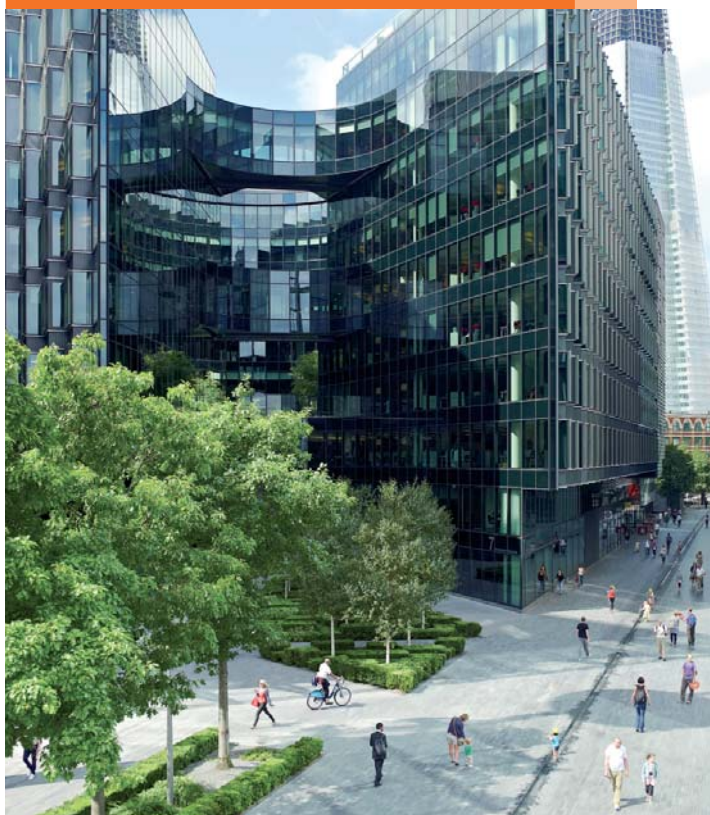


Pocket Guide

COSO 2013

Une opportunité
pour optimiser votre
contrôle interne
dans un environnement
en mutation



pwc

Pocket Guide rédigé sous la direction de

Jean-Pierre HOTTIN, Associé PwC

Françoise BERGE, Associée PwC

Catherine JOURDAN, Directeur PwC

Alix GUILLON, Senior Manager, PwC

Philippe MOCQUARD, Délégué Général IFACI

A partir de propos tenus lors du Colloque du 21 mai 2013

Juillet 2013

Introduction

Depuis plus de vingt ans, le COSO est une référence incontournable dans le domaine du contrôle interne à travers le monde.

Le référentiel COSO Contrôle Interne – Une Approche Intégrée publié en 1992 a défini les fondamentaux du contrôle interne. Cependant, pour mieux tenir compte de l'évolution de l'environnement économique et réglementaire dans lequel évoluent les organisations - nouveaux risques, attentes accrues en matière de gouvernance, rôle toujours plus important de la technologie, recours intensifié à l'externalisation, exigences de reporting au-delà de la communication financière - une mise à jour du référentiel a vu le jour le 14 mai 2013.

Le référentiel de 1992 ainsi que sa mise à jour en 2013 ont été rédigés par PwC, sous l'autorité du COSO, dont fait notamment partie l'Institute of Internal Auditors (IIA). En tant que membre de l'IIA, l'IFACI a participé à cette élaboration. De plus, PwC et l'IFACI se chargent, conjointement, de la traduction en langue française.

Le 21 mai 2013, l'IFACI et PwC ont organisé en partenariat un colloque pour présenter le COSO 2013 : « une opportunité d'optimiser le contrôle interne dans un environnement en mutation ».

Ce Pocket Guide présente les points clés abordés lors du colloque mettant en avant les enjeux de la mise en œuvre du contrôle interne en 2013, observations et témoignages de bonnes pratiques à date.

Sommaire

Contexte et objectifs 7

1. Pourquoi une mise à jour du référentiel COSO sur le contrôle interne ? 7
2. Qui a participé à l'élaboration de la mise à jour ? 8
3. En quoi consiste le COSO 2013 ? 8
4. Qu'est-ce qui change par rapport au référentiel d'origine ? 9
5. Pourquoi le référentiel COSO ERM reste-t-il à part ? 10

Des concepts clés 11

6. Comment les 17 principes sont-ils constitués et quelle valeur apportent-ils ? 11
7. Comment utiliser les principes ? 12
8. Comment utiliser les points d'attention ? 12

Les acteurs du contrôle interne 13

9. Comment les rôles et responsabilités liés au contrôle interne dans le COSO 2013 sont-ils définis ? 13
10. Comment les responsabilités des tiers sont-elles traitées ? 14
11. Quelle est l'articulation visée entre les auditeurs internes et les commissaires aux comptes en matière d'évaluation de l'efficacité du contrôle interne ? 14

Middle Management : Relais Indispensable 15

12. Pourquoi le COSO insiste-t-il sur le « tone in the middle » ? 15
13. Quels sont les apports notables du COSO 2013 pour aider à renforcer ce relais indispensable qu'est le middle management ? 16
14. Que faire en pratique pour améliorer le « tone in the middle » ? 16

Contexte et objectifs

1. Pourquoi une mise à jour du référentiel COSO sur le contrôle interne ?

L'objectif de la mise à jour du Référentiel COSO sur le contrôle interne est l'adaptation du dispositif de contrôle interne aux enjeux d'aujourd'hui et de demain. Le projet a permis de prendre du recul par rapport aux évolutions des vingt dernières années, depuis la parution du référentiel d'origine. En particulier :

- Les risques nouveaux qui émergent et qui sont autant de nouveaux enjeux de contrôle interne (la cyber-criminalité, le cloud-computing, etc.) ;
- Le rôle toujours plus important de la technologie (performance, sécurité, continuité, etc.) ;
- Le recours intensifié à l'externalisation, avec un enjeu de bonne définition des attentes en matière de contrôle interne vis-à-vis des prestataires ;
- Les attentes accrues en matière de gouvernance (notamment les rôles des

comités au niveau du conseil mais aussi de la direction générale sur des enjeux importants comme les risques, la conformité, etc.) ;

- La responsabilisation du personnel à tous les niveaux de la hiérarchie et dans toutes les entités de l'organisation (le « tone in the middle » et le lien entre les objectifs, les risques encourus et l'évaluation de la performance) ;
- La nécessité de s'adapter en permanence à un environnement interne et externe en mutation ;
- L'efficacité et l'efficience du dispositif de contrôle interne (l'articulation entre les opérationnels, les fonctions support, et l'audit interne) ; et
- Les exigences de reporting au-delà de la communication financière (développement durable, environnement, qualité, etc.).



« Depuis 1992, nos entreprises ont changé. Nous sommes tous dans un rythme de transformation rapide. Nous nous sommes développés, globalisés, avons vu le renforcement des systèmes d'informations et avons externalisé une partie de notre activité, autant de situations nouvelles sur lesquelles la version d'origine du référentiel n'apportait pas tout l'éclairage nécessaire. »

Florence Vincent, Michelin

2. Qui a participé à l'élaboration de la mise à jour ?

Le projet de mise à jour a été commandité et piloté par le conseil d'administration du COSO. Celui-ci a engagé PwC pour mener le projet et rédiger la mise à jour, avec l'appui d'un comité (« Advisory Council »), composé de représentants de cabinets de conseil, d'experts comptables, d'associations professionnelles (telles que Financial Executives International, Institute of Management Accountants, AICPA, ISACA, IFAC, etc.), de représentants d'organisations

utilisatrices de référentiels (par ex. Pfizer, Campbell Soup, Community Trust Bank, GAVI Alliance, etc.), et d'auditeurs internes (Institute of Internal Auditors).

Au-delà de l'enquête initiale lancée par le COSO en janvier 2011, le projet a fait l'objet de deux phases de consultations publiques, qui ont généré plus de 1000 commentaires provenant du monde entier.

3. En quoi consiste le COSO 2013 ?

Le COSO 2013 comprend :

- Un résumé ;
- Le référentiel et ses annexes qui définissent le contrôle interne, le positionnent par rapport à trois catégories d'objectifs, présentent les cinq composantes du contrôle interne, déclinées en 17 principes structurants, et décrivent les exigences en matière d'efficacité ;
- Des outils qui présentent des tableaux d'évaluation et de synthèse, divers scénarios pour faciliter l'évaluation des 17 principes qui constituent un dispositif de contrôle interne efficace ; et
- Un recueil d'approches et d'exemples dans le domaine du reporting financier externe (Internal Control over External Financial Reporting, « ICEFR ») qui propose des exemples de mise en pratique des 17 principes dans le cadre de la réalisation des états financiers.



4. Qu'est-ce qui change par rapport au référentiel d'origine ?

Le référentiel de 2013 reprend les éléments essentiels du référentiel COSO de 1992, en particulier la définition, les cinq composantes, et les critères d'évaluation.

Les principales évolutions concernent :

1. L'élargissement du domaine d'application au-delà du reporting financier (par exemple la responsabilité sociale et environnementale) ;
2. Le renforcement des attentes en matière de gouvernance (par exemple les rôles des comités et l'alignement avec le business model) ;
3. La gestion des collaborateurs clés du contrôle interne (par exemple plans de successions pour la direction générale) ;
4. L'articulation des 3 « lignes de maîtrise » dans l'organisation (les opérationnels, les fonctions support, et l'audit interne) ;
5. La relation entre risque, performance et rémunération (notamment le principe portant sur la responsabilisation) ;

6. L'articulation du « tone at the top » avec les comportements à travers l'organisation (« tone in the middle ») ;
7. La prise en compte des sous-traitants et des autres intervenants clés (par exemple leur adhésion au code de conduite, au respect des contrôles au-delà du reporting financier) ; et
8. L'exigence de l'adaptabilité et l'adéquation du dispositif par rapport à l'évolution de l'organisation, liée par exemple à la mise en place de nouveaux processus, rôles, structures, systèmes d'information, centres de services partagés, périmètre d'activité, etc.

Enfin, le COSO 2013 définit les éléments essentiels du contrôle interne au travers de 17 principes structurants (cf. Annexe).

La mise en œuvre des bonnes pratiques est illustrée de manière plus concrète par des approches et des exemples.



« L'intérêt de ce nouveau référentiel est qu'il élargit le spectre couvert : il ne s'agit plus simplement des domaines comptables et financiers, de la conformité, et des sujets opérationnels, mais aussi toute la communication extra-financière, le reporting sur la responsabilité sociale et environnementale, la sécurité, tant d'éléments essentiels à la bonne gouvernance. »

Serge Villepelet, PwC

5. Pourquoi le référentiel COSO ERM reste-t-il à part ?

Le COSO 2013 est une mise à jour du référentiel de 1992 portant sur le contrôle interne. Il n'élargit donc pas, à ce stade, le périmètre du contrôle interne aux objectifs stratégiques, à l'appétence pour le risque ou autres sujets du ressort de l'Enterprise Risk Management et du référentiel de 2004. En effet, dans la pratique, les deux concepts correspondent toujours à des usages distincts.

Cependant, le COSO 2013 apporte un éclairage utile sur des sujets éminemment

pertinents pour l'ERM. Il intègre des éléments du référentiel ERM de 2004 sur les sujets pertinents pour le contrôle interne, tels que les facteurs d'évaluation des risques, l'impact du changement de l'environnement, etc.

Le COSO 2013 s'articule logiquement avec le COSO ERM, le contrôle interne étant défini comme une partie intégrante de l'ERM (cf. Annexe G du référentiel COSO 2013).



« Le COSO 2013 reste distinct du référentiel ERM. Cependant on constate qu'il en intègre certains éléments. L'enjeu pour nos organisations soumises à une diversité de réglementations et référentiels est en effet la convergence entre ceux-ci. »

Marie-Hélène Laimay, Sanofi

Des concepts clés

6. Comment les 17 principes sont-ils constitués et quelle valeur apportent-ils ?

Le COSO 2013 décline 17 principes essentiels liés aux cinq composantes du contrôle interne (cf. Annexe).

Chaque principe a sa raison d'être. Ainsi, dans certains cas un principe peut avoir été établi pour traiter d'un cas particulier. Par exemple, le principe n°8, portant sur l'évaluation de la fraude, pourrait être perçu comme une déclinaison du principe n°7 qui porte sur l'analyse des risques. De même, le principe n°11, sur les contrôles informatiques, pourrait être compris comme un cas particulier du principe n°10 sur les activités de contrôle. C'est bien l'importance de la lutte contre la fraude et de la maîtrise des moyens informatiques qui justifient l'insertion de ces principes spécifiques.

Chaque principe est applicable à tout secteur, nature d'activité, et taille d'organisation.

Au-delà de la formalisation des attentes en matière de contrôle interne, le COSO 2013 a vocation à :

- Renforcer les contrôles et gagner en confiance sur les opérations, le reporting et les objectifs de conformité ;
- Identifier les risques nouveaux et définir des dispositifs de maîtrise appropriés ;
- Analyser comment les ressources, la technologie et les processus peuvent potentiellement causer des défaillances de contrôle et comment les éviter ; et
- Cibler les contrôles pour mieux répondre aux évolutions de l'environnement.

7. Comment utiliser les principes ?

La mise en place des 17 principes permet un contrôle interne efficace. Il est important qu'ils ne soient pas considérés comme des éléments distincts et discontinus, mais qu'au contraire ils fonctionnent conjointement au sein d'un système intégré. Chacun des dix-sept principes fonctionnant conjointement contribue à réduire à un niveau acceptable le risque qu'un objectif ne soit pas atteint.

Un principe non mis en œuvre ou des principes ne fonctionnant pas conjointement met le dispositif à risque.

A titre illustratif :

- L'évaluation des changements (principe n°9) liés à l'externalisation de certaines activités de contrôle (principes n°10) fait appel, notamment, à une redéfinition des structures, des rôles et des responsabilités

(principe n°3), des canaux de communication avec des tiers sur des problématiques de contrôle interne (principe n°15) et des activités d'évaluation continues et ponctuelles (principe n°16).

- Les activités de pilotage (principe n°16) qui détectent les résultats non conformes aux attentes et en analysent les causes permettent de maîtriser le risque d'erreur récurrente dans le traitement des transactions (principe n°7).
- Les efforts déployés par l'organisation pour maintenir et accroître les compétences des collaborateurs (principe n°4) et les responsabiliser sur le dispositif de contrôle interne (principe n°5) réduisent le risque d'erreur dans les activités de contrôle (principes n°10, 11 et 12).



« Les 17 principes du COSO 2013 ne doivent pas simplement être présents et fonctionner, mais ils doivent aussi interagir entre eux ».

Catherine Jourdan, PwC

8. Comment utiliser les points d'attention ?

Le COSO 2013 identifie 81 points d'attention associés aux principes. Ceux-ci représentent des caractéristiques importantes des principes. Il peut arriver que, lors de la conception et de la mise en place d'un dispositif de contrôle interne, la direction générale estime que certaines de ces caractéristiques ne sont pas pertinentes au regard de la situation spécifique de l'organisation et qu'elle tienne compte d'autres critères plus appropriés. Le

Référentiel n'exige pas que la direction générale évalue la mise en œuvre de chaque point d'attention de façon exhaustive.

En revanche, le management peut s'appuyer sur les points d'attention pour concevoir, mettre en place et piloter le système de contrôle interne et pour évaluer dans quelle mesure les principes sont effectivement mis en place et s'ils fonctionnent correctement.

Les acteurs du contrôle interne

9. Comment les rôles et responsabilités liés au contrôle interne dans le COSO 2013 sont-ils définis ?

Le contrôle interne demeure la responsabilité de tous au sein de l'organisation. Le COSO 2013 utilise le modèle des trois lignes de maîtrise pour décrire les responsabilités essentielles de chaque grande fonction :

- En premier lieu, ce sont les opérationnels (par exemple les chargés de production, des ventes, etc.) qui doivent s'assurer de la bonne conception et du bon fonctionnement du dispositif de contrôle interne ;
- En second lieu, les fonctions support (par exemple les chargés de conformité, sécurité, gestion des risques) apportent expertise et conseil par rapport aux objectifs de performance et de contrôle ; et
- En dernière instance, l'audit interne permet un regard indépendant et des revues variées dans un but, notamment, d'améliorer le contrôle interne de l'organisation.



« Auparavant, les opérationnels comptaient essentiellement sur l'audit interne ou sur les fonctions risques et conformité. Désormais, comptez un peu moins sur eux, vous êtes responsables ».

Alain Lemarcis, SNCF

10. Comment les responsabilités des tiers sont-elles traitées ?

Bien que l'organisation puisse faire appel à un prestataire de services extérieur chargé de mettre en œuvre les processus, les règles et les procédures pour le compte de l'entité, la direction générale demeure responsable en dernier ressort du respect des conditions fixées par le référentiel en matière d'efficacité du dispositif de contrôle interne.

Les tiers qui interagissent avec l'entité, tels que les auditeurs externes et les régulateurs,

ne font pas partie du système de contrôle interne. Ils ne font donc pas non plus partie du processus d'évaluation managériale du système.

Cela ne veut pas dire pour autant qu'il faille ignorer leur travaux. Une coordination efficace contribue à éviter les redondances et à assurer que les risques majeurs sont bien couverts.

11. Quelle est l'articulation visée entre les auditeurs internes et les commissaires aux comptes en matière d'évaluation de l'efficacité du contrôle interne ?

Cette articulation 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.

Des éléments clés à prendre en compte sont : les échanges sur le plan d'audit interne et externe, l'organisation de rendez-vous réguliers de partage d'information, et la transmission des rapports d'audit qui concernent le contrôle interne.

Comme le soulignent non seulement le COSO 2013 mais aussi d'autres guides tels que celui de l'IFA de novembre 2009 sur les Comités

d'Audit et Commissaires aux Comptes, le Comité d'Audit, en étroite relation avec les commissaires aux comptes et les auditeurs internes, a un rôle majeur à jouer pour encourager et faciliter les échanges. Le Comité d'Audit est d'ailleurs le premier bénéficiaire d'une bonne communication entre ces deux instances de contrôle car il en tire une vision beaucoup plus complète et plus intégrée de la gestion des risques de l'organisation.

Enfin, les opérationnels bénéficieront également d'une meilleure coordination entre les Commissaires aux comptes et l'audit interne, les missions redondantes étant ainsi évitées.

Middle Management : Relais Indispensable

12. Pourquoi le COSO insiste-t-il sur le « tone in the middle » ?

Passée la définition des attentes, c'est au niveau du middle management que s'effectue réellement la mise en œuvre du contrôle interne, ou non... C'est en effet à ce niveau opérationnel de l'organisation que se croisent de multiples directives relatives à la performance et à l'innovation mais aussi à la réduction des coûts et aux

restructurations, sans délaisser pour autant le bon fonctionnement du contrôle interne. Il s'agit alors de s'assurer que le middle management définisse, communique et applique les priorités, de manière à ce que les bons contrôles soient effectués aux bons endroits.



« Si l'engagement de la direction reste primordial, le middle management est aussi une cible et un relais clé pour faire évoluer la culture de la gestion des risques et du contrôle interne. »

Isabelle Dreyssé, ADP



13. Quels sont les apports notables du COSO 2013 pour aider à renforcer ce relais indispensable qu'est le middle management ?

Le COSO 2013 accorde une importance significative au middle management, notamment au travers des principes suivants :

- L'engagement en faveur de l'intégrité et des valeurs éthiques (principe n°1), qui consiste à donner l'exemple, à établir les normes de conduite, à évaluer l'adhésion aux normes de conduite, et à gérer les écarts en temps voulu ;
- La définition des structures, des rattachements, ainsi que des pouvoirs et des responsabilités appropriés pour atteindre les objectifs (principe n°3) ; et
- L'instauration pour chacun d'un devoir de rendre compte de ses responsabilités en matière de contrôle interne (principe n°5), passant par l'établissement et le suivi d'indicateurs de performance et de mesures d'incitation, en étant vigilant face aux pressions excessives.

14. Que faire en pratique pour améliorer le « tone in the middle » ?

Dans cette perspective, il est important de mettre l'accent sur la contribution du contrôle interne à la maîtrise des opérations. Cela peut notamment se faire dans le cadre de revues managériales au cours desquelles les responsables de l'entité et le responsable du contrôle interne échangent sur les résultats des contrôles réalisés et le traitement des écarts ou dysfonctionnements repérés. L'objectif est de dégager la contribution du contrôle interne à l'amélioration de la performance.

La filière contrôle interne doit se positionner en appui et à l'écoute du management pour l'aider à concevoir un dispositif de contrôle interne répondant à ses attentes et permettant de couvrir les risques métiers et transverses. Pour gagner en « lisibilité », il y a un intérêt fort à mettre en synergie les démarches qualité/processus (quand elles existent), management des risques et contrôle interne.

Un autre axe est d'intégrer la responsabilité du contrôle interne dans les objectifs et critères d'évaluation.



« Un bon moyen d'améliorer le « tone in the middle » est d'intégrer des objectifs de contrôle interne dans les lettres de mission et/ou contrats de gestion des managers. La réalisation de ces objectifs est évaluée et prise en compte dans la détermination de leur rémunération variable. Cette approche s'avère efficace ! »

Marie-Hélène Sinnassamy, GDF Suez

Application au Domaine Comptable et Financier

15. Pourquoi un recueil séparé sur le contrôle interne sur le reporting financier externe, et quel apport ?

On constate que le COSO est devenu une référence universelle en matière de contrôle interne, particulièrement dans le cadre comptable et financier. En effet, bon nombre de réglementations à travers le monde y font référence de manière explicite (par exemple la SEC aux États-Unis pour l'application de la loi Sarbanes-Oxley) ou de fait s'appuient dessus (par exemple le Tabaksblat aux Pays-Bas). Il a ainsi été jugé utile de décliner au domaine comptable et financier les concepts de ce référentiel mis à jour pour en faciliter l'application.

Le recueil COSO Internal Control over External Financial Reporting (ICEFR) 2013 a pour but d'apporter diverses approches et cas pratiques pour illustrer la mise en œuvre

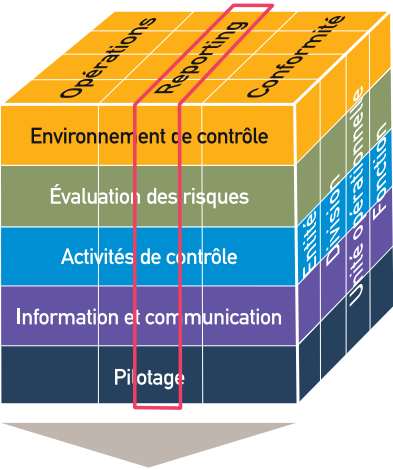
des 17 principes du contrôle interne relatif à l'établissement des rapports financiers.

Il se concentre ainsi sur une sous-partie des objectifs d'une organisation. Par exemple, par rapport au principe n°6 portant sur l'établissement des objectifs, l'ICEFR illustre comment tenir compte de la matérialité, revoir et mettre à jour la compréhension des normes applicables.

Il est concevable que des recueils similaires soient élaborés par la suite sur l'application des 17 principes à d'autres objectifs, tels que le reporting non-financier et les divers reporting internes, la conformité ou l'opérationnel.

16. Comment utiliser ce recueil ?

L'ICEFR s'articule autour des 17 principes et points d'attention établis dans le référentiel, comme illustré ci-dessous.



5 Composantes	17 Principes	85 Points d'attention illustratifs	Approches	Exemples
1. Environnement de contrôle	Principes 1 à 5	20 points d'attention	...	...
2. Évaluation des risques	Principe 6 : Définir des objectifs appropriés Principe 7 : ... Principe 8 : ... Principe 9 : ...	25 points d'attention dont les suivants pour le Principe 6 : • Respecte les normes comptables applicables • Tient compte de la matérialité • Dispose d'un reporting reflétant les activités de l'entité	• Identifier les critères de qualité dans les états financiers • Définir les objectifs en matière de reporting financier • Déterminer la matérialité • Revoir et mettre à jour la compréhension des normes applicables • Prendre en compte les domaines d'activité de l'entité	• Établir des liens entre les comptes, les critères de qualité et les risques • Évaluer la pertinence des objectifs fixés • Déterminer la matérialité pour les états financiers d'une société non cotée • Revoir et mettre à jour la compréhension des normes applicables • Prendre en compte l'étendue des activités d'évaluation ...
3. Activités de contrôle	Principes 10 à 12	16 points d'attention	...	...
4. Information et communication	Principes 13 à 15	14 points d'attention	...	...
5. Pilotage	Principes 16 et 17	10 points d'attention	...	...



« Le recueil ICEFR apporte pour chacun des 17 principes plusieurs approches et exemples pour aider à confirmer la bonne mise en œuvre, ou au contraire aider à identifier des axes d'amélioration. »

Nicolas Brunetaud, PwC

17. En pratique, quels sont les points nécessitant encore souvent des efforts ?

Les activités de contrôle sont souvent les premiers éléments concrets de contrôle interne mis en œuvre. Cependant, il reste souvent bien du chemin à parcourir pour que l'organisation dans son ensemble, ses processus et ses outils viennent s'inscrire dans un dispositif global de contrôle interne. Concrètement :

- Environnement de contrôle : un conseil d'administration qui challenge le management ; les compétences nécessaires à tous les niveaux de l'organisation, notamment dans la fonction financière et comptable ; des structures de reporting clairement établies ; le « tone at the top » ;
- Évaluation des risques : veille constante et une analyse des risques internes et externes à l'organisation ; dispositif efficace de prévention et de détection de fraude ; capacité de réaction et d'intégration du changement ;
- Activités de contrôle : établissement d'un nombre limité de contrôles aux bons endroits dans les processus (contrôles de cohérence, séparation des tâches, contrôles compensatoires, etc.) ; déclinaison des politiques et procédures comptables, financières et autres à travers l'organisation, « tone in the middle » ;
- Information et Communication : Qualité et pertinence de l'information financière ou non financière circulant au sein de l'organisation ; et
- Pilotage : Identification et suivi des défaillances de contrôle interne (auto-évaluation de l'efficacité du contrôle, audit interne puissant fonctionnant sur la base de la cartographie des risques) ; remontée de l'information significative et pertinente au conseil d'administration via son comité d'audit.



Un sondage réalisé lors du Colloque auprès des participants révèle que l'évaluation du dispositif de contrôle interne se fait souvent par une auto-évaluation ou une évaluation indépendante, mais surtout par une combinaison des deux



Externalisation et contrôle interne

18. Pourquoi insister sur l'externalisation ?

On constate de plus en plus de recours à des partenaires commerciaux et prestataires de services à tous niveaux de la chaîne de valeur ainsi qu'au niveau des fonctions support. Ces structures peuvent apporter des expertises clés, une ouverture sur de nouveaux marchés, des opportunités de réduction de coût, et d'autres avantages. Cependant, elles présentent également des enjeux de

maîtrise des risques associés à ce mode de fonctionnement « en entreprise étendue ».

Il s'agit d'assurer un contrôle interne efficace, tant chez le prestataire que dans l'organisation utilisatrice, et aux interfaces entre les deux. Le COSO 2013 reflète ces attentes à travers l'ensemble des 17 principes.



« Les 17 principes s'appliquent à tous les niveaux de l'organisation, mais aussi aux partenaires commerciaux et prestataires essentiels de l'organisation. »

Anne-Christine Marie, PwC

19. Quels sont les enjeux pour les organisations utilisatrices de services externalisés ?

Au-delà d'un niveau de performance recherché, l'organisation doit s'assurer que le niveau de contrôle interne de ses prestataires est adéquat. En particulier :

- La transparence relative aux risques et aux contrôles mis en place (protection de données confidentielles client, propriété intellectuelle, fiabilité des données, etc.)
- Le maintien de la responsabilité ultime au niveau de l'entreprise utilisatrice et le bon pilotage des activités à travers toute la chaîne de valeur, y compris les rôles, les responsabilités et les interfaces humaines et automatisées (par le biais d'indicateurs tels que des Key Performance Indicators, Key Risk Indicators ou Key Process Indicators) ; et
- La cohérence du dispositif de contrôle interne du prestataire par rapport aux attentes de l'organisation utilisatrice (les activités de contrôle mais aussi l'environnement de contrôle, le pilotage, etc.).

20. Comment le prestataire de services peut-il répondre à ces attentes ?

En premier lieu il est important pour le prestataire et l'organisation utilisatrice de services de définir ensemble les attentes respectives. La contractualisation entre ces parties se doit alors de porter non seulement sur le niveau de performance requis mais aussi sur les attentes en matière d'activités de contrôle, d'adhésion aux valeurs de l'organisation, de droit de regard, d'audit et d'assurance donnée par un tiers. Ensuite, les processus et les outils informatiques mis en œuvre doivent permettre, de manière efficace, d'accéder aux informations sous-jacentes requises par l'organisation utilisatrice.

On constate que le niveau de satisfaction et d'alignement par rapport aux attentes dépend souvent particulièrement de :

- La nature des services externalisés (prestation essentielle, à forte visibilité, ou non) ;
- La qualité et la fréquence des procédures de sensibilisation et de rappel, et de la surveillance du respect des normes de conduite par ses collaborateurs ;
- L'envergure et la complexité des processus du prestataire et de son modèle économique.

Ainsi, le succès de l'externalisation dépend bien souvent du niveau d'effort des deux parties.



« La finalité de la maîtrise des risques est la même que sans externalisation. Mais les moyens à mettre en œuvre peuvent être différents. Ce n'est pas parce que l'on paie pour un service que l'on a toutes les assurances de la bonne maîtrise des risques. »

Yann Boucrault, Bouygues

21. Quelles sont les étapes clés pour gérer au mieux les opportunités et les risques associés à l'externalisation et s'assurer du bon niveau de contrôle interne ?

1. **La sélection du prestataire** est une étape fondamentale. C'est à ce stade que sont définis les critères (coût, mais aussi adéquation et efficacité des contrôles, plan de continuité d'activité, etc.) qui formeront la base pour la contractualisation. La « due diligence » prestataire est ensuite effectuée pour évaluer les processus, structures et outils informatiques pour s'assurer de leur fiabilité. Au-delà des experts techniques (pour la négociation achats, la contractualisation, l'expertise métier, etc.), les responsables du contrôle interne doivent apporter un regard critique sur l'adéquation du dispositif du prestataire. Ces échanges ont pour objectif de permettre la sélection d'un prestataire capable de répondre aux attentes de performance mais aussi de s'insérer dans le dispositif de contrôle interne de l'organisation utilisatrice des services.
2. **L'établissement et le suivi du contrat** donnent une base d'évaluation de la qualité

de la relation prestataire-client. La direction des achats, les juristes et les experts métier jouent un rôle important. Les responsables du contrôle interne se doivent d'aider à définir le niveau de maîtrise requis. Le contrôle interne soutient ainsi la direction générale qui doit accepter les risques liés à la mise en place d'un processus d'externalisation. L'organisation est alors en mesure de mettre en œuvre les moyens nécessaires pour gérer et piloter de manière opérationnelle le contrat (indicateurs à vérifier, clause d'audit à exercer...).

3. **Les contrôles de cohérence au fil de l'eau** par les opérationnels utilisateurs sont importants dans la mesure où ils confèrent un niveau d'assurance régulier. Dans ce sens, il est souvent utile de désigner dans l'organisation un propriétaire du processus d'externalisation, permettant de centraliser la connaissance et la supervision des contrôles délégués.

22. Comment rendre compte à ses parties prenantes ?

La confiance quant à la fiabilité des services rendus et des contrôles associés peut être renforcée par des audits conduits par le service d'audit interne et par le biais d'une assurance donnée par un tiers (« Third Party Assurance »), produisant des rapports normés selon ISAE 3402, ISAE 3000, etc. Cela nécessite de l'expertise en matière d'évaluation de contrôle interne, mais permet une harmonisation de l'approche et une réduction des temps requis pour permettre

l'évaluation et une meilleure transparence, voire même un avantage concurrentiel.

Une évaluation du contrôle interne des prestataires permet d'identifier, le cas échéant, les améliorations à apporter au dispositif pour répondre aux attentes des parties prenantes.

23. Quels sont les apports notables du COSO 2013 relatifs à l'externalisation ?

Le COSO s'applique dans son intégralité à l'externalisation. C'est-à-dire que l'ensemble des 17 principes doivent être mis en œuvre tant dans l'organisation utilisatrice de services que chez le prestataire, avec une articulation logique entre leurs dispositifs.

Par exemple, l'identification et l'évaluation des risques associés à la réalisation des objectifs (principe n°7) doivent donner une vision complète des risques et des activités de contrôle mises en face (principe n°10) sur l'ensemble du processus, tant pour les parties réalisées en interne que celles qui sont externalisées.

Transformation et contrôle interne

24. Pourquoi insister sur la transformation ?

Des transformations mal conduites peuvent déboucher sur un constat de coût trop élevé, un manque de maîtrise des nouveaux processus/outils, une détérioration temporaire de la performance, ou d'autres décalages par rapport aux objectifs de l'organisation. On constate que les projets de transformation impactent souvent directement les fondamentaux du contrôle interne. La question est alors : comment réaliser les bénéfices attendus des projets de transformation (tels que la mutualisation de certaines activités, l'accélération de la

production, la réduction des coûts, etc.) sans dégrader le niveau de maîtrise des risques associés ?

La transformation dans les organisations nécessite un regard proactif en matière de contrôle interne tout au long du projet de transformation. Ce regard se doit d'être porté par un ensemble de responsables du contrôle interne, de la gestion des risques et de l'audit interne, en liaison étroite avec les opérationnels impliqués dans le projet de transformation.

25. De quels types de transformations parle-t-on?

On s'intéresse ici aux changements que l'organisation peut conduire, tels que :

- Le changement de système d'information ;
- L'adoption de nouvelles technologies (media sociaux, etc.) ;
- La mise en place d'un centre de services partagés ;
- L'externalisation ou établissement d'alliances (joint ventures, etc.) ;
- L'application d'une nouvelle réglementation ou l'évolution des attentes des organes de gouvernance ;

- L'ouverture vers de nouveaux marchés ; et
- L'évolution du périmètre d'activité de l'entreprise (fusions, acquisitions, cessions, etc.).

Tous ces changements vont bouleverser les rôles et responsabilités, la nature des risques, les contrôles nécessaires, etc. Bref, les 17 principes sont concernés.



« Le changement (interne et externe) est permanent, et l'organisation se doit de s'adapter et se transformer en continu. »

Annie Bressac, Consultante

26. À quelles étapes est-il particulièrement important d'impliquer le contrôle interne dans les projets de transformation ?

Le contrôle interne se doit d'accompagner la transformation de bout en bout. En amont, il apporte une perspective dans les études de faisabilité et d'impact de la transformation. En effet, il évalue le dispositif de contrôle interne par rapport aux objectifs de l'organisation. Il contribue également à définir des facteurs clés de succès liés au projet de transformation (qualité opérationnelle, communication adéquate, maîtrise des risques, conformité, etc.).

Au cours du projet, le contrôle interne joue un rôle essentiel dans l'élaboration ou la refonte des contrôles, l'harmonisation ou la refonte des dispositifs (processus métier, plans de continuité d'activité,

reporting, etc.), la gestion du changement (communications, formations, etc.), et le pilotage des indicateurs clés. L'enjeu est de suivre et de responsabiliser, par exemple au moyen de primes ne portant pas uniquement sur la performance à court terme mais aussi à la bonne maîtrise des risques, ou par la réalisation d'audits pour identifier les lacunes de compétences.

En aval, le contrôle interne peut apporter un regard sur l'adéquation et l'efficacité de l'ensemble du dispositif de contrôle interne post-transformation. Il facilite alors la remontée et correction de défaillances de contrôle interne constatées.



« L'adaptation du dispositif de contrôle interne commence à la conception d'une transformation organisationnelle et continue au cours de sa réalisation. »

France Hanniet, Orangina Schweppes

27. En quoi le COSO 2013 permet-il à l'organisation de fiabiliser et d'optimiser l'exécution des priorités, et d'améliorer sa résilience et son adaptation face aux transformations ?

Le COSO 2013 met en avant l'importance de l'adaptabilité du dispositif de contrôle interne face aux changements. Un principe essentiel du COSO porte sur l'évaluation du changement (principe n°9). En effet, la capacité d'anticipation et d'adaptation au changement, de se remettre de tout type d'évènement à risque (y compris les situations inédites) et d'en saisir les opportunités est importante pour fiabiliser et optimiser l'exécution des priorités de l'organisation.

Ceci étant, ce principe essentiel se doit d'interagir avec les autres principes du COSO. Ainsi, cette capacité dépend de et alimente les autres principes de contrôle

interne, tels que la responsabilisation pour le contrôle interne (principe n°5), les flux de communication interne (principe n°14), et le pilotage (processus, outils) permettant la transparence sur l'avancement des chantiers de transformation et sur l'atteinte des objectifs définis (taux de réalisation, seuils de tolérance, etc.) permettant d'évaluer, de remonter et d'adresser des défaillances éventuelles en matière de contrôle interne (principe n°17).

L'adoption du COSO facilite ainsi la résilience en ce qu'elle permet l'adoption d'un langage commun dans le cadre des transformations de l'organisation.



« Des transformations en cours au ministère rendent nécessaire un contrôle interne sur le champ métier, opérationnel. Ceci nous permet notamment de hiérarchiser les risques liés à nos missions. »

Arnauld Marrou, Ministère de l'Écologie, du Développement Durable et de l'Énergie



Et maintenant ?

28. Quelle est la date préconisée pour l'adoption du COSO 2013 ?

Le COSO laisse à disposition le référentiel de 1992 jusqu'au 15 décembre 2014, date à laquelle il sera retiré du marché et définitivement remplacé par la mise à jour de 2013. Il ne pourra donc plus être

fait référence à l'ancien COSO à partir de cette date (par exemple pour une clôture au 31 décembre 2014), et le périmètre du contrôle interne à prendre en compte alors sera celui du COSO 2013.

29. Pourquoi utiliser le nouveau COSO ?

La vie des organisations, les événements internes ou externes qui les affectent nécessitent une remise en cause permanente des dispositifs de contrôle interne.

D'une part, on constate que de nombreuses escroqueries relèvent de principes fondamentaux de contrôle interne (double signature, mise à jour des pouvoirs bancaires, suivi des comptes de bilan, etc.). Chacun a en tête également des exemples de fraudes comptables, d'ampleur plus ou moins importante, ainsi que des affaires plus graves dans le domaine de la santé ou dans le domaine alimentaire qui peuvent soulever une incompréhension du public sur la nature des contrôles réalisés, par exemple par les contrôleurs publics ou les organismes externes - sans pour autant interroger les dispositifs de contrôle interne propres à l'organisation.

D'autre part, les organisations se retrouvent bien souvent devant une démultiplication des dispositifs par rapport aux diverses attentes (contrôles de qualité opérationnelle, sécurité, prévention contre la fraude, la corruption, le blanchiment, etc.) souvent avec des redondances mais aussi des manquements. Il en ressort un besoin de meilleure articulation logique et d'une meilleure efficacité des dispositifs de contrôle interne pour éviter « les trous dans la raquette » tout en optimisant les budgets alloués.

Par ailleurs, les obligations particulières liées à la huitième directive relative au droit des sociétés en Europe, exigent des sociétés cotées une communication formelle sur les facteurs de risque et les dispositifs de gestion de ces risques (chapitre Facteurs de Risque du document de référence), et description

des dispositifs de contrôle interne dans le Rapport du Président.

L'utilisation d'un outil tel que le COSO 2013 en complément du cadre de référence de l'AMF en France permet aux organisations concernées de se conformer efficacement à

ces obligations. Ces pratiques de gestion des risques et de contrôle interne sont d'ailleurs prises comme référence non seulement par les sociétés cotées mais aussi les sociétés non cotées et, au-delà, au sein du secteur public et associatif.



« Le COSO 2013 est un outil qui aide les organisations à mettre en œuvre et à faire évoluer leurs dispositifs de contrôle interne afin qu'ils restent adaptés à leurs besoins. »

Jean-Pierre Hottin, PwC

30. Qui doit se référer au COSO 2013 ?

Les organisations qui utilisent actuellement le COSO dans leur document de référence ou leur rapport au président doivent dorénavant utiliser le COSO 2013.

Les organisations qui n'ont pas d'obligation légale auront un avantage à utiliser le COSO 2013 car il constitue une remarquable référence en matière de mise en œuvre et maintenance du dispositif de contrôle interne.

31. Quelle est l'articulation entre le Cadre de Référence de l'AMF et le COSO 2013 ?

Le Cadre de Référence de l'AMF repose notamment sur les concepts élaborés dans le référentiel COSO d'origine, qui évoluent dans le COSO 2013.



« Une réflexion est en cours pour déterminer si une mise à jour du Cadre de Référence est à réaliser »

Martine Charbonnier, AMF

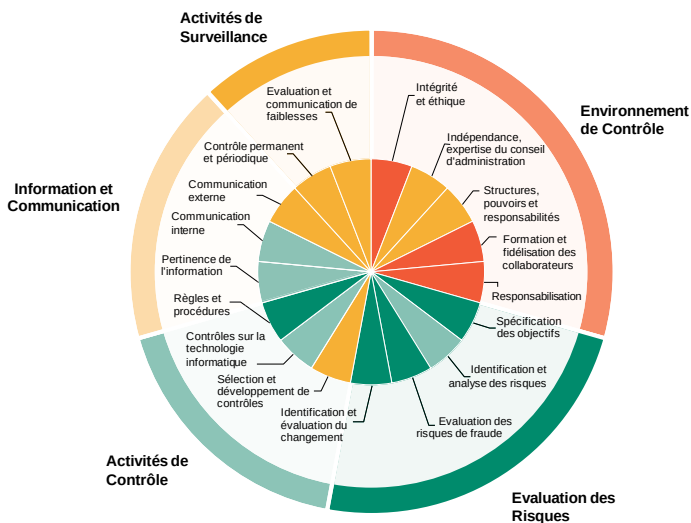
32. Quelles actions sont à envisager pour se mettre en conformité avec le COSO 2013 ?

Pour se mettre en conformité, l'organisation peut :

- Faire un diagnostic sur la base des 17 principes pour identifier les axes d'amélioration nécessaires au niveau du groupe et des entités ;
- Approfondir certains sujets sur la base des 17 principes (par exemple la prise en compte des tiers dans l'évaluation du

contrôle interne, l'utilisation des nouvelles technologies, notamment en ce qui concerne la sécurité des bases de données et le cloud-computing qui peut connaître une défaillance, etc.).

Et cela tout en veillant à l'articulation effective de ces 17 principes.



Annexes

A. Définition du contrôle interne selon le COSO 2013

Le contrôle interne est un processus mis en œuvre par le conseil, le management et les collaborateurs, et qui est destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité.

B. Les 17 principes structurants

Composantes	Principes
Environnement de contrôle	1. L'organisation manifeste son engagement en faveur de l'intégrité et de valeurs éthiques. 2. Le Conseil fait preuve d'indépendance vis-à-vis du management. Il surveille la mise en place et le bon fonctionnement du dispositif de contrôle interne. 3. Le management, agissant sous la surveillance du Conseil, définit les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour atteindre les objectifs. 4. L'organisation manifeste son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs. 5. Afin d'atteindre ses objectifs, l'organisation instaure pour chacun un devoir de rendre compte de ses responsabilités en matière de contrôle interne.
Évaluation des risques	6. L'organisation définit des objectifs de façon suffisamment claire pour rendre possible l'identification et l'évaluation des risques susceptibles d'affecter leur réalisation. 7. L'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre et procède à leur analyse de façon à déterminer comment ils doivent être gérés. 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 contrôles généraux informatiques pour faciliter la réalisation des objectifs. 12. L'organisation met en place les activités de contrôle par le biais de règles qui précisent les objectifs poursuivis, et de procédures qui mettent en œuvre ces règles.

Composantes	Principes
Information & communication	13. L'organisation obtient ou génère, et utilise, des informations pertinentes et fiables 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 matière d'objectifs et de responsabilités associés au contrôle interne. 15. L'organisation communique avec les tiers sur les points qui affectent le fonctionnement des autres composantes du contrôle interne.
Activités de pilotage	16. L'organisation sélectionne, développe et réalise des évaluations continues et/ou ponctuelles afin de vérifier si les composantes du contrôle interne sont mise en place et fonctionnent. 17. L'organisation évalue et communique les faiblesses de contrôle interne en temps voulu aux parties chargées de prendre des mesures correctives, notamment à la direction générale et au Conseil, selon le cas.

C. Programme du Colloque

Président de séance

Florence Vincent, *Directeur Audit Interne et Risk Management Groupe, Michelin*

8h30-9h00 **ACCUEIL**

9h00-9h15 **OUVERTURE**

Farid Aractingi, *Président, IFACI et Directeur Audit, Maîtrise des Risques et Organisation, Renault*

Serge Villepelet, *Président, PwC France*

9h15-10h30 **TABLE-RONDE (en anglais) : Contexte et objectifs de la mise à jour du référentiel**

Moderateur : **Margie Bastolla**, *IIA Research Foundation, Vice President*

Catherine Jourdan, *Directeur, PwC Risk Assurance & Advisory Services*

Marie-Hélène Laimay, *Senior Vice President Audit & Internal Control Assessment, Sanofi et Présidente, ECIIA*

Christopher Page, *Directeur de l'Audit Interne Groupe, Eurotunnel*

10h30-11h00 **PAUSE**

11h00-12h00 **TABLE-RONDE : Le middle management : relais indispensable dans un dispositif de contrôle interne efficient**

Moderateur : **Isabelle Dreyssé**, *Responsable du Contrôle Interne, Aéroports de Paris*

Alain Lemarcis, *Responsable du Contrôle Interne, SNCF*

Marie-Hélène Sinnassamy, *Directrice Contrôle Interne Risques Achats Immobilier Logistique, GDF SUEZ*

Grégory de Lagrange Chancel, *Responsable Risque Opérationnel, Société Générale*

12h00-13h00 TABLE-RONDE : Présentation du guide d'application au domaine comptable et financier

Moderateur : **Nicolas Brunetaud**, Associé, PwC Audit

Sandra Bues-Piquet, Directeur Contrôle interne, Veolia Environnement

Jean-Marie Pivard, Directeur d'Audit interne, Nexans

Alain Josserand, Responsable du Contrôle Interne Comptable de l'État, DGFIP, Ministère de l'Économie et des Finances

13h00-14h15 DÉJEUNER

14h15-15h30 Atelier A : Sous-traitance et contrôle interne : pour une plus grande maîtrise des dispositifs

Moderateur : **Anne-Christine Marie**, Associée, PwC Risk Assurance & Advisory Services

Yann Boucraut, Directeur Central Contrôle Interne et Audit, Bouygues

Jean-Denis Malpelet, Directeur d'Audit Interne, Allianz France

Atelier B : Transformation, gestion des risques et contrôle interne

Moderateur : **Annie Bressac**, Consultante

France Hanniet, Group Risk & Compliance Director, Orangina Schweppes

Alain Hocquet, Risk Manager Corporate, Orange

Arnaud Marrou, Responsable Adjoint de la Mission d'appui ministériel d'audit interne, Ministère de l'Écologie, du Développement Durable et de l'Énergie

15h30-16h00 PAUSE

16h00-16h30 DEBRIEFING DES ATELIERS : Présentation des travaux

Anne-Christine Marie, Associée, PwC Risk Assurance & Advisory Services

Annie Bressac, Consultante

16h30-17h15 TABLE-RONDE : Ce qu'engendre cette mise à jour pour les parties prenantes et les régulateurs

Moderateur : **Jean-Pierre Hottin**, Associé, PwC Risk Assurance & Advisory Services

Martine Charbonnier, Secrétaire Général Adjoint, Autorité des Marchés Financiers

Michel Behar, Administrateur ETI, membre de l'APIA, Responsable de la Région Ile-de-France

Témoignage d'un Directeur Financier

17h15-17h30 CLÔTURE : Optimisation du dispositif grâce à l'application des trois lignes de maîtrise

Farid Aractingi, Président, IFACI et Directeur Audit, Maîtrise des Risques et Organisation, Renault

D. Liens

www.coso.org/CI

pour accéder au référentiel (payant)

www.pwc.fr/accompagner_votre_service_audit_interne_a_chaque_etape_de_son_developpement.html

10 minutes : un résumé de l'essentiel sur le COSO 2013 pour les dirigeants

« Building agility and empowerment into internal control » sur la base du COSO 2013

www.ifaci.com/coso2013

pour accéder à la documentation du Colloque du 21 mai

