

Intégrer systématiquement l'ORM et le SCI

La législation suisse déclare le système de contrôle interne et la gestion des risques comme étant obligatoires. A condition de procéder systématiquement, l'intégration de ces deux disciplines qui, jusqu'alors, étaient souvent gérées de manière indépendante devrait permettre de créer de nombreuses synergies.

Avec l'ancrage du système de contrôle interne (SCI) et de la gestion des risques dans la législation suisse (Code des obligations à partir de la mi-2007 et Loi sur la surveillance des assurances depuis le 1^{er} janvier 2006), ce sont deux composantes essentielles du corporate governance qui sont déclarées obligatoires. La Suisse réagit ainsi au nouvel environnement des assureurs: les scandales financiers et la chute boursière d'il y a quelques années ont requis l'intervention des agences de notation, des législateurs et des régulateurs dans le monde entier. La demande des stakeholders d'établir des systèmes de contrôle internes et une gestion des risques a sensiblement renforcé les exigences au niveau international (liste non exhaustive):

- nouvelles exigences pour les systèmes de contrôle internes (p. ex. Loi Sarbanes-Oxley, SOX, aux Etats-Unis, Loi sur la sécurité financière en France, 4^e, 7^e et 8^e directives UE ainsi que Code des obligations et Loi sur la surveillance des assurances en Suisse);
- nouvelles exigences en matière de solvabilité (Swiss Solvency Test en Suisse et Solvabilité II dans l'UE);
- Enterprise Risk Management (Standard & Poors).



Marcel Stalder
Certified Public Accountant
Partner
Industry Leader Insurance
Audit Services
marcel.stalder@ch.ey.com



Stephanie Furger
lic. oec. HSG
Senior Manager
Advisory Services
stephanie.furger@ch.ey.com

ORM et SCI: autrefois indépendantes ...

Là où ils étaient en place, les concepts de gestion des risques, en particulier la gestion des risques opérationnels (ORM), et le système de contrôle interne ont été traités pendant longtemps comme des disciplines indépendantes:

- De la gestion des risques est née l'ORM, dont est généralement chargé le Chief Risk Officer et qui est surveillée dans de nombreuses sociétés par un Risk Management Committee.
- Le SCI a été développé à partir des concepts de gestion en tant qu'élément de la direction et de la surveillance de l'entreprise, en étant assorti de différentes responsabilités: le domaine Financial Reporting est subordonné au Chief Financial

Officer et est surveillé par l'Audit Committee; le domaine Operations relève du Chief Operations Officer et le domaine Compliance du Chief Compliance Officer. Dans le cadre des scandales financiers, le législateur a uniquement déclaré obligatoire la partie Financial Reporting du SCI (p. ex. SOX aux Etats-Unis et nou-

La gestion des risques, en particulier la gestion des risques opérationnels (ORM), et le système de contrôle interne (SCI) ont été traités pendant longtemps comme des disciplines indépendantes.

velle réglementation *ad hoc* de la révision dans le CO en Suisse). De ce fait, de nombreuses entreprises ont placé le SCI dans son ensemble sous la responsabilité du CFO et donc de l'Audit Committee.

L'évolution parallèle de ces deux disciplines complémentaires a créé des doublons. Bien qu'ils n'aient pas la même origine et impliquent des responsabilités différentes, l'ORM et le SCI se recoupent souvent. Car ces deux disciplines reposent sur la structure des processus de l'entreprise et soutiennent la direction dans la gestion de l'entreprise. C'est la raison pour laquelle de nombreuses sociétés sont confrontées aux problèmes suivants:

- les managers se plaignent de l'obligation croissante de documentation. Il n'est pas rare qu'ils doivent documenter leurs processus, les risques et les contrôles plusieurs fois par an auprès de différents interlocuteurs (SCI, ORM, gestion de la qualité, etc.);
- c'est ainsi que s'est développé dans de nombreuses entreprises une culture de contrôle qui n'est plus conciliable avec la gestion basée sur le risque;
- d'importantes dépenses sont souvent envisagées pour améliorer les contrôles sans considérer l'aspect coûts/utilité.

... ces disciplines doivent être coordonnées aujourd'hui

En raison de ces exigences, conjuguées à une pression croissante en matière de coûts et de performance, l'efficacité de la gestion des risques devient de plus en plus un facteur de compétitivité. C'est pourquoi les derniers développements visent à intégrer et à coordonner le SCI, l'ORM et d'autres initiatives, comme la gestion de la qualité (EFQM, ISO, entre autres).

A cet égard, il faut utiliser les pratiques existantes tout en renforçant l'efficacité opérationnelle, l'efficacité et la cohérence. Les principaux objectifs de ces efforts de coordination et d'intégration sont les suivants:

- éviter les chevauchements importants ou les lacunes des différentes fonctions de contrôle et de gestion des risques: tous les risques, contrôles et tâches essentiels doivent être identifiés et traités de façon homogène;
- répartir les tâches entre les personnes et les services les plus appropriés: tous les risques identifiés doivent être attribués à un «Risk Taker», à un «Risk Controller» et à un «Risk Owner» et gérés par les tâches correspondantes;
- ancrer le système dans les affaires, car la gestion des risques ne peut plus assumer seule cette responsabilité (fonction «Risk Taker»);
- assouplir le système afin de pouvoir intégrer les nouveaux risques, les chan-

gements organisationnels ou les besoins locaux;

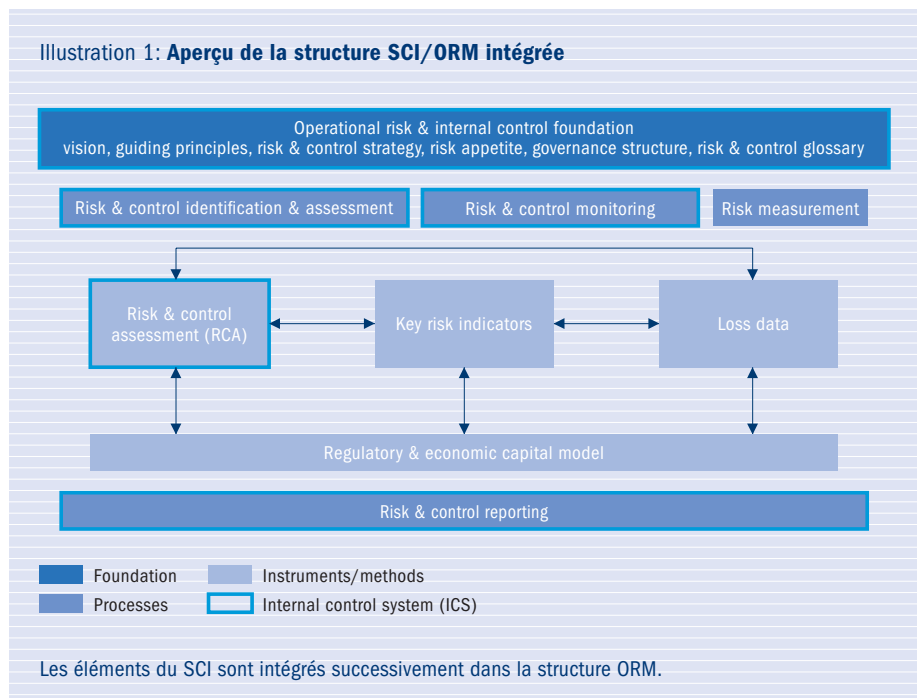
- rendre la révision du système possible et donc permettre la traçabilité des activités; la documentation en découle en tant que conséquence logique.

Un modèle éprouvé de gestion intégrée de l'ORM et du SCI est décrit ci-après.

Modèle SCI/ORM intégré

Le point de départ d'une telle intégration du SCI, de l'ORM et d'autres fonctions de contrôle se situe au niveau de la structure de l'ORM, dans laquelle seront intégrés successivement les éléments du SCI (voir illustration 1).

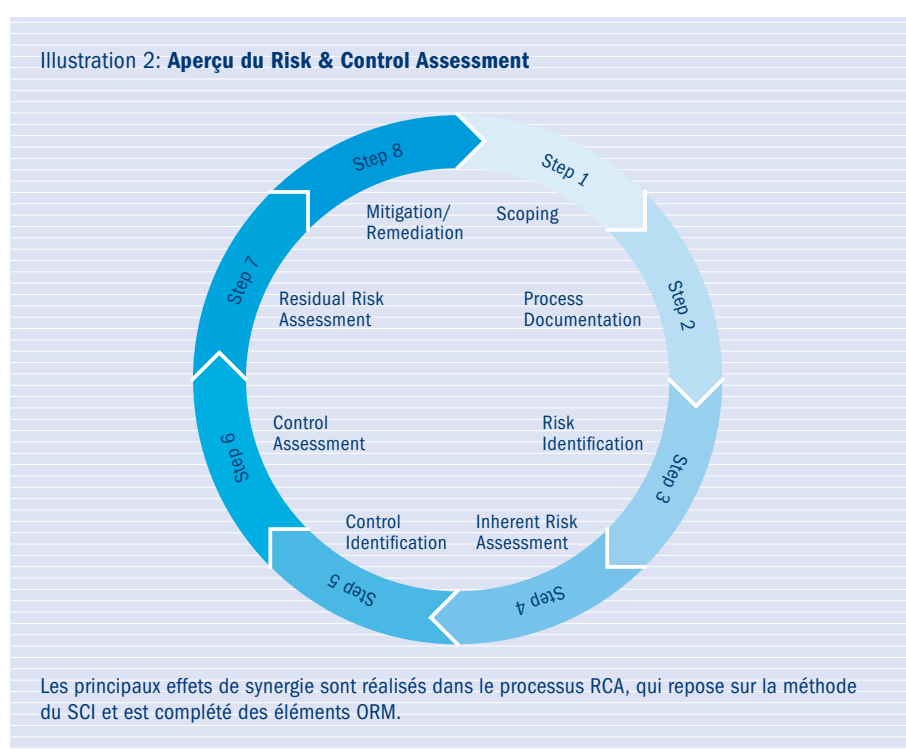
Illustration 1: Aperçu de la structure SCI/ORM intégrée



A la base d'une telle structure-cadre se trouvera la Operational Risk and Internal Control Foundation et c'est ici que les composantes existantes telles que Vision, Guiding Principles, Risk & Control Strategy, Risk Appetite, Governance Structure, Risk & Control Glossary devraient être complétées avec la composante SCI. Loss Data (référence au passé), en tant qu'élément du Risk Measurement, sera repris sans modification car il n'y a pas de nouvelles exigences du côté du SCI. Du point de vue purement réglementaire, les Key Risk Indicators (référence à l'avenir), qui constituent un élément du Risk & Control Monitoring, ne doivent pas être obligatoirement mis en place en Suisse. Les Risk & Control Assessments (référence au présent) sont au cœur de l'association de ces deux approches. C'est ici que les principaux parallèles étaient autrefois créés; c'est donc ici également que l'on pourra réaliser aujourd'hui les principales synergies. C'est pourquoi nous nous pencherons plus en détail sur ces composantes dans la partie suivante. Pour les Regulatory and Economic Capital Models, il n'existe pas encore, dans le domaine ORM, d'exigences réglementaires pour les compagnies d'assurance en Suisse. Cette composante sera cependant importante pour les sociétés qui doivent répondre aux exigences de Solvabilité II. Le Risk & Control Reporting doit être élargi de manière à intégrer les besoins d'information de tous les domaines du SCI (Financial Reporting, Operations et Compliance) et intégré dans l'ORM.

Risk & Control Assessment

C'est au niveau du Risk & Control Assessment (RCA) qu'il est possible d'obtenir les plus grandes synergies. La méthode SCI en constitue la base et les éléments ORM



seront ajoutés. Le processus RCA peut être subdivisé en huit étapes (voir illustration 2):

1. Scoping: dans le Scoping, les processus et les opérations de l'entreprise sont reliés aux comptes annuels (domaine Financial Reporting), aux objectifs de l'entreprise et aux objectifs de performance (domaine Operations) ainsi qu'aux exigences en matière de compliance (domaine Compliance). Cela permet d'identifier les processus d'entreprise qui exercent une influence déterminante sur l'atteinte des objectifs

dans les domaines mentionnés. Ces processus phares constituent la base de la mise en place du système SCI/ORM intégré (voir illustration 3).

Etant donné que l'efficacité de la gestion des risques devient de plus en plus un facteur de compétitivité, les nouveaux développements visent l'intégration et la coordination du SCI, de l'ORM et d'autres initiatives.

2. Documentation des processus: les processus jugés importants dans l'étape 1 «Scoping» sont désormais documentés sur la base des documents déjà existants.

3. Risk Identification: les principaux risques pour l'atteinte des objectifs dans les domaines Financial Reporting, Operations et Compliance sont maintenant identifiés et documentés au niveau du processus. Sur la base du catalogue de risques défini pour l'entreprise dans son ensemble, ils sont répartis en quatre catégories: facteur humain, processus, systèmes et influences externes.
4. Inherent Risk Assessment: les risques identifiés sont évalués au niveau de la probabilité de survenance et de l'étendue du dommage.
5. Control Identification: les contrôles qui ont été mis en place pour gérer les risques identifiés sont déterminés et documentés.
6. Control Assessment: les contrôles identifiés sont évalués au niveau de leur efficacité en terme de conception et de performance.
7. Residual Risk Assessment: le risque résiduel est défini en combinant l'Inherent Risk Assessment (étape 4) et le Control Assessment (étape 6).
8. Mitigation/Remediation: le risque résiduel est mis en relation avec la tolérance au risque de l'entreprise. Si le risque résiduel se situe au-dessus de la limite de tolérance, des Mitigation Actions devront être définies pour réduire le risque encore existant.
- Le modèle intégré décrit peut être résumé comme présenté dans l'illustration 4 (voir page 12).

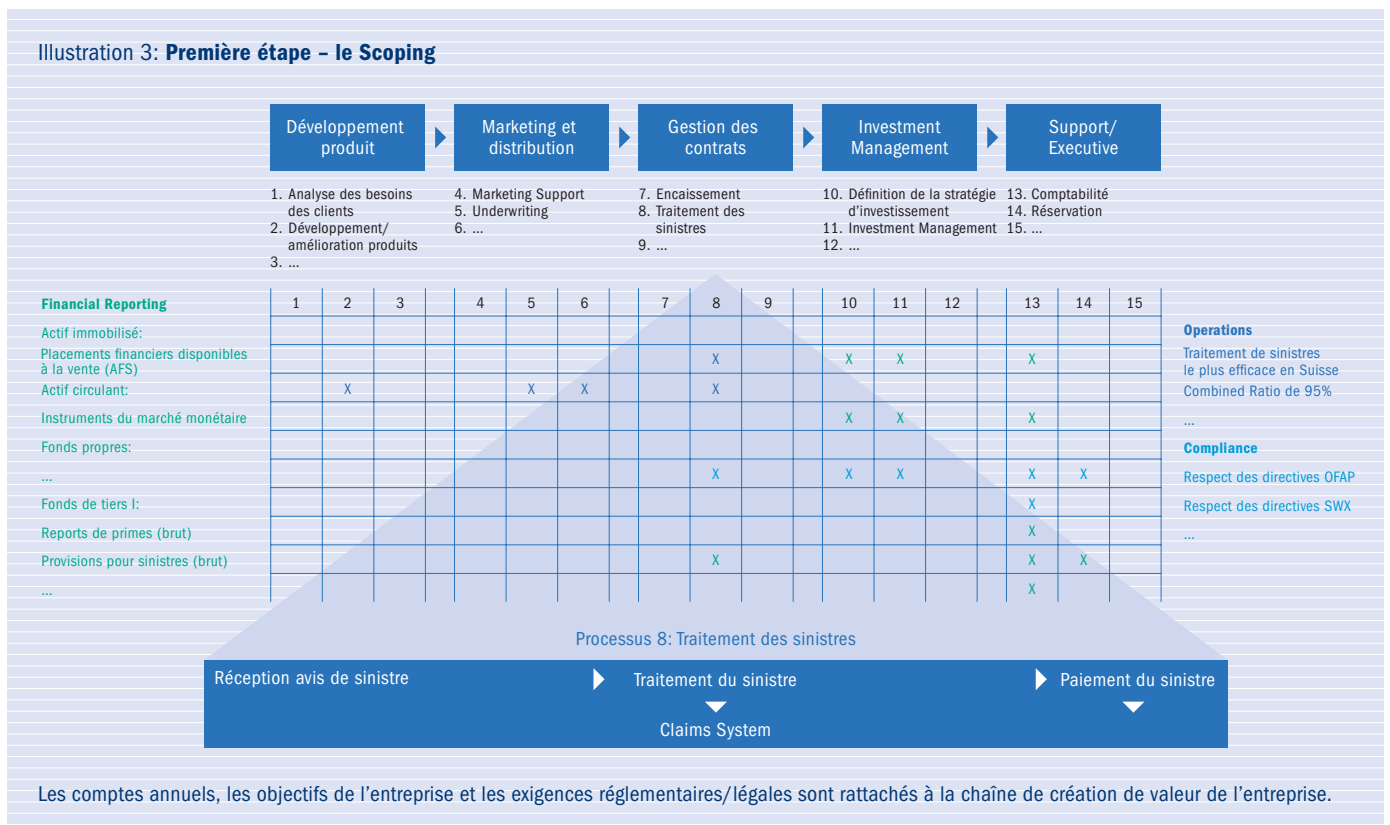
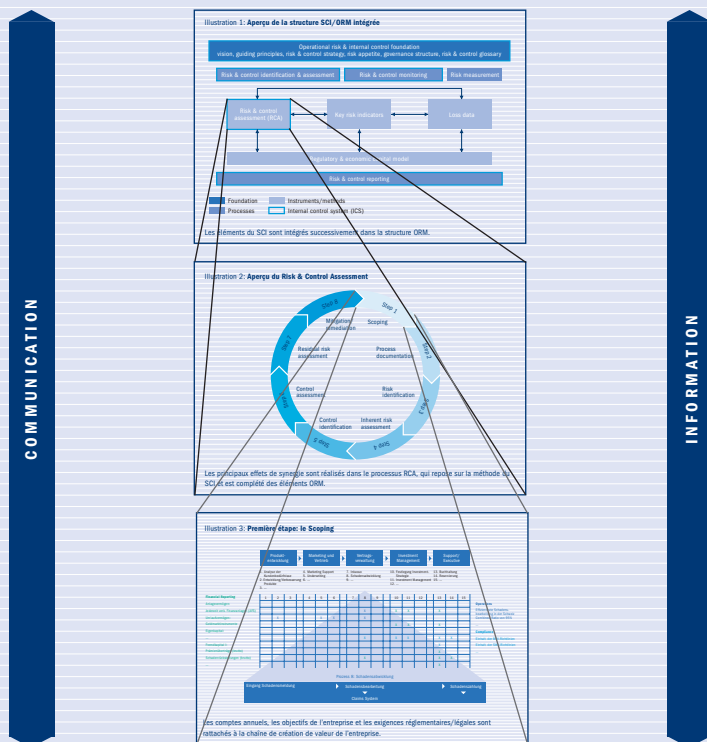


Illustration 4: Structure SCI/ORM intégrée



L'information et la communication sont des éléments essentiels dans le processus de mise en œuvre.

Avantages et difficultés

L'avantage d'un modèle SCI/ORM intégré réside dans l'association systématique des organes de gouvernance, de risque et de contrôle d'une entreprise. Les processus de risque et de contrôle sont définis uniformément et les processus d'Assessment et de Reporting sont harmonisés. Cela permet de supprimer les doublons, de combler les lacunes – et de condenser les reportings en un énoncé global. Ce qui compte, c'est la

sécurité dans son ensemble, et non pas les considérations fragmentées au sein de différentes fonctions. C'est la génération d'une plus-value et non pas la satisfaction isolée d'exigences réglementaires qui est au cœur de cette approche. Ceci accroît en même temps l'acceptation au sein de la direction ainsi que dans l'organisation hiérarchique.

Les exigences de ce modèle ORM et SCI intégré se situent à plusieurs niveaux. Il exige la fusion de domaines et de disciplines

jusqu'alors indépendants. Dans le modèle intégré, la connaissance isolée d'une discipline ne suffit pas. La mise en œuvre ne peut aboutir que par l'engagement d'équipes de spécialistes possédant des connaissances approfondies de tous les thèmes et disposant d'une expérience de plusieurs années dans la branche. Etant donné que ce modèle est nouveau, de nombreuses entreprises ont besoin d'un conseil professionnel. ■