. Surveillance des contrôles internes

1. Conseil d'administration et comité d'audit
2. Direction
3. Auto-évaluation des contrôles (control (risk) self assessment)
4. Révision interne
5. Révision externe
6. Législateur et autorités de surveillance

VIII. Résumé et perspectives

Annexe A. Tableau d'évaluation du système de contrôle interne

Annexe B. Glossaire des composantes du contrôle

Bibliographie spécifique et autres ouvrages pertinents

BERTSCHINGER Peter/SCHAAD Martin, Prüfung amerikanischer und internationaler Konzerngesellschaften in der Schweiz, L'Expert-comptable suisse 5/2004 (cit : BERTSCHINGER/SCHAAD, Konzerngesellschaften); BERTSCHINGER Peter/SCHAAD Martin, Der amerikanische Sarbanes-Oxley-Act of 2002 – M gliche Auswirkungen auf die amerikanische und internationale Wirtschaftspr fung und Corporate Governance, L'Expert-comptable suisse 10/2002, p. 883 ss. (cit : BERTSCHINGER/SCHAAD, Auswirkungen); B CKLI Peter, Schweizer Aktienrecht, 3e  d., Zurich 2004 (cit : B CKLI, Aktienrecht); B CKLI Peter, Corporate Governance auf Schnellstrassen und Holzwegen, L'Expert-comptable suisse 3/2000, p. 133 ss. (cit : B CKLI, Schnellstrassen); BUMBACHER Robert-Jan/SCHWEIZER Markus, Gegenseitige Anforderungen an die Interne Revision, L'Expert-comptable suisse 11/2002, p. 1039 ss.; CHORAFAS Dimitris, Implementing and Auditing the Internal Control System, New York 2001; Coso, Committee of Sponsoring Organizations of the Treadway Commission, Internal Control – Integrated Framework, Jersey City, New Jersey 1992; Coso, Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Framework (projet), www.erm.coso.org, 2004 (cit : Coso, Enterprise Risk Management Framework); ENGAMMARE Val rie, Syst me de contr le interne et information des actionnaires, L'Expert-comptable suisse 6/2003, p. 491 ss.; FORSTMOSER Peter, Aufgaben, Organisation und Verantwortlichkeit des Verwaltungsrates, L'Expert-comptable suisse 5/2002, p. 485 ss.; Normes d'audit, Chambre fiduciaire, Zurich 2003; KLINGER Michael/KLINGER Oskar, ABC der Gestaltung und Pr fung des Internen Kontrollsystems (IKS) im Unternehmen, Vienne 1998; KLINGER Michael/KLINGER Oskar, Das Interne Kontrollsystem im Unternehmen, Munich 2000; KPMG UK, Internal Control: A Practice Guide, 2e  d., Londres 2000; JANS Victor, Erfahrungen mit Control & Risk Self Assessment, L'Expert-comptable suisse 1/2003, p. 27 ss.; MARBACHER Lukas, Risikoorientierte Pr fung – ein Muss, L'Expert-comptable suisse 11/2000, p. 1179 ss.; PALAZZESI Mauro/PFYFFER Hans-Ulrich, Ein neues Verst ndnis von Interner Revision, L'Expert-comptable suisse 3/2002 (cit : PALAZZESI/PFYFFER, Neues Verst ndnis); PALAZZESI Mauro/PFYFFER Hans-Ulrich, Interne Revision und Unternehmens berwachung – von der Konkurrenz zur Kooperation, L'Expert-comptable suisse

1-2/2004 (cité: PALAZZESI/PFYFFER, Kooperation); PICKETT Spencer, *Internal Control: A Manager's Journey*, New Jersey 2001; ROOT Steven, *Beyond COSO: Internal Control to Enhance Corporate Governance*, New Jersey 1998; ROTH James, *COSO Implementation Guide for The Internal Auditing Department*, Altamonte Springs 1995; SCHNEIDER Thomas, *Controlling und Interne Revision im Internen Kontrollsystem*, *L'Expert-comptable suisse* 1/2003, p. 33 ss.; *Manuel suisse d'audit* 1998, Chambre fiduciaire, Zurich 1998; STRAUB Ralf Michael, *Verantwortlichkeit des Verwaltungsrats und Kodex*, *L'Expert-comptable suisse* 5/2002, p. 494 ss.; WIDMER Dieter/WHEY Hans, *Neuregelung der Revision – Erwartungen und Chancen*, *L'Expert-comptable suisse* 5/2004, p. 361 ss.

Documents de référence

Message du 23 juin 2004 concernant la modification du Code des obligations (obligation de révision dans le droit des sociétés) et la Loi fédérale sur l'agrément et la surveillance des réviseurs, FF 2004, p. 3745 ss.; *Guidance on Control*, The Canadian Institute of Chartered Accountants, Toronto 1995; Directive de la SWX Swiss Exchange concernant les informations relatives au Corporate Governance du 1er juillet 2002; *Code suisse de bonne pratique pour le gouvernement d'entreprise*, *economiesuisse*, Zurich 2002; *The Professional Practices Framework*, The Institute of Internal Auditors, Altamonte Springs 2003 (traduction allemande: *Grundlagen der Internen Revision*, Deutsches Institut für Interne Revision e.V., Frankfurt-sur-le-Main 2002); «Turnbull Report», *The Turnbull Proposal on Internal Control*, Londres 1999.

I. Remarques préliminaires

1. Résumé de la situation

Ces derniers temps, les scandales financiers survenus dans quelques entreprises suisses importantes ont défrayé la chronique, suscitant la méfiance des investisseurs et du public à l'égard des conseils d'administration et des directions des grandes entreprises. Un point commun aux reproches émis relevait que le manque de «checks and balances» avait probablement conduit à un abus de pouvoir, ouvrant ainsi la voie à des pratiques inappropriées ou illégales. Des mécanismes de contrôle n'avaient donc consciemment pas été mis en place ou de manière incorrecte en raison d'une structure d'organisation déficiente, ou encore des contrôles existants sciemment éludés.

2. Obligations du conseil d'administration et de la direction

La responsabilité des entreprises est aujourd'hui plus importante que jamais. Il incombe au conseil d'administration et à la direction d'assumer leurs tâches respectives en distinguant bien leurs attributions et d'être parfaitement informés de ce qui se passe dans l'entreprise, afin de pouvoir gérer prudemment et de manière prévoyante son évolution. Pour répondre à cette exigence, il faut disposer de mécanismes de contrôle adéquats, d'une bonne connaissance des processus et d'un concept clair de gestion des risques.

La gouvernance de l'entreprise, qui inclut également ses obligations à l'égard des stakeholders, doit lui permettre d'assurer son existence à long terme. La condition à remplir pour une bonne gouvernance à long terme est un système de contrôle et de surveillance efficace couvrant tous les domaines de l'entreprise. La durabilité de cette gouvernance et par conséquent des contrôles incombe d'abord à la tête de l'entreprise, c'est-à-dire au conseil d'administration et à la direction. A cet égard, l'information et la communication jouent un rôle clé. D'autre part, il faut non seulement définir une culture d'entreprise et de contrôle, mais encore la mettre en pratique jour après jour.

3. Le contrôle interne en tant que moyen pour atteindre les objectifs de l'entreprise

Celui qui veut diriger une entreprise de manière responsable doit avoir la certitude que les processus se déroulent de manière efficace et sûre conformément aux mécanismes de contrôle mis en place. Le contrôle interne est un moyen permettant d'atteindre les objectifs de l'entreprise, ses limites étant représentées par les faiblesses humaines telles que les oublis, les malentendus et les mauvaises décisions. Des personnes peuvent aussi s'entendre pour éluder les contrôles.

4. Le contrôle interne en tant qu'instrument au service des propriétaires

Ces remarques montrent bien l'importance que revêt le système de contrôle interne (SCI). Les entreprises qui veulent remédier aux problèmes susmentionnés et accorder à la protection des actionnaires l'importance requise sont invitées à mettre en place et à entretenir un SCI global et efficace. Un tel système constitue un élément clé d'une gouvernance d'entreprise moderne et représente une condition essentielle pour une gestion des risques appropriée. Il contribue aussi en particulier à accroître notablement la qualité du rapport financier. Les actionnaires sont très intéressés par les informations qu'il leur fournit, qui leur servent de point de repère pour évaluer la pérennité de l'entreprise et la qualité de leur investissement. La publication d'informations pertinentes est en outre de plus en plus exigée – à ce sujet, on peut par exemple mentionner la loi Sarbanes-Oxley (SOX), le Turnbull Report ou la Directive de la SWX Swiss Exchange concernant les informations relatives au Corporate Governance.

5. Recommandations du Code suisse de bonne pratique pour le gouvernement d'entreprise

Selon le chiffre 19 du Code suisse de bonne pratique pour le gouvernement d'entreprise (Code suisse), une entreprise doit disposer d'un SCI adapté à sa taille, à sa complexité et à ses risques potentiels. Vu uniquement sous l'angle de son contenu, le système mentionné par le Code suisse comporte trois domaines: la gestion des risques, la conformité aux normes et, par conséquent, le contrôle interne et la révision interne. Le Code suisse propose en outre de constituer un

comité d'audit, qui devrait se composer de membres non exécutifs du conseil d'administration (ch. 23 Code suisse). Ce comité exerce un rôle clé pour l'information du conseil d'administration, ainsi que pour la discussion préalable avec les fonctions de surveillance et leur évaluation. C'est cependant au conseil d'administration qu'il incombe, dans le cadre de ses attributions intransmissibles et inaliénables, de mettre sur pied le SCI efficace requis et de remettre les confirmations sur l'efficacité des contrôles internes parfois exigées sur la base des normes, par exemple la SOX.

6. La révision interne en tant qu'organe de surveillance du contrôle interne

La révision interne se voit attribuer un nouveau rôle plus étendu à cet égard. Sa fonction d'instrument de gestion et de soutien actif du conseil d'administration et de la direction a récemment gagné en importance. La révision interne peut également fournir une importante contribution aux organisations de droit public et à but non lucratif ainsi qu'à l'administration publique en matière de gouvernance d'entreprise, d'efficacité des contrôles internes et de création de valeur, puisqu'elle évalue les processus de l'entreprise – notamment ceux de gestion des risques, de pilotage et de contrôle interne ainsi que de gouvernance d'entreprise – et signale le cas échéant des possibilités d'amélioration. Elle devient donc un fournisseur indépendant, objectif et fiable d'informations importantes pour la prise des décisions par les responsables de l'entreprise. Voilà pourquoi le chiffre 19 du Code suisse recommande d'instituer une révision interne.

7. But et structure de la présente partie

La présente partie 6 a pour but de donner un aperçu des principes du contrôle interne, des différents modèles, responsabilités et mesures de contrôle ainsi que de la surveillance des contrôles internes. Elle sert à démontrer l'importance d'un système de contrôle efficace pour l'entreprise.

La composition de la partie 6 est la suivante:

Le chapitre II «Nouvelles exigences des Etats-Unis et conséquences pour la Suisse» présente les exigences de renforcement de la réglementation concernant le fonctionnement du contrôle interne à la suite des scandales survenus au sein d'entreprises (citons par exemple Enron, Worldcom et Parmalat). A cet égard, il faudra dorénavant se fonder davantage sur des normes telles que celles du Committee of Sponsoring Organizations of the Treadway Commission (COSO) américain pour le contrôle interne.

Le chapitre III donne une définition du contrôle interne et présente ses objectifs. Il le délimite par rapport à la révision interne et à la révision externe.

Le contrôle interne est une notion très vaste et difficile à cerner. Les modèles de contrôle permettent d'en visualiser les exigences concrètes. Le chapitre IV décrit le modèle COSO, qui s'impose comme le plus important sur le plan international. D'autres modèles sont cités brièvement.

Le chapitre V traite des tâches et responsabilités des divers organes et fonctions relatifs au contrôle interne. En Suisse, la responsabilité générale du contrôle interne incombe au conseil d'administration. Il peut cependant se faire aider par des organes tels que la révision interne.

Le chapitre VI montre que les mesures de contrôle concrètes constituent des éléments importants qui font partie intégrante d'un système de contrôle interne global. Il contient la description de certains processus, méthodes et mesures (tels que la séparation des fonctions). Il indique à l'échelon opérationnel comment les contrôles peuvent être intégrés de manière rentable et efficace dans les processus de l'entreprise.

Quant au chapitre VII, il résume les principales caractéristiques du contrôle interne.

II. Nouvelles exigences des Etats-Unis et conséquences pour la Suisse

A la suite des scandales survenus dans diverses entreprises, le législateur américain a adopté la loi Sarbanes-Oxley¹. Ces nouvelles dispositions doivent permettre aux actionnaires et aux autres intéressés de retrouver confiance dans les rapports financiers. La SOX oblige la direction de l'entreprise à assumer l'intégralité et l'exactitude des informations contenues dans les rapports trimestriels et annuels. Il en résulte en outre de nouvelles exigences pour la direction de l'entreprise, en ce sens qu'elle doit donner régulièrement des indications sur le fonctionnement du SCI dans le cadre de ses rapports périodiques. La SOX doit être appliquée par les entreprises suisses ayant des titres de participation cotés dans une Bourse américaine, ainsi que par les filiales suisses de sociétés mères ayant des titres de participation cotés dans une Bourse américaine.

L'article 404 SOX (SOX 404) exige la mise en place d'un SCI adéquat et l'établissement d'une documentation². Cette disposition s'applique à tous les contrôles internes relatifs à l'établissement des comptes. Une attestation de l'évaluation du bien-fondé de ce système de contrôle par la direction de l'entreprise – concrètement, le président de la direction générale et le responsable financier - doit être publiée en même temps que le rapport annuel. La révision externe contrôle l'évaluation régulière de la direction et établit un rapport à ce sujet. Il s'agit donc d'un processus en deux étapes: l'entreprise atteste d'abord la qualité du SCI, puis la révision externe contrôle cette attestation et la confirme le cas échéant.

Ces nouvelles dispositions légales des Etats-Unis exigent l'application de normes pour le SCI. Les entreprises choisissent généralement le COSO Framework³, qui s'est imposé comme cadre de référence.

¹ BERTSCHINGER/SCHAAD, Auswirkungen, p. 883 ss.; BERTSCHINGER/SCHAAD, Konzerngesellschaften, p. 421 ss.

² BERTSCHINGER/SCHAAD, Konzerngesellschaften, p. 423.

³ Pour d'autres explications sur les modèles de contrôle, voir le chapitre IV.

Il faut s'attendre à ce que l'évolution aux Etats-Unis et ses répercussions sur d'autres régions et pays – notamment en Europe – entraînent également des exigences accrues pour la structure du SCI des entreprises qui ne sont pas cotées aux Etats-Unis. La Commission européenne a par exemple communiqué le 16 mars 2004 qu'elle se conformera en majeure partie à la SOX.

Concrètement, la Commission européenne a proposé une nouvelle réglementation de l'audit au sein de l'Union européenne, que les Etats membres doivent introduire d'ici 2006. Il s'agit d'une nouvelle version de la 8e directive CEE de 1984 sur la révision des comptes, aussi connue sous le nom de «Lex Parmalat». Conformément à cette directive, le réviseur externe doit communiquer au comité d'audit les principales faiblesses du SCI (material weaknesses of internal control).

Compte tenu de cette situation, de nombreux Etats membres ont déjà pris des mesures juridiques allant dans le sens des propositions présentées. C'est ainsi que la France a adopté dès juillet 2003 la Loi sur la sécurité financière, le pendant français de la SOX.

En Suisse aussi, des signes montrent que le SCI revêtira encore davantage d'importance. Dans le projet de réorganisation de la révision⁴, l'art. 728a CO prévoit que la révision externe vérifiera désormais s'il existe un système de contrôle interne qui fonctionne et s'il a été effectuée une évaluation des risques. Cela signifie qu'à l'avenir, le conseil d'administration devra décrire de manière appropriée dans l'annexe des comptes annuels le SCI et la gestion des risques de sa société⁵ (art. 728a al. 1 ch. 4 et 5, art. 663b ch. 12 projet CO).

Certaines sociétés suisses ont intégré de leur propre chef les dispositions de l'art. 404 SOX, en ce sens qu'elles surveillent déjà maintenant davantage le SCI, établissent des documents sur les processus et contrôles internes et les évaluent régulièrement.

⁴ Cf. à ce sujet le Message concernant la modification du Code des obligations, p. 3745.

⁵ WIDMER/WEY, p. 361 ss.

III. Qu'est-ce que le contrôle interne?

1. Définition du contrôle interne

Par contrôle interne, il faut entendre tous les processus, méthodes et mesures ordonnés par le conseil d'administration ou la direction de l'entreprise servant à garantir le déroulement correct des activités de l'entreprise. Les mesures d'organisation du contrôle interne sont intégrées aux processus de travail, ce qui signifie qu'elles accompagnent leur exécution ou la précèdent ou la suivent immédiatement. Il faut entendre par contrôle interne non seulement les activités de contrôle proprement dites, mais encore celles de pilotage et de planification, raison pour laquelle on parle aussi souvent de processus de pilotage et de planification.

Le contrôle interne aide notamment

- à atteindre les objectifs de l'entreprise grâce à une gestion efficace et rentable,
- à respecter les normes applicables telles que lois, ordonnances, règlements et directives (compliance),
- à protéger le patrimoine de l'entreprise,
- à empêcher, réduire et détecter les erreurs et irrégularités,
- à garantir la fiabilité et l'intégralité de la comptabilité et
- à établir à temps des rapports financiers fiables.

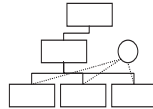
Le contrôle interne doit garantir – dans le cadre d'un processus continu – que les risques ne s'accroissent pas au-delà des valeurs tolérées définies par la gestion des risques, que les écarts par rapport aux objectifs sont reconnus et que les mesures adéquates à prendre sont identifiées et mises en œuvre. Cela nécessite, comme déjà dit, la participation du conseil d'administration, de la direction et de tous les collaborateurs. Le principe du double contrôle, la séparation des fonctions et le contrôle d'accès font partie intégrante du contrôle interne.



Activités de contrôle



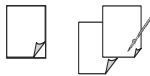
Collaborateurs



Direction/organisation



Instruments de pilotage



Directives



Culture d'entreprise

Figure 1. Le contrôle interne en tant que système de processus, méthodes et mesures

La nécessité du contrôle interne résulte aussi, entre autres, des principes régissant l'établissement régulier des comptes (but: garantir un rapport financier fiable). Il incombe au conseil d'administration et à la direction de définir les mesures d'organisation et d'assurer l'efficacité durable du contrôle interne.

Pour garantir un rapport financier fiable et par conséquent l'établissement régulier des comptes, il faut mettre en place des mesures de contrôle appropriées⁶ assurant

- l'intégralité, l'exactitude et la validité des données employées,
- l'existence et l'authenticité des états concernés,
- une délimitation correcte des résultats dans le temps et
- une évaluation, une structure et une présentation correctes conformément aux normes choisies.

Le contrôle interne présente une grave lacune si l'établissement régulier des comptes n'est pas assuré dans des domaines importants.

⁶ Pour d'autres explications sur les mesures de contrôle, voir le chapitre VI.

2. Délimitation par rapport à la révision interne

Contrairement au contrôle interne, la révision interne⁷ est une fonction indépendante non intégrée aux processus de travail de l'entreprise, qui a notamment pour tâche de superviser le contrôle interne.

La révision interne fournit des services indépendants et objectifs de révision et de conseil⁸ destinés à améliorer les processus de l'entreprise et à apporter une plus-value. Elle aide l'entreprise à atteindre ses objectifs, en évaluant, sur la base d'une approche systématique et ciblée, l'efficacité de la gestion des risques, des contrôles ainsi que des processus de direction et de surveillance en essayant de les améliorer⁹.

3. Délimitation par rapport à la révision externe

La révision externe est indépendante du SCI et tient compte de la qualité du contrôle interne dans le cadre d'une approche d'audit orientée sur les risques. Le contrôle interne devient donc l'objet de la vérification de la révision externe et sa structure influence les autres tâches d'audit. Contrairement à la révision interne, la révision externe ne vérifie cependant que les aspects du contrôle interne qui ont une incidence sur les finances et la comptabilité. Ce sont ces contrôles-là qui doivent garantir que les opérations sont intégralement et correctement reflétées dans les comptes annuels et intermédiaires.

4. Délimitation par rapport aux autres fonctions de contrôle

A part la révision interne et la révision externe, il existe encore d'autres fonction de contrôle au sein des entreprises, telles que le

⁷ PALAZZESI/PFYFFER, Neues Verständnis, p. 137 ss.; PALAZZESI/PFYFFER, Kooperation, p. 7 ss.

⁸ A part ses tâches de contrôle proprement dites, la révision interne peut aussi se voir confier des tâches de conseil. Selon les normes professionnelles de révision interne de l'Institute of Internal Auditors (IIA), ces activités doivent cependant être clairement distinctes de celles de contrôle et être désignées comme telles.

⁹ Il s'agit là d'une adaptation de la traduction allemande officielle de la définition selon les normes de l'Institute of Internal Auditors (IIA). L'IIA est l'association professionnelle internationale des réviseurs internes.

contrôle stratégique, la gestion des risques ou la compliance. Si ces fonctions font rapport au conseil d'administration ou au comité d'audit, elles peuvent être désignées comme des «fonctions d'audit». Etant donné que toutes ces fonctions vérifient certains aspects du SCI, il peut en résulter des chevauchements ou des lacunes en matière de contrôle. Il est donc nécessaire d'assurer la coordination dès la planification, ainsi qu'avant les contrôles.

Exemple 1 – Assurance map

Dans une entreprise, les diverses fonctions internes et externes ont exécuté leurs contrôles isolément. Les rapports au comité d'audit ont été établis séparément. A la demande du comité d'audit, la figure 2 suivante a été créée pour optimiser le contrôle. Elle montre les objectifs et tâches des différentes fonctions ainsi que les chevauchements et les lacunes.

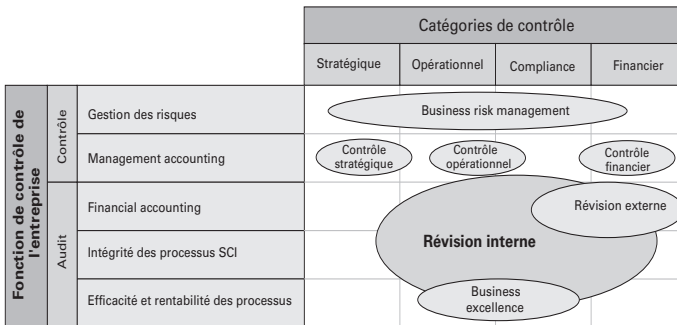


Figure 2: Assurance map¹⁰

Pour d'autres explications sur les interactions entre les différentes fonctions de contrôle du SCI, nous vous renvoyons à l'article «Interne Revision und Unternehmensüberwachung – von der Konkurrenz zur Kooperation»¹¹.

¹⁰ Par «business excellence», il faut entendre les fonctions internes de l'entreprise visant à accroître les performances, par exemple le contrôle et l'optimisation des processus ou la gestion de la qualité.

¹¹ PALAZZESI/PFYFFER, Kooperation, p. 7 ss.

IV. Modèles de contrôle

Quelles sont en fait les exigences concrètes auxquelles doit répondre un système de contrôle? Le chiffre 19 du Code suisse précise qu'un SCI dépend de facteurs spécifiques à l'entreprise. Il cite comme tels sa taille, sa complexité et son profil de risques. Chaque entreprise doit mettre en place un système de contrôle optimal en tenant compte de ces facteurs et en assurer le fonctionnement.

Les exigences concrètes que doit remplir un système de contrôle efficace figurent dans les normes internationales du COSO Framework américain ou du Standard Guidance on Criteria of Control (CoCo) canadien. Ces deux cadres de référence sont commentés ci-après. A part le concept COSO, l'autorité américaine de surveillance des titres et opérations boursières (Securities and Exchange Commission; SEC) cite expressément le concept CoCo ainsi que le Turnbull Report of Chartered Accountants in England and Wales en tant qu'exemples de modèles de contrôle appropriés généralement reconnus.

A des fins de délimitation, le présent chapitre aborde aussi brièvement les systèmes de gestion de la qualité¹².

1. COSO Framework

COSO, qui jouit aux Etats-Unis d'un large soutien de la part de différentes organisations professionnelles, a intégré les divers concepts et définitions du contrôle interne dans un concept de base, le COSO Framework. COSO définit le contrôle interne comme un processus influencé par le conseil d'administration, la direction et les collaborateurs, conçu pour offrir une sécurité appropriée en vue d'atteindre les trois objectifs clés suivants:

- efficacité et rentabilité des activités;
- fiabilité et intégrité du rapport financier;

¹² Les systèmes de gestion de la qualité orientés sur la norme ISO 9000 de l'International Organization for Standardization (ISO) sont l'exemple le plus connu.

- respect des normes applicables (compliance).

Ces trois objectifs clés représentent l'une des trois dimensions du cube COSO, comme le montre la figure 3. Ils peuvent être atteints par les deux autres dimensions – les composantes, d'une part, et l'entreprise et ses divisions, d'autre part. Les cinq composantes

- environnement de pilotage et de contrôle,
- évaluation des risques,
- activités de pilotage et de contrôle,
- information et communication ainsi que
- contrôle

doivent être définies, mises en œuvre, harmonisées et coordonnées entre elles pour les objectifs clés ainsi que pour l'entreprise et ses divisions.

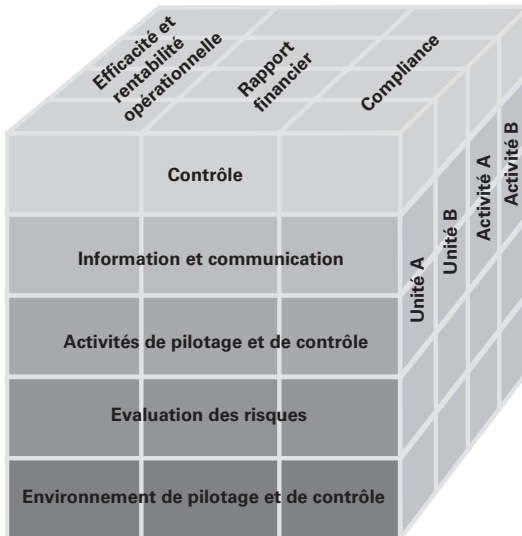


Figure 3: COSO Framework

Les cinq composantes sont commentées ci-dessous, les principaux éléments à vérifier étant chaque fois indiqués¹³.

1.1 Environnement de pilotage et de contrôle

L'environnement de pilotage et de contrôle constitue la base du pilotage et du contrôle interne et influence de ce fait la structure des activités de l'entreprise ainsi que la gestion des risques. Il incombe au conseil d'administration et à la direction que toutes les mesures nécessaires soient prises pour garantir un environnement de contrôle optimal¹⁴. Par leur comportement, le conseil d'administration et la direction imprègnent la culture d'entreprise, notamment celle en matière de risque et de contrôle, qui doit se caractériser par un haut degré d'intégrité. La manière d'aborder les risques et la culture en matière de contrôle doivent être précisées et communiquées par écrit. Les collaborateurs de tous les échelons hiérarchiques doivent connaître et comprendre leur responsabilité, leurs tâches et leurs attributions dans le cadre du processus de contrôle interne. A cet égard, le conseil d'administration et la direction sont responsables de la définition et de la mise en place de l'environnement de pilotage et de contrôle.

Les principales caractéristiques de l'environnement de contrôle sont:

- l'intégrité et les valeurs éthiques appliquées;
- engagement en matière de compétence et de diligence;
- le professionnalisme du conseil d'administration et de la direction ainsi que la qualification professionnelle et l'indépendance du comité d'audit;
- une conception de direction et un mode de travail intègres;
- une structure d'organisation appropriée;

¹³ Voir à ce sujet les explications du chapitre IV 1.1-1.5.

¹⁴ Voir à ce sujet les autres remarques du chapitre V 3 sur les cadres et les collaborateurs.

- l'attribution claire des tâches, compétences et responsabilités;
- la politique du personnel et son application au recrutement, à l'évaluation, à la rémunération et au développement des collaborateurs.

Exemple 2 – Autorité et responsabilité

L'entreprise n'a pas réglé clairement la question des responsabilités et des montants limites pour renoncer à des créances sur des débiteurs. Le comptable responsable des débiteurs accorde une renonciation sur des créances de CHF 1 million, bien que cela ne rentre pas dans son domaine de compétence.

Exemple 3 – Conseil d'administration et comité d'audit

Le conseil d'administration d'une société cotée en Bourse est désigné en fonction de critères politiques. Il n'est pas tenu compte du fait que ses membres ne disposent pas des compétences sectorielles ou professionnelles nécessaires. Comme aucun membre ne possède de connaissances financières et comptables approfondies, il est également décidé de renoncer à constituer un comité d'audit. Le risque existe que le conseil d'administration ne soit pas en mesure de contrôler l'entreprise de manière appropriée.

Exemple 4 – Valeurs éthiques

Le président de la direction générale d'une grande société ne respecte pas les directives internes, en ce sens qu'il se laisse inviter par un client important, lui et sa famille, pour des vacances luxueuses. Il ne respecte donc pas son devoir de servir de modèle, entraînant le risque que d'autres collaborateurs ne s'en tiennent pas non plus aux directives internes.

1.2 Evaluation des risques

Le risque est défini comme une incertitude quant à la survenance d'un événement susceptible d'avoir une incidence sur la réalisation des objectifs. Il est mesuré en fonction de ses conséquences quantitatives et de sa probabilité de survenance. Les risques auxquels une

entreprise doit faire face aujourd'hui sont complexes et exigent des processus de gestion clairement structurés. Les dirigeants d'entreprise sont obligés d'accepter des risques; le vieil adage «Qui ne risque rien n'a rien» n'a pas été formulé par hasard.

L'une des principales exigences à remplir par la direction d'une entreprise moderne consiste donc à définir un concept de gestion des risques évolutif qui soit entièrement intégré aux processus de planification et de gestion existants et qui vise aussi bien

- à empêcher et à réduire les risques de perte
- qu'à identifier, analyser et évaluer les chances à saisir¹⁵.

Dans ce contexte, le SCI doit garantir que tous les risques susceptibles d'influencer notablement la réalisation des objectifs de l'entreprise soient détectés et évalués à temps et continuellement. Il faut notamment inclure dans cette évaluation les risques des domaines suivants de l'entreprise:

- stratégie, planification et controlling;
- direction, organisation;
- marché de vente et d'approvisionnement;
- fourniture de prestations et production;
- financement et investissement;
- personnel;
- emplacement;
- environnement.

¹⁵ Voir à ce sujet la partie 1, annexe B, dans laquelle l'Enterprise Risk Management (ERM) est décrite comme un processus de direction important de l'entreprise.

Le SCI doit en outre faire preuve de la souplesse nécessaire pour pouvoir réagir rapidement et adéquatement à des genres de risques nouveaux ou incontrôlés jusque-là.

A propos de l'évaluation des risques, COSO définit quatre aspects principaux dont il faut tenir compte:

- les objectifs de l'ensemble de l'entreprise;
- les objectifs concernant un processus (par exemple ventes, achats, personnel);
- l'identification et l'évaluation des risques;
- la gestion des changements.

Exemple 5 – Identification et évaluation des risques

L'entreprise acquiert des machines sans procéder aux examens nécessaires et sans avoir clarifié complètement la question de leur financement. Les machines achetées s'avèrent surdimensionnées et le coût de l'investissement met en danger la survie de l'entreprise.

La direction ne peut mettre sur pied une gestion des risques efficace et rentable que si elle connaît bien les activités de l'entreprise, les objectifs à atteindre et les facteurs qui peuvent compromettre leur réalisation. Il est aussi indispensable de disposer d'une évaluation des risques axée sur les processus en y associant les divers groupes d'intéressés. Elle garantit que des éléments non financiers (qualitatifs), tels que la réputation ou des aspects environnementaux, sont pris en considération, ce qui favorise la formulation de critères mesurables et permet d'organiser la gestion des risques en tant que système d'alarme précoce. La gestion des risques doit toujours être faite par l'échelon d'organisation approprié. Il faut en outre s'assurer que toutes les informations relatives à la gestion des risques sont disponibles en fonction du besoin de regroupement et du degré de détail appropriés à l'échelon. Une collaboration et une communication franche à l'échelon de l'entreprise ainsi qu'entre le conseil d'administration, la direction, les révisions interne et externe, et

particulièrement la fonction de gestion des risques, jouent d'autre part un rôle important pour que les risques soient bien gérés.

La gestion des risques doit être adaptée aux spécificités de l'entreprise et tenir compte de sa situation particulière. Il faut prendre en considération aussi bien les facteurs d'influence internes (tels que la complexité de la structure d'organisation ou de l'activité de l'entreprise) que les externes (tels que les conditions-cadres économiques ainsi que l'évolution technologique ou sociologique).

Chaque entreprise devrait élaborer une stratégie pour gérer ses risques spécifiques, cette stratégie étant fortement déterminée par la volonté du conseil d'administration et de la direction d'assumer les risques ainsi que par la capacité de l'entrepreneur à les assumer. Mais l'essentiel est de connaître la totalité des risques, exprimés d'une part sous la forme de «risques bruts» et d'autre part sous la forme de «risques nets ou résiduels» en tenant compte des mesures prises.

Il existe quatre possibilités principales de gérer les risques d'entreprise:

- *Les éviter.* En renonçant aux activités qui les comportent, il est possible d'écarter les risques, mais en réduisant aussi du même coup les perspectives de gain.
- *Les réduire.* L'entreprise prend des mesures qui atténuent les conséquences potentielles des risques. Il faut trouver un juste équilibre entre la volonté d'assumer les risques et le coût de la maintenance des systèmes de pilotage et de contrôle.
- *Les répercuter.* En contractant une assurance, en se couvrant contre les risques («hedging») ou en mettant en place différents instruments de financement, l'entreprise peut reporter une partie de l'incidence financière des risques sur des tiers.
- *En assumer soi-même les conséquences.* Ne tenant pas compte de l'évaluation permanente, l'entreprise décide de ne pas prendre de mesures spécifiques pour gérer les risques, ou elle ne connaît pas les risques spécifiques, ce qui fait qu'elle doit

assumer elle-même les conséquences financières ou autres en cas de survenance d'un événement négatif.

1.3 Activités de pilotage et de contrôle

Par activités de pilotage et de contrôle, il faut entendre les dispositions et processus destinés à garantir que les mesures requises par la direction pour identifier et maîtriser les risques sont prises. Les activités de contrôle font partie intégrante des processus de travail; il faut distinguer les contrôles orientés processus, les contrôles orientés résultats et les contrôles directs du comportement:

- Les contrôles orientés processus servent à déterminer à un stade précoce les écarts par rapport aux objectifs, afin que des corrections puissent encore facilement être faites (ex ante).
- Les contrôles orientés résultats vérifient la réalisation des objectifs en comparant ce qui a été défini avec ce qui a été effectivement obtenu. Ils sont utilisés lorsqu'une correction immédiate n'est pas nécessaire et/ou pas possible (ex post).
- Quant aux contrôles du comportement, ils vérifient directement celui des unités individuelles et d'organisation. Ils sont notamment utilisés lorsque les résultats prévus ne sont pas observables.

Sur le plan des méthodes, il est possible d'employer différents types de contrôle¹⁶. Pour un pilotage et un contrôle interne efficaces, à part les mesures de contrôle formelles (lois, directives, descriptions de processus, structures d'organisation, séparation des fonctions, contrôles financiers), ce sont aussi surtout des mesures de contrôle informelles (connaissances, confiance, règles éthiques élevées, ouverture et transparence) qui sont requises.

COSO résume comme suit les principaux critères à évaluer dans le cadre des activités de pilotage et de contrôle:

¹⁶ Voir à ce sujet d'autres explications sur les mesures de contrôle au chapitre VI.

- existence de directives et processus appropriés;
- efficacité des contrôles définis.

Exemple 6 – Efficacité des contrôles définis

Les directives internes d'une entreprise prévoient que le collaborateur responsable des stocks ne peut remettre des marchandises qu'aux personnes autorisées qu'elles citent nommément.

Le collaborateur en question ayant insuffisamment exécuté le contrôle requis et son supérieur ayant également négligé de vérifier périodiquement le respect des directives, des marchandises ont été remises à des personnes non autorisées. L'entreprise a par conséquent subi un préjudice financier.

1.4 Information et communication

Comme pour tous les autres processus de direction, l'information et la communication jouent un grand rôle dans le domaine du pilotage et du contrôle. Il faut identifier les informations importantes, les préparer et les communiquer sous une forme et à un moment tels que les personnes concernées puissent assumer leurs responsabilités.

En ce qui concerne l'information et la communication, COSO renvoie aux deux critères principaux suivants:

- qualité des informations (complètes, conformes à la vérité, claires, adéquates);
- efficacité de la communication (au bon moment et pertinente).

Exemple 7 – Qualité des informations

Les rapports mensuels établis par un collaborateur de la comptabilité financière pour la direction n'ont pas été contrôlés par une deuxième personne depuis des mois. Ce n'est que l'année suivante qu'il est constaté que les chiffres comparatifs indiqués dans chaque rapport étaient faux et que les rapports mensuels ne contenaient pas

toutes les informations importantes. Fondée sur des données insuffisantes, l'analyse de la direction a donc perdu de sa valeur.

Pour que le contrôle interne soit efficace, il est indispensable qu'il existe un système approprié garantissant que toutes les informations importantes sur les domaines d'activité de l'entreprise sont recueillies, diffusées et traitées de manière fiable et en temps opportun (Management Information System). Par informations importantes, il faut entendre d'une part les informations opérationnelles, financières et relatives à la compliance qui permettent de piloter et de contrôler une entreprise, d'autre part celles concernant les événements, situations et activités externes qui sont destinées au système d'alarme précoce, servent à améliorer la prise des décisions et facilitent la communication de l'entreprise.

La communication appropriée à l'échelon des objectifs, résultats et mesures de contrôle interne revêt aussi une grande importance. Tous les collaborateurs doivent connaître les principes, rapports et processus du contrôle interne dans la mesure où leur responsabilité les y contraint.

La création d'une structure d'organisation adéquate doit garantir le flux d'informations nécessaire à la coordination et à la capacité de réaction tant de bas en haut que de haut en bas ainsi qu'horizontalement et avec l'environnement de l'entreprise. Primordiaux sont la préparation d'informations de qualité ainsi que l'établissement du rapport en temps utile.

1.5 Contrôle

Les principaux critères COSO à cet égard sont:

- surveillance permanente;
- contrôle spécial;
- rapport sur les points faibles identifiés par le contrôle et l'élimination de ces points.

Exemple 8 – Surveillance permanente

Afin de réduire les pertes sur débiteurs, l'entreprise a défini pour les principaux d'entre eux des limites de crédit fondées sur une évaluation des risques. Le montant de ces limites devrait être révisé une fois par an sur la base d'une nouvelle évaluation des risques. Or le responsable de la comptabilité débiteurs ne connaissait pas cette disposition, raison pour laquelle les limites n'ont jamais été adaptées. Son chef n'a constaté l'absence de ce contrôle périodique qu'après trois ans, à cause d'une importante perte sur débiteurs.

Exemple 9 – Surveillance permanente

Pour des raisons financières, une grande société cotée en Bourse renonce à une révision interne. Le conseil d'administration se fie entièrement à la direction. Il court ainsi le risque que la gestion des risques et le SCI ne soient pas régulièrement contrôlés et évalués par un organe indépendant et objectif.

L'efficacité du contrôle interne devrait être contrôlée en permanence. Il est garanti que le SCI demeure efficace par le biais d'activités de contrôle permanentes et/ou d'évaluations séparées (contrôles spéciaux) ainsi que par la correction des points faibles identifiés. Les contrôles effectués et les résultats doivent être enregistrés le plus concrètement possible sous une forme appropriée.

Il faut tenir dûment compte de l'évolution des conditions internes et externes de l'entreprise. Différents changements peuvent donner lieu à des mesures de contrôle appropriées: introduction de nouveaux produits, croissance rapide de certains domaines/activités, fluctuation du personnel, nouveaux systèmes d'information, changement de structure d'organisation, fusions, modification de l'environnement législatif et réglementaire ou changement d'activité internationale.

Si des écarts et lacunes sont constatés, il faut s'assurer que des mesures de correction sont mises en œuvre. Les fonctions et échelons hiérarchiques concernés doivent être informés à temps des problèmes en question et le conseil d'administration ainsi que la direction avisés des cas graves.

2. COSO ERM Framework

L'Enterprise Risk Management Framework (ERM Framework) est une version évoluée du COSO Framework qui tient compte en plus des objectifs stratégiques clés¹⁷. L'ERM Framework identifie et analyse les risques d'un point de vue global. Ce framework élargi permet de disposer d'un modèle de gestion des risques complet.

Les cinq composantes COSO initiales¹⁸ ont été complétées par trois autres:

- définition des objectifs (objective setting): notamment définition de la stratégie, volonté d'assumer des risques, capacité à assumer des risques;
- identification des événements (event identification): notamment risques et occasions à saisir, catégories d'événements, dépendance par rapport aux événements;
- réaction face aux risques (risk response): notamment identification et évaluation du traitement possible des risques.

¹⁷ Cette version devrait entrer en vigueur encore en 2004.

¹⁸ Voir d'autres remarques à ce sujet au chapitre IV 1.

Le schéma ci-dessous montre les huit composantes du contrôle du COSO ERM qui se reflètent dans l'entreprise et ses divisions.¹⁹

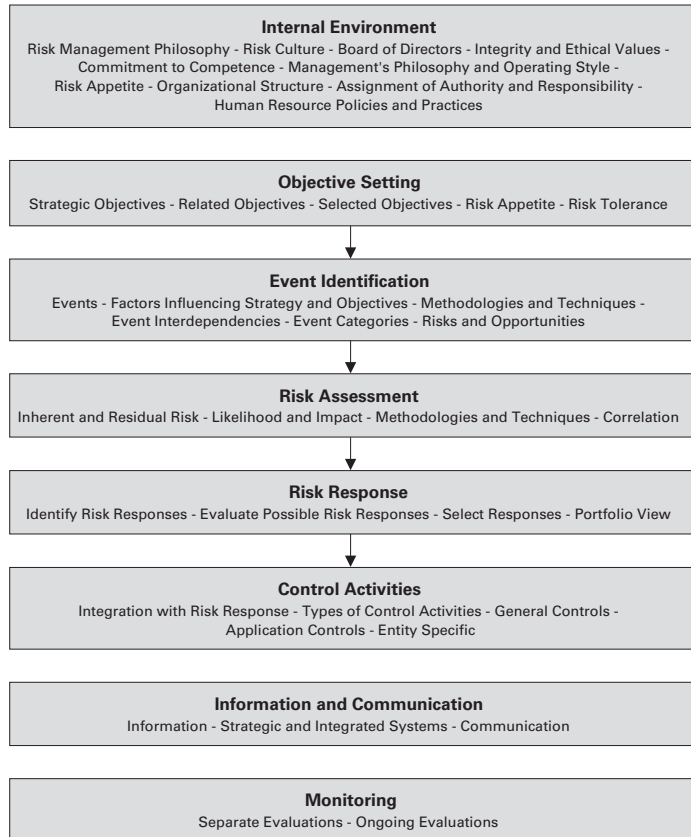


Figure 4. Composantes COSO ERM

Toute mesure stratégique et opérationnelle comporte des risques. Le facteur de succès déterminant pour l'entreprise consiste à les identifier globalement, à les évaluer correctement et à intégrer les conclu-

¹⁹ COSO, Enterprise Risk Management Framework, p. 14 ss. Cf. à ce sujet www.erm.coso.org.

sions spécifiques à ces risques dans la direction stratégique et opérationnelle. Un ERM efficace au sens d'un système d'alarme précoce est la condition à remplir pour assumer consciemment les risques et fournit la transparence nécessaire pour que les dirigeants puissent prendre des décisions ciblées. Un système ERM proactif permet d'anticiper les risques et de les piloter. Cela se traduit en premier lieu par un accroissement de la sécurité en matière de planification, moins d'erreurs de contrôle et une plus grande probabilité pour l'entreprise d'atteindre ses objectifs et de tirer parti des chances qui s'offrent à elle, et en fin de compte par une augmentation de sa valeur.

3. CoCo Framework

Le CoCo Framework a été élaboré par le Canadian Institute of Chartered Accountants pratiquement en même temps que le COSO américain. Ses objectifs comprennent:

- l'efficacité et la rentabilité des activités,
- la fiabilité des rapports internes et externes,
- la conformité aux lois, ordonnances et directives internes.
- Ils sont donc pratiquement identiques aux trois objectifs clés du COSO.

Le modèle CoCo est plus dynamique et plus orienté sur la direction que le COSO. Malgré cela, il ne s'est guère imposé et n'est que peu employé. Pour de plus amples informations, nous vous renvoyons au Canadian Institute of Chartered Accountants²⁰.

²⁰ Voir à ce sujet le site Internet www.cica.ca et la remarque Guidance on Control.

4. Systèmes de gestion de la qualité

La gestion de la qualité ne constitue plus une fonction indépendante isolée au sein de l'entreprise, mais revêt une importance stratégique. La qualité est décisive pour le succès de l'entreprise et lui permet de devancer des concurrents. La Total Quality Management (TQM) poursuit une approche globale, en tenant compte des parties et fonctions les plus diverses qui participent aux processus de l'entreprise. Un contrôle permanent de la qualité permet de développer et d'améliorer le système, garantissant ainsi le maintien de la qualité. Il est donc possible de retenir comme principe stratégique qu'à long terme, le principal facteur de succès d'une unité d'exploitation est la qualité de ses collaborateurs, produits et services par rapport à ses concurrents.

Les systèmes de gestion de la qualité deviennent donc cruciaux pour la direction de l'entreprise. Ce n'est pas le système avec lequel l'entreprise veut travailler qui est primordial (par exemple ISO²¹, EFQM²², Six Sigma²³), mais les objectifs et exigences qui s'y rattachent. Sur le plan opérationnel, on distingue quatre domaines d'activité:

- planification, organisation et développement (planification de la qualité);

²¹ L'International Organization for Standardization (ISO) gère différentes normes internationales pour l'économie, les institutions étatiques, le public et la société. Voir à ce sujet www.iso.org.

²² La European Foundation for Quality Management (EFQM) a élaboré le modèle EFQM et aide à le mettre en œuvre. Voir à ce sujet www.efqm.com.

²³ Le but de Six Sigma est de changer la manière de voir au sein de l'entreprise. Le point central de l'approche Six Sigma est l'amélioration permanente de la Total Quality Management et l'amélioration substantielle des résultats de l'entreprise. Il s'agit d'un critère pour une gestion de la qualité axée sur la perfection. Le principe Six Sigma vise des stratégies qui se basent sur des mesures quantitatives et essaient d'optimiser les processus, de limiter les écarts et différences et d'éliminer les erreurs ou problèmes de qualité de toute nature. Pour y parvenir, des techniques éprouvées de garantie de la qualité employant des méthodes simples et sophistiquées d'analyse des données sont combinées avec la formation systématique des collaborateurs de tous les échelons de l'entreprise. La mise en œuvre de Six Sigma dans l'entreprise nécessite une structure et une équipe avec des rôles et responsabilités définis. Voir à ce sujet www.quality.de.

- achat, production et vente (orientation de la qualité);
- garantie (garantie de la qualité);
- amélioration (amélioration continue).

Dans le cadre des certifications de la qualité, il est procédé à des audits dans les entreprises (par exemple dans le cadre des certifications ISO 2000)²⁴. Ces audits ne remplacent pas le SCI et ne suffisent pas non plus pour se prononcer sérieusement sur la qualité du contrôle interne. Les conclusions de ces audits ou reviews peuvent cependant fournir des informations utiles sur le contrôle interne et servir de point de départ à des améliorations.

Exemple 10 – Amélioration

Lors de son voyage réussi avec la «Santa Maria», Christophe Colomb a lui aussi déjà dû procéder à un contrôle de la qualité.

Nous sommes en l'an 1492. Christophe Colomb est à la recherche d'une route maritime plus courte vers les Indes. Après des jours de voyage et de nombreuses tempêtes, la flotte arrive aux îles Canaries. Des problèmes de navigation et un manque de clarté dans le commandement de l'équipage ont entraîné des pertes de vivres.

Christophe Colomb demande au premier officier d'examiner les problèmes et de proposer des mesures d'amélioration. L'officier constate qu'il y a eu des malentendus entre le capitaine et le navigateur lors de la détermination de la nouvelle route, ce qui a fait faire des détours. D'autre part, l'équipage avait mal interprété certains des ordres et une partie des vivres était déjà avariés à cause d'un mauvais entreposage.

Les malentendus ont été dissipés, de meilleures règles formulées et les vivres entreposées correctement.

²⁴ Appelées parfois aussi contrôles de qualité.

5. Mise en place d'un modèle de contrôle

Dans toutes les entreprises, des contrôles internes sont effectués à différents échelons, mais ne sont pas forcément effectués de manière standardisée ni dans le cadre d'un modèle de contrôle global et reconnu. Si un tel modèle doit être introduit (par exemple pour satisfaire aux exigences de la SEC), les six étapes suivantes sont indispensables pour que la mise en œuvre soit réussie :

- constitution d'une équipe de projet pour évaluer les contrôles et définir le calendrier;
- choix du modèle de contrôle;
- évaluation et documentation des contrôles internes à l'échelon de l'entreprise;
- évaluation et documentation des contrôles internes à l'échelon des processus, des transactions ou de l'application (selon des considérations d'importance et en tenant compte des processus clés);
- évaluation de l'efficacité des contrôles et identification des points faibles, contrôle des mesures de correction, y compris la formation requise des collaborateurs et des cadres concernés par les processus de contrôle;
- établissement du rapport de contrôle de la direction ainsi que vérification et attestation par la révision externe.

La tâche principale consistera à établir ou à compléter la documentation, car on peut présumer qu'il n'existera souvent pas de documentation ou qu'elle sera déficiente.

L'équipe de projet doit naturellement pouvoir compter sur l'appui du conseil d'administration, de la direction et des ressources nécessaires, par exemple en faisant appel à l'IT, à la révision interne et/ou externe, ainsi que sur la formation et la sensibilisation des collaborateurs.

V. Tâches et responsabilités

La condition de base pour qu'un système de contrôle fonctionne est une séparation claire entre le conseil d'administration, la direction et les organes de révision (révisions interne et externe). Pour garantir l'indépendance nécessaire des différentes fonctions, il faut éviter le plus possible leur cumul.

1. Conseil d'administration

Il incombe au conseil d'administration²⁵, dans le cadre de ses attributions intransmissibles et inaliénables conformément à l'art. 716a al. 1 CO, de veiller à ce que la gestion des risques et le SCI soient adaptés à l'entreprise²⁶:

- Le SCI doit être adapté à la taille, à la complexité et au profil de risque de l'entreprise.
- Le SCI recouvre aussi, selon les spécificités de l'entreprise, la gestion des risques; celle-ci se réfère aussi bien aux risques financiers qu'aux risques opérationnels.
- L'entreprise institue une révision interne. Celle-ci fait rapport au comité de contrôle (comité d'audit) ou, le cas échéant, au président du conseil d'administration.

Le conseil d'administration prend en outre des mesures pour assurer le respect des normes applicables («compliance»)²⁷:

- Le conseil d'administration institue la fonction de respect des normes applicables («compliance») en fonction des particularités de l'entreprise; il peut intégrer cette fonction au SCI.

²⁵ Voir à ce sujet les explications de la partie 1, II 3 Conseil d'administration et direction.

²⁶ Voir à ce sujet le chiffre 19 du Code suisse.

²⁷ Voir à ce sujet le chiffre 20 du Code suisse.

- La question de savoir si les principes de conformité aux règles applicables à lui-même et à l'entreprise sont suffisamment connus et régulièrement respectés est examinée au moins une fois par an.

Conformément à l'art. 716a al. 1 ch. 1 CO, le conseil d'administration exerce la haute direction de l'entreprise. Il est donc responsable de toutes les décisions importantes, une délégation des tâches étant possible et judicieuse²⁸. L'élaboration des variantes et projets peut être déléguée à la direction, mais c'est le conseil d'administration qui tranche et assume la responsabilité²⁹.

Le Combined Code (Turnbull Report) de la London Stock Exchange³⁰ souligne également l'importance du contrôle interne. Il n'y est pas seulement mentionné comme une exigence générale pour l'entreprise, mais encore directement mis en relation avec le conseil d'administration: «The Board should maintain a sound system of internal control (Principle D.2)».

Le conseil d'administration assume notamment la responsabilité:

- de l'approbation et du réexamen périodique des décisions ayant une importance stratégique;
- de la fixation de la limite supérieure adéquate pour les types de risques choisis et définis;
- de la garantie de la mise en œuvre des mesures à prendre par la direction dans le cadre du contrôle interne (identification, détermination, surveillance et contrôle des risques courus par l'entreprise);
- de la garantie du contrôle approprié de l'efficacité du SCI par la direction.

²⁸ BÖCKLI, Aktienrecht, §13 n. 303.

²⁹ Voir à ce sujet les remarques de la partie 1, II 3.1.3 Délégation à la direction.

³⁰ Résultant des trois rapports Cadbury, Greenbury et Hampel; depuis fin 2000, les sociétés cotées en Bourse doivent respecter intégralement ce code unifié.

Pour assumer ces responsabilités, le conseil d'administration devrait discuter régulièrement de l'efficacité des mesures de contrôle interne avec la direction, faire évaluer le SCI par la direction, évaluer à temps les révisions interne et externe et éventuellement les autorités de surveillance et en tirer les conséquences. Le conseil d'administration devrait en outre contrôler que des mesures de correction sont prises et respectées et réexaminer régulièrement la stratégie et les limites définies pour les risques. Il incombe en particulier au conseil d'administration de garantir la mise en œuvre de mesures de correction appropriées s'il est constaté que le SCI comporte des déficiences.

Le conseil d'administration peut désigner un comité d'audit pour l'aider et le décharger dans le domaine du contrôle interne³¹. Cela ne le libère cependant pas de sa responsabilité générale à l'égard du contrôle interne³².

2. Direction

Il incombe à la direction d'élaborer et de mettre en œuvre les stratégies et principes définis par le conseil d'administration³³. Elle est notamment responsable:

- de l'élaboration de processus appropriés pour l'identification, la détermination, la surveillance et le contrôle des risques couvrus par l'entreprise;
- du respect et de la documentation d'une structure d'organisation définissant clairement les responsabilités, compétences et flux d'information;
- de la garantie de l'exécution des tâches déléguées;
- de la vérification de l'emploi optimal des ressources dans le domaine du contrôle interne.

³¹ Voir à ce sujet l'Audit Committee Institute de KPMG Suisse, sous le site Internet www.auditcommittee.ch.

³² Voir à ce sujet les explications de la partie 1, II 3.1.1 Haute direction de la société.

³³ Voir à ce sujet les explications de la partie 1, II 3 Conseil d'administration et direction.

Une définition plus détaillée des objectifs et une délégation plus poussée des responsabilités permet d'associer les collaborateurs des différents échelons à la mise en œuvre des stratégies et à la responsabilité du contrôle interne. La direction garantit le nombre et la qualité des collaborateurs employés, notamment leur formation et leur expérience. Les structures de rémunération et de promotion ne doivent pas comporter d'incitation à négliger les mécanismes de contrôle interne.

3. Cadres et collaborateurs

Tous les collaborateurs de tous les échelons assument une responsabilité en matière de contrôle (controls are everybody's business). Pratiquement tous les collaborateurs fournissent des informations qui sont utilisées par le SCI ou exécutent des activités qui doivent être contrôlées. Ils devraient donc tous connaître les principes du contrôle interne et être informés en détail sur les contrôles qui les concernent. Les collaborateurs doivent être conscients de leur responsabilité à l'égard du processus de contrôle et garantir l'exécution efficace et rentable des tâches de contrôle qui leur sont confiées. Il faut donc accorder l'attention nécessaire à leur formation.

4. Révision interne

Le Code suisse recommande d'instituer une révision interne (ch. 19 Code suisse)³⁴. Le droit suisse n'impose pas une révision interne aux entreprises (à l'exception des sociétés financières soumises à des règles spéciales). L'activité de la révision interne n'est pas liée à des lois ou ordonnances nationales, mais peut être exercée dans le monde entier selon les mêmes concepts et principes. Ces principes figurent dans le volumineux cadre normatif de l'association internationale des auditeurs internes (IIA)³⁵. En particulier dans les entreprises multinationales, la révision interne peut rendre de précieux services grâce à son activité internationale et à sa vision globale.

³⁴ Voir à ce sujet les remarques de la partie 1, II 3.6 Système de contrôle interne, gestion des risques et compliance.

³⁵ Appelé «Framework for the Professional Practices».

La révision interne aide principalement le conseil d'administration à assumer sa fonction de haute direction en tant qu'organe suprême de l'entreprise. A ce titre, elle évalue les processus de gestion des risques, de pilotage et de contrôle ainsi que de gouvernance de l'entreprise, communique ses observations au conseil d'administration ou au comité d'audit et propose des améliorations pour ces processus. La révision interne conseille aussi la direction, en évaluant les processus de gestion de l'entreprise qui accompagnent la chaîne de création de valeur. Grâce à sa vision intégrée et à sa connaissance globale de l'entreprise, la révision interne est en mesure d'indiquer des possibilités d'améliorer l'efficacité et la rentabilité. En plus des domaines mentionnés, la révision interne peut exécuter d'autres activités pour les organes dont elle relève, en général le conseil d'administration.

5. Révision externe

La révision externe ne fait pas partie intégrante du SCI, mais il est tenu compte de la qualité du contrôle interne dans le cadre de l'approche orientée sur les risques. La Norme d'audit 14³⁶ a pour objet l'intégration du contrôle interne dans la planification et l'exécution de l'audit des comptes annuels. Il en découle que le réviseur doit axer ses opérations de vérification sur le risque d'audit (renvoi à la Norme d'audit 11). Cela signifie qu'il analyse l'organisation du contrôle interne et qu'il en tient compte dans son appréciation des risques. A cet égard, l'analyse et l'évaluation du contrôle interne représentent un élément important pour la détermination des opérations de vérification de la révision externe, notamment dans les entreprises qui traitent un volume de transactions important ou qui ont des flux de valeurs et de données sensibles. La vérification du contrôle interne donne en outre des informations sur la régularité de la comptabilité et de la présentation des comptes. La management letter sur les constatations de l'audit contribue donc de manière importante au renforcement et à l'amélioration de la surveillance et du contrôle de l'entreprise.

³⁶ Les Normes d'audit actuellement en vigueur seront remplacées au 1er janvier 2005 par les Normes d'audit suisses (NAS). Voir à ce sujet les remarques du chapitre VII 5.

6. Collaboration entre les différentes fonctions de contrôle

La collaboration entre les différentes fonctions de contrôle telles que la révision interne, la révision externe, mais aussi la gestion des risques, revêt une importance croissante. Elles contribuent en effet de manière importante à la prospérité de l'entreprise en contrôlant des domaines déterminés, en vérifiant le respect des objectifs, des lois et des directives ou en détectant les erreurs et les irrégularités. Les fonctions de contrôle font partie intégrante du SCI et de ses organes de surveillance³⁷.

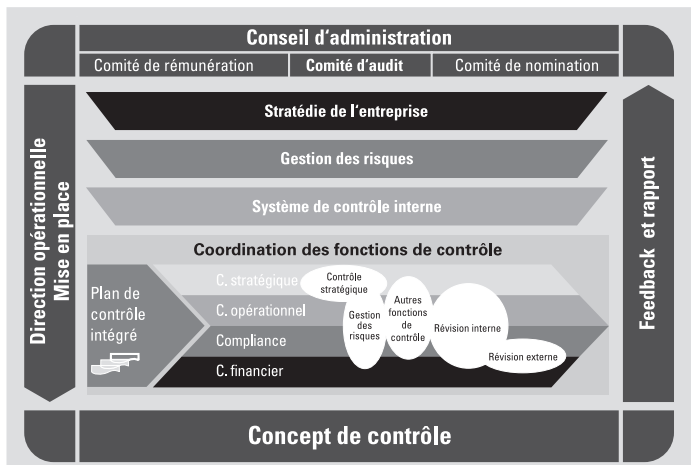


Figure 5. Concept de contrôle

Un concept de contrôle global est indispensable pour que les divers processus de contrôle et de surveillance puissent être évalués et harmonisés. Il facilite en outre la coordination des activités, permettant ainsi de garantir la sécurité et l'efficacité des activités d'audit. Il s'agit donc d'éviter les lacunes et les chevauchements en matière de contrôle. Le conseil d'administration, le comité d'audit et la direction sont responsables de la mise en place et de l'application du concept.

³⁷ Voir autres explications au chapitre IV 1.5.

VI. Mesures de contrôle

1. Mesures de contrôle

Les contrôles sont les différentes opérations, méthodes et mesures prévues dans le cadre d'un SCI. L'urgence ne doit pas devenir le facteur qui décide si et comment il faut procéder aux contrôles. Il va de soi que toutes les unités d'exploitation situées dans le pays ou à l'étranger (départements, services, filiales) d'une entreprise doivent être incluses dans le processus de contrôle.

Les mesures de contrôle peuvent être classées en trois catégories:

- contrôles préventifs et détectifs;
- contrôles automatiques, programmés et manuels;
- contrôles faits par les cadres.

1.1 Contrôles préventifs et détectifs

Par *contrôles préventifs*, on désigne les contrôles obligatoires qui constatent immédiatement les erreurs qui se présentent. Ces contrôles sont destinés à empêcher que des erreurs puissent être faites. Les contrôles préventifs peuvent prendre la forme de contrôles automatiques, indépendants ou faits par les cadres, manuels ou programmés respectivement automatisés. Il est capital que ces contrôles préventifs soient mis en place sous une forme correcte et à l'échelon approprié, par exemple séparation des fonctions, mots de passe et autorisations d'accès, mesures de protection physiques.

Par *contrôles détectifs*, il faut entendre ceux qui servent à déceler des erreurs. Ils sont entre autres effectués si les contrôles préventifs font apparaître des erreurs trop fréquentes, par exemple lors de l'examen de rapports de contrôle, de concordance, d'inventaires physiques, de reviews.

Exemple 11 – Contrôles détectifs – contrôles préventifs

L'entreprise a l'obligation légale de dresser un inventaire à la fin de chaque exercice annuel (art. 958 al. 1 CO). Cet inventaire se base soit sur l'état déterminé à la date du bilan soit sur la comptabilité des stocks.

L'entreprise procède à l'inventaire physique prévu et constate (contrôle détectif) qu'il existe d'importantes différences d'existants. Les contrôles ultérieurs montrent que les entrepôts n'ont pas été fermés comme prévu (contrôle préventif).

1.2 Contrôles automatiques, programmés et manuels

Les contrôles automatiques sont les plus efficaces et les plus rentables, car il sont directement intégrés dans les processus de l'entreprise par des mesures techniques ou d'organisation. Ces mesures d'organisation sont par exemple la séparation des fonctions, l'établissement d'échelons de compétence et la réglementation des processus de travail.

Il est par exemple possible de classer parmi les *contrôles programmés* les contrôles de chiffres et de totaux ou la comparaison des données.

Les *contrôles manuels* complétant les contrôles programmés sont par exemple les approbations, l'examen critique, les concordances, les contrôles physiques et l'examen de listes d'erreurs.

Contrôles automatiques, programmés et manuels (mesures d'organisation)	Moyens d'organisation	
Pilotage et contrôle par les méthodes choisies par l'entreprise, par exemple: <ul style="list-style-type: none"> ■ séparation des fonctions ■ échelons de compétence, approbations ■ réglementation des processus de travail 	Pilotage et contrôle par l'utilisation de moyens techniques, par exemple par des: <ul style="list-style-type: none"> ■ systèmes de mesure ■ dispositifs de sécurité ■ contrôles informatiques, p. ex. contrôles de chiffres et de totaux 	Plan d'organisation, manuels, diagramme de cheminement et de fonctionnement, formulaires et justificatifs, directives d'imputation, numéros et domaines de concordance, enregistrement des heures, droit de signature, visas, codes de blocage, etc.

Tableau 1. Mesures d'organisation et moyens de pilotage et de contrôle

Exemple 12 – Séparation des fonctions

Le collaborateur responsable des achats peut effectuer directement toutes les commandes et donner l'ordre de payer les factures. Comme il s'occupe en outre lui-même du contrôle matériel des marchandises commandées à leur réception, ce n'est qu'après une longue absence de ce collaborateur qu'il est constaté que pendant des années, des factures ont été payées pour des marchandises jamais livrées à l'entreprise et que le collaborateur du fournisseur lui a servi de complice au détriment de l'entreprise.

Si la séparation des fonctions ne peut pas être complètement réalisée en raison de la taille de l'entreprise, il faut porter une attention particulière à la responsabilité accrue des supérieurs en matière de contrôle.

1.3 Contrôles par les cadres

Les contrôles indépendants par les cadres dirigeants (notamment conseil d'administration et direction) reposent sur leurs connaissances techniques et leur manière d'assumer les tâches de gestion et de surveillance. Des exemples à cet égard sont: contrôles des résultats, notamment en cas de séparation insuffisante des fonctions dans de petites unités d'exploitation ou évaluation des écarts par rapport au budget en cas d'absence de contrôle des transactions. C'est pourquoi tous les échelons hiérarchiques concernés (conseil d'administration et direction inclus) devraient recevoir régulièrement (chaque jour, chaque semaine, chaque mois) des rapports sur les résultats appropriés à leur échelon et les examiner de manière critique (par exemple évolution des résultats financiers par rapport au budget et aux objectifs).

Contrôles indépendants par la direction		Moyens d'organisation
Pilotage et contrôle par la direction et les cadres: ■ sur la base de directives internes ■ selon l'appréciation personnelle	Pilotage et contrôle par des mandataires (principe de la délégation): ■ assistants, organes d'exécution, comités, secrétariats, organisations de projet ■ spécialistes et conseillers externes	Règlements d'organisation, cahiers des charges, procédures d'approbation, budgets, propositions et offres, calendriers, etc.

Tableau 2. Contrôles indépendants par la direction et moyens de pilotage et de contrôle

Exemple 13 – Contrôles par la direction

La direction reçoit chaque mois de la comptabilité financière les résultats accompagnés des chiffres du mois et de l'exercice précédent. Les membres de la direction sont tenus de regarder ces rapports d'un œil critique. Les rapports sont discutés lors de la séance mensuelle et le responsable de la comptabilité financière répond aux questions éventuelles. Il est établi un procès-verbal de la séance.

2. Risques de contrôle

Par risques de contrôle, il faut entendre ceux qui résultent des faiblesses et/ou déficiences du contrôle interne. Comme certains contrôles prévus ne sont pas efficaces, ou seulement insuffisamment, et que des cadres ou des collaborateurs n'assument pas leur fonction de contrôle, il en résulte un risque d'erreurs ou d'irrégularités. En font par exemple partie:

- le détournement de fonds ou de biens;
- la facturation de marchandises ou de services qui n'ont pas été réellement fournis à l'entreprise;
- les opérations exécutées en violation des lois, ordonnances, directives ou contrats;

- l'acceptation de commissions occultes ou de pots-de-vin;
- la transmission à un collaborateur à titre privé ou à des tiers d'une affaire prometteuse en principe lucrative pour l'entreprise;
- l'omission intentionnelle ou la présentation erronée d'événements ou d'informations.

VII. Surveillance des contrôles internes

Les problèmes liés aux contrôles ont évolué avec le temps. Les principales questions classiques qui se posaient étaient par exemple les suivantes:

- Les processus de l'entreprise indiqués sont-ils conformes aux directives?
- Les contrôles effectués dans le cadre des processus de l'entreprise sont-ils définis adéquatement et mis en œuvre efficacement?
- Les résultats et critères financiers sont-ils conformes au plan?

Ou, en d'autres termes: faisons-nous les choses correctement? Les contrôles étaient ainsi clairement axés sur les opérations et les processus. Ces derniers temps, d'autres questions sont venues s'ajouter, par exemple:

- L'entreprise est-elle orientée sur l'accroissement et le maintien durable de sa valeur pour ses actionnaires (ainsi que pour ses autres stakeholders)?
- Les risques d'entreprise (au sens des dangers éventuels et des occasions à saisir) sont-ils en permanence et complètement pris en compte?
- Les processus d'entreprise destinés à la réalisation des objectifs stratégiques ont-ils été définis correctement?

Ou, en d'autres termes: faisons-nous les choses correctement? D'autres éléments stratégiques sont donc venus s'ajouter et la focalisation s'est déplacée vers la gestion des risques et leur contrôle.

1. Conseil d'administration et comité d'audit

Les vérifications et analyses effectuées par le conseil d'administration ou le comité d'audit doivent permettre une évaluation fiable, afin que l'efficacité des contrôles internes soit clairement établie.

Comme déjà mentionné plus haut, les dispositions américaines exigent que la surveillance soit effectuée sur la base d'un modèle de contrôle reconnu. Le COSO Framework contient un programme de vérification d'environ 300 points basés sur les cinq composantes COSO, qui constitue donc un instrument de contrôle utile. L'annexe A montre un exemple de tableau d'évaluation qui identifie les risques principaux et se focalise sur les trois objectifs clés. Cela permet d'émettre une appréciation pour chaque objectif, telle que bon, satisfaisant, avec réserve, insuffisant. A part les vérifications spécialement axées sur l'efficacité des contrôles internes, le conseil d'administration et le comité d'audit devraient recevoir en permanence les rapports importants sur le contrôle interne et les évaluer. En font également partie les rapports des révisions interne et externe.

Chaque année, le conseil d'administration fait le point sur sa performance et celle de ses membres (ch. 14 point 4 Code suisse). Avec cet examen annuel (auto-évaluation), le conseil d'administration doit pouvoir déterminer dans quels domaines il existe des faiblesses ou sur quels points la gouvernance d'entreprise doit être améliorée³⁸.

2. Direction

Dans le cadre de sa responsabilité, la direction doit également veiller à ce que le SCI soit efficace et rentable. De la même manière que pour le conseil d'administration et le comité d'audit, les contrôles peuvent être intégrés dans le processus de travail (rapports de travail) ou avoir lieu sous forme de vérifications directes. La direction doit en outre faire rapport au conseil d'administration sur l'efficacité du contrôle interne.

³⁸ A propos des questions que les membres d'un comité d'audit peuvent poser aux organes de l'entreprise et aux responsables techniques, voir partie 1, annexe D.

3. Auto-évaluation des contrôles (control (risk) self assessment)

A part les vérifications habituelles destinées à évaluer les processus de pilotage et de contrôle, il est aussi possible de procéder à des auto-évaluations des contrôles, en identifiant également leurs faiblesses et en prenant des mesures pour y remédier. L'auto-évaluation des contrôles est un processus formel documenté lors duquel la direction et les collaborateurs directement concernés par des processus de l'entreprise les analysent en se localisant sur les points suivants:

- identification des risques et des dangers potentiels;
- évaluation des processus de pilotage et de contrôle permettant de les réduire et de les gérer;
- élaboration de mesures destinées à ramener les risques à un niveau acceptable;
- définition de possibilités d'amélioration de l'efficacité et de la rentabilité des processus;
- détermination de la probabilité de réalisation des objectifs de l'entreprise.

Le fait de procéder à une auto-évaluation des contrôles permet par ailleurs d'accroître sensiblement la compréhension de la gestion des risques à tous les échelons hiérarchiques. A cet égard, la révision interne assume souvent le rôle d'un régulateur, d'une part en pratiquant un mode de travail basé sur la coopération, d'autre part en utilisant les évaluations des risques et informations provenant des réunions de travail pour planifier les futures révisions.

4. Révision interne

La révision interne doit évaluer le bien-fondé et l'efficacité du SCI. En accomplissant cette tâche, elle doit notamment vérifier:

- si l'environnement d'organisation favorise la prise de conscience des contrôles;
- si les objectifs d'organisation sont réalistes;
- si des procédures d'approbation appropriées ont été définies et sont appliquées pour les transactions;
- si des directives, processus et rapports ainsi que d'autres mécanismes ont été élaborés pour surveiller les activités et garantir les biens – surtout dans les domaines à haut risque;
- si les moyens existants permettent au conseil d'administration et à la direction de disposer d'informations appropriées et fiables;
- s'il existe des normes de comportement définissant les activités interdites et des sanctions en cas de violation.

Il est concevable et souhaitable que les tâches de la révision interne comportent des travaux de vérification spécifiques du SCI et constituent donc notamment la base du rapport sur le contrôle interne exigé du conseil d'administration conformément à la SOX et aux autres normes de gouvernance d'entreprise. On peut aussi envisager que la révision interne évalue l'exactitude et l'intégralité des informations sur la gouvernance du chapitre supplémentaire exigé dans le rapport annuel des sociétés suisses ouvertes au public.³⁹

La garantie systématique de la qualité et l'amélioration de l'accomplissement des tâches de la révision interne sont importantes moins pour des raisons de coût que de réputation. L'évaluation de la qualité du travail de la révision interne doit être faite périodiquement – d'une part par des organes qualifiés de l'entreprise et d'autre

³⁹ Voir à ce sujet la Directive SWX concernant les informations relatives au Corporate Governance.

part par des spécialistes externes (par exemple sociétés de révision, collègues d'autres départements de révision interne).

5. Révision externe

Dans le cadre de l'examen du respect des procédures, la révision externe doit effectuer des opérations de vérification lui permettant de tirer des conclusions sur l'efficacité des contrôles internes. Cet examen par sondages comprend normalement la vérification du respect des procédures (contrôle formel), ainsi qu'éventuellement la re-constitution des contrôles (contrôle matériel). Il existe diverses techniques pour documenter l'environnement de contrôle et les contrôles, par exemple des questionnaires, des check-lists ou des diagrammes de cheminement. La révision externe peut se fonder en partie sur les travaux et résultats de tiers (par exemple ceux de la révision interne), mais doit se faire ensuite sa propre opinion pour dé-finir ses opérations de vérification concernant le contrôle interne.

Les normes applicables à la révision externe sont notamment:

- en Suisse: le Manuel suisse d'audit (MSA) ainsi que les Normes d'audit;
- en Grande-Bretagne: le Turnbull Report;
- aux Etats-Unis: les Public Company Accounting Oversight Board (PCAOB) Standards ainsi que les US Generally Accepted Auditing Standards (US GAAS);
- sur le plan international: les International Standards on Auditing (ISA).

6. Législateur et autorités de surveillance

Dans le cadre des activités de surveillance (Autorité de contrôle en matière de lutte contre le blanchiment d'argent, Office fédéral des assurances privées, Commission fédérale des banques, Office fédéral de l'aviation civile, chimistes cantonaux, inspecteurs des denrées alimentaires), les contrôles portent sur des aspects généralement considérés comme dignes de protection. Ces autorités de surveil-

lance garantissent par des contrôles ciblés que, par exemple, les intérêts des consommateurs ou des investisseurs sont préservés et que les lois et ordonnances sur la protection de ces groupes sont respectées. Les autorités de surveillance disposent des compétences requises pour procéder à des contrôles et pour prendre les mesures nécessaires en cas d'irrégularités.

VIII. Résumé et perspectives

Comme les contrôles internes donnent très souvent lieu à des conceptions erronées ou peu claires, nous en précisons ici quelques caractéristiques essentielles:

- Le contrôle interne se fonde sur une culture de contrôle mise en place et pratiquée par le conseil d'administration et la direction.
- La responsabilité du contrôle incombe à tous les collaborateurs de tous les échelons, la responsabilité principale étant assumée par conseil d'administration.
- Les contrôles internes couvrent tous les domaines de l'entreprise et sont intégrés dans les processus appropriés.
- Les contrôles internes donnent une certitude plus grande, mais pas absolue, que les objectifs de l'entreprise seront atteints.
- Les contrôles internes peuvent être éludés - intentionnellement ou non.
- La révision interne vérifie les contrôles internes.
- La révision externe se prononce sur l'organisation des contrôles internes et en tient compte lors de son évaluation des risques ainsi que lors de la définition de ses opérations de vérification.

Les systèmes normatifs nationaux et internationaux élaborés ces dernières années ont considérablement renforcé les exigences en matière de gouvernance d'entreprise et par conséquent aussi de contrôle interne. Il faut s'attendre à ce que ces systèmes fassent l'objet d'autres adaptations. Ainsi, il ne peut pas être exclu qu'en révisant leurs propres dispositions dans certains domaines, des autorités ne se fondent par exemple sur la SOX très détaillée, mais aussi très formaliste.

Annexe A. Tableau d'évaluation du système de contrôle interne

Composantes	Principaux critères à évaluer	Risques importants	Evaluation des objectifs clés (classement):		
			Efficacité et rentabilité des activités	Fiabilité et intégrité du rapport financier	Conformité avec les lois et les normes
Environnement de pilotage et de contrôle	<ul style="list-style-type: none"> - Intégrité et valeurs éthiques pratiquées dans l'entreprise - Engagement en matière de compétence et de vigilance - Conseil d'administration et comité d'audit - Conception de la direction et mode de travail - Bien-fondé de la structure d'organisation - Attribution claire de compétences et responsabilités - Politique du personnel (directives et pratique) 	Par exemple <ul style="list-style-type: none"> - Pas de code de conduite, code non communiqué ou pas mis en pratique - Conseil d'administration et/ou comité d'audit inactifs, dépendants ou mal informés 	B	S	B
Evaluation des risques	<ul style="list-style-type: none"> - Objectifs globaux de l'entreprise - Objectifs concernant les processus - Identification et évaluation des risques - Gestion des changements 	Par exemple <ul style="list-style-type: none"> - Objectifs pas examinés quant aux risques - Pas de culture en matière de risques - Conception différente des risques au sein de la direction - Tolérance des risques pas définie - Fonction de gestion des risques pas acceptée 	R	R	R
Activités de pilotage et de contrôle	<ul style="list-style-type: none"> - Existence de directives et processus appropriés - Efficacité des contrôles définis 	Par exemple <ul style="list-style-type: none"> - SCI n'existant que ponctuellement - Directives pas organisées - Contrôles ne fonctionnant pas - SCI examiné irrégulièrement 	S	B	S
Information et communication	<ul style="list-style-type: none"> - Qualité des informations (à temps et efficaces) - Efficacité de la communication (moyens et canaux de communication) 	Par exemple <ul style="list-style-type: none"> - Le MIS ne fournit pas d'informations à temps - Pas d'accès à l'Intranet par les sociétés étrangères - Les informations du groupe et des filiales ne concordent pas 	B	B	B
Contrôle	<ul style="list-style-type: none"> - Surveillance permanente - Contrôle spécial - Rapport sur les faiblesses des contrôles identifiées et leur élimination 	Par exemple <ul style="list-style-type: none"> - Pas de fonction de révision interne - Recommandations des révisions interne et externe pas mises en œuvre - Comité d'audit composé de membres sans connaissances financières 	I	B	I

Classement: B = bon; S = satisfaisant; R = avec une réserve; I = insatisfaisant

Annexe B. Glossaire des composantes du contrôle

Pilotage et contrôle adéquats (adequate control) – Le pilotage et le contrôle sont adéquats lorsque la direction garantit de manière suffisante par sa planification et son organisation (structure) que les risques de l'entreprise peuvent être gérés et ses objectifs atteints de façon efficace et rentable.

Services d'audit (assurance services) – Les services d'audit sont des prestations de contrôle indépendantes qui accroissent la qualité des informations concernant la prise des décisions – à savoir notamment leur fiabilité et leur pertinence. Grâce à son indépendance, à son objectivité, à ses compétences professionnelles et à sa vigilance ainsi qu'à sa connaissance globale de l'entreprise, la révision interne est un prestataire de services d'audit approprié. A titre d'exemple, citons les audits en matière de finances, de compliance ou de sécurité des systèmes.

Services de conseil (consulting services) – Il s'agit du conseil ou des prestations analogues dont la nature et l'étendue sont convenues avec le client et qui sont destinées à améliorer les activités de l'entreprise ainsi qu'à faciliter la réalisation de ses objectifs. A titre d'exemples, citons les prestations de conseil ou analogues («counsel», «advice», «facilitation») telles que la participation lors de l'exécution de l'auto-évaluation des contrôles, l'intervention lors de l'optimisation des processus ou la formation continue des collaborateurs.

CoCo – Modèle de contrôle analogue au COSO, mais plus dynamique grâce aux quatre éléments définition des objectifs, garantie, possibilités, surveillance.

Processus de gouvernance d'entreprise – Les principes et règles, structures, stratégies et méthodes par le biais desquels une entreprise est dirigée et contrôlée afin de faire face à ses responsabilités à l'égard de ses stakeholders.

COSO – Le COSO Framework est un concept de pilotage et de contrôle interne. Il comprend les cinq éléments (i) environnement de pilotage et de contrôle, (ii) évaluation des risques, (iii) activités de contrôle, (iv) information et communication ainsi que (v) surveillance.

Compliance – Capacité de garantir dans une mesure suffisante la conformité et le respect des directives de l'entreprise, plans, processus, lois, ordonnances et contrats.

Enterprise Risk Management (ERM) – Gestion ciblée des risques. Il est important à cet égard de définir soigneusement des priorités lors de l'évaluation des facteurs de risque et de gérer à bon escient leur incidence.

Prestataire de services externe (external service provider) – Personne ou société indépendante de l'entreprise qui possède des connaissances spécifiques, des compétences et de l'expérience dans un certain domaine. Font notamment partie des prestataires de services externes les actuaires, les spécialistes en comptabilité, les taxateurs, les environnementalistes, les enquêteurs lors de cas de fraude, les avocats, les ingénieurs, les géologues, les experts en sécurité, les statisticiens, les spécialistes en technologie de l'information, les experts-comptables de l'entreprise et les autres organisations d'audit.

Normes d'audit – Normes de la Chambre fiduciaire qui garantissent la qualité de la révision des comptes et sont destinées à uniformiser la pratique en la matière. Au 1er janvier 2005, les Normes d'audit actuelles seront remplacées par les Normes d'audit suisses (NAS).

Révision interne – La révision interne est un département, un domaine de l'entreprise ou une équipe de spécialistes qui fournissent des services de révision et de conseil indépendants et objectifs et s'efforcent de créer de la valeur ajoutée ainsi que d'améliorer les processus de l'entreprise. La révision interne aide l'entreprise à atteindre ses objectifs en évaluant et en optimisant l'efficacité de la gestion des risques, du pilotage et des contrôles ainsi que de la gouvernance d'entreprise par le biais d'une approche systématique et ciblée. La révision interne peut aussi être fournie par des prestataires de services externes (par exemple des sociétés d'audit). Dans le cadre de la présente partie, la notion de «révision interne» inclut toujours aussi les prestataires de services externes.

Contrôle interne – Voir pilotage et contrôle.

Qualité – Par qualité, il faut entendre l'ensemble des critères et valeurs des critères d'une unité et sa capacité à satisfaire à des exigences définies ou supposées.

Risque (risk) – Survenance éventuelle d'un préjudice ou d'une perte de patrimoine ou chance non saisie. Un risque élevé correspond à une haute probabilité de survenance et/ou à une forte éventualité de perte.

Contrôle des risques (risk control) – Surveillance indépendante du profil de risque voulu par l'entreprise. Le contrôle des risques fixe la base de la politique de l'entreprise en matière de risques (risk policy), de la volonté d'assumer des risques (risk appetite) ainsi que des limites de risque qui doivent être établies par les organes compétents, et surveille le respect du cadre ainsi fixé.

Gestion des risques (risk management) – Pilotage et orientation globale et systématique des risques sur la base des données économiques et statistiques. La gestion des risques comprend l'identification, la mesure, l'évaluation, le pilotage de risques et groupes de risques ainsi que l'établissement de rapports.

Pilotage et contrôle (control) – Toute mesure prise par le conseil d'administration, la direction ou d'autres organes visant à améliorer la gestion des risques et à accroître la probabilité que les objectifs fixés soient atteints. Le concept le plus connu de pilotage interne et de contrôle est le COSO Framework.

Processus de pilotage et de contrôle (control processes) – Directives, méthodes et activités qui font partie intégrante du pilotage interne et du contrôle. Elles servent à piloter et à contrôler les risques de manière à ce qu'ils ne dépassent pas les limites prévues.

Environnement de pilotage et de contrôle (control environment) – L'attitude et les actes du conseil d'administration et de la direction ainsi que d'autres responsables face à l'importance du pilotage et du contrôle au sein de l'entreprise. L'environnement de contrôle détermine le cadre et la structure permettant d'atteindre les principaux objectifs du pilotage interne et du contrôle. Les éléments suivants en font partie:

- intégrité et valeurs éthiques;
- conception et mode de travail de la direction;
- structure d'organisation;
- attribution de compétences et responsabilités;
- politique du personnel et sa mise en œuvre;
- qualification du personnel.

TQM (total quality management) – Voir qualité.

Entreprise (organization) – Dans la présente partie, le terme «entreprise» comprend toutes celles qui revêtent la forme juridique des sociétés de capitaux et de personnes ainsi que les corporations, autorités administratives, associations à but non lucratif et autres associations.