Le nouveau COSO

… et ses 17 principes fondateurs pour un contrôle interne efficient

16 **Plaidoyer pour des principes justes et pertinents : Comment donner du sens aux systèmes de contrôle interne ?**
Béatrice Ki-Zerbo

22 **Le COSO 2013 : une mise à jour du référentiel d'origine pour mieux maîtriser les évolutions**
Serge Villepelet

25 **Le COSO 1992 est mort, vive le nouveau COSO**
Laurent Arnaudo

29 **Le COSO 2013 et le cadre de l'AMF ne s'excluent ni ne s'opposent, ils sont complémentaires**
Anne Bosche-Lenoir et Raymond Marfaing

Plaidoyer pour des principes justes et pertinents : Comment donner du sens aux systèmes de contrôle interne ?

Béatrice Ki-Zerbo - Directeur de la Recherche, **IFACI**

La mise à jour du référentiel COSO de contrôle interne est formellement caractérisée par l'explicitation de **17 principes** complétés par des **points d'attention** et des illustrations. Cette version 2013 est donc plus précise et plus aisée à actionner. Loin d'être des « a priori » théoriques et intemporels, ces principes bénéficient de plusieurs décennies de pratiques du contrôle interne et de gestion des risques.

Cet article a bénéficié des échanges fructueux au sein des groupes de recherche de l'IFACI ; en particulier celui qui avait été constitué dans le cadre de la consultation publique lancée par le COSO en 2012.
Impossible de résumer ici toute la richesse de ce référentiel dont des professionnels chevronnés nous ont avoué qu'il méritait le détour. Nous vous proposons donc un survol orienté vers ce qui nous semble être fondamental pour un contrôle interne efficace : la qualité de l'« environnement de contrôle » et du « pilotage ». Ces composantes sont pourtant les laissées pour compte des chantiers de contrôle interne. Dans le meilleur des cas, elles sont exaltées lors de grandes messes suivies de plans d'actions purement formels dépourvus de sens ou sans ressources adéquates. Au moindre incident, ce vernis de façade ne tardera pas à se craqueler mettant ainsi à mal la confiance au pouvoir de transformation du contrôle interne. Les fossoyeurs du contrôle interne ne se demanderont jamais si les fondations de l'édifice pimpant qui leur était présenté étaient réellement robustes.

L'idée de recourir à des principes fondateurs pour une saine gestion n'est pas nouvelle. En 1916 déjà, Fayol proposait 14 principes généraux d'administration dont la plupart n'ont rien à envier à ceux proposés par le COSO. Cet ingénieur des mines est reconnu pour son pragmatisme. Il avait également une visée universelle de ses principes qu'il proposait d'appliquer à l'administration publique.
Plus proche de nous, Larry Rittenberg (2007) présentait les 20 principes du référentiel *COSO for smaller public companies* comme un moyen de rendre plus accessibles les fondamentaux d'un contrôle interne efficace aux managers de sociétés cotées de taille moyenne. Il notait que ces principes étaient tout à fait adaptés pour les autres types d'organisations. Les constats de l'ancien président du COSO ont été suivis d'effet. En effet, les 17 principes de la nouvelle version du référentiel de contrôle interne s'inspirent visiblement de ces 20 principes initiaux. Leur rédaction gagne néanmoins en clarté et met en exergue les points d'attention. Un aperçu en est donné dans le tableau ci-après.

Ces principes sont développés dans le document de référence *(Framework)* et illustrés dans deux documents complémentaires *(Illustrative Tools et Internal Control over External Financial Reporting)*. Eléments fondateurs et incontournables de la conception, de la mise en place et du fonctionnement de tout système de contrôle interne ayant l'ambition de contribuer à la performance d'une organisation ; ces principes ont isolément porteur de sens. Néanmoins, leur pouvoir de transformation ne s'exprimera réellement que dans une mise en œuvre concertée. Les principes ne sont donc pas une fin en soi, cette nouvelle édition permet de s'en servir pour s'assurer de la cohérence globale du système par une mise en lumière des interactions entre composantes. Il est d'ailleurs dommage que l'illustration sous forme de cube ne rende pas mieux compte de cette interpénétration des composantes. C'est

Environnement de contrôle	**1. L'organisation démontre son engagement en faveur de l'intégrité et de valeurs éthiques.** **2. Le conseil d'administration fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.** **3. La direction, agissant sous la surveillance du conseil d'administration, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs.** **4. L'organisation démontre son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs.** **5. L'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.**
Evaluation des risques	**6.** L'organisation **spécifie les objectifs** de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs. **7.** L'organisation identifie les risques associés à la réalisation de ses objectifs dans **l'ensemble de son périmètre de responsabilité** et elle procède à leur analyse de façon à déterminer les **modalités de gestion des risques appropriées.** **8.** L'organisation intègre le **risque de fraude** dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs. **9.** L'organisation **identifie et évalue les changements** qui pourraient avoir un impact significatif sur le système de contrôle interne.
Activités de contrôle	**10.** L'organisation **sélectionne et développe les activités de contrôle** qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs. **11.** L'organisation sélectionne et développe des activités de contrôle général en matière de **système d'information** pour faciliter la réalisation des objectifs. **12.** L'organisation met en place les activités de contrôle par le biais de **directives** qui précisent les objectifs poursuivis, et de **procédures** qui mettent en œuvre ces directives.
Information et communication	**13.** L'organisation obtient ou génère puis utilise des **informations pertinentes et de qualité** pour faciliter le fonctionnement des autres composantes du contrôle interne. **14.** L'organisation **communique en interne** les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne. **15.** L'organisation **communique avec les tiers** au sujet des facteurs qui affectent le bon fonctionnement des autres composantes du contrôle interne.
Pilotage	**16.** L'organisation sélectionne, met au point et réalise des **évaluations continues et/ou ponctuelles** afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent. **17.** L'organisation **évalue et communique les faiblesses de contrôle interne en temps voulu** aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration.

Aperçu des 17 principes proposés par le COSO *(Traduction non officielle)*

cette dynamique qui fonde l'efficacité de l'ensemble du système de contrôle interne. Comme nous le verrons, sans ce mouvement d'ensemble impossible de faire jouer au contrôle interne son rôle **de traduction des options de gouvernance et de gestion des risques dans les métiers.**

Dire que tous les 17 principes sont indispensables n'exclut pas une mise en œuvre **modulée** selon des critères tels que :

- la taille de l'entité ;
- l'autonomie (groupe vs filiale) ;
- la complexité des opérations ;
- la maturité des systèmes de gestion des risques et de gouvernance. En particulier :
  - l'implication des organes délibérants et exécutifs ;
  - la formalisation des valeurs ;
  - la qualité du processus de définition des objectifs et de l'appétence pour les risques ;
- la compétence des collaborateurs (qui déterminera par exemple les modalités et les objectifs de supervision).

Comme pour l'ensemble de cette mise à jour, la nouveauté se découvre dans une lecture attentive. Si ces trois objectifs sont connus, le COSO 2013 en étend

la portée et nous alerte sur leur imbrication :

- **Les objectifs opérationnels** concernent l'efficacité et l'efficience des opérations. Au-delà de la performance opérationnelle et financière, le COSO y inclut explicitement la protection des actifs.
- **Les objectifs de** ***reporting*** sont spécifiés : il s'agit à la fois de la communication interne et externe d'informations financières et extra-financières. Outre l'élargissement du champ, il nous est recommandé de ne pas nous cantonner à la fiabilité mais d'être également attentif aux attentes des destinataires internes et externes notamment en termes de délais et de transparence.
- **Les objectifs de conformité** prennent une place de plus en en importante du fait de la multiplication des lois et règlements applicables aux organisations. Ils sont sous-tendus par les deux autres catégories d'objectifs et vice-versa.

Selon les organisations, la place accordée à chacune des trois catégories d'objectifs pourra également être modulée. Cet impératif de modulation montre que les bénéfices de cette nouvelle version résultent nécessairement d'une appropriation fine et personnalisée de son contenu qu'il est impossible de résumer en quelques pages.

Les éléments proposés ci-dessous sont à prendre comme autant de points de départ possibles de cette appropriation.

L'environnement de contrôle

Selon le principe 1, **intégrité et valeurs éthiques** sont fixées par les instances dirigeantes, elles-mêmes exemplaires en la matière. Pour être **comprises** à tous les niveaux, elles doivent être explicitées dans l'organisation mais également aux **prestataires et aux partenaires**. Le niveau d'adhésion à ces valeurs est **vérifié** et des décisions effectivement mises en œuvre **en cas d'écart.**

Le principe 2 met l'accent sur **l'indépendance du conseil d'administration** vis-à-vis du management. Pour ce faire, le conseil dispose-t-il des **compétences** et de l'expertise adéquate ? Les administrateurs sont-ils effectivement conscients de leurs responsabilités en matière de contrôle interne ? Exercent-ils une surveillance appropriée à chaque phase du processus de contrôle interne (conception, mise en œuvre, pilotage)? Le référentiel aide à trouver des éléments de réponses à ces questions qui sont loin d'être binaires. Ainsi, des **exemples d'implication du conseil dans le suivi de chaque composante** sont donnés.

Le principe 3 rappelle ce qui peut paraître être le B.A-BA du contrôle interne : Définir clairement les **pouvoirs et responsabilités**, assurer la séparation des tâches notamment à travers le système d'information. Pourtant, **cette évidence est loin d'être une réalité** dans toutes les organisations. Si tant est que la répartition formelle des pouvoirs et responsabilités a été effectuée à chaque échelon de la ligne hiérarchique, il restera à s'assurer qu'ils sont tout aussi clairement définis au niveau des différentes instances de gouvernance (comités émanations du conseil, comités managériaux), dans les relations entre chaque entité légale, dans le réseau de distribution et avec les prestataires. De plus, pour reprendre les mots de Fayol, en anglais dans son texte, la définition des rôles n'aura de sens qu'avec « *the right man in the right place* ».

Ainsi le principe 4 est clairement lié au principe précédent. Il présente une **vision dynamique** d'un élément clé de l'efficacité de toute organisation, la prise en compte des hommes et des femmes qui la font fonctionner. Il ne s'agit pas seulement d'employer des ressources qui seraient à disposition et inertes. Il faut pouvoir être en capacité **d'attirer, de développer et de maintenir des compétences** en lien avec les objectifs de l'organisation. Cette gestion stratégique des ressources s'appuie bien sûr sur des politiques et des procédures mais celles-ci ne doivent pas empêcher toute réactivité notamment par rapport aux besoins futurs.
Dans ses développements sur l'évaluation et la rémunération, ce principe est également relié au principe 1. Ils sont empreints des travaux sur la justice organisationnelle qui selon Langevin et Mendoza (2013), favorise la satisfaction au travail, l'adhésion à la politique de l'entreprise, la résolution des conflits et les comportements civiques. Ces trois derniers objectifs sont explicitement l'un des enjeux des composantes « environnement de contrôle » et « pilotage » du COSO (2013). Classiquement, la **justice organisationnelle** s'entend selon trois approches :

- la justice distributive qui s'intéresse à l'explicitation des critères d'allocation des ressources et des récompenses ;
- la justice procédurale qui met l'accent sur les conditions de cette allocation. Est-elle :
  - pertinente (en temps opportun, individualisée) ?
  - sans biais ?
  - fondée sur des informations fiables ?
  - révisable (possibilité de faire appel et de corriger les injustices) ?
  - équilibrée (prise en compte de toutes les parties concernées) ?
  - conforme à des valeurs éthiques et morales ?
- la justice interactionnelle qui interroge la nature des relations interpersonnelles pendant la mise en œuvre des procédures.

Il n'est pas inutile de rappeler l'importance de la beauté du geste dans des organisations qui ont tendance à réduire leur fonctionnement à des séquences de procédures et subissent donc une recrudescence du mal-être au travail.

Le principe 5 sera également difficile à appliquer sans un minimum de justice organisationnelle favorisant une adhésion au **devoir de rendre compte**. Il est

relié aux autres principes de l'environnement de contrôle (valeurs de référence et propice à la confiance, instances dirigeantes jouant leur rôle, responsabilités clairement définies, compétences et pouvoir de rendre compte). Il s'appuie également sur la robustesse des composantes « information et communication » et « pilotage ». Ce principe reflète la maturité croissante des systèmes de contrôle interne qui ne se limitent plus à la maîtrise des activités. En tant que système de pilotage de la performance, le contrôle interne nécessite une information ascendante qui avait peut-être été un peu passée sous silence sous le poids du *tone at the top*. Sans devoir de rendre compte, impossible également de diriger des entreprises de plus en plus étendues, soumises à la pression de parties prenantes qui ne cessent de clamer leur droit à l'information. Une organisation qui n'aura pas su anticiper ces besoins pourra être mise à mal. Le devoir de rendre compte ne sera bénéfique que s'il ne réduit pas les acteurs à un statut de simples émetteurs d'indicateurs. C'est seulement s'ils sont responsabilisés et sûrs que leurs messages seront suivis d'effets, que les acteurs pourront véritablement tirer profit de ce mécanisme en le mettant au service de l'amélioration continue.

Evaluation des risques

C'est l'occasion ici de rappeler que cette nouvelle publication n'est pas un COSO 3 qui viendrait remplacer le référentiel « *Entreprise Risk Management* », plus connu en tant que COSO 2. Une partie de la publication de 2013 est d'ailleurs consacrée à la complémentarité entre les deux référentiels. Les objectifs et les seuils de tolérance définis par le management dans le cadre du système de gestion des risques sont des données d'entrée du système de contrôle interne. Si le lien avec la composante « évaluation des risques » semble être le plus naturel, l'articulation avec le système de gestion des risques permet de réussir la modulation des principes évoquée au début de cet article. Elle détermine l'efficience du système de contrôle interne par la prise en compte d'indicateurs de performance opérationnelle et financière appropriés et la correcte allocation des ressources.

Le référentiel de contrôle interne envisage les risques sous l'angle des menaces à l'atteinte des objectifs ; ce n'est pas pour autant qu'il ignore le fait que les organisations doivent également saisir des opportunités. Néanmoins celles-ci ne sont pas directement gérées par le système de contrôle interne. Elles doivent d'abord être analysées dans le cadre du système de gestion des risques. Si elles sont confirmées par les directives des instances dirigeantes, elles deviennent explicitement des objectifs dont le contrôle interne contribuera à la réalisation.

« L'un des atouts de l'édition de 2013 est de clarifier les limites du système de contrôle interne pour mieux l'actionner »

L'un des atouts de l'édition de 2013 est de clarifier les limites du système de contrôle interne pour mieux l'actionner.

Outre les étapes classiques d'identification et d'analyse des risques pour la mise en œuvre des mesures de traitement appropriés, la nouvelle formulation de la composante « évaluation des risques » met clairement l'accent sur le risque de fraude (principe 8) et la nécessité d'adapter le système aux changements significatifs (principe 9). S'il est assez classique de s'intéresser aux changements significatifs dans l'environnement externe comme menaces potentielles, il s'agit d'être également vigilants face à des changements de *business model* ou de dirigeants.

Activités de contrôle

Une lecture rapide des principes 10 à 12 pourrait laisser penser que c'est la partie la moins innovante du nouveau référentiel. Sans doute parce qu'elle est inhérente à toute forme d'organisation. Et pourtant, cette approche pourra également être matière à progrès. Par exemple, ces activités visent-elles un niveau acceptable des risques ? Ces seuils sont-ils clairement définis dans toutes les organisations ? Dans l'affirmative le sont-ils par les instances appropriées (cf. principe 2 et 3) ? Veille-t-on à retenir une combinaison optimale des différentes catégories de contrôle (automatiques vs. manuels / prévention vs. détection) au regard des risques à maîtriser ?

Le principe 11 rappelle des éléments d'une bonne gouvernance des systèmes d'information. Il invite les professionnels du contrôle et de l'audit internes à s'intéresser à des domaines qui leur sont moins familiers tels que l'infrastructure ou la sécurité. Ils constituent pourtant des zones à risques particuliers à l'ère de l'informatique mobile et du *cloud computing*.

Le principe 12 permet d'éviter des activités de contrôle dépourvues de sens. Il fait le lien avec les composantes « environnement de contrôle » (il est question de directives, de responsabilités et de devoir de rendre compte, de personnel compétent, d'actions correctives), « information et communication » (indispensables pour une mise en œuvre en temps opportun) et bien sûr de « pilotage » (avec l'évaluation périodique des activités de contrôle et leur mise à jour éventuelle).

Information et communication

Désormais, les technologies permettent de générer et de diffuser des milliers de données en interne ou en externe.

Déterminer celles qui sont vraiment pertinentes ; y accéder en toute légalité et les traiter de manière efficiente constitue un enjeu de gouvernance.

Le principe 14 permet d'organiser le système de contrôle interne selon le sens donné au niveau de l'environnement de contrôle et en fonction des signaux des composantes « évaluation des risques » ; « activités de contrôle » et « pilotage ». Sans **communication interne adéquate** (en termes de délais, de destinataires, de contenu) difficile d'assumer ses responsabilités en matière de contrôle interne. Deux canaux de communication sont particulièrement détaillés : celle qui concerne le conseil d'administration et celle qui peut être mobilisée dans des circonstances exceptionnelles (par exemple les lignes d'alerte éthique).

Le principe 15 concernant la **communication externe** tient compte de la multiplication des interlocuteurs externes (actionnaires, analystes, régulateurs, clients, fournisseurs, associations…) ayant parfois des centres d'intérêt différents. Au-delà, de la maîtrise des messages de l'organisation notamment concernant la fiabilité du contrôle interne, nous sommes invités à contribuer à une exploitation efficace de la communication entrante. Il s'agira par exemple de s'assurer de l'adéquation des moyens, de la conformité des processus ou de la pertinence des données.

Pilotage

Le principe 16 a le plus grand nombre de points d'attention. Ils peuvent être résumés par des mots clés tels que :

- équilibre (entre **évaluations permanentes et périodiques**). En pratique cette complémentarité pourra se fonder sur le modèle des trois lignes de défense ;
- adaptation (à l'état du système, au rythme des changements dans l'environnement et dans les métiers) ;
- intégration (des évaluations permanentes dans les processus métiers) ;
- flexibilité (périmètre et rythme des évaluations périodiques) ;
- objectivité (des évaluations périodiques) ;
- compétence. Ainsi, la description des rôles et responsabilités des auditeurs internes est conforme aux normes professionnelles IIA.

Le principe 17 est celui de la boucle de retour. Le mécanisme n'est pas nouveau mais la mise à jour nous invite à dépasser une démarche incrémentale pour une vision globale. En effet, le management et le conseil d'administration doivent disposer de l'information adéquate pour décider des actions correctives en temps opportun et suivre leur mise en œuvre.

De plus, les principes précédents et en particuliers ceux de l'environnement de contrôle n'ont de sens que s'ils sont surveillés et que **des actions sont effectivement mises en œuvre en cas d'écart** (modification de la cible ou du plan de maîtrise).

* *
*

En conclusion, l'idée de s'appuyer sur des principes pour la bonne marche d'une organisation n'est pas nouvelle. Néanmoins l'originalité de la proposition du COSO vient de l'articulation dynamique de plusieurs axes. Il permet ainsi de viser, avec la même approche, plusieurs objectifs et de gérer leur interconnexion. Il est plus aisé d'identifier les domaines sous contrôle et les zones de faiblesses pour prioriser les actions. Nous avons pu mettre en évidence des résonnances entre principes et composantes. Toutes les composantes ressortent grandies de cette mise à jour. Celles relatives à l'évaluation des risques et aux activités de contrôle bénéficient des avancées de l'ERM. Les formulations et illustrations des trois autres composantes devraient en faciliter l'adoption.

Les rédacteurs ont réussi le pari d'être suffisamment générique pour une utilisation dans différents contextes tout en donnant plusieurs pistes pour le déploiement de systèmes de contrôle interne justes. Bien que tombée en désuétude nous préférons nous référer à cette notion de justice plutôt que d'invoquer « le bon sens ». En effet, elle recouvre plusieurs caractéristiques d'un système de contrôle interne efficace qui se doit d'être : raisonné, intègre, adéquat, raisonnable, pertinent, exact, précis…

Le document n'intègre sans doute pas assez une vision plus positive des personnes qui ne sont pas tous des fraudeurs en devenir. Le jugement du management est clairement mis en avant mais un lecteur non avisé ne sera pas forcément sensibilisé aux variables culturelles (et non pas uniquement structurelles) du contrôle interne. Il est pourtant indispensable d'avoir conscience de ces aspérités pour ne pas se bercer de l'illusion d'un contrôle interne sans failles (cf. Atwood et al, 2012).

Bref, un vaste programme pour les managers, une opportunité d'innovation pour les professionnels de l'audit et du contrôle internes, et de nouveaux chantiers pour la recherche à commencer par l'actualisation de nos publications sur le contrôle interne. Je pense en particulier aux cahiers de la recherche sur *« La création valeur par le contrôle interne », « Des clés pour la mise en œuvre et l'optimisation du contrôle interne », « Les variables culturelles du contrôle interne »* accessibles sur notre site internet mais qui mériteront d'être revisités pour profiter des propositions particulièrement intéressantes du COSO. ●

Références bibliographiques

- Atwood, B., Raiborn C. et Butler J. 2012. *The illusion of internal controls. Strategic Finance (October):* 30-37
- COSO. 2006. *Internal Control over Financial Reporting – Guidance for Smaller Public Companies*
- COSO. 2013. *Internal Control – Integrated Framework, Ilustrative Tools for Assessing Effectiveness of a System of Internal Control and the Internal Control over External Financial Reporting (ICEFR): A Compendium of Approaches and examples.* Traduction à paraître
- Dumez H. (dir) 2008. Rendre des comptes : nouvelle exigence sociétale, PRESAJE, Dalloz
- Fayol H. 1962. Administration industrielle et générale – Prévoyance, organisation, commandement, coordination, contrôle, Dunod 151p
- IFACI et PWC. 2005. Le management des risques de l'entreprise. Editions Eyrolles. Traduction de *Entreprise Risk Management* publié en 2004 par le COSO
- Langevin P. et Carla M. 2013. La justice : un revenant au pays du contrôle ? Revue Comptabilité Contrôle Audit, tome 19, vol.1, pp 33-58
- Rittenberg, L. Martens E. et. Landes C. 2007. *Internal control guidance: Not just a small matter. Journal of Accountancy (March):* 46-50
- Simons R. 1994. *Levers of organization design: How managers use accountability systems for greater performance and commitment,* Harvard Business Press
- Tysiac, K. 2012. *Internal control revisited. Prominent COSO officials discuss proposed updates to framework. Journal of Accountancy (March):* 24-29

Le COSO 2013 : une mise à jour du référentiel d'origine pour mieux maîtriser les évolutions

Serge Villepelet

Président, **PwC France**

Les piliers du nouveau COSO 2013 restent les mêmes que ceux du COSO 1992. Cependant, les évolutions des vingt dernières années ont nécessité des prises en compte d'exigences nouvelles à la hauteur des nouveaux enjeux. Le COSO 2013 rassemble des perspectives plus larges que celles des organismes fondateurs qui sont des organisations comptables et financières ; sa vocation est bien d'étendre son application au-delà de ce qui est comptable et financier.

Le nouveau COSO

Louis Vaurs : *Le COSO 1 sur le contrôle interne vient de faire l'objet d'une mise à jour publiée le 14 mai 2013 aux Etats-Unis. Pouvez-vous indiquer à nos lecteurs les raisons qui ont poussé le* Committee of Sponsoring Organisations *à procéder à cette mise à jour :*

- *S'agit-il d'une simple mise à jour ou d'une refonte ?*
- *De quels éléments se compose le nouveau package ?*
- *Quelles en sont les principales nouveautés ?*

Serge Villepelet : Il s'agit en effet essentiellement d'une mise à jour plutôt que d'une refonte. Notamment, la définition, les composantes et les concepts clés restent les mêmes que ceux du référentiel d'origine qui date de 1992. Ceci étant, il est nécessaire de reconnaître l'impact des évolutions de ces 20 dernières années en matière de technologie (par exemple : la cyber criminalité), d'externalisation, d'attentes plus fortes en matière de transparence, et bien d'autres. Toutes ces évolutions nécessitent plus d'agilité et de « résilience » de la part des entreprises pour faire face à de tels enjeux.

C'est par le biais de 17 principes structurants que le COSO 2013 définit les éléments essentiels en matière de contrôle interne pour aider les organisations – quels que soient leur taille ou leur domaine d'activité – à faire face dans un monde qui devient de plus en plus complexe.

Les principales nouveautés sont donc :

1. L'élargissement du domaine d'application au-delà du *reporting* financier (par ex. : responsabilité sociale et environnementale).
2. Le renforcement des attentes en matière de gouvernance (par ex. : les rôles des comités et l'alignement avec le *business model*).
3. La gestion des collaborateurs clés au contrôle interne (par ex. : la direction générale).
4. L'articulation des « 3 lignes de défense » dans l'organisation (à savoir les opérationnels, les fonctions support et l'audit interne).
5. Le rapprochement entre risque, performance et rémunération (notamment l'un des principes portant sur la responsabilisation pour le contrôle interne).
6. L'articulation du *« tone at the top »* avec les comportements à travers l'entreprise *(« tone in the middle »)*.
7. La prise en compte des sous-trai-

tants / autres intervenants clés (par ex. : leur adhésion au code de conduite, respect des contrôles au-delà du *reporting* financier).

8. L'exigence de l'adaptabilité et l'adéquation du dispositif par rapport à l'évolution de l'entreprise (telles que de nouveaux processus, rôles, structures, SI, CSP, périmètre d'activité, etc.).

L.V. : *Depuis toujours, PwC est directement associé à l'élaboration de ce référentiel. Quel est plus précisément son rôle ?*

S.V. : En effet, le COSO nous avait sollicité pour écrire le référentiel sur le contrôle interne de 1992 ainsi que l'*Enterprise Risk Management* en 2004 et bon nombre d'autres éléments de « *thought leadership* » que nous avons élaboré ensemble. Nous avons une relation de travail continue fondée sur un échange en continu par rapport aux évolutions pour pouvoir ensemble livrer au marché des réflexions pertinentes et des référentiels qui apportent de la valeur aux entreprises. C'est ainsi que nous travaillons depuis toujours étroitement avec le COSO.

L. V. : *Le* Committee of Sponsoring Organisations *est composé essentiellement d'organisations comptables et financières alors que le cadre de référence de l'AMF a été élaboré avec un groupe de Place où l'AFEP / MEDEF ont joué un rôle non négligeable. N'est-ce pas un handicap pour le COSO qui a voulu élaborer un référentiel de contrôle interne opérationnel ?*

S.V. : Le COSO rassemble des perspectives bien plus larges que celles de ces organismes fondateurs qui sont, certes, des organisations comptables et financières (pour rappel : *American Institute of Certified Public Accountants, American Accounting Association, Financial Executives International, Institute of Internal Auditors,* et *Institute of Management Accountants).*

Au cours de ce projet d'élaboration du référentiel COSO 2013, le COSO a obtenu l'apport de bien d'autres :

1) au début du projet, une enquête a été lancée depuis le site du COSO, annoncé par divers communiqués de presse, et collectant plus de 700 réponses à travers le monde ; au-delà des 35 % de voies issues du monde comptable et financier, les réponses provenaient largement des fonctions de la gestion de risques, de la conformité, des opérations, de l'IT, de la RSE, et d'autres ;
2) une consultation publique sur le référentiel recueillant plus de 200 réponses ;
3) puis, une dernière consultation publique portant sur l'ensemble des publications COSO 2013 recueillant encore une bonne cinquantaine de réponses, avec un découpage démographique similaire.

Le COSO 2013 a donc bien pour vocation d'étendre son application au-delà de ce qui est comptable et financier.

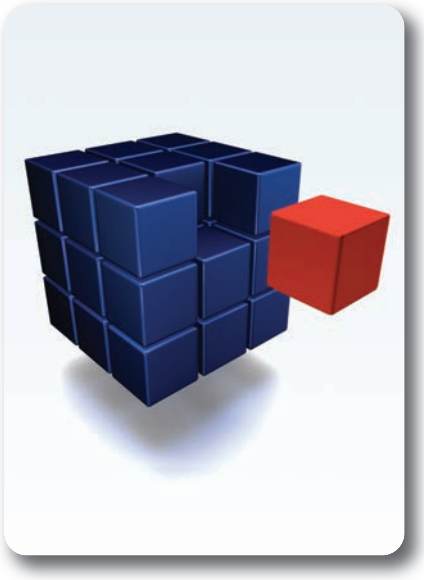
L.V. : *L'AMF a élaboré deux cadres de référence de contrôle interne, l'un pour les sociétés d'une certaine importance, l'autre pour les valeurs moyennes et petites. A qui plus particulièrement le COSO 1 nouveau s'adresse-t-il ?*

S.V. : Le COSO 1 nouveau intègre ces deux visions. Il met à jour non seulement le référentiel de 1992 mais aussi celui de 2006 « *Guidance for Smaller Public Companies* » moins connu en France car il n'avait pas été traduit en langue française. Le COSO 2013 vient donc remplacer ces deux documents car il s'appuie en premier lieu sur des principes applicables à toute taille d'organisation, et en second lieu met en avant des spécificités particulières aux plus petites structures à travers le référentiel, ses approches et ses exemples.

L. V. : *Le COSO 1 nouveau n'est pas un COSO 3. Il ne remplace pas non plus le COSO 2 qui est consacré au management des risques de l'entreprise. Est-il envisagé toutefois un toilettage du COSO 2 ?*

S.V. : Une révision du référentiel portant sur l'ERM n'est pas envisagée à ce stade. A cet effet, deux sujets ont été longuement débattus :

1) L'intégration CI et ERM, mais le marché semblait globalement ne pas vouloir un amalgame des deux concepts. Le contrôle interne est défini comme étant une sous-partie de l'ERM (élaboré en annexe G du référentiel COSO 2013).



2) La mise à jour en parallèle du référentiel ERM, mais son contenu et son articulation avec le contrôle interne, en particulier le COSO 2013, sont vus comme étant toujours valables aujourd'hui. Le COSO 2013 intègre toutefois les éléments du référentiel ERM de 2004 sur les sujets pertinents au contrôle interne.

Le COSO continue donc à apporter des réflexions sur ces sujets, mais davantage en matière d'éclairages sur la pratique que sur les fondements des référentiels de 2004 et 2013 à ce stade.

Auditeurs internes vs commissaires aux comptes

L. V. : *La coordination des travaux entre auditeurs internes et commissaires aux comptes prévue par les normes de l'IIA s'avère indispensable. Comment concrètement cette coordination s'opère-t-elle sur le terrain ?*

S. V. : Cette coordination passe par une grande transparence mutuelle de ces deux instances sur la nature et le périmètre de leurs travaux. Il est fondamental que les commissaires aux comptes disposent d'une vision précise des travaux réalisés par l'audit interne qui concernent la revue du contrôle interne comptable et financier.

L. V. : *Comment, selon vous, cette coordination devrait-elle s'organiser ?*

S. V. : J'identifie immédiatement les éléments suivants : échanges sur le plan d'audit interne et externe, organisation de rendez-vous réguliers de partage d'information, transmission des rapports d'audit qui concernent le contrôle interne.

Au delà de ces éléments, il est évident que le comité d'audit qui est en étroite relation avec les commissaires aux comptes et les auditeurs internes a un rôle majeur à jouer pour encourager et faciliter les échanges. Ces comités d'audit seront d'ailleurs les premiers bénéficiaires d'une communication accrue entre ces deux instances de contrôle car ils en retireront une vision beaucoup plus intégrée de la gestion des risques de l'entreprise.

Enfin, les opérationnels eux aussi bénéficieront d'une meilleure coordination entre les commissaires aux comptes et l'audit interne en évitant que des missions similaires soient réalisées par les deux organes de contrôle.

L. V. : *Quelles sont les conditions qui pourraient permettre aux CAC de s'appuyer sur les travaux des auditeurs internes ?*

S. V. : Tout d'abord il faut bien évidemment que les sujets d'audit aient porté sur des thématiques qui apporteront du confort au CAC pour sa mission. En effet, souvent une part importante des travaux des auditeurs internes porte sur des processus très opérationnels, de l'amélioration de processus, des *dues diligences*…

Il faut ensuite que l'audit interne démontre une forte indépendance vis-à-vis du management et pour cela il faut s'attacher à comprendre quelles sont ses lignes réelles de *reporting* et d'influence.

Enfin, il faut avoir une certaine assurance quant à la qualité des travaux produits par l'audit interne et pour cela une revue de leur organisation, outils et livrables est une façon simple de se constituer une opinion.

Sous-traitance de l'audit interne

L. V. : *Avant les grands scandales comptables et financiers de la fin des années 90 et des premières années 2000, l'externalisation de l'audit interne était en vogue aux Etats-Unis mais avait peu touché la France. On parle actuellement davantage de* co-sourcing. *Comment voit-on chez PwC la coopération avec les services d'audit interne ?*

S. V. : La cotraitance est quasiment devenue une nécessité pour l'audit interne.
En effet, les processus des entreprises se sont considérablement complexifiés ces dernières années sous l'impulsion de nouvelles réglementations, le déploiement de nouveaux outils informatiques et l'internationalisation des implantations géographiques.

Pour que l'audit interne puisse livrer des travaux de qualité – à savoir une assurance raisonnable sur les processus audités mais également des éléments de *benchmark* et des idées pour améliorer le fonctionnement des processus – il devient quasiment impossible de se passer d'experts pour réaliser les audits internes. Force est de constater qu'il est très difficile pour les départements d'audit interne de maintenir des compétences spécialisées et de très haut niveau dans tous les domaines (par ex. : valorisation, modélisation, technologie, etc.). Néanmoins, la présence des auditeurs internes reste une nécessité forte car ceux-ci sont garants de la méthodologie d'audit, connaissent les enjeux de l'entreprise, les contingences politiques et peuvent assurer la mise en perspective et la transversalisation des conclusions.

« Il devient quasiment impossible de se passer d'experts pour réaliser les audits internes »

Alors oui, il faut maintenant penser à la cotraitance tout en disposant d'un département d'audit interne senior et sponsorisé par la direction générale !

Pour les sociétés de tailles inférieures le problème est différent : la sous-traitance reste un modèle bien adapté car il permet à l'entreprise de disposer d'auditeurs internes professionnels avec des structures d'équipe adaptées à chaque mission, incluant les bons experts. ●

Le COSO 1992 est mort, vive le nouveau COSO

Laurent Arnaudo

Senior vice-président – audit interne groupe, **Sodexo**

Le COSO 1992 a fait son temps. Il sera remplacé par le COSO 2013 à la fin de l'année 2014. Reconnaissons tout de même que le COSO 1992 a permis de franchir une étape supplémentaire et de renforcer les dispositifs existants ; il nous a confortés sur les directions à prendre en matière de contrôle interne ; il a permis de s'attaquer aux vrais sujets. L'objectif du COSO 2013 est de réduire les risques, accroître la conformité aux lois, politiques et procédures et renforcer les systèmes de contrôle interne. C'est un beau programme.

Voici une phrase bien connue que l'on proclame lors de l'avènement d'un nouveau monarque. C'est exactement ce qui nous arrive dans le royaume du contrôle et de l'audit internes car, depuis quelque temps, nous avons appris que notre Grand Roi, le COSO 92, se portait mal et allait tout doucement se retirer, pour mourir le 15 décembre 2014. Nous allons donc perdre notre référence, notre roi qui régnait depuis plus de 20 ans. Et pourtant, la plupart de ses sujets ne semblent pas si tristes…

Il est vrai qu'il a fait son temps, ce référentiel du contrôle interne. Envisagé dès 1985 par « *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)* », il ne fut publié qu'en 1992. A cette époque, il ne fut utilisé, en France, que par un certain nombre de grands groupes présents à l'international. Il gagna réellement ses lettres de noblesse avec l'arrivée du Sarbanes-Oxley Act et de la Loi de Sécurité Financière, dans les années 2000. C'est alors devenu le référentiel incontournable, que de nombreuses entreprises ont souhaité suivre et mettre en avant dans leur document de référence.
On a bien essayé de lui redonner un petit coup de jeune à partir de 2006, avec la publication de deux documents, mais aujourd'hui, il est sous respiration artificielle.

Le Coso 1992 est mort, vive le Coso 2013

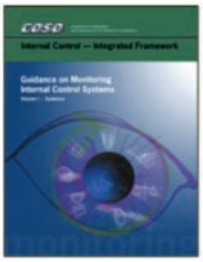
Comme les choses sont toujours bien faites dans le beau royaume du contrôle et de l'audit internes, le conseil du COSO a déjà identifié et même présenté son successeur : le fabuleux COSO 2013. Il est tout jeune et a beaucoup de bonnes idées. Il est né le 14 mai 2013.

Pour tous ceux qui ont mis en place le COSO – version 1992 – dans leur entreprise, il y a eu de vrais changements. Ce référentiel a permis de franchir une étape supplémentaire et renforcer les dispositifs existants. Il nous a donné un cadre et surtout, il nous a conforté sur les directions à prendre en matière de contrôle interne :

- en mettant des mots derrière des contrôles que nous avions déjà identifiés, le COSO a apporté une structure à nos matrices de risques et de contrôles existants ;
- en identifiant des activités de contrôles que nous souhaitions déployer dans nos entreprises mais pour lesquelles nous avions besoin d'un soutien et d'une certaine crédibilité auprès des opérationnels et des dirigeants. Le fait de montrer leur

1992


2006



2009


2013

existence dans le COSO nous permettait de prouver qu'il s'agissait des meilleures pratiques.

Avant l'arrivée du COSO, de nombreuses personnes, dans nos sociétés, avaient une vision assez limitée du contrôle interne : il s'agissait des rapprochements bancaires, des inventaires physiques, de la séparation des tâches, des procédures, etc., et plus généralement de tout ce qui était formel et relatif au domaine de la comptabilité et de la finance. Il s'agissait principalement des activités de contrôles. Les auditeurs se battaient pour démontrer que le contrôle interne était bien plus large que cela. Tous les éléments informels, en dehors du champ de la comptabilité, étaient malheureusement bien souvent oubliés. Ces éléments sont, bien entendu, les plus difficiles à appréhender et à déployer. Expliquer, en réunion de clôture, que le fait de travailler la porte ouverte crée un bon environnement de contrôle n'est pas toujours évident. Ceux qui ont essayé sont sans doute passés pour des extra-terrestres, jusque dans les années 2000. Et si on les voyait, le vendredi soir dans les couloirs, en train de tester ces contrôles, ils passaient pour des fous.

Le COSO 1992, nous a vraiment permis de mettre sur la table les vrais sujets que nous avions du mal à aborder dans le passé :

- le mode de rémunération des dirigeants et la pression sur les résultats,
- le rôle du conseil d'administration,
- l'organisation des structures de la société,
- les mesures disciplinaires en cas de non-respect des politiques et procédures du groupe,
- le système de remonté des incidents,
- le processus d'identification et d'évaluation des risques,
- etc.

C'est surtout pour ceux qui devaient se mettre en conformité avec la Loi Sarbanes-Oxley, dans les années 2006, que le référentiel du COSO a été d'une grande aide. L'exercice de conformité a été réalisé en large partie grâce à la mise en place de ce document. Dans les années 2006, nous avions à l'IFACI monté un groupe de travail SOX. L'objectif, pour plusieurs entreprises françaises concernées par la loi américaine, était de discuter des pratiques et d'identifier des positions communes. Le COSO était un sujet très souvent abordé dans ce groupe de travail car de nombreuses entreprises ne comprenaient pas comment le mettre en œuvre concrètement.

Nos discussions portaient principalement sur l'environnement de contrôle et la gestion des risques, qui étaient les composantes les plus complexes à appréhender. Certains points étaient franchement difficiles à imposer à nos sociétés qui se demandaient pourquoi nous allions dans ces activités, si éloignées de notre périmètre de travail. Nous étions, en fait, dans le cœur de notre métier.

L'autre tâche souvent prise en charge par ce groupe de travail consistait à identifier, pour chaque composante du contrôle interne, des activités de contrôles réalistes et pragmatiques que nous pouvions tester, en tant qu'auditeurs internes.

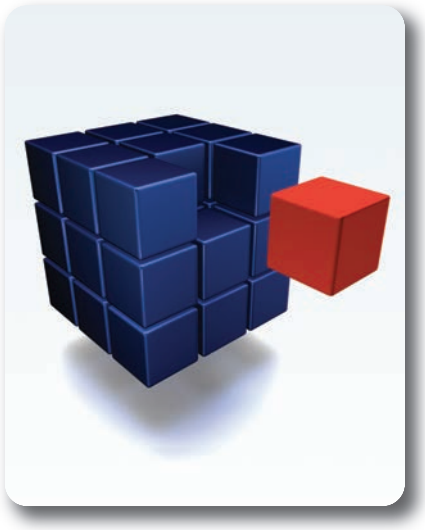
- Comment vérifier que la structure de son organisation est efficace c'est-à-dire qu'elle permet de porter la stratégie définie par son entreprise ?
- Comment tester que le style de management de sa société est adéquat et adapté ?

Autant de bonnes questions qui méritaient de la réflexion et du partage d'expériences. Encore un autre exemple : comment mettre en place un dispositif de remontées des incidents ? Ce n'était pas un dispositif banal en France jusque dans les années 2010. L'idée était certes très intéressante et riche d'informations mais il fallait comprendre jusqu'où nous pouvions aller. La CNIL nous a beaucoup aidés sur ce sujet en encadrant la mise en place du dispositif d'alerte professionnel. Cela demeure toujours un véritable sujet.

Exemple de tests pour les éléments du COSO : *« le conseil et la direction générale montrent l'exemple en ce qui concerne l'importance du contrôle interne et notamment les normes de conduites attendues.*

- *Il existe un code d'éthique.*
- *Il existe une communication faite par la direction générale sur l'éthique au cours de ces 12 derniers mois. Il existe des messages de la DG sur l'intranet, des brochures, etc., destinés à l'ensemble des employés.*
- *La direction explique dans un document communiqué au personnel ce qui est permis et ce qui ne l'est pas (en matière de dépenses avec des clients par exemple).*
- *Il existe des programmes de formation sur le code d'éthique (e-learning…). Toutes les populations dites « sensibles » (commerciaux, acheteurs…) ont suivi ce programme de sensibilisation.*
- *Prendre un cas de non-respect du code / d'écart de bonne conduite au cours de ces 12 derniers mois et examiner les sanc-*

tions et mesures prises par la direction. Ces sanctions sont-elles cohérentes et homogènes d'un cas à l'autre ?
- *Les incidents potentiels et les écarts de bonne conduite donnent lieu rapidement à des investigations, faites par des professionnels indépendants et objectifs.*
- *Le conseil d'administration demande à suivre les incidents les plus significatifs et les actions prises. »*



L'arrivée du nouveau COSO 2013 n'est pas passée inaperçue. Mais beaucoup d'entre nous ne voient pas de révolution. Ce nouveau référentiel n'est finalement que le digne fils de son père. Il suit le même programme et son contenu n'a pas ou peu changé. *« Sa mise en place sera toujours aussi difficile surtout pour les petites structures »* disent certains. *« Tout cela restera encore très théorique pour nos entreprises »* disent d'autres. Ou encore, *« Il n'y a rien de nouveau, mais il est vrai que les points identifiés tomberont maintenant dans notre radar »*. Il existe donc beaucoup de sceptiques.

Le nouveau monarque a des idées révolutionnaires !

Je ne suis pas d'accord. La révolution est en marche car le COSO 2013 présente de nombreux aspects novateurs.

C'est justement ce qui a poussé à sa naissance :
- Les sujets du Roi, eux-mêmes, demandaient un référentiel plus compréhensible et plus utilisable.
- L'ensemble des parties prenantes qui finançait le Royaume, réclamaient depuis longtemps plus de transparence et un système permettant une meilleure gouvernance, gestion des risques, prévention et détection des fraudes.
- Et puis notre Royaume a beaucoup changé en 20 ans. Nous avons des nouveaux risques, notamment dans le domaine IS&T. Les systèmes d'information sont maintenant intégrés à nos dispositifs. Notre environnement n'est plus du tout le même. Il est devenu global et beaucoup plus complexe.

Il fallait réagir. Le COSO 2013 a annoncé son objectif : il veut réduire les risques, accroître la conformité aux lois, politiques et procédures et renforcer les systèmes de contrôle interne. C'est un beau programme.

Bien entendu, la définition du contrôle interne n'a pas changé. Les trois objectifs et les cinq composantes sont toujours les mêmes. Ils doivent permettre d'évaluer l'efficacité du dispositif de contrôle interne. Le changement réside principalement dans les 17 nouveaux principes attachés aux composantes et ses points d'attention, dans le renforcement du *reporting* extra financier et enfin dans la prise en compte des petites entreprises.

Trois domaines sont clarifiés :
- La responsabilité de l'entreprise quand elle décide d'externaliser des services, notamment (mais pas seulement) dans le domaine informatique. En matière de contrôle interne, il est maintenant clair que la responsabilité reste dans nos entreprises – cette responsabilité ne se transfère pas.
- La fraude revient sur le devant de la scène. Ce ne sont plus des activités de contrôles dilués un peu partout que nous devons évaluer.
- Les systèmes d'information sont partout dans nos entreprises et doivent être encore plus intégrés dans la nature de nos contrôles.

Laurent Arnaudo *a débuté sa carrière en 1990 chez Ernst & Young Paris puis San Francisco, après avoir obtenu une maîtrise de gestion à l'Université de Paris-Dauphine. En 1997, il rejoint l'équipe d'audit interne d'Alcatel où il y occupera différentes fonctions dont celle de directeur d'audit pour la région d'Europe du Sud, Afrique et Proche-Orient. En 2004, il devient directeur des projets Sarbanes-Oxley et LSF pour Alcatel, couvrant les 34 entités majeures du groupe. Après la fusion Alcatel-Lucent en 2006, il est nommé directeur de l'audit interne avec une équipe de 80 personnes, basées à Paris, New Providence (New Jersey - USA) et Shanghai. Il est lui-même basé aux Etats-Unis.*

En 2009, il rejoint le groupe Sodexo en tant que senior vice-président – audit interne groupe où il dirige une équipe de 25 auditeurs, basés à Londres, Washington et Paris.

Laurent Arnaudo est CIA, CCSA et CRMA. Il est membre du conseil d'administration et vice-président de l'IFACI. Il est également très actif au sein de l'IIA (The Institute of Internal Auditors) après avoir été membre de son conseil d'administration.

Concrètement, dans les entreprises rencontrées qui réfléchissent à la mise en place du COSO 2013, les actions suivantes sont en route :

- Renforcer l'automatisation des contrôles dans les systèmes grâce aux outils ACL, IDEA, Magnifier et bien d'autres. Cela nous permet d'allouer nos contrôleurs / auditeurs à des tâches à plus forte valeur ajoutée, tout en améliorant le périmètre de couverture puisque l'ensemble des transactions sont examinées en continu.
- Les auditeurs et contrôleurs internes ne doivent pas oublier les contrôles qui sont chez les prestataires. Les auditeurs doivent aller faire des audits chez eux après avoir vérifié l'existence de clauses d'audit dans les contrats, ou en s'appuyant sur des formes d'évaluations externes, faites par des entreprises indépendantes et objectives.
- Les contrôles et les audits de conformité reviennent en force dans nos référentiels et dans nos plans d'audit. Les entreprises ne peuvent plus se passer de solides programmes anti-fraude (identification, communication, prévention et détection des fraudes). Les comités d'audit doivent poser des questions sur leur existence et leur efficacité.
- Enfin, si ce n'est pas déjà fait, il faut passer à la vitesse supérieure et mettre en place un véritable modèle de gestion des risques intégrés (ERM), avec une méthodologie et un langage commun.

Il faut dorénavant évaluer de façon beaucoup plus formelle chacun des 17 principes clés alloués aux 5 composantes du COSO pour conclure au bon fonctionnement de son dispositif de contrôle interne. C'est une véritable révolution, car dans le COSO de 1992, il n'y avait pas ces principes si explicitement définis par des points d'attention. Le jugement de chacun joue toujours un grand rôle, mais les directives sont beaucoup plus claires. On sait ce qu'il faut mettre en place pour être en conformité avec le COSO 2013.

Pour ceux qui sont soumis aux règles de Sarbanes-Oxley, les changements ne seront pas majeurs : l'attestation sur l'efficacité du dispositif de contrôle interne relatif aux informations comptables et financières s'appuiera sur le COSO 2013. Les 17 nouveaux principes permettront de clarifier comment appliquer le référentiel et aideront à évaluer l'efficacité des contrôles internes dans leur conception et leur fonctionnement opérationnel. Les seules différences résideront dans la classification des faiblesses de contrôle interne, dans la documentation du processus d'identification des risques, et enfin dans la nécessité de recalculer le seuil de matérialité au moment de la clôture :

« Il faut mettre en place un plan d'actions permettant de répondre aux nouveautés du COSO de 2013 avant le 15 décembre 2014 »

- Le COSO 2013 parle de déficiences majeures et de déficience de contrôle interne alors que le PCAOB qualifie les faiblesses de contrôles pour Sarbanes-Oxley comme soit une erreur matérielle *(« material deficiency »)* soit une déficience significative *(« significant deficiency »)*. Le PCAOB devra se positionner, dans les mois à venir, sur un alignement (ou pas) avec la définition du COSO. Mais finalement, cela ne change pas grand chose pour un grand nombre d'entreprises. En interne, nous évitions déjà d'utiliser le vocabulaire du PCAOB qui restait le jargon des auditeurs externes. Nous préférons parler de faiblesses de contrôle interne.
- Il faut dorénavant aussi expliquer, plus en détail, comment la sélection des risques a été réalisée (et donc la sélection des comptes, processus, et entités significatifs pour la clôture de l'exercice). On pourra, par exemple, démontrer l'utilisation d'ateliers avec des opérationnels et fonctionnels, etc.
- Il faut aussi s'assurer que la qualification des faiblesses et la sélection des contrôles (dans les comptes, les processus, les entités) en fonction du seuil de matérialité calculé en début d'exercice reste toujours valable en fin d'année, après la clôture des résultats.

Dans le court terme, les actions à mener sont les suivantes : il faut lire le référentiel COSO 2013 ! Les membres des comités d'audit doivent demander à leur contrôleur ou auditeur internes des explications sur ce nouveau COSO. Ils doivent comprendre quelles seront les modifications à apporter dans l'entreprise. S'ils ne le demandent pas, il faut leur en parler et les éduquer sur les nouveaux éléments du COSO 2013. Enfin, pour les sociétés utilisant déjà le COSO de 1992, il faut mettre en place un plan d'actions permettant de répondre aux nouveautés du COSO de 2013 avant le 15 décembre 2014. Cela se fera sans douleur et permettra sans doute de rassurer sur les forces. Pour les entreprises qui n'ont pas mis en place le COSO 1992, l'effort sera plus grand mais les directives données sont maintenant beaucoup plus claires et permettent de mieux comprendre comment déployer le référentiel. C'est un nouveau Roi qui a un bel avenir devant lui, ce COSO. Longue vie au COSO 2013… ●

Le COSO 2013 et le cadre de l'AMF ne s'excluent ni ne s'opposent, ils sont complémentaires

Raymond Marfaing
Directeur adjoint en charge des risques et du contrôle interne, **SNCF**

Anne Bosche-Lenoir
Directrice de l'audit et des risques, **SNCF**

La sortie du COSO 2013 provoque une remise en question et des choix quant à l'utilisation de tel ou tel référentiel. Le cadre de référence de l'AMF, retenu par SNCF, présente, entre autres avantages, celui d'être cohérent avec le COSO, d'être très concret, adapté à la culture SNCF, et tourné vers la mise en œuvre opérationnelle. Néanmoins, le COSO 2013 est une source d'enrichissement dont l'AMF doit tenir compte.

Le cadre de référence de l'AMF : un cadre souple et agile tourné vers la mise en œuvre

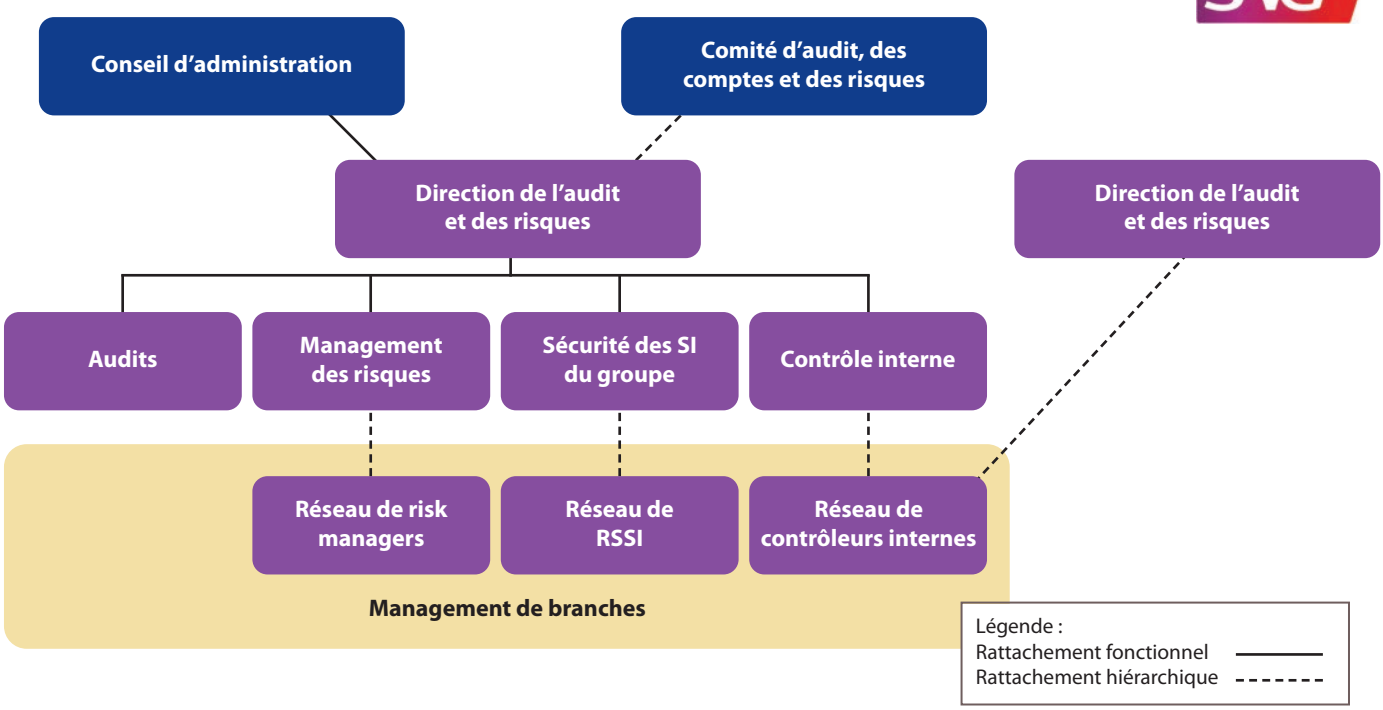
La sortie du COSO 2013 est un événement important pour nous responsables d'audit, de contrôle interne et de management des risques. C'est l'occasion de se remettre en question, d'abord de se familiariser avec les évolutions, puis d'identifier nos points forts, nos points faibles et enfin de revoir éventuellement nos objectifs. C'est aussi l'occasion de s'interroger sur nos référentiels : doit-on les faire évoluer voire en changer ?

Le contrôle interne à SNCF est animé par la direction de l'audit et des risques en liaison avec la direction financière groupe. La direction de l'audit et des risques définit les méthodes et outils, fixe les objectifs et assure le *reporting* et l'évaluation d'ensemble. Elle coordonne l'élaboration des référentiels de contrôle interne et pilote les démarches d'auto-évaluation. De leur côté, les différentes branches d'activité *(Business units)* conçoivent leur organisation du contrôle interne sur leur périmètre, définissent avec la direction de l'audit et des risques leurs objectifs, organisent leur évaluation et assurent leur rendu compte.

Le choix du cadre de référence de l'AMF : un choix naturel

Fin 2009, à SNCF, la direction de l'audit et des risques et la direction financière groupe ont décidé de mettre en place une nouvelle organisation du contrôle interne afin de le rendre plus efficace tout en accompagnant les évolutions managériales de l'entreprise qui renforçait son fonctionnement par branche d'activités : SNCFVoyages, SNCF Proximités, SNCF GEODIS, Gares et Connexions et SNCF Infra. Notre constat était que beaucoup d'acteurs

La direction de l'audit et des risques dans l'organisation de la SNCF



travaillaient sur le contrôle interne mais que leurs travaux étaient peu connectés entre eux et n'étaient pas « tirés » par une politique d'entreprise. Une des conséquences était que le contrôle interne n'était pas vraiment perçu par le management comme un moyen de maîtriser ses opérations ni comme un outil lui permettant de mieux assumer ses responsabilités.

Nous avons alors défini des objectifs simples : réussir en 3 ans à mettre en place une organisation claire au service du management tout en limitant les frais de structure. Pour cela, nous avons d'abord précisé le rôle des différents acteurs depuis le comité d'audit jusqu'aux opérationnels tout en prenant en compte les échelons fonctionnels. Ce premier travail nous a permis de montrer que le contrôle interne ne peut se concevoir que dans une chaîne qui concerne toute l'entreprise et qui implique tous les acteurs.

Après ce premier travail, très vite s'est posée la question du référentiel à suivre, quel cadre de travail commun devions-nous prendre. Assez naturellement nous nous sommes tournés vers le cadre de référence de l'AMF. Nous avions préalablement adopté ce cadre pour le rapport du président sur le contrôle interne et étions déjà, à la direction de l'audit et des risques de SNCF, familiarisés avec ce cadre. De plus, ce cadre à l'époque évoluait dans la suite de la transposition des 4èmes et 8èmes directives européennes. Ce cadre présentait à nos yeux beaucoup d'avantages :

- très adapté à notre culture, à un environnement français ;
- très concret, facilement communicable ;
- tourné vers la mise en œuvre opérationnelle avec en particulier le questionnement et le guide d'application qu'il propose.

Il faut également ajouter qu'il offrait l'avantage avec sa révision de traiter en un seul document du contrôle interne et de la gestion des risques en intégrant les travaux les plus récents en la matière. Le cadre de référence s'appuie en effet sur les évolutions constatées à l'époque dans les principaux référentiels internationaux et notamment le COSO II et la norme ISO 31 000. Pour une direction qui réunit audit, contrôle interne et risques, c'était très appréciable.

Nous ne nous sommes pas trop interrogés sur la possibilité de prendre comme référence le COSO dans la mesure où, comme nous venons de le dire, le cadre de référence de l'AMF est cohérent avec le COSO et que nous trouvions dans le cadre AMF un guide répondant à nos attentes. Nous avons alors défini un objectif clair : avoir mis sous contrôle à échéance 2013 notre environnement de contrôle et les 14 processus identifiés par l'AMF dans son guide d'application sur le contrôle interne de l'information comptable et financière.

Le fait d'avoir utilisé le guide d'application a également constitué un levier interne. Cela nous a permis de mettre en mouvement les « propriétaires » de processus. Nous avons alors commencé par les processus présentant le plus d'enjeux pour l'entreprise, que ce soit en termes d'euros ou en termes de risques, à savoir la paie, les achats et les immobilisations. Nous avions dans le cadre un guide facile d'accès, ce qui est important pour appréhender ces processus qui sont complexes pour une entreprise de la taille de SNCF.

Après plus de 2 ans de travail, nous avons atteint ainsi les objectifs fixés et respectons notre tableau de marche. Même s'il reste bien sûr beaucoup à faire, nous estimons que nous avons atteint un bon niveau de maturité dans plusieurs domaines : l'analyse et la description des processus, l'identification des points de contrôle clés, la rédaction de guides de contrôle interne, la formation des acteurs, le déploiement de campagnes d'auto-évaluation auprès de nombreux acteurs en entités mais aussi en centres de services partagés. Nous pensons que le fait d'avoir choisi le cadre AMF nous a aidés ; les avantages que nous pressentions se sont confirmés dans les faits.

La grande similitude COSO / cadre de l'AMF a été déterminante

Même si nous n'avons pas retenu le COSO, la similitude COSO / cadre de référence AMF a été pour nous un élément important. D'abord, nous avions une garantie qu'il n'y aurait pas de contradiction. Nous utilisons le COSO dans nos travaux internes à la direction de l'audit et des risques de SNCF. Il reste une référence essentielle pour *benchmarker* nos travaux d'audit et former nos auditeurs et/ou nos spécialistes de contrôle interne. Ne pas avoir cette garantie de cohérence aurait risqué de nous mettre en forte difficulté voire de lever des incompréhensions avec des non spécialistes.

Notamment, il est important et rassurant de constater que les 5 composantes du contrôle interne sont les mêmes à quelques écarts minimes près. La logique est préservée : l'organisation / la diffusion d'information / le dispositif de gestion des risques / les activités de contrôle / la surveillance. Pour nous cela est essentiel. Il s'agit principalement d'écarts de terminologie. D'ailleurs, l'AMF disait en 2007 à propos du COSO : *« le groupe de place s'est inspiré des cinq composantes du COSO même si l'on ne retrouve pas à l'identique, dans le document de place, la terminologie utilisée par le référentiel américain ».*

Certes le COSO est un bon guide et donne beaucoup d'exemples mais le cadre de référence, comme nous l'avons vu plus haut, avec son questionnement et son guide d'application, est davantage orienté vers la mise en œuvre ; le travail d'adaptation / transcription au contexte de l'entreprise s'avère relativement simple et aisé.

Le « new COSO » : un enrichissement pour nos travaux

Nous n'opposons pas le COSO et le cadre de référence de l'AMF. Nous préférons y voir davantage une complémentarité. Pour nous, le COSO 2013 va nous aider à avoir un nouveau regard sur le contrôle interne et à identifier des pistes d'amélioration. C'est clairement un enrichissement pour tous nos travaux.

Nous avons aussi besoin de continuité dans les objectifs affichés. Nous avons largement communiqué sur le fait qu'il fallait que l'environnement de contrôle et les 14 processus du guide d'application sur le contrôle interne de l'informa-

Anne Bosche-Lenoir *est directrice de l'audit et des risques du groupe SNCF depuis avril 2013. Diplômée de l'ENA et de HEC, elle a occupé plusieurs postes à la direction du budget au ministère de l'Economie et des Finances dont celui de sous directrice en charge des Affaires Européennes. Elle a également été Senior Banker à la Banque Européenne pour la Reconstruction et le Développement (BERD), responsable du montage et du financement de projets dans les secteurs publics et privés en lien avec les banques locales. Elle a ensuite été DGA Finances, Audit et Contrôle de gestion au Conseil Régional d'Ile-de-France dans une période où le budget de la Région a crû de 70 % et les effectifs ont été multipliés par six.*

Raymond Marfaing*, diplômé de l'Ecole Centrale de Paris, a exercé différents postes de responsabilité à SNCF dans les directions centrales, aux achats, à l'organisation, aux ressources humaines et dans la direction régionale de Paris-Rive-Gauche où il était directeur délégué gestion finances. Il a rejoint la direction de l'audit et des risques en 2001 comme chef de mission puis comme directeur adjoint en charge des risques et du contrôle interne.*


© SNCF - Traismille

tion comptable et financière soient sous contrôle. Nous considérons que toute évolution de la cible serait un facteur de fragilisation. Beaucoup d'acteurs, notamment les opérationnels, commencent à bien comprendre ce qu'est le contrôle interne et ce qu'on attend d'eux. Ils ne perçoivent plus ce sujet comme un sujet de spécialiste dans lequel ils auront du mal à entrer. La continuité est essentielle pour nous.

En revanche, le COSO 2013, comme nous venons de le dire est une source d'enrichissement. On le voit bien à la lecture des thèmes suivants :

- la prise en compte des risques extra-financiers ;
- la mise en exergue du risque sous-traitance ;
- l'identification de 17 principes sur les attentes en matière de contrôle interne ;
- la présentation de 81 points d'attention avec pour chaque point des questions qui traduisent les grandes caractéristiques des principes.

Pour nous cela est une aide précieuse mais surtout dans nos missions de responsable de la politique de contrôle interne, en tant qu'entité qui définit les principes. En 2010, nous avons clairement défini une priorité : « être conforme AMF » sur les 14 processus et sur l'environnement de contrôle. Dans un premier temps, cela doit constituer le noyau dur de notre approche. Dans un deuxième temps, nous travaillerons sur les thèmes autres que financiers.

Ces raisons font que dans l'immédiat, il est difficilement imaginable de revenir sur le choix du cadre de référence de l'AMF.

L'AMF doit prendre en compte le COSO 2013

Le COSO 2013 introduit des changements importants comme sur les valeurs éthiques, l'importance de l'intégrité sur lesquels nous ne pouvons qu'adhérer. Ce sont d'ailleurs des axes forts à SNCF. Le COSO 2013 pointe également des sujets de fond comme la RSE, l'articulation des 3 lignes de défenses, l'articulation du « *tone at the top* » avec les comportements, la prise en compte des sous-traitants…

Ces évolutions ne sont pas incompatibles avec le cadre de référence de l'AMF. En effet, à la lecture approfondie du cadre AMF, on voit que la partie II sur les principes généraux de gestion des risques et de contrôle interne portent sur un périmètre qui ne se limite pas au domaine comptable et financier. Ce sont les parties relatives au questionnaire et au guide d'application qui ciblent sur ces domaines.

Compte tenu des apports du COSO 2013, il est important que le cadre de référence de l'AMF en tienne compte tout en gardant son côté souple, agile et facile d'accès qui constitue pour nous utilisateurs un atout et une attente. ●

Le groupe SNCF à fin 2012 : 5 branches / 33,8 milliards € de chiffre d'affaires

SNCF INFRA	SNCF PROXIMITÉS	SNCF VOYAGES	SNCF GEODIS	GARES & CONNEXIONS
Gestion, exploitation, maintenance du réseau pour RFF et ingénierie d'infrastructure	Services de transport public urbain, périurbain et régional pour les voyageurs du quotidien	Transport ferroviaire de voyageurs à grande vitesse	Opérateur global multi-modal de transport et logistique de marchandises	Gestion et développement des gares (indépendamment de l'activité de transporteur)
Activité en France + ingénierie en Europe, Asie, Moyen-Orient, Afrique, Amériques	TER, Transilien et Intercités en France, Trains d'Equilibre du Territoire (TET) Keolis en France, Europe, USA, Canada et Australie	Europe (France, Espagne, Royaume-Uni, Belgique, Pays-bas, Allemagne, Autriche, Suisse et Italie)	120 pays 5 continents	3 000 gares françaises et activité de l'AREP au niveau international
5,5 Mds € (15%)	12,8 Mds € (35%)	7,5 Mds € (20%)	9,5 Mds € (26%)	1 Md € (4%)