

# Contrôle Interne : pour la gouvernance et la maîtrise des risques

Laurent de CASTELBAJAC, Manager  
Vivien NJEWEL, Consultant Confirmé

*Depuis une dizaine d'années, différentes réglementations (CRBF 97-02, Sarbane Oxley ; Loi de Sécurité Financière, Kon Trag en Allemagne, Directives Européennes, etc.) ont fait du contrôle interne un élément clé en matière de gouvernance et de maîtrise des risques. Elles ont été motivées par de multiples accidents et scandales financiers (Barings, Enron, Parmalat, etc.).*

*Les récents événements (pertes de la Société Générale, "incident" des Caisses d'Epargne, Affaire Madoff) nous rappellent les enjeux du contrôle interne et les failles des dispositifs actuels.*

*Après avoir rappelé les grandes lignes du "dispositif" de contrôle interne, nous présenterons les limites et les perspectives du contrôle interne dans les entreprises (sachant que, comme disait Winston Churchill, "la prévision est difficile, surtout en ce qui concerne l'avenir...").*

*On voit ainsi se dessiner deux tendances contradictoires : d'un côté une aversion croissante pour le risque, et de l'autre, les résistances probables à un contrôle de plus en plus contraignant.*

## Le dispositif de contrôle interne

### Définition du contrôle interne

Les définitions du contrôle interne sont nombreuses. Beaucoup d'organismes ou Groupes de Place ont ainsi publié leurs définitions : COSO (Committee of Sponsoring Organizations of the Treadway Commission est une initiative privée américaine qui fait suite à une série de faillites "suspectes" survenues dans les années 80. Cette commission dirigée par le Sénateur Treadway a abouti à la publication du rapport COSO en 1992), Ordre des Experts Comptables, IFACI (Institut Français de l'Audit et du Contrôle Interne), Comité Bâle, Solvency II, AMF, etc. Les textes réglementaires y vont également de leurs définitions (CRBF, Décret Assurances, Décret pour les Mutuelles). Toutefois, les réglementations récentes (SOX, LSF) font référence explicitement ou implicitement aux travaux du COSO. Actuellement, près de 2/3 des entreprises utilisent le COSO comme référentiel.

C'est donc la définition du COSO que nous reprendrons à notre compte. Le 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, représentant la 1ère dimension du cube :

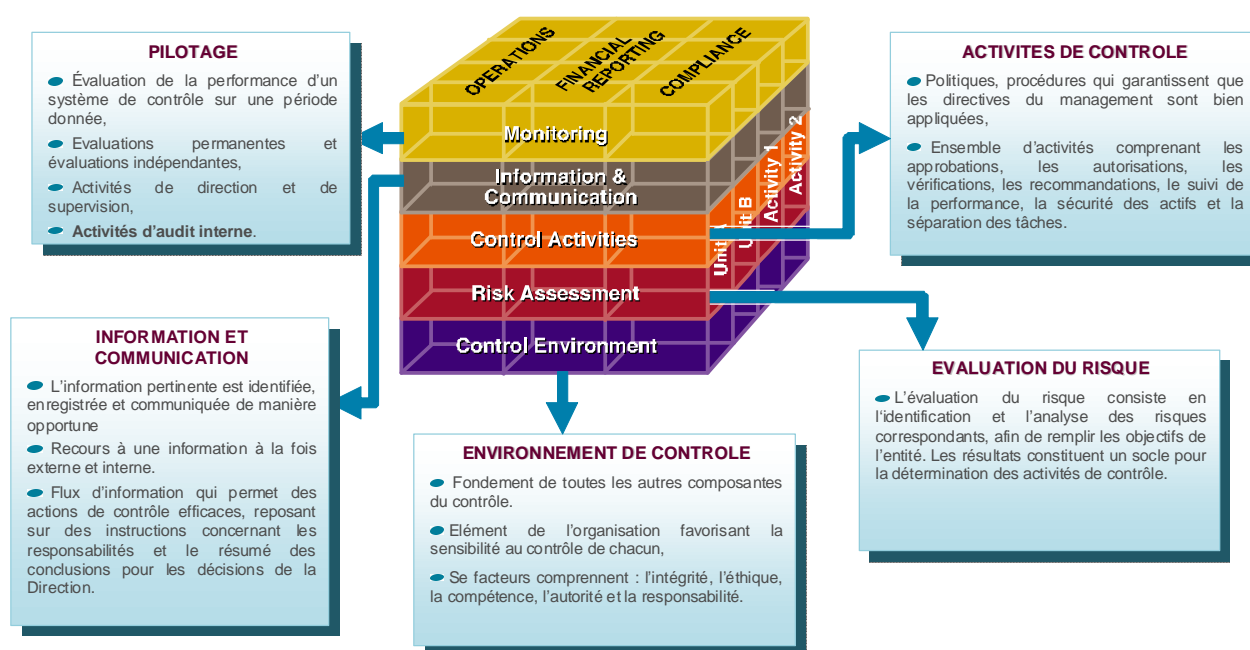
- La réalisation et l'optimisation des opérations,

- La fiabilité des informations financières,
- La conformité aux lois et règlements.

La nature "raisonnable" est une constante que l'on retrouve dans toutes les définitions, les différentes commissions précitées ayant prudemment tenu compte des limites inhérentes à toute organisation humaine : le "risque zéro" n'existe pas.

Le référentiel COSO définit le dispositif de contrôle interne comme un assemblage de cinq composantes qui contribuent aux trois objectifs précités, représenté par un cube multicolore. Les cinq composantes sont : l'environnement de contrôle, l'évaluation des risques et les activités de contrôle, la communication, et le pilotage.

## LES COMPOSANTES DU COSO



La troisième dimension du cube correspond aux différentes activités ou filiales de l'entreprise, concernées par le dispositif.

## Le processus de contrôle interne

La mise en œuvre du dispositif de contrôle interne est une obligation réglementaire pour les entreprises cotées en France. Elle s'appuie sur les objectifs stratégiques définis par le management et nécessite l'implication de tous les acteurs de l'organisation. Le processus de contrôle doit alors s'intégrer dans l'ensemble des processus opérationnels et fonctionnels des organisations.

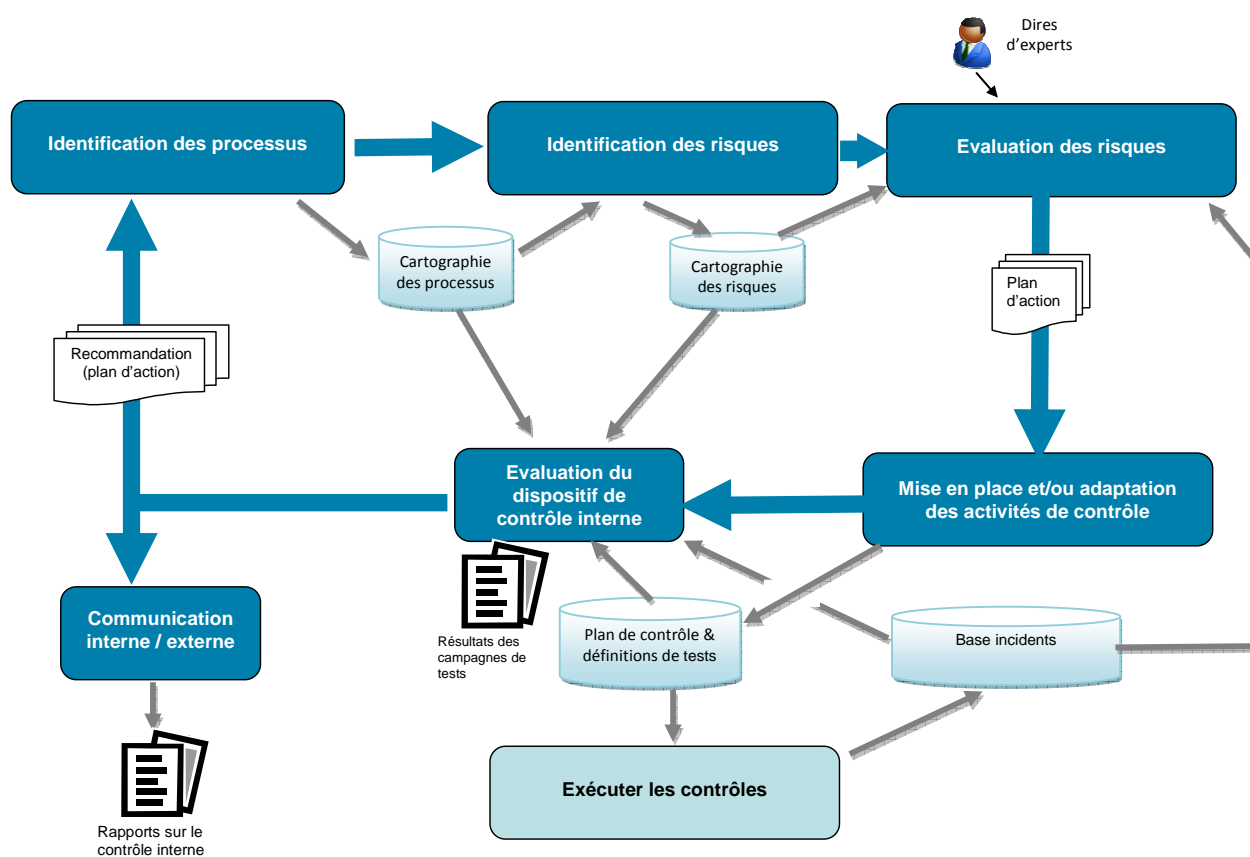
Le processus de contrôle interne s'apparente à un cercle vertueux où la cartographie des processus apporte aux parties prenantes de la clarté sur leur organisation : elle structure ainsi l'identification et l'évaluation des risques. A partir de là, on peut identifier et mettre en place les contrôles qui aideront à maîtriser ces risques.

En bout de chaîne, l'évaluation du dispositif permet d'en détecter les possibilités d'amélioration (contrôles manquants ou non pertinents, évolution des risques, nouvelles activités,...).

Ce processus s'appuie sur un certain nombre de référentiels et bases de données : cartographie des processus et des risques, plans de contrôles, base incidents.

Ce processus est piloté en général par une fonction dédiée dont le nom peut varier en fonction des entités (Direction du Contrôle Interne, Direction du Contrôle Permanent, Direction de la Conformité, RCSI,...).

## PROCESSUS DE CONTROLE INTERNE



Le processus de Contrôle Interne s'organise autour de 6 points:

- **Identification des processus** : la modélisation des activités de l'organisation par l'approche processus permet de comprendre le fonctionnement de l'organisation. Cette étape aboutit à la cartographie des processus de l'entreprise. La description des processus permet d'identifier et de qualifier les zones à risque.
- **Identification des risques** : elle consiste à mettre en évidence des facteurs pouvant empêcher la réalisation des objectifs de l'organisation. Au-delà de l'identification, l'objectif pour les organisations est d'évaluer le risque réellement encouru.
- **Evaluation des risques** : évaluer un risque, c'est non seulement mesurer sa probabilité de survenance mais aussi qualifier son impact sur le résultat et la pérennité de l'organisation. Il est important également de déterminer le niveau de risque accepté (appétence au risque). L'évaluation peut être entreprise de façon qualitative (à partir de la connaissance des experts métiers) ou quantitative (à partir des données de la base incidents).

Deux approches peuvent être utilisées : Bottom-up (approche de type "bas vers le haut" reposant sur une démarche inductive menée à partir de l'analyse du déroulement des processus) ou Top-down (approche de type "haut vers le bas" reposant sur une démarche déductive menée sur la base d'interviews) pour évaluer les risques. Une fois l'évaluation faite, il convient de suivre l'évolution des risques. Ce suivi passe par l'identification d'indicateurs pertinents dont la qualification est propre à chaque risque identifié.

- **Mise en place et/ou adaptation des activités de contrôle** : la définition des contrôles découle de l'évaluation des risques et du niveau de risque accepté, et de l'efficacité des éventuels contrôles existants. Elle permet à l'organisation de mettre en place les activités de contrôle (les contrôles peuvent être des actions préventives ou détectives). Ces contrôles sont documentés dans un plan de contrôle. L'exécution des contrôles permet de mesurer le risque réellement encouru et alimente la base d'incidents.
- **Evaluation du dispositif de contrôle interne** : le dispositif une fois mis en place doit être évalué au regard des objectifs définis par le management. Pour cela, les organisations procèdent à des campagnes de tests ou d'auto-évaluations. L'évaluation du dispositif aboutit à des recommandations et nourrit la communication externe.
- **Communication externe** : ce dispositif et les modalités de sa mise en œuvre font l'objet d'une communication externe exigée par les différents régulateurs.

Au terme de cette démarche, l'organisation aura entamé le processus vertueux d'amélioration continue et transformé en opportunité (du moins en théorie) l'obligation réglementaire de mettre place le dispositif de contrôle interne.

### **Organisation autour du contrôle interne et niveaux de contrôles**

Le contrôle interne repose sur un socle de contrôles permanents et périodiques dans le cadre d'une organisation où sont clairement définis les pouvoirs et les responsabilités. Trois niveaux de contrôle se dégagent.

- **Premier niveau** : les contrôles sollicitent l'ensemble des acteurs de l'organisation. Ce sont en général des contrôles quotidiens, exhaustifs, supervisés et formalisés (= pouvant être retracés).

Exemple : vérification pour un client de la banque des factures CB susceptibles d'être frauduleuses.

Séparation des tâches : à ce niveau, le dispositif de contrôle interne doit veiller à ce que les tâches d'exécution et de contrôle / validation soient assurées par des personnes différentes (exemple : la personne qui effectue les virements bancaires est différente de celle qui effectue les rapprochements).

- **Deuxième niveau** : l'organe de contrôle "permanent" ou tout autre acteur n'ayant pas participé au contrôle de premier niveau s'assure de l'efficacité du contrôle de premier niveau, via des auto-évaluations (évaluation du contrôle par l'opérationnel) ou des campagnes de tests (contrôle du contrôle).

Exemple de test : refaire le contrôle et comparer les résultats avec ceux obtenus par l'opérationnel en charge du contrôle.

Outre l'effet dissuasif sur des acteurs opérationnels qui pourraient relâcher les contrôles ou les détourner, le contrôle de deuxième niveau est surtout un moyen d'évaluer le dispositif de maîtrise des risques, afin d'en détecter les faiblesses.

- **Troisième niveau** : la Direction de l'Audit et/ou l'Inspection Générale assurent la mise en œuvre de contrôles "périodiques". L'audit interne est une activité indépendante qui effectue des audits au cours de missions ciblées (alors que le contrôle de deuxième niveau a un caractère plus systématique). Il a la responsabilité de diagnostiquer l'ensemble du dispositif et d'en recommander des améliorations.

La séparation des deux organes (contrôle permanent et audit) est soulignée par le fait que la Direction du Contrôle Permanent dépend de "l'organe exécutif" (Direction Générale ou Directoire) alors que la Direction de l'Audit rend compte à "l'organe délibérant" - nous reprenons ici la terminologie du règlement CRBF 97-02 qui a le mérite d'être assez générique (Conseil d'administration ou de surveillance).

Même si les terminologies et les dispositifs de contrôle interne divergent d'une organisation à l'autre, l'architecture principale reste la même dans toutes les organisations soumises à la réglementation.

### ***Evaluation du dispositif de contrôle et communications externes***

Les contrôles internes de deuxième et troisième niveaux sont ainsi des outils d'évaluation du dispositif de contrôle interne dans son ensemble.

Cette évaluation qui correspond à la couche supérieure du cube COSO, est un processus intrinsèque au contrôle interne. Elle participe au processus d'amélioration continue du dispositif.

Pour l'évaluer, il convient de déterminer dans quelle mesure le dispositif de contrôle interne correspond aux attentes des parties prenantes de l'organisation et du régulateur.

Les méthodes d'évaluation dépendent des organisations. Toutefois, celles qui reviennent le plus souvent sont les campagnes de tests et d'auto-évaluations.

L'évaluation du dispositif fait l'objet d'une communication interne et externe à l'organisation.

En effet, la plupart des sociétés cotées sont astreintes par le régulateur à communiquer sur leur dispositif de contrôle interne :

- **Rapport du président et du directeur financier** : Sarbanes Oxley Act,
- **Rapport d'évaluation de l'audit** : Sarbanes Oxley Act,
- **Rapport du président** : Loi sur la Sécurité Financière,
- **Rapport du Commissaire aux Comptes** : Loi sur la Sécurité Financière,
- **Comité d'audit responsable de la supervision** : 8ème directive.

En fonction des lois, les exigences en matière de communication sont plus ou moins fortes.

Les différents régulateurs s'appuient sur le dispositif de contrôle interne des entreprises pour assurer la maîtrise de risques et particulièrement la sécurité financière des investisseurs.

Après avoir décrit le dispositif de façon théorique, il est intéressant de voir comment ces dispositifs ont été intégrés par les entreprises, et quelles sont les perspectives pour l'avenir en termes de contrôle interne.

## **Les perspectives du contrôle interne**

### ***Etat des lieux***

La mise en application des lois SOX et LSF a déjà été la source de nombreux projets.

Actuellement, toutes les entreprises du CAC 40 ont à ce jour mis en place leur dispositif en réponse à la LSF.

La réaction des entreprises à ces deux lois a été ambivalente : de nombreuses critiques ont fusé sur les contraintes supplémentaires imposées aux entreprises (surtout pour la loi SOX, plus contraignante que LSF), mais les grandes entreprises ont reconnu que cette mise en place a permis de formaliser les procédures internes, ce qui a été globalement bénéfique.

La contrainte a surtout été ressentie par les petites entreprises, ce qui a amené un aménagement de la LSF via la loi Breton en 2005.

Concernant la loi SOX, il est symptomatique que nombre d'entreprises françaises soumises à SOX se soient décotées de la Bourse de NY.

### ***Perspectives***

La crise de 2008 va-t-elle ajouter de nouvelles contraintes réglementaires pour les banques, mais aussi pour les entreprises, telles l'adaptation de la 8ème Directive Européenne.

Les informations de début 2009 semblent aller dans ce sens, pour les banques en tout cas : encadrement des bonus aux Etats-Unis, méfiance généralisée de l'opinion publique par rapport au management des grandes entreprises, ...

Cela dit, on peut se demander si cette régulation croissante ne butera pas un jour contre des difficultés pratiques de mise en application et à une résistance aux contraintes bureaucratiques. "Trop de réglementation tue la réglementation".

### ***Un signe des temps***

D'autre part, on sent bien que les efforts en termes de contrôle interne n'empêcheront jamais les accidents majeurs. Après l'affaire Nick Leeson (Barings), toutes les banques avaient juré leurs grands dieux que de tels incidents ne pouvaient pas arriver chez elles et que leurs procédures de contrôle étaient parfaitement au point... On connaît la suite.

Doit-on assigner aux Banques le même niveau de sécurité que les Compagnies aériennes ou les Centrales Nucléaires, qui sont les organismes les plus avancés en termes de sécurité? Les enjeux sont-ils de même nature (des vies humaines ou l'irradiation des sols pendant plusieurs générations d'un côté, des épargnants floués de l'autre).

On peut se demander si cette montée croissante des exigences en termes de contrôle interne n'est pas un signe des temps.

Dans les années 80, on ne jurait effectivement que par la Qualité Totale, l'amélioration continue des processus. Cette époque se caractérisait par un secteur bancaire fortement encadré, ceci expliquant peut-être cela.

Le curseur est maintenant placé sur la prévention des catastrophes et le contrôle interne (même si dans le discours officiel, on va "utiliser telle contrainte réglementaire comme une opportunité pour améliorer l'organisation et la performance").

Cette aversion croissante pour le risque ne va-t-elle pas à l'encontre de l'esprit d'initiative et de la créativité ("No venture no gain") ·