COSO

Le **COSO** est un référentiel de contrôle interne défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*. Il est utilisé notamment dans le cadre de la mise en place des dispositions relevant des lois Sarbanes-Oxley, SOX ou Loi de sécurité financière, LSF, pour les entreprises assujetties respectivement aux lois américaines ou françaises. Le référentiel initial appelé COSO 1 a évolué depuis 2002 vers un second corpus dénommé *COSO 2*.

Historique

COSO est l'acronyme abrégé de Committee Of Sponsoring Organizations of the Treadway Commission, une commission à but non lucratif qui établit en 1992 une définition standard du contrôle interne et crée un cadre pour évaluer son efficacité. Par extension ce standard s'appelle aussi COSO.

En 2002, le Congrès américain, en réponse aux scandales financiers et comptables (Enron, Worldcom…), promulgue la loi Sarbanes–Oxley (the Sarbanes-Oxley Act ou SOX act). Cette loi oblige les sociétés faisant appel à l'épargne publique à évaluer leur contrôle interne et à en publier leurs conclusions dans les états demandés par la Securities and Exchange Commission (SEC). Imposant en outre l'utilisation d'un cadre conceptuel, le SOX act a favorisé l'adoption du COSO comme référentiel. En France, la loi de sécurité financière (dite loi LSF) promulguée peu après en 2003, a également contribué à sa diffusion.

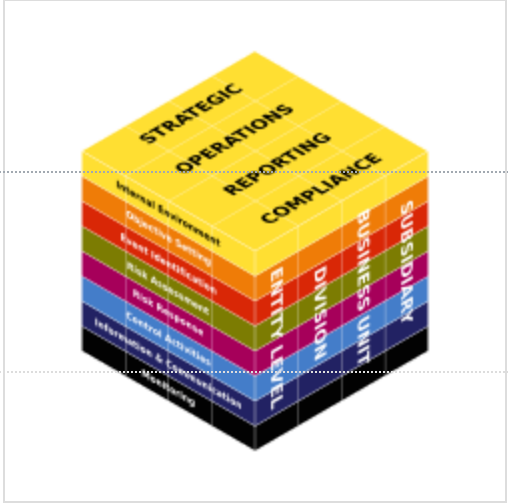
Le référentiel COSO (Internal Control – Integrated Framework)

Les principes

Le référentiel COSO est basé sur les principes de base suivants :

- Le contrôle interne est un processus : c'est un moyen, pas une fin ; il ne se cantonne pas à un recueil de procédures mais nécessite l'implication de tous à chaque niveau de l'organisation.
- Le contrôle interne doit procurer l'assurance raisonnable (mais non absolue) d'un management et d'une direction respectueuse des lois.

- Le contrôle interne est adapté à la réalisation effective des objectifs.



Visualisation du framework COSO.

Le cadre : le cube COSO

Le cadre COSO repose sur les notions d'objectifs et de composants.

Les trois objectifs

Le référentiel COSO définit le contrôle interne comme *un processus mis en œuvre par les dirigeants à tous les niveaux de l'entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants* :

- l'efficacité et l'efficience des opérations,
- la fiabilité des informations financières,
- la conformité aux lois et règlements.

On notera que ces objectifs correspondent en grande partie aux préoccupations des investisseurs.

Les cinq composants

Le contrôle interne, tel que défini par le COSO, comporte cinq composants. Ces composants procurent un cadre pour décrire et analyser le contrôle interne mis en place dans une organisation. Il s'agit de :

- l'**environnement de contrôle**, qui correspond, pour l'essentiel, aux valeurs diffusées dans l'entreprise ;
- l'**évaluation des risques** à l'aune de leur importance et fréquence ;
- les **activités de contrôle**, définies comme les règles et procédures mises en œuvre pour traiter les risques, le COSO imposant la matérialisation factuelle des contrôles ;
- l'**information et la communication**, qu'il s'agit d'optimiser ;

- le pilotage, c'est-à-dire le « **contrôle du contrôle** » interne.

Le cube

Après les objectifs et composants, le COSO impose de distinguer les structures de l'entreprise (sociétés, entités, fonctions, ...).
La combinaison des trois objectifs, des cinq composants et des structures de l'entreprise, vus comme trois axes d'analyse distincts, constitue ce qui est appelé le cube COSO.

COSO 2 - Enterprise Risk Management Framework

Le COSO 2, "Enterprise Risk Management Framework" est aujourd'hui le cadre de référence de la gestion des risques. Le présent chapitre vise à en réaliser une synthèse, notamment en se basant sur les concepts développés dans le COSO 1, "Internal Control – Integrated Framework".

Positionnement du COSO 2 par rapport au COSO 1

Pour rappel, le COSO 1 propose un cadre de référence pour la gestion du contrôle interne. Le contrôle interne est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- L'efficacité et l'efficience des opérations,
- La fiabilité des informations financières,
- La conformité aux lois et aux réglementations en vigueur.

Le COSO 2 propose un cadre de référence pour la gestion des risques de l'entreprise (Enterprise Risk Management Framework). La gestion des risques de l'entreprise est un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, exploité pour l'élaboration de la stratégie et transversal à l'entreprise, destiné à

- identifier les événements potentiels pouvant affecter l'organisation,
- maîtriser les risques afin qu'ils soient dans les limites du « Risk Appetite (**appétence au risque**)» (cf. ci-dessous) de l'organisation,
- fournir une assurance raisonnable quant à la réalisation des objectifs de l'organisation.

Il apparaît que **le COSO 2 inclut les éléments du COSO 1** au travers du troisième point et le complète sur le concept de gestion des risques. Le COSO 2 est basé sur une vision orientée risques de l'entreprise.

Une nouvelle notion, le « Risk Appetite »

La notion de « Risk Appetite » est nouvelle dans le COSO 2. Le « Risk Appetite » est le niveau de prise de risque accepté par l'organisation dans le but d'accroître sa valeur. Différentes stratégies exposeront l'organisation à différents risques. En conséquence, le « Risk Appetite » doit être pris en compte dans la définition de la stratégie de l'organisation afin de s'assurer que les résultats de cette stratégie sont cohérents avec le « Risk Appetite » défini pour l'organisation.

Synthèse des modifications opérées sur le cube COSO

Le modèle du cube et son architecture à trois plans sont conservés:

1. Niveaux de l'organisation
2. Éléments de contrôle interne (qui devient Éléments de gestion des risques)
3. Objectifs de l'organisation

En revanche, les différents plans sont modifiés ou enrichis.

1. Axe "Niveaux de l'organisation"

- Apport d'un cadre plus strict de décomposition de la structure d'une organisation
- Mise en évidence de la nécessité de prendre en compte l'ensemble de l'organisation pour que le COSO 2 soit appliqué avec succès.

2. Axe "Objectifs"

- Apport d'un nouvel objectif: « stratégique ».
- Élargissement de la notion de reporting : cette notion couvre désormais non seulement le reporting financier, mais aussi la remontée d'informations non-financières. De plus, cette notion couvre dorénavant à la fois la remontée d'informations externes mais aussi internes.

3. Axe "Éléments de contrôle"

Enrichissement de l'axe « éléments de contrôle » qui devient « éléments de gestion des risques » et qui passe de cinq à huit éléments :

1. L'élément **environnement interne** (anciennement *environnement de contrôle*) est complété de la notion d' « appétence au risque » (qui signifie acceptation et tolérance d'un risque, dans le cadre d'un niveau d'efficacité recherchée),
2. L'élément *évaluation des risques* est éclaté en quatre éléments dont les notions existaient déjà dans le COSO-1 mais étaient moins détaillées : 2a **Définition d'objectifs**, 2b **Identification des événements**, 2c **Évaluation des risques**, 2d **Réponse aux risques**,
3. L'élément **activités de contrôle** reste inchangé,
4. L'élément **Information et Communication** est complété des notions de temps et de granularité de l'information,

5. L'élément **Supervision** (ou pilotage) reste inchangé.

Modifications opérées sur l'axe « Niveaux de l'organisation »

Le COSO 2 s'applique à l'ensemble de l'entreprise, aussi bien au niveau le plus haut (« entité ») qu'au niveau opérationnel (« business unit »). Mais pour appliquer le COSO 2 avec succès, il faut prendre en compte l'ensemble du périmètre des activités d'une organisation. Le COSO 2 considère les activités à différents niveaux de l'organisation :

- Au niveau de l'organisation (« entity ») pour des activités telles que la planification stratégique ou l'allocation des ressources,
- Au niveau des unités de métier (« business unit ») pour des activités telles que le marketing, et les ressources humaines,
- Au niveau des processus métier (« business process ») pour des activités telles que la production, les achats,
- Et aussi aux niveaux des projets ou initiatives qui n'ont pas encore de place définie dans la structure de l'organisation.

Par rapport au COSO 1, le COSO 2 apporte :

- un cadre plus strict de décomposition de la structure d'une organisation - par niveaux - que le COSO 1 qui ne retient pas de structure de décomposition spécifique pour une organisation. Cette décomposition est utile à la vision en portefeuille de risque (cf. ci-dessous) exposée par le COSO 2.
- la nécessité de prendre en compte l'ensemble de l'organisation pour être appliqué avec succès.

La notion de portefeuille de risques (« Portfolio »)

Il est demandé à l'organisation d'avoir une vision de ses risques sous forme d'un portefeuille. Ce portefeuille doit caractériser les risques à chaque niveau de l'organisation. La compilation du portefeuille permet donc d'avoir une vision globale des risques de l'organisation. Cette vision pourra alors être rapprochée de l' « appétence au risque » définie pour l'organisation.

De plus, la compilation du portefeuille de risques permet au management :

- de mettre en évidence des risques qui peuvent être tolérés au niveau d'une unité mais qui en s'additionnant ne seraient plus dans les limites de l' « appétence au risque » définie pour l'organisation.
- d'appréhender des événements potentiels (au niveau global) plutôt que des risques et donc de mieux comprendre comment les risques interagissent entre eux au niveau de l'organisation. Par exemple, une baisse des taux d'intérêt pourrait affecter positivement le coût du capital mais négativement les produits de taux.

Modifications opérées sur l'axe « Objectifs de l'organisation »

Apport d'un nouvel objectif : « stratégique ».

Un objectif stratégique est un objectif « high-level », qui soutient et concourt à la mission/vision de l'organisation. Les objectifs stratégiques reflètent les choix du management quant à la recherche de création de valeur par l'organisation pour ses actionnaires.

Les trois autres types d'objectifs : opérationnel, reporting, et réglementaire, sont dépendants des objectifs stratégiques. Ils sont appelés les « related » objectifs. Par exemple, pour une organisation, il s'agira de définir :

- Quelle est sa mission/vision,
- Quels sont les objectifs stratégiques soutenant cette mission/vision,
- Quelle est la stratégie à mettre en œuvre pour atteindre ces objectifs stratégiques,
- Et en déduire les « related » objectifs qui soutiennent la stratégie mise en œuvre.

À la différence du COSO 1, la mise en œuvre de COSO 2 nécessite donc d'avoir une vision des objectifs stratégiques de l'entreprise en plus des « related » objectifs.

Élargissement de la notion de reporting

Par rapport au COSO 1, cette notion couvre désormais :

- non seulement le reporting financier, mais aussi la remontée d'informations non-financières,
- non seulement la remontée d'informations externes mais aussi la remontée d'informations internes.

Modifications opérées sur l'axe « Éléments »

L'axe « éléments de contrôles», qui devient « éléments de gestion des risques », a été légèrement modifié et surtout enrichi : L'élément environnement de contrôle est complété de la notion d' « appétence au risque »,

- L'élément évaluation des risques est éclaté en quatre éléments dont les notions existaient déjà dans le COSO 1 mais sous forme moins détaillée : définition d'objectifs, Identification des événements, Évaluation des risques, Réponse aux risques,
- L'élément activités de contrôle reste inchangé,
- L'élément Information et Communication est complété des notions de temps et de granularité de l'information,
- L'élément pilotage reste inchangé.

À la suite de ces modifications, la lecture de ce nouveau plan met en évidence un bloc homogène que l'on peut qualifier «de bloc d'éléments de risques »* et qui contient les cinq éléments : définition d'objectifs, identification des évènements, évaluation des risques, réponse au risque et activités de contrôle.

** cette notion de* bloc d'éléments de risques *n'est pas présente dans le COSO 2. Elle est ici proposée au lecteur dans un but pédagogique.*

Remarque :

La pyramide qui schématisait la partie « éléments de contrôle interne » disparaît dans le COSO 2.

Environnement interne

L'élément *environnement interne* reprend les notions de l'élément *environnement de contrôle* du COSO 1 : importance des individus (compétence, éthique), du style de management, de la délégation des responsabilités,…

En revanche, ce nouvel élément s'enrichit d'une nouvelle notion : celle d' ***Appétence au risque*** : c'est-à-dire la prise de risque acceptée par l'entreprise dans le but d'accroître sa valeur. Cette « appétence au risque » permet ensuite de déterminer le niveau de la tolérance de risque aux différents niveaux de l'organisation. Cette notion est nécessaire et précède la définition de la stratégie de l'entreprise.

Le bloc « Éléments de risques »

Par rapport à COSO 1, les différents composants de ce bloc sont plus détaillés et fixent un cadre plus précis :

- pour l'identification des événements potentiels (tendances, événements passés)
- pour l'évaluation des risques (risque inhérent, risque résiduel),
- pour les réponses aux risques (catégorisation des types de réponses).

Ce bloc comporte les cinq éléments suivants :

1. Définition d'objectifs
2. Identification des événements
3. Évaluation des risques
4. Réponses aux risques
5. Activités de contrôle

Le management doit tout d'abord se fixer des objectifs(1) en dehors des événements susceptibles de venir les perturber. Ces objectifs sont de quatre types : stratégiques, opérationnels, liés au reporting et à l'adéquation avec la réglementation.

Puis le management détermine pour chacun de ses objectifs les événements (2) susceptibles d'avoir des impacts, que ceux-ci soient positifs ou négatifs. Les événements avec impacts négatifs représentent des risques, ceux avec des impacts positifs représentent des opportunités. L'identification des événements potentiels passe par l'utilisation de combinaison de méthodes : tendances, événements déclencheurs, corrélation avec les événements passés.

On passe ensuite à une évaluation des risques (3) pour les événements négatifs. Cette évaluation doit déterminer la probabilité que cet événement survienne et les impacts alors engendrés. Cette évaluation des risques doit présenter dans un premier temps le risque inhérent, c'est-à-dire le risque qui existe si le management ne met en place aucune action corrective. Dans un second temps, lorsque l'élément de réponse au risque aura été traité, il sera possible de déterminer un risque résiduel. (Boucle unique de processus itératif). Il est suggéré d'utiliser un système d'unité de mesure cohérent entre la mesure des « Définitions d'objectifs » et l'évaluation des risques.

Le risque évalué, il est ensuite demandé de définir les différentes parades possibles. C'est la réponse au risque (4). Plusieurs options sont parfois possibles. Il est alors nécessaire de les expliciter. Ces réponses peuvent être classées dans les quatre catégories suivantes : l'évitement, la réduction, la mutualisation ou l'acceptation du risque. Si la méthode de formalisation (option, classification) est incluse dans le périmètre de COSO 2, le choix de la solution n'en fait en revanche pas partie. Une fois la réponse au risque définie, l'organisation peut s'assurer que le risque résiduel correspond à sa tolérance de risque (3).

Il est ensuite nécessaire de mettre en place des activités de contrôle (5) qui se concrétisent sous la forme de normes (« ce qui doit être fait ») et se voient déclinée en procédures (« comment le faire »).

Information et communication

Par rapport à COSO 1, COSO 2 apporte les concepts suivants :

- la nécessité de considérer que les informations sont issues des événements passés, présents et futurs. Cette vision doit notamment permettre :
  - une comparaison des performances de l'organisation (passées, et potentielles futures) et l'identification des évolutions et tendances de l'activité de l'organisation,
  - l'aide à la détection des potentiels événements futurs qui affectent le profil de risques actuel de l'organisation, ce profil de risques devant donc être rapproché de l' « appétence au risque ».
- la nécessité de s'assurer que la granularité des informations (niveau de détail et périodicité), est suffisante pour identifier, analyser, et répondre aux risques et ainsi rester dans les limites de son « appétence au risque ».

De plus, COSO 2 insiste sur le concept de présentation de l'information pour communiquer, i.e. l'information doit être communiquée sous une forme adaptée en fonction de l'interlocuteur destinataire.

Pilotage

Pas d'ajout sur l'élément « Pilotage ».

Rôles et responsabilités

Le COSO 2 souligne l'importance de la prise de responsabilité dans une entreprise et détaille ce qu'elle recouvre pour chacun des acteurs. On retrouve dans cette partie des analogies fortes avec la loi Sarbanes-Oxley.

Par rapport au COSO 1, le COSO 2 apporte quelques modifications aux rôles des intervenants :

- Un nouveau rôle apparaît: le « Risk officer »,
- Le rôle du board of directors est plus étendu que dans le COSO 1.

Les acteurs responsables (« Responsible parties »)

- Niveau 1: Opérationnelles

- Niveau 2: Fonction filière risque
- Niveau 3: Audit-inspection
- Niveau 4: Organe délibérant / Organe exécutif

Le Board of directors supervise avec attention la gestion des risques :

- Il connaît le périmètre de couverture efficace de gestion des risques mis en place par le management de l'organisation,
- Il connaît et est en accord avec le « Risk appetite » de l'organisation,
- Il revoit le portefeuille de risques et effectue son rapprochement avec le « Risk Appetite »
- Il est informé des risques les plus significatifs et de la pertinence de la prise en charge de ces risques.

Le « Risk Officer»

Le Risk Officer (RO) est le facilitateur de la mise en œuvre du COSO 2. Il travaille avec les autres responsables afin de les aider à mettre en place une gestion efficace des risques pour leur périmètre de responsabilité. Sans être exhaustif, ses attributions pourraient être :

- l'élaboration de procédures de gestion des risques (incluant les rôles, responsabilités),
- l'élaboration d'un langage commun de gestion des risques (uniformisation des mesures de probabilité et d'impact, des catégories de risques..),
- l'accompagnement des managers dans l'élaboration de leur réponse aux risques (aide directe, formation…),
- la supervision des managers pour l'élaboration des tolérances de risques,
- l'accompagnement des managers pour l'établissement des activités de contrôles,
- la supervision du processus de reporting de gestion des risques,

Son intervention porte donc sur l'ensemble des éléments de gestion des risques.

Les auditeurs internes

De la même manière que dans COSO 1, ceux-ci n'ont pas la responsabilité première de la mise en œuvre de COSO 2. Par contre, ils ont un rôle prépondérant dans l'évaluation du système de gestion des risques.

Les auditeurs externes

Ceux-ci travaillent au niveau « entité ». Ils donnent une opinion sur la constitution des états financiers. L'approche moderne pour se prononcer sur les états, consiste en l'évaluation du système de contrôle interne suivant les normes de travail de l'audit.

Voir aussi

Bibliographie

- *COSO 1, "Internal Control – Integrated Framework"*

- *COSO 2, "Enterprise Risk Management Framework"*

Articles connexes

- Gestion du risque
- Contrôle interne
- Loi Sarbanes-Oxley

Liens externes

- `(fr)` COSO Cadre de référence du management des risques de l'entreprise (http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary_french.pdf).
- `(en)` Site du *Committee of Sponsoring Organizations of the Treadway Commission* (http://www.coso.org/). COSO
- (fr) Le Coso, kesako (http://audit-controle-interne.com/le-coso-kesako/)
