Contrôle interne et système d'information

2ème édition

Version validée
Version 2.2

Groupe de travail Contrôle Interne de l'AFAI :
Nicolas Bonnet
Laurent Gobbi
Jean-Florent Girault
Jean-Michel Mathieu
Vincent Manière
Gina Gulla-Menez
François Renault
Claude Salzman
Serge Yablonsky

Groupe de validation :
Pascal Antonini
Maryvone Cronnier
Renaud Guillemot
Michel Leger
Stéphane Lipski
Bertrand Maguet
Philippe Trouchaud

Paris, 6 juillet 2008
V 2.2

Sommaire

Table des illustrations

1 Executive Summary

Aux Etats-Unis la loi Sarbanes-Oxley et en France la loi sur la Sécurité Financière ont rendu obligatoire la mise en place de dispositifs de contrôle interne. Cette contrainte a eu un effet positif. L'expérience a montré que le renforcement des procédures a eu un certain coût mais, si cette démarche est bien managée, elle peut en rapporter encore plus. C'est un investissement rentable en rationalisation et en renforcement de l'efficacité de l'entreprise. L'allégement des structures est devenu un enjeu primordial. L'amélioration des processus les rend plus performantes. Il est pour cela nécessaire de disposer de procédures internes efficaces et de maîtriser les risques.

La mise en place de dispositif de contrôle interne repose en grande partie sur le contrôle de l'informatique. C'est un point de passage obligé. En effet, dans la plupart des grandes et des moyennes entreprises, la quasi-totalité des procédures repose aujourd'hui sur des traitements informatiques, des serveurs, des bases de données, …. La mise en place de différents dispositifs de contrôle interne efficaces se fait et se fera de plus en plus à l'aide de systèmes d'information conçus à cet effet. Toutes les applications informatiques existantes doivent en tenir compte et le cas échéant doivent être revues pour prendre en compte des règles de contrôle interne et pour, éventuellement, corriger d'éventuelles fragilités des dispositifs de contrôle interne en place.

La loi fait aujourd'hui obligation de mettre en place et de développer des dispositifs de contrôle interne. Ceci exige d'analyser et de perfectionner les principaux processus de l'entreprise et de mettre en place des dispositifs de contrôle interne. C'est le cœur de la démarche. Il est aussi nécessaire de renforcer le contrôle des données car l'expérience montre que c'est un domaine encore fragile qui nécessite des dispositifs de contrôle rigoureux.

Il est pour cela nécessaire de plonger dans les applications informatiques et des bases de données de façon à imaginer des solutions plus sûres, plus efficaces, plus productives,… C'est le rôle de l'audit informatique. C'est un des moyens les plus efficaces pour s'assurer que les bonnes pratiques en matière de système d'information sont effectivement appliquées. Cette démarche garantit que les contrôles et les sécurités nécessaires sont en place et donnent les résultats attendus.

Le développement du contrôle interne va donc se faire, en grande partie, grâce au renforcement les démarches de contrôle et d'audit informatique. Il faut s'y préparer et s'organiser en conséquence. Il est pour cela nécessaire de mettre en place un programme de renforcement des pratiques grâce à un plan d'action qui doit être planifié et mené dans la durée.

2 Préface

Le développement du contrôle interne est une nécessité. Si certains y voient encore la multiplication de contraintes sans contrepartie, la majorité considère désormais que la mise en œuvre d'un contrôle interne efficace est indissociable d'une bonne gouvernance des entreprises.

L'objet de ce document est de montrer l'importance, dans une démarche de revue du niveau de contrôle interne, d'évaluer le contrôle interne « embarqué» dans le système d'information et le rôle capital de l'audit informatique dans cette démarche.

Les processus opérationnels des entreprises étant pour la plupart informatisés, le système d'information est le support de nombreuses procédures de contrôle interne. Il est nécessaire de garantir que les contrôles nécessaires sont en place dans les applications et les systèmes, qu'ils sont efficaces et qu'ils le resteront dans le temps.

Le maintien d'un dispositif de contrôle interne efficace dans le temps ne peut être obtenu que par une bonne gouvernance des systèmes d'information, intégrant la maîtrise des risques et la conformité aux lois et règlements. Le référentiel CobiT, aujourd'hui dans sa quatrième version, apporte aux organisations et à leurs parties prenantes les notions et les outils leur permettant de gouverner efficacement leur système d'information et, de là, de contribuer à l'instauration d'un bon niveau de contrôle interne par l'informatique, en alliant performance et sécurité.

François Renault
Président de l'AFAI

3 Introduction

On assiste depuis quelques années au renforcement de la notion de contrôle interne. Elle s'est rapidement imposée à la suite de divers incidents qui ont fait apparaître des fragilités croissantes dans les processus de reporting financier des grandes entreprises elles-mêmes dues en grande partie à des fragilités organisationnelles. L'exigence de contrôle interne s'est renforcée à la suite de la sur-communication de ces insuffisances. Les dirigeants d'entreprises sont d'autant plus sensibles à ces recommandations que depuis plusieurs années les législateurs s'efforcent d'imposer aux entreprises une plus grande transparence.

Simultanément, on constate le développement accéléré des systèmes d'information poussés par les progrès rapides des technologies informatiques. Ils sont devenus l'ossature des entreprises. La plupart des opérations effectuées se font à l'aide des outils informatiques disponibles. Les applications de gestion, en particulier les ERP, structurent profondément la manière de travailler et déterminent la manière dont se font les échanges avec les différents partenaires. Elles contribuent à la structuration des processus de l'entreprise.

On a ainsi progressivement pris conscience de l'importance de leur rôle dans le fonctionnement de l'entreprise. Traditionnellement les opérations étaient analysées par fonction : les comptables, les gestionnaires du personnel, les acheteurs, le planning de production, les méthodes, … Progressivement les processus ont structuré les opérations de façon à les enchaîner de manière transverse. C'est une mutation majeure dans l'approche classique des organisations. Au lieu de structurer les opérations par les fonctions, elles sont organisées par processus. Cela permet d'avoir une vision d'ensemble des activités de l'entreprise.

Pour cela il est nécessaire de suivre le flux des données d'un bout à l'autre de l'entreprise et mettre en place des contrôles d'étape en étape. Il est aussi possible de contrôler les bases de données qui stockent ces informations. C'est le cœur de la démarche de contrôle interne des systèmes d'information.

Son but est de s'assurer que tout se passe bien. C'est aussi le rôle de l'audit informatique. Les démarches à mettre en œuvre sont très voisines. Les entreprises doivent mettre en place des procédures adaptées. Elles interviennent de trois manières différentes :

- L'informatique est un élément clé de la gouvernance de l'entreprise. Pour améliorer son efficacité, on doit s'efforcer de renforcer la maîtrise de l'informatique.

- Les contrôles propres à l'informatique, y compris les procédures de sécurité, permettent d'améliorer la qualité et l'efficacité des différentes activités de l'entreprise.

- On insère de plus en plus souvent des contrôles «embarqués» dans la plupart des traitements informatisés. Ces contrôles permettent de mieux maîtriser les opérations gérées par l'entreprise et donc d'améliorer son efficacité.

Face à ces préoccupations, le cadre législatif a évolué : LSF (Loi sur la Sécurité Financière), SOX (Sarbanes-Oxley Act), J-SOX (SOX japonais). On assiste au développement de démarches sur la base de cadres de référence, comme celui de l'AMF (Autorité des Marchés Financiers) ou celui du COSO, Committee of Sponsoring Organizations of the Treadway Commission (1). Pour l'informatique, on utilise le CobiT, Control Objectives for Information and related Technology (2).

Pour répondre à ces attentes nous allons examiner les points suivants :

Chapitre 4. Les contrôles internes en environnement informatisé.
Chapitre 5. Les processus au cœur de ces démarches.
Chapitre 6. Un exemple de processus clients.
Chapitre 7. La maîtrise des données .
Chapitre 8. Les stratégies de mise en œuvre du contrôle interne en milieu informatisé.
Chapitre 9. L'audit informatique, outil privilégié du contrôle interne.
Chapitre 10. L'importance des contrôles continus.
Chapitre 11. Le cas d'une mission d'audit d'un processus.
Chapitre 12. Un guide opérationnel, qui propose un certain nombre de recommandations.

Ce rapport est complété par trois annexes :

1. Application du cadre de l'AMF aux systèmes d'information.
2. Le COSO appliqué aux systèmes d'information. Il est important de comprendre les concepts sous-jacents à la première et à la deuxième version de ce document de référence.
3. Une bibliographie sur le sujet.

1 - Voir annexe 2.
2 - CobiT : Gouvernance, Contrôle et Audit de l'Information et des technologies associées – ITGI (IT Gouvernance Institute) – édition française AFAI. CobiT est le référentiel d'audit informatique le plus largement reconnu.

4 Le contrôle interne en environnement informatisé : le rôle du cadre de l'AMF

Le cadre de référence de l'AMF définit le contrôle interne par ses objectifs :

- veiller à « la conformité aux lois et règlements »,
- assurer « l'application des instructions et des orientations fixées par la Direction générale ou le Directoire » de l'entreprise,
- maintenir « le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde de ses actifs »,
- garantir « la fiabilité des informations financières ».

Le contrôle interne comprend cinq composantes :

- une organisation, s'appuyant sur des systèmes d'information appropriés,
- une diffusion efficace de l'information pertinente,
- un dispositif d'identification, de suivi et de gestion des risques,
- des activités de contrôle proportionnées aux enjeux,
- une surveillance permanente du dispositif de contrôle interne.

Le fait que l'entreprise soit informatisée ou non n'a pas d'influence sur la définition du contrôle interne. Cependant, cela a un impact fort sur certaines de ces composantes. (Voir l'analyse détaillée dans l'annexe 1 "Application du cadre de l'AMF aux systèmes d'information").

Aujourd'hui, les systèmes informatiques sont un des éléments clés des processus des organisations. Ils constituent la base des activités de contrôle. C'est la quatrième composante du contrôle interne.

Ces contrôles peuvent être :

- manuels,
- automatisés,
- manuels à partir d'états produits par des systèmes informatiques.

En ce qui concerne les contrôles automatisés, ils sont codés dans des applications qui retranscrivent les logiques métiers. Il est donc indispensable, pour que le contrôle interne soit efficace, de vérifier que :

- les contrôles automatisés sont pertinents, adaptés, correctement implémentés et pérennes,
- seules les versions valides des applications sont mises en production,
- les contrôles automatisés ne peuvent pas être contournés au moyen d'utilitaires, que ce soit au niveau des bases de données, du middleware, du système d'exploitation ou du réseau.

En ce qui concerne les contrôles manuels réalisés à partir d'états issus de systèmes informatiques, ils ne seront efficaces que si ces états sont fiables. On en revient donc à des préoccupations voisines de celles relatives aux contrôles automatisés :

- L'origine de l'information est-elle pertinente ?
- Les applications produisant les états sont-elles valides ?
- Les données peuvent-elles être altérées avant leur impression ou leur affichage ?

D'où l'importance du rôle des systèmes d'information dans le dispositif de contrôle interne, soulignée par les auteurs du cadre de référence dans la description de la première composante du contrôle interne, l'organisation.

Les objectifs relatifs aux systèmes d'information sont les suivants : ils doivent être conçus et mis en œuvre dans le but de traiter et délivrer en temps voulu, en toute circonstance, une information fiable et adaptée aux besoins de l'organisation. Ils doivent assurer la protection des informations contre l'altération et la divulgation à des tiers non autorisés. Ils doivent également permettre de reconstituer les opérations effectuées. L'évolution de ces systèmes doit être maîtrisée et conforme aux objectifs de l'organisation.

L'usage de systèmes informatisés impose le respect de lois spécifiques et introduit de nouveaux risques, qu'il faut identifier et traiter. Nous citerons, par exemple, les risques suivants :

- l'excès de confiance dans des systèmes ou des applications traitant incorrectement les données, ou traitant des données incorrectes, ou les deux à la fois ;
- l'accès non autorisé à des données, pouvant entraîner l'altération ou la destruction d'information, l'enregistrement de transactions frauduleuses ou le passage d'écritures comptables erronées ;
- les droits d'accès accordés au personnel informatique aux systèmes pouvant entraîner une violation du principe de séparation des fonctions ou du principe de besoin d'en connaître ;
- la modification non autorisée de données de référence ;
- la modification non autorisée de programmes ou de paramètres ;
- l'incapacité à apporter les modifications requises dans les systèmes et les programmes ;
- les interventions manuelles intempestives dans les systèmes ;
- la perte de données ou l'incapacité à accéder aux données lorsque c'est nécessaire.

L'environnement de contrôle interne de l'organisation doit intégrer l'informatique. Trop souvent on considère l'informatique comme une activité séparée des métiers et son environnement de contrôle est déconnecté de celui de l'organisation. Or, on l'a vu, l'informatique peut introduire de nouveaux risques, qui exigent des contrôles compensatoires nouveaux ou améliorés. L'attribution de la responsabilité des contrôles est parfois peu claire entre l'informatique et les métiers.

Enfin, il est de plus en plus fréquent que des processus informatisés ou des composants informatiques soient externalisés. Dans ce cas, l'organisation garde la responsabilité du contrôle interne des activités externalisées et doit prendre des mesures visant à garantir le maintien du niveau de contrôle interne de bout en bout, y compris chez les tiers.

5 Les processus au cœur de ces démarches

La mise en place d'un contrôle interne efficace passe par la compréhension détaillée, de bout en bout, des activités de l'entreprise. A cette fin, la représentation des processus s'impose comme un outil performant. La cartographie des processus distingue ceux qui:

- concernent l'activité principale de l'entreprise,
- assurent un rôle de support,
- remplissent un rôle de pilotage.

Dans une entreprise il faut vendre, acheter, produire,….et aussi tenir la comptabilité et gérer les ressources humaines. Il existe différentes manières de représenter et de modéliser une entreprise et ses processus. La figure 1 ci-dessous n'en est qu'une illustration générale. Chaque entreprise étant différente, la cartographie de ses processus lui est spécifique.

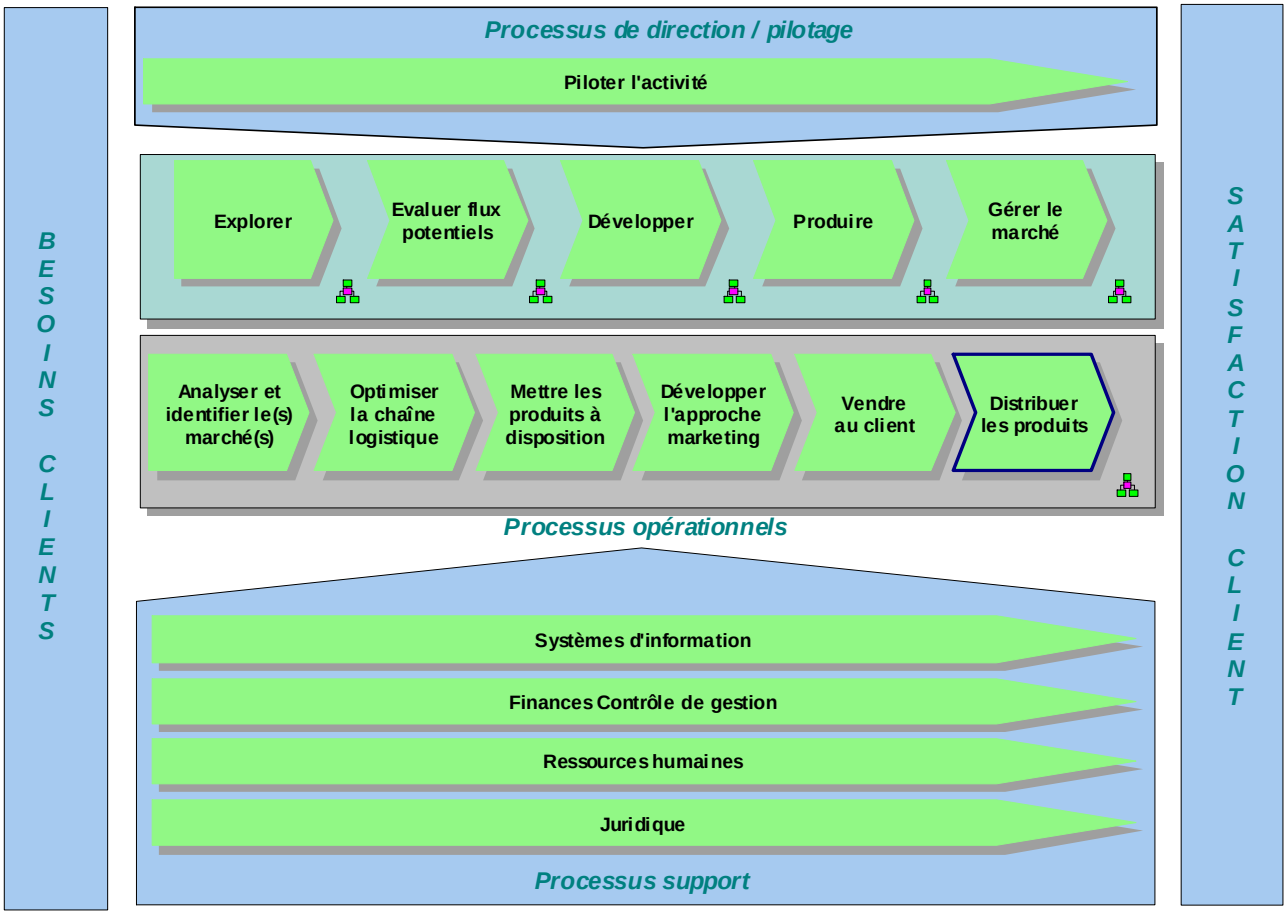

Figure 1 – Exemple de cartographie des processus de l'entreprise

Dans une logique de marché on peut, comme l'illustre cet exemple, regrouper les processus en trois grandes familles :

1. **Les processus opérationnels** vont de la conception à la réalisation des produits et des services que l'entreprise fournit à ses clients. Ceux-ci comprennent par exemple les achats, la production, la logistique, la vente et le support après-vente. Le bon fonctionnement de ces processus conditionne l'excellence opérationnelle de la société et exige une vigilance toute particulière en matière de contrôle interne.

2. **Les processus support** regroupent toutes les fonctions de soutien à la mise en œuvre et à l'exploitation des processus liés aux produits et services de l'entreprise ainsi que ceux destinés au bon fonctionnement de celle-ci. Ce sont notamment la gestion des ressources humaines, la gestion financière, la gestion des connaissances, l'informatique, le juridique….

3. **Les processus de direction et de pilotage** où vont être concentrées toutes les responsabilités et les autorités relevant de la direction, en particulier tous les aspects liés à la stratégie de développement de l'entreprise et son déploiement opérationnel, à la stratégie produit-service ainsi qu'à la mise à disposition de toutes les ressources nécessaires, et au pilotage de l'ensemble sous les angles financiers, humains, technologiques, industriels, commerciaux et qualité, ainsi, bien sûr que de contrôle. Ce sont par exemple : la définition des orientations stratégiques, la culture et l'éthique, les délégations de pouvoirs, les contrôles et les évaluations,….

Ces différents processus interagissent en permanence selon des cycles très variables, rythmés par différents évènements, que ce soit la décision d'investissement dans une nouvelle gamme de produits et de prestations, la mise à disposition d'un produit, ou encore la fin d'un exercice fiscal, etc. Certains de ces processus s'exercent en continu et sont liés à des activités récurrentes, d'autres sont momentanés, liés à une action ponctuelle ou relèvent de la conduite de projet.

Maîtriser un processus, c'est d'abord le documenter en tenant compte de sa complexité. Il faut pour cela procéder en trois étapes :

1. **Le schéma global des processus** permet d'avoir une vision d'ensemble de l'activité et du fonctionnement de l'entreprise. Cette approche est la même que pour une démarche qualité, un schéma directeur informatique, une cartographie des risques…

2. **La représentation détaillée de chacun des processus** met en évidence l'enchaînement des activités et les principaux flux d'informations.

3. **L'analyse détaillée des processus** documente les tâches manuelles et automatisées et précise leurs enchaînements sous

forme de diagrammes. Cet exercice de différenciation des tâches informatisées et manuelles fait apparaître pour de nombreux processus de l'entreprise que le système d'information en constitue en fait la colonne vertébrale. D'où l'importance majeure accordée au système d'information en matière de contrôle interne.

Cette représentation permet :

- de déterminer les points de contrôle : type, localisation,
- de mesurer l'efficacité du contrôle.

La forme la plus aboutie de contrôle interne devrait permettre en définitive d'évaluer :

- les performances internes du processus : le processus s'exécute bien et de façon répétable et efficace sous le contrôle de la direction de l'entreprise ;
- les performances externes du processus : le processus fournit un niveau de performance cohérent avec celui des autres processus pour atteindre des objectifs généraux de l'entreprise.

Ainsi les processus deviennent le langage commun de tous les acteurs qui pratiquent le pilotage, l'organisation, la conception des systèmes d'information ou l'audit dans l'entreprise.

C'est par ce langage commun que peut être mis en place un dialogue d'amélioration permanente au sein de l'entreprise. Il lui garantit la pérennisation de ces processus mais aussi de rester **agile** pour adapter en permanence son organisation à l'évolution de son environnement et des besoins de ses clients. A cet égard, le contrôle interne est un outil essentiel à la détection le plus en amont possible des besoins d'évolutions des processus.

6 Exemple pratique d'un processus

Pour bien comprendre l'importance des processus dans la démarche de contrôle interne, prenons par exemple la représentation simplifiée d'un processus commercial, couvrant les tâches allant de la prospection des clients au paiement des factures.

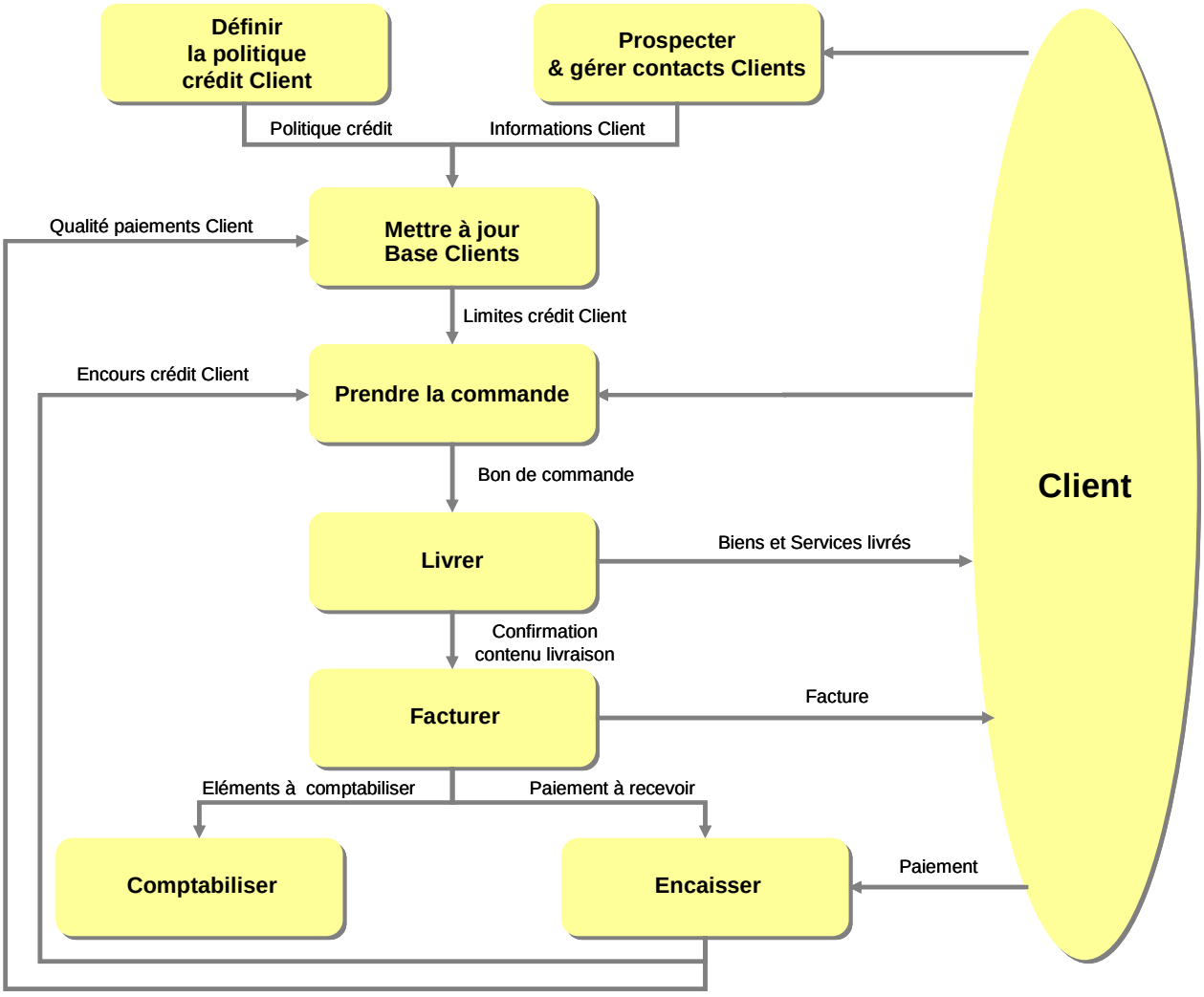

Figure 2 - Description du processus clients

Ce schéma résume les 3 grandes étapes du processus :

- La prospection et l'enrichissement de la base Clients :
  - par la création de nouveaux clients ou prospects,
  - par la mise à jour de la politique de crédit pour chaque prospect ou client, en fonction de la situation financière de sa

Société, mais aussi d'éventuels incidents constatés sur ses paiements ;

- La prise de commande (tenant compte des limites de crédit du client et des encours de paiement à recevoir) et la livraison ;

- Le suivi administratif de la vente qui se traduit par :
  - l'édition de la facture,
  - la comptabilisation du chiffre d'affaires correspondant en comptabilité clients,
  - le suivi du paiement effectif, et la détection des retards ou incidents de paiement.

Chaque activité de ce processus peut être elle-même décomposée en tâches élémentaires, affectées aux différents acteurs ou services de l'entreprise, de façon à définir une procédure de travail.

Par exemple, les tâches du Service d'administration des ventes, concernant l'activité « Prendre la commande », peuvent être développées selon le schéma ci-dessous.

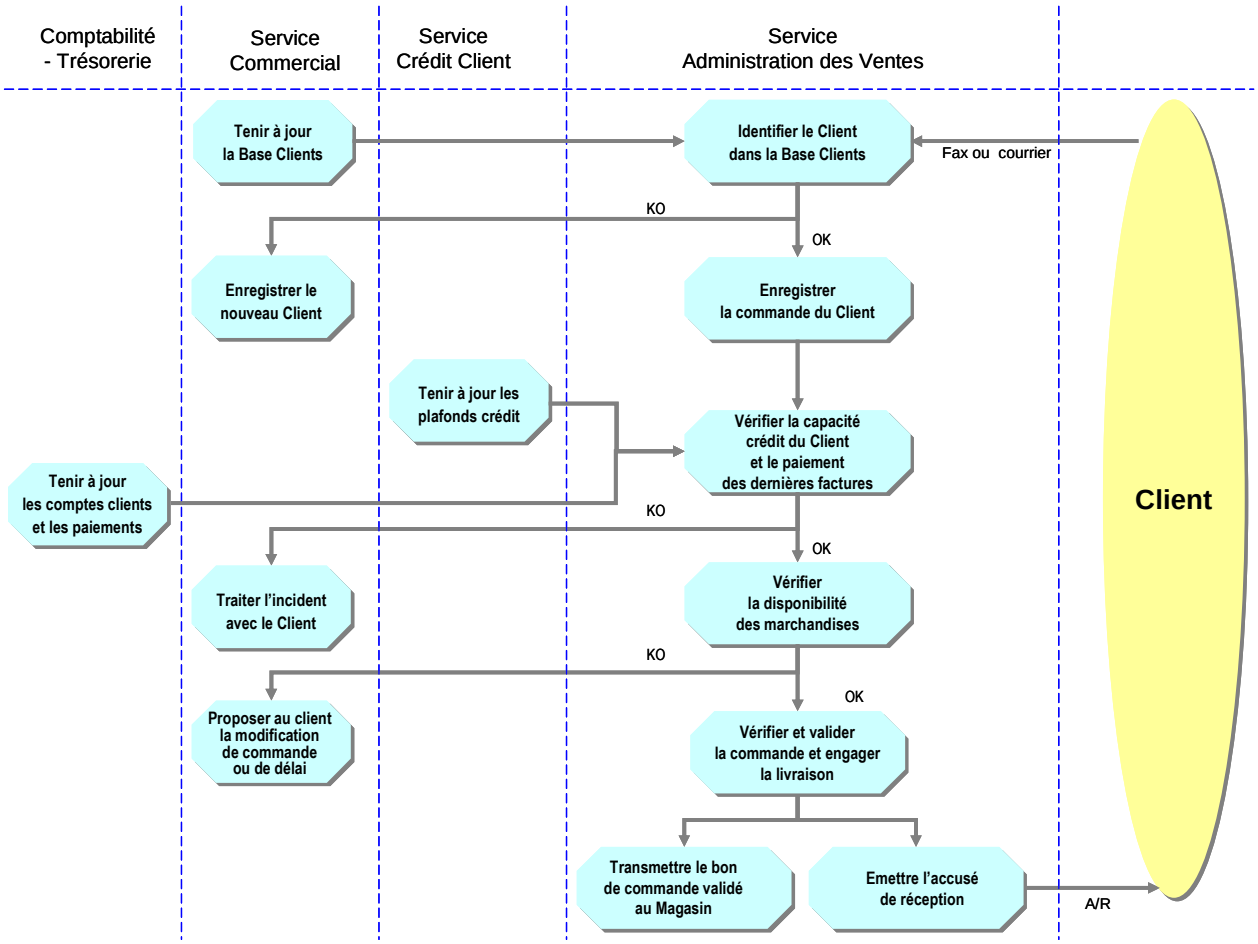

Figure 3 - Description de l'activité "Prendre la commande"

Pour maîtriser les risques qui leur sont attachés, la mise en œuvre de ces tâches s'accompagne de règles de gestion et de contrôles tels que :

- n'accepter que les commandes complètes et autorisées par les personnes habilitées,
- vérifier que l'ensemble des commandes et des annulations de commandes est enregistré de manière correcte,
- rejeter les commandes de tout client en défaut de paiement,
- traiter les commandes uniquement dans les limites de crédit autorisées.

De la même façon, concernant les autres activités, des règles de gestion et des contrôles appropriés devront être mis en place :

- l'activité « Mettre à jour la Base Clients » comprend :
  - vérification et justification de toute information créée ou modifiée dans la base clients,
  - accès autorisés et limités à la base clients,
  - approbation des limites de crédit,
  - contrôle et validation des conditions de paiement,
  - vérification de l'unicité du client et du compte client.

- l'activité « Livrer » comprend :
  - rapprochement du bon de commande avec les marchandises ou les prestations livrées (quantité & qualité),
  - validation par le client de la complétude de la commande livrée,
  - contrôle de l'exhaustivité des bons de livraison retournés.

- les activités « Facturer » et « Comptabiliser » comprend :
  - conformité de la facture par rapport aux conditions des bons de commande et des contrats (conditions générales de vente, prix, conditions de paiement,…),
  - justification des factures (bon de commande, bon de livraison),
  - contrôle de l'exhaustivité de la facturation,
  - enregistrement correct des factures et avoirs dans la période comptable appropriée,
  - validation et justification des avoirs émis,
  - rapprochement des comptes auxiliaires et des comptes généraux,
  - validation du calcul et de l'enregistrement des taxes (TVA).

- l'activité « Encaisser » comprend :
  - affectation correcte du règlement client au compte client associé et suivi des règlements non affectés,
  - contrôle du bordereau de remise de chèques,
  - analyse des impayés,
  - contrôle des écarts de règlement,
  - suivi des acomptes reçus,
  - enquête financière pour les clients à risque,
  - contrôle de la sortie des clients douteux du compte 411,
  - contrôle du calcul de la provision pour clients douteux,
  - justification des passages en pertes sur créances irrécouvrables,
  - suivi des dossiers contentieux.

7 La maîtrise des données

La traçabilité et la fiabilité des informations produites sont deux éléments clés du concept de transparence financière, tel qu'il est développé par les nouvelles règlementations relatives à l'élaboration et à la production de l'information financière (notamment le Sarbanes Oxley Act aux Etats-Unis, la Loi sur la Sécurité Financière en France).

Pour répondre à ces exigences, il est nécessaire de maîtriser les quatre points suivants :

- Identifier les flux de données,
- Contrôler ces données,
- Obtenir une cartographie des bases de données,
- Vérifier l'existence de chemins de révision.

Ces exigences structurent les applications et déterminent leurs caractéristiques essentielles.

7.1 Identifier les flux de données

Pour déterminer les contrôles à mettre en place, il est nécessaire d'avoir une vue globale de la circulation des données tout au long de la chaîne des traitements, allant de la saisie initiale des données jusqu'à leur archivage final, en passant par leurs modifications et leurs mises à jour, leurs stockages, leurs éditions, ….

Cette vue globale découle, en grande partie, d'une analyse des processus ; mais celle-ci, au lieu de s'attacher à détailler les traitements, se concentre sur les données. Elle a pour objectif d'identifier l'ensemble des bases de données mises en œuvre, et les opérations qui sont faites pour transférer les données d'une base à l'autre.

Prenons pour illustration le cas d'une application commerciale. Comme le montre la Figure 4 ci-dessous, on commence par saisir les commandes des clients, et on constitue une première base de données comprenant les bons de commande. Après contrôle des informations saisies par rapport à la base produits, un premier traitement permet de créer les bons de livraison. Une fois le client livré, un second traitement établit les factures, qui sont ensuite déversées dans la comptabilité clients. Une fois qu'elles sont soldées, ces écritures sont archivées à fin de contrôle.

Comme on le voit, cette circulation des données n'est pas simplement un déversement des données d'une base dans l'autre mais un enchaînement de contrôles, de traitements et d'agrégations de données.

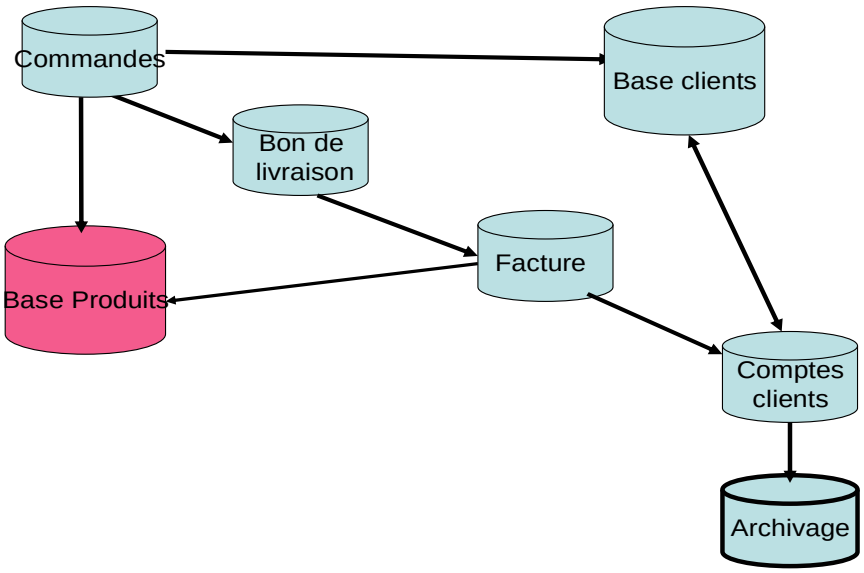

Figure 4 - Diagramme de flux d'une facturation

7.2 Contrôler ces données

L'ensemble des données doit être contrôlé tout au long de cette circulation. Le niveau des contrôles est déterminé en fonction des niveaux des risques estimés. Il faut prévoir suffisamment de contrôles sans pour autant verser dans une prolifération excessive. Par exemple, dans le cas d'une base de données clients, il faut avant tout veiller à ne pas avoir de doublon et évacuer le plus vite les clients inactifs depuis plusieurs années. Par contre, il ne sert à rien de vérifier les numéros de téléphone ou de télécopie.

Les données sont normalement contrôlées au moment de la saisie. Le but est de détecter des anomalies comme des codes erronés, des totaux inexacts, des oublis significatifs, … Les concepteurs veillent à mettre tous ces contrôles en début de traitement de façon à ne pas avoir ultérieurement de rejets. Par exemple, dans le cas d'une facturation, il ne faut pas rejeter une commande au moment de l'édition. Les contrôles doivent avoir été faits précédemment.

Mais ce n'est pas suffisant. Il est ensuite nécessaire d'effectuer des contrôles lors des différents traitements pour s'assurer que les opérations se déroulent normalement. Dans le cas d'une application commerciale, on va, par exemple, s'assurer que :

- toutes les commandes saisies ont donné lieu à l'émission d'un bon de livraison,

- toutes les livraisons faites se sont traduites par le transfert de ces données vers la facturation,
- toutes les factures sont justifiées par un ou plusieurs bons de commandes,
- toutes les factures émises sont déversées en comptabilité clients,
- toutes les écritures soldées ayant plus de X mois d'ancienneté sont archivées,
- …

De même, les principales bases de données, comme les bases clients et produits, doivent être périodiquement contrôlées pour s'assurer que :

- tous les clients et tous les produits existent : dans le cas des clients y a-t-il une circularisation ? Est-elle suffisante ? Dans le cas des produits existe-t-il des doublons, des erreurs de codification ou de localisation ?
- toutes les mises à jour faites sur ces bases sont tracées : ceci concerne les données saisies, mais aussi les transferts de données, les mises à jour des bases au cours des traitements,…
- les bases de données sont exhaustives : il faut être capable de détecter des disparitions accidentelles ou volontaires de données.
- l'intégrité des données stockées a été protégée, et par exemple certains cumuls n'ont pas pu être faussés à la suite de fausses manœuvres,
- le chaînage des informations entre différentes bases est complet et fonctionne correctement,
- ….

L'expérience montre ici encore que les contrôles actuels ne sont pas suffisants et qu'il est nécessaire de les renforcer.

7.3 Obtenir une cartographie des bases de données

Pour expliquer et analyser les incohérences potentielles, il est nécessaire de disposer d'un document identifiant les principales bases de données de l'entreprise et les relations qu'elles ont entre elles. Il ne s'agit pas du modèle de données logique mais bien du modèle physique.

Ce schéma doit faire apparaître un certain nombre d'informations fondamentales pour maîtriser le système :

- la localisation des données : serveur ou système disque où les données sont stockées,
- le volume de la base : nombre d'occurrences, taille théorique, taille réelle,…
- le type de sauvegarde des bases et la périodicité des sauvegardes,
- l'éventuelle recopie des données des bases sur le système disque,
- la journalisation des mises à jour, en indiquant leur lieu de stockage,
- la duplication ou la synchronisation des données,
- …

Le but de la cartographie est de faciliter la connaissance opérationnelle et la localisation des bases de données et de s'assurer que les sauvegardes sont suffisantes compte tenu du niveau de risque.

7.4 Vérifier l'existence de chemins de révision

L'objectif est de retrouver une information ou une donnée à partir d'une autre, issue d'une application informatique logiquement et physiquement éloignée. Il est ainsi possible, par exemple, de remonter d'un compte du bilan au détail des comptes puis aux écritures et, le cas échéant, aux pièces justificatives.

Il faut pour cela mémoriser le parcours suivi par une information. C'est ce que permet le « chemin de révision » aussi appelé « piste d'audit » ou « audit trail ».

Ce parcours doit être enregistré à l'aide de pointeurs ou d'index. Il peut aussi être inscrit sur la « carte d'identité » de la donnée. Il est aussi possible de stocker ces données dans un datawarehouse ou entrepôt de données. Pour retrouver les données, il est nécessaire de disposer de logiciels permettant de remonter des cumuls vers les détails justificatifs.

Le défaut de chemins de révision doit être considéré comme une fragilité certaine des procédures de contrôle interne.

En conclusion, la maîtrise des données est un point fondamental de la démarche de contrôle interne. Elle impose de prévoir des dispositifs adaptés, notamment la gestion des flux de données, leur contrôle, l'établissement de la cartographie des bases de données et l'existence de chemins de révision.

8 Stratégie de mise en œuvre du contrôle interne en milieu informatisé

Pour effectuer la mise en place de leur système de contrôle interne, la plupart des entreprises ont recours au référentiel COSO (voir en annexe 2) et notamment pour assurer :

- La définition de l'environnement de contrôle,
- L'évaluation des risques,
- La définition des activités de contrôle,
- L'information et la communication,
- La supervision des contrôles.

Ce référentiel ne traite pas spécifiquement les Systèmes d'Information ce qui a conduit l'ISACA et l'ITGI à proposer de localiser le contrôle interne du système d'information comme présenté sur le schéma suivant en mettant au cœur de l'entreprise les processus métier.

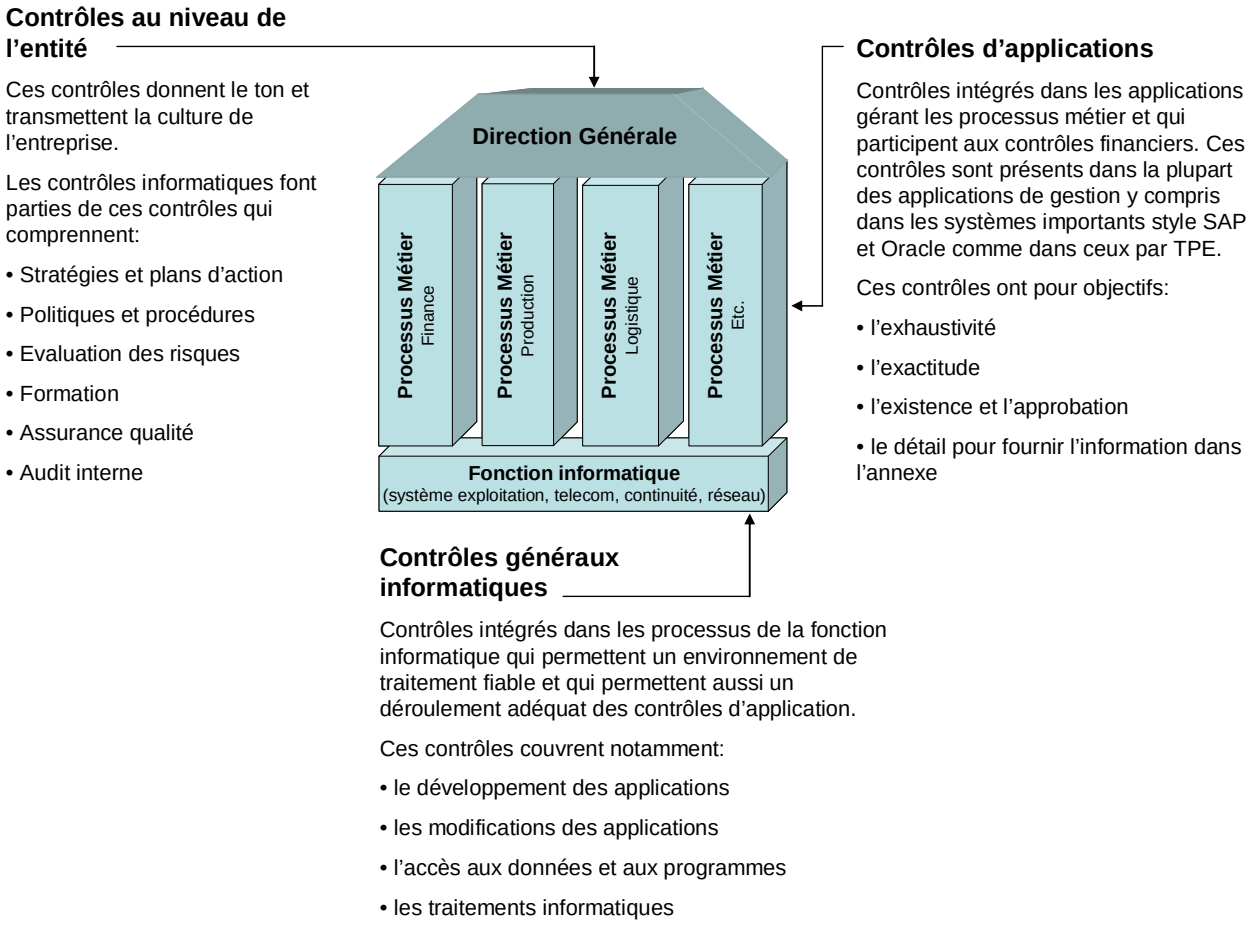

Figure 5 - Familles de contrôle du Système d'Information

Les trois familles de contrôle sont donc :

- les contrôles au niveau de l'entité,
- les contrôles généraux informatiques,
- les contrôles applicatifs qui sont partie prenante du contrôle interne des processus métier.

A partir de l'analyse des principaux processus il est donc possible :

- d'identifier le flux d'opérations traitées et les principales bases de données concernées,
- de décider des contrôles à mettre en place pour s'assurer que les traitements se font conformément aux objectifs du contrôle interne,
- de vérifier ensuite que les contrôles souhaitables ont été mis en place et qu'ils fonctionnent correctement, ce qui constitue la mission de l'auditeur.

De tels contrôles existent depuis plusieurs décennies. Il apparaît aujourd'hui qu'il est nécessaire de les renforcer. Ceci est dû à la conjonction de plusieurs facteurs :

- la taille des entreprises et le degré de décentralisation de l'entreprise. Il y a une vingtaine d'années, seules quelques très grandes entreprises de taille mondiale dépassant le milliard d'euros de chiffre d'affaires, toutes américaines, avaient des politiques de contrôle interne. Aujourd'hui, des centaines, voire des milliers sont concernées partout dans le monde. Il est vital de savoir ce qui se passe réellement dans les très nombreuses entités qui composent ces entreprises, dont les métiers sont souvent très hétérogènes.

- l'internationalisation des activités. La part de l'activité domestique de ces entreprises va en décroissant, et il faut aujourd'hui mettre sous contrôle des filiales présentes sur les cinq continents, afin de maîtriser leur gestion et leurs résultats, mais aussi de s'assurer qu'elles respectent toutes les règles de contrôle interne du groupe.

- le développement des systèmes d'information. L'informatique est aujourd'hui au cœur de la plupart des processus de l'entreprise, les ordinateurs de l'entreprise travaillent en liaison directe avec ceux de ses clients et de ses fournisseurs. Il est fondamental de réguler et de coordonner l'ensemble de ces systèmes.

Il est donc nécessaire de mettre en place un certain nombre de contrôles permettant de maîtriser l'ensemble des processus. Pour les structurer, plusieurs types d'approches sont possibles. Un modèle simple consiste à faire apparaître quatre niveaux de contrôle :

- **Les contrôles opérationnels :** c'est le premier niveau de contrôle. Ils sont mis en œuvre par les équipes opérationnelles. Ils permettent de repérer les erreurs et de limiter les fraudes. Ce sont pour l'essentiel des contrôles applicatifs dont le but est de s'assurer que des données erronées ne se sont pas glissées dans celles qui ont été saisies et que les traitements effectués sont conformes à ce

qui était prévu. Les contrôles possibles sont très variés. Ils peuvent être globaux ou analytiques, manuels ou informatiques, ….

- **Les contrôles d'ensemble.** Le deuxième niveau est assuré par les responsables encadrant les opérationnels, dont la mission est double : s'assurer que tout se passe bien et que les flux sont sous contrôle, détecter les situations anormales et prendre les mesures nécessaires pour les corriger.

- **La détection des situations anormales.** C'est le troisième niveau. Il fait appel à différentes fonctions de contrôle spécialisées comme la gestion de la sécurité, le contrôle de gestion, la gestion de la qualité,… Toutes ces fonctions ont à la fois une mission technique spécialisée, comme d'améliorer la qualité ou le niveau de la sécurité, et une mission de surveillance générale du fonctionnement des principaux processus.

- **L'audit.** Enfin, le niveau de contrôle ultime est assuré par l'audit, interne ou externe. A ce niveau, l'audit informatique, et notamment l'audit des applications, est le moyen le plus efficace pour maîtriser les principaux processus de l'entreprise.

Comme on le voit, il existe une hiérarchie des lignes de défense. A la base il y a les contrôles opérationnels assurés par les personnes chargées des opérations courantes et au sommet de l'édifice il y a les audits et notamment les audits informatiques.

L'ensemble de ce dispositif repose, en grande partie, sur l'engagement du management qui est chargé de mettre en place des outils de contrôle nécessaires et de s'assurer de leur utilisation correcte : une faiblesse ou une défaillance de l'encadrement peut avoir des conséquences importantes.

9 L'audit informatique outil privilégié du contrôle interne

L’audit informatique constitue dans ces conditions un pilier du contrôle interne. La maîtrise des processus de l’entreprise et la maîtrise du système d’information deviennent imbriquées et relèvent d’une même approche du contrôle interne.

Nous analyserons d’abord ici les synergies entre l’audit informatique et les autres démarches contribuant au contrôle interne. Puis nous examinerons de façon plus approfondie les apports des trois domaines couverts par l’audit informatique : la stratégie informatique, la fonction informatique et les processus informatisés.

9.1 Les démarches de contrôle et de supervision au sein de l'entreprise

Les démarches mises en œuvre en matière de contrôle interne sont :

- **l'audit comptable** : son objectif est de garantir la sincérité des comptes ; les missions d’audit comptable sont souvent effectuées par le service d'audit interne, par les commissaires aux comptes ou, le cas échéant, par les autorités de tutelle ;

- **l'audit interne** : ses missions, allant de l'inspection à l'audit de gestion en passant par l'audit opérationnel, ont pour but de permettre aux directions générales d'avoir l'assurance d'un niveau de sécurité adapté à chacun de ses processus ;

- **la gestion des risques** : elle permet d’évaluer périodiquement le niveau des risques opérationnels et des risques bilanciels des entreprises ;

- **la sécurité des systèmes d'information** : elle a pour but de s'assurer que les dispositifs de sécurité organisationnels, matériels et logiciels fonctionnent correctement ;

- **l’audit informatique** a pour but d'évaluer l'efficacité des activités telle que l'exploitation, les études, la gestion de projets,…

- **l'audit du système d'information** permet de s'assurer que les ressources informatiques consommées contribuent à l'efficacité de l'entreprise.

- **l'audit qualité** : il vérifie que les dispositifs d'assurance qualité sont opérationnels, efficaces et permettent de garantir un niveau de qualité satisfaisant.

Chacune de ces approches a naturellement tendance à privilégier ses méthodes et ses points de contrôle.

Mais pour en tirer la pleine valeur ajoutée, et mieux répondre aux attentes imposées par le nouveau cadre légal, il est nécessaire d'assurer leur cohérence et leur complémentarité, notamment par une meilleure utilisation de l'audit informatique au service des autres démarches de contrôle interne. Il s'agit d'organiser la coopération entre les métiers et les compétences connexes mais bien distincts, liés au contrôle interne et à l'audit informatique.

Plus précisément, à l'observation des missions d'audit informatique, il est possible de les segmenter en trois grands domaines :

- **Stratégie informatique de l'entreprise** : les missions d'audit de ce type ont pour but de s'assurer de **la pertinence du système d'information**, de son adéquation aux objectifs de l'entreprise, et de son alignement sur ses stratégies globales ;

- **Fonction informatique de l'entreprise** : ces audits portent sur **la qualité des processus informatiques**, c'est-à-dire des processus mis en œuvre par la fonction informatique elle-même ;

- **Processus informatisés de l'entreprise** : ce dernier domaine couvre les audits portant sur **l'efficacité des contrôles intégrés dans les applications, et la sûreté du fonctionnement** quotidien de l'informatique.

La Figure 6 montre les principaux apports potentiels de chacun de ces domaines de l'audit informatique aux cinq autres démarches de contrôle interne rappelées ci-dessus.

		Champs de l'audit informatique		
		Stratégie informatique	Fonction informatique	Processus informatisés
Autres démarches de contrôle interne	Audit comptable	X		X
	Audit interne	X	X	X
	Analyse des risques	X	X	X
	Audit de sécurité		X	X
	Audit Qualité		X	X

Figure 6 - Relations de l'audit informatique au contrôle interne

Ainsi, à travers ses trois domaines d'intervention, l'audit informatique joue

un rôle majeur au service du contrôle interne.

9.2 Les trois domaines de l'audit informatique et leur apport au contrôle interne

Il est possible de préciser ce rôle et ces apports de l'audit informatique au contrôle interne, en approfondissant les objectifs et les caractéristiques de chacun de ces trois domaines d'intervention : stratégie informatique, fonction informatique et processus informatisés.

Audit de la stratégie informatique

L'objectif de ce type d'audit est de s'assurer que le système d'information est en ligne avec la stratégie de l'entreprise, avec ses enjeux et ses risques spécifiques. Il ne suffit pas d'avoir des processus maîtrisés et conformes aux règles de l'art pour produire le système d'information pertinent. Force est de constater que ce résultat est fortement lié à l'organisation de l'entreprise, à sa culture et à la maturité de la fonction informatique.

Aussi l'audit informatique, dans son acception la plus complète, doit-il analyser la **pertinence du système d'information** lui-même, c'est-à-dire l'efficacité de l'appui qu'il fournit aux différents processus de l'entreprise, et la pertinence des efforts et des investissements consentis pour le faire évoluer et l'adapter aux besoins nouveaux ou futurs.

Le référentiel ValIT (3) fournit un cadre très utile, pour analyser la qualité des processus de décision et de suivi des investissements liés aux projets de systèmes d'information. Il définit en effet 40 « bonnes pratiques » liées aux trois grands processus de gouvernance de la valeur (GV), de gestion du portefeuille de projets SI (GP), et de gestion de l'investissement consenti sur chaque projet (GI). Voir Figure 7.

Par contre, il n'existe pas de référentiel permettant de mesurer directement la pertinence du système d'information d'une entreprise. En effet, les besoins et les enjeux à prendre en compte sont spécifiques à chaque entreprise, car fonctions de son domaine d'activité et de ses métiers, mais aussi de sa culture, de son positionnement stratégique et de son environnement.

Pour cela, on va évaluer au cas par cas les applications informatiques, en tant que support de l'ensemble des règles de gestion, des flux d'information internes et externes, des modes opératoires de la plupart des postes de travail.

---

3 - Val IT : Création de valeur pour l'entreprise : La Gouvernance des Systèmes d'Informations – ITGI (IT Gouvernance Institute) – édition française AFAI

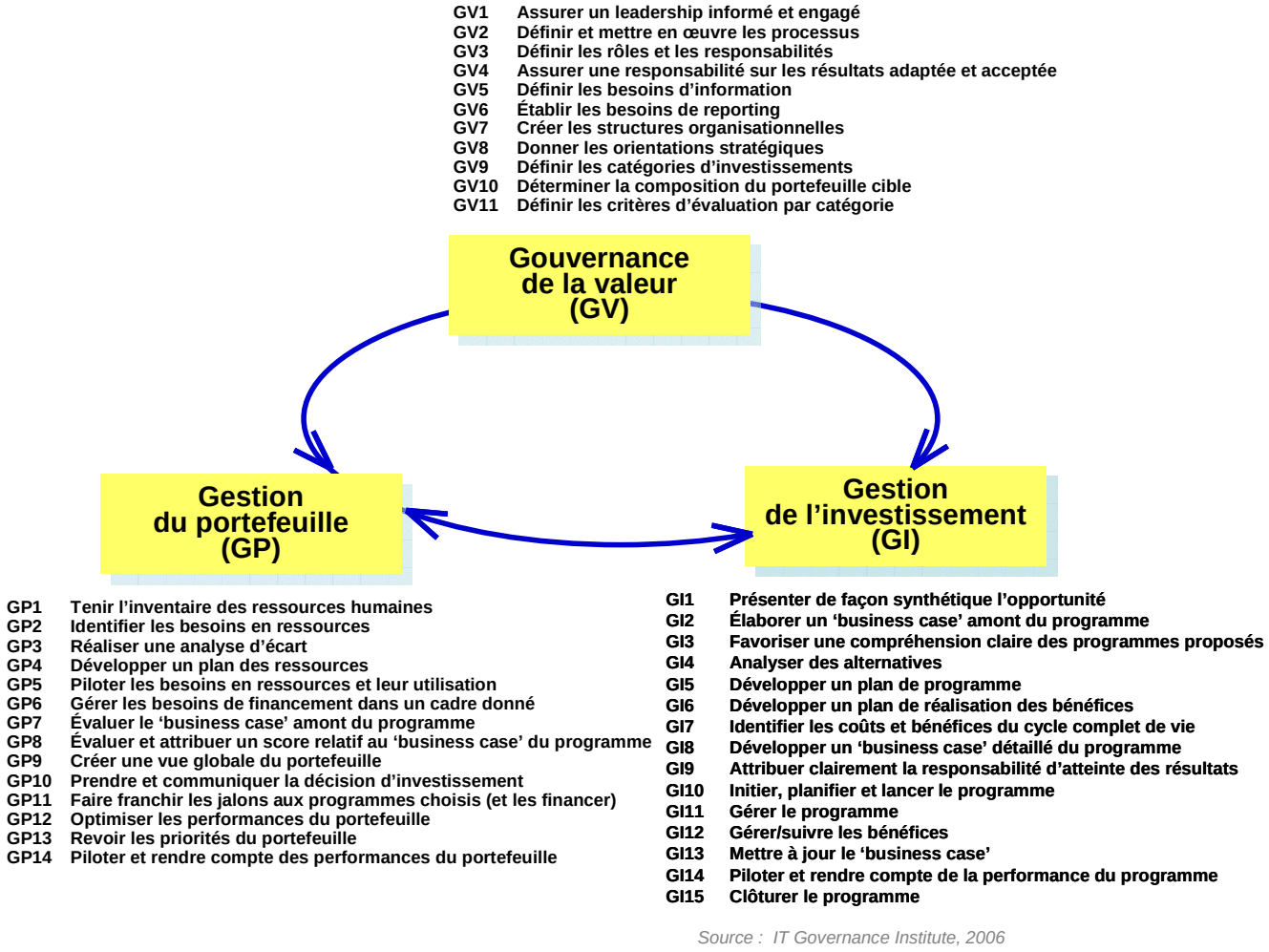

Figure 7 - Le référentiel ValIT

Inversement, l'analyse du système d'information constitue une clé majeure pour analyser et mesurer l'efficacité et la pertinence d'une grande partie des processus opérationnels et des processus de pilotage de l'entreprise : le système d'information constitue en effet bien souvent la seule trace concrète et auditable de leur fonctionnement réel.

Audit de la fonction informatique

L'objectif de l'audit de la fonction informatique est de s'assurer que son organisation et ses processus sont pertinents et conformes aux règles de l'art, qu'il s'agisse des processus de planification, de pilotage, de développement de nouvelles applications, de mise à disposition des services ou de support.

Notons que la fonction informatique et les processus à prendre en compte englobent, bien au-delà des équipes informatiques internes, l'intervention des dirigeants et des maîtrises d'ouvrage métiers, et l'ensemble des

acteurs externes (éditeurs, prestataires et fournisseurs) qui contribuent au bon fonctionnement du système d'information.

Il faut également souligner que la capacité du système informatique à bien fonctionner doit intégrer sa capacité à évoluer et notamment pour prendre en compte les changements propres à l'informatique : évolutions des technologies, nouveaux logiciels et progiciels, changements de versions, …

La qualité de fonctionnement et l'efficacité actuelles et futures des processus de l'entreprise dépendent ainsi étroitement de la qualité des processus de la fonction informatique. L'audit de la fonction informatique constitue dès lors un point d'action essentiel du contrôle interne.

Le référentiel majeur de ce second type d'audit informatique est CobiT : Control Objectives for Information and related Technology. CobiT V4.1 identifie les 4 grands domaines et les 34 processus, voir Figure 8. Il décrit de façon détaillée les objectifs, les indicateurs, et les bonnes pratiques associés à chacun de ces processus, et propose les modèles de maturité associés.

Pour une grande part, ces bonnes pratiques définissent les réponses qui doivent être apportées par la fonction informatique aux préoccupations qui sont celles du contrôle interne.

C'est notamment le cas pour :

- les processus PO 4, PO 5, PO 8, PO 9, et PO 10 du domaine Planifier et Organiser (Voir Figure 8),
- les processus AI5 et AI6 du domaine Acquérir et Implémenter,
- les processus DS4, DS5, DS8, DS10 et DS11 du domaine Délivrer et Supporter,
- l'ensemble des processus du domaine Surveiller et Évaluer, qui portent sur le contrôle interne des autres processus.

L'auditeur doit sélectionner, en fonction de ses objectifs, et des caractéristiques particulières de l'entreprise et de ses systèmes informatiques, quels processus doivent être analysés de façon plus approfondie.

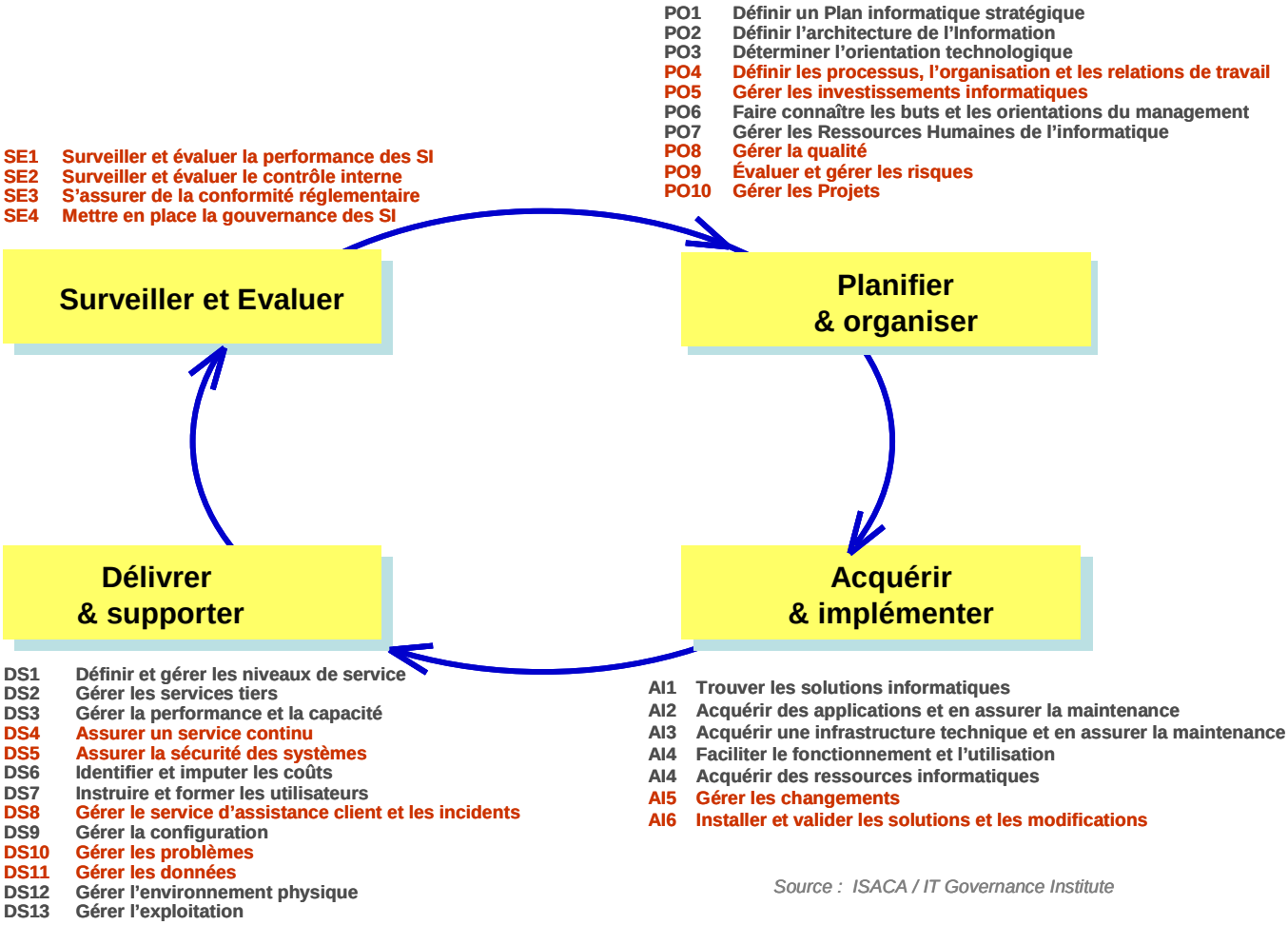

Figure 8 - Les 34 processus de CobiT

Audit des processus informatisés de l'entreprise

Enfin, ce troisième domaine de l'audit informatique a pour objectif de s'assurer que le système d'information est sûr : les missions menées dans ce domaine portent principalement sur la sûreté de fonctionnement, et les contrôles embarqués dans les applications (développés au chapitre suivant), devenus des points d'attention majeurs du contrôle interne.

La **sûreté du fonctionnement** de l'outil informatique est en effet une des conditions clés de la continuité des activités de l'entreprise, certaines défaillances pouvant aller jusqu'à mettre en cause sa survie :

- Les pannes informatiques causent des dommages directs.

- Les pertes de données accidentelles sont généralement irréparables si des sauvegardes suffisantes n'ont pas été mises en œuvre.

- Le réseau informatique, nécessairement ouvert au monde extérieur (relations clients et fournisseurs, utilisation généralisée de la

messagerie, …) est devenu le point d'entrée d'attaques incessantes.

La sûreté du fonctionnement informatique doit donc être appréciée sous tous ses aspects (disponibilité des systèmes, continuité de service, fiabilité, sécurité, maintenabilité), et ici encore en s'intéressant non seulement à la situation actuelle, mais aussi aux risques liés aux évolutions futures.

Ainsi, à l'issue de ce survol rapide des trois domaines de l'audit informatique, l'importance des objectifs de contrôle confirme son apport essentiel au contrôle interne.

10 Importance des contrôles continus

La plupart des entreprises qui tirent le bilan des travaux de contrôle interne menés dans le cadre de la loi Sarbanes-Oxley ou de la loi de Sécurité Financière constatent :

- un degré encore excessif des contrôles manuels,
- un coût élevé de mise à niveau,
- trop d'erreurs encore détectées lors d'audits internes ou externes,
- plus de contrôles détectifs que de préventifs,
- beaucoup trop d'exceptions et de détournements de contrôles,
- une insuffisante prise en compte des risques opérationnels.

L'objectif est ici de mettre en place un contrôle permanent, selon une démarche appelée aujourd'hui CCM, pour « Continuous Control Monitoring ».

Dans cette démarche, **les contrôles embarqués** dans les applications constituent un des points clés permettant de s'assurer de contrôles suffisants :

- des données saisies,
- de l'exhaustivité des traitements,
- de l'intégrité des bases de données,
- des accès.

Avant d'engager une telle démarche, il est intéressant de mesurer le degré de maturité du contrôle interne de l'entreprise sur une échelle à quatre niveaux, en fonction du degré d'automatisation des contrôles et de leur valeur ajoutée :

- traditionnel : contrôles manuels essentiellement,
- intermittent : contrôles manuels ou automatisés réalisés de façon espacée,
- périodique : contrôles en grande partie automatisés et récurrents,
- continu : contrôles très automatisés, réalisés au fil de l'eau.

Pour se situer dans ce modèle de maturité, l'entreprise doit donc se poser les questions suivantes :

- quel est le niveau d'automatisation des contrôles ?
- sont-ils très variables en fonction des processus ou des unités considérées ?
- quelle est la valeur ajoutée de ces contrôles, et la Direction souhaite-t-elle la renforcer ?

Le champ d'application peut être très variable dans l'entreprise elle-même, et concerner les systèmes suivants :

- ERP : SAP, Oracle, JD Edwards, Peoplesoft, …

- autres systèmes applicatifs : Supply Chain, Customer Relationship Management, …
- systèmes techniques : sécurité réseau, infrastructure, help desk, contrôles d'accès, …

Les indicateurs utilisables dans une démarche CCM sont de nature très variés et déterminés en fonction des objectifs de contrôle poursuivis. Ce sont par exemple :

- passage de seuil : achats supérieurs à 100.000 €,
- accès aux transactions sensibles : liste des utilisateurs concernés,
- changements interdits dans les fichiers maîtres : modification de coordonnées bancaires,
- transactions interdites : déblocage d'un paiement indu,
- doublons : clients en double dans les fichiers,
- enregistrements mal renseignés : absence de code TVA,
- mauvaise ségrégation de fonction : possibilité de créer un client et de payer sa facture,
- cohérence des dates : réception des biens le jour même de la création de la commande.

Rares sont encore les entreprises françaises à avoir adopté des approches d'ensemble pour le CCM, même si beaucoup d'entre elles sont en recherche d'outils et de solutions.

La démarche CCM porte ses fruits si l'entreprise constate que son environnement de contrôle est renforcé de manière durable, avec un gain d'efficacité, une automatisation visible des alertes, beaucoup de prévention, et moins d'anomalies détectées au cours des audits.

11 Cas d’une mission d’audit du processus d’achats

Pour apprécier l'importance et la richesse des audits de processus notamment pour renforcer les règles de contrôle interne, il est intéressant de décrire une mission d'audit d'un processus d'achats. C'est un domaine complexe et souvent les outils informatiques et les démarches mises en œuvre sont fragiles et peuvent être améliorées.

Contexte de l'intervention

Dans le cadre du plan d’audit annuel de cette grande société, il est prévu de réaliser un audit du processus d’achats de frais généraux, qui inclut :

- les fournitures diverses,
- les « petits » matériels informatiques et leur maintenance,
- l’entretien des locaux,
- l’organisation d’événements au sein de l’entreprise.

Cet audit se justifie en raison des enjeux liés à la nature et au volume de ces achats, et aux risques inhérents, notamment de fraude. Par ailleurs, les utilisateurs se plaignent d’un manque de fiabilité des applications informatiques correspondantes.

Les commandes de services généraux sont réalisées de façon transverse par l’ensemble des Directions de la société. Le responsable des achats souhaite améliorer ce processus, dans ses différentes composantes et leurs imbrications :

- commande,
- approbation,
- réception physique,
- réception de la facture,
- bon à payer,
- paiement.

L’objectif fixé à l’audit consiste à :

- caractériser les forces et les faiblesses du processus de gestion des achats de services généraux et des applications le supportant,
- établir un diagnostic de l’existant en termes de contrôle interne,
- améliorer l’efficacité générale du processus,
- identifier les points de contrôle clés à mettre en œuvre.

Démarche de l'audit

Les actions sur site de la mission d'audit portent alors sur les points suivants :

- étude de la documentation existante : organigramme, processus, tableaux de bord, …
- entretiens avec les acteurs clés du département Services généraux,
- entretiens avec la Direction Comptable afin de caractériser les « lourdeurs » et les dysfonctionnements induits par le processus existant et d'identifier les axes d'amélioration,
- entretiens avec la Direction Informatique afin de comprendre les principes de l'application informatique utilisée, et d'apprécier les possibilités d'évolution technique de cette solution, ainsi que les processus supports de l'application,
- analyse des risques et des contrôles présents au sein du processus manuel ou de l'application informatique,
- analyse de la séparation des tâches au sein du processus et vérification de l'alignement des droits d'accès des utilisateurs à l'application informatique,
- tests d'efficacité des contrôles en place.

Constats et faits marquants

Ces analyses font apparaître un certain nombre de dysfonctionnements :

- nombre élevé de commandes « hors circuit » ou « hors budget »,
- pas de suivi en « temps réel » du budget des achats des directions,
- délai excessif entre la réception physique et l'approbation de la direction acheteuse,
- paiements réalisés en l'absence d'approbation formelle,
- hétérogénéité du processus d'approbation et du niveau hiérarchique des approbateurs suivant les directions acheteuses,
- séparation de fonctions insuffisante dans le processus d'approbation : la personne qui commande est souvent la même que celle qui approuve,
- absence de limites d'achat suivant la nature des biens commandés et le niveau hiérarchique de l'auteur de la commande.

Par ailleurs des opportunités d'automatisation du processus méritent d'être explorées :

- mise en œuvre d'un workflow d'approbation,
- traçabilité des approbations de chaque commande,
- archivage des preuves d'approbation.

Recommandations

L'audit se conclut par les trois recommandations suivantes.

- Il propose d'abord de rationaliser le processus et les seuils d'approbation des commandes via la mise en place d'un workflow :
  - identification pour chaque flux de commande d'un approbateur et d'un délégué (l'assistant de l'approbateur, le plus souvent),
  - mise en œuvre de seuils d'approbation automatisés et ajouts d'approbateurs supplémentaires au-delà d'un certain montant de commandes,
  - préservation des preuves d'approbation électroniques, dans la solution.

- Il recommande de vérifier la séparation de fonctions, en s'appuyant sur cet outil de workflow, par la mise en place de contrôles applicatifs :
  - élaboration et intégration dans la solution d'une matrice d'approbation par direction acheteuse afin d'éviter l'auto-approbation,
  - mise en œuvre de nouvelles habilitations dans le module achat et dans le module comptabilité fournisseurs de l'application : accès limité à la fonction de réception physique, et limite d'accès à la consultation suivant les natures de commandes.

- Enfin, l'audit recommande d'alléger le processus d'approbation et de mieux intégrer processus d'achat de frais généraux avec les processus budgétaire et fournisseurs:
  - décrémentation du budget des directions acheteuses dès l'initialisation de la commande,
  - déclenchement du bon à payer lors de la saisie de la réception dans l'application.

Ainsi, cet audit a contribué à :

- **optimiser ce processus et rationaliser la gestion des approbations,**
- **mieux coordonner ce processus et les processus budgétaire et fournisseurs,**
- **renforcer le contrôle interne sur le processus.**

12 Guide opérationnel

Le renforcement des pratiques (4) de contrôle interne des systèmes d'information nécessite de définir un plan d'action. La démarche à mettre en œuvre est itérative. Elle doit être planifiée et menée dans la durée. Elle peut inclure les neuf domaines suivants qui peuvent être traités dans l'ordre le plus adapté par les entreprises :

1. développer l'approche par les processus,
2. identifier les domaines à fort niveau de risques,
3. évaluer les dispositifs de contrôle interne de l'entreprise,
4. maîtriser l'approche par les processus,
5. mettre en place des mesures a minima concernant l'activité informatique,
6. renforcer les dispositifs de contrôle intégrés,
7. mettre en place un système d'information dédié aux contrôles,
8. évaluer la qualité et l'efficacité des contrôles en place,
9. renforcer les processus informatiques.

Comme on le voit, les efforts nécessaires pour renforcer les contrôles et avoir un système d'information fiable et conforme sont importants et doivent être soigneusement évalués et planifié.

12.1 Développer l'approche par les processus

L'amélioration des contrôles repose pour une bonne partie sur une approche permettant de mettre sous contrôle l'ensemble des processus, de bout en bout :

- s'assurer que les principaux processus de l'entreprise ont été identifiés, analysés et correctement documentés, et si ce n'est pas le cas, le faire d'urgence : c'est un des principes de base du

4 - Compte tenu de la situation actuelle, nous n'avons pas pris en compte le cas d'une entreprise qui souhaiterait alléger les dispositifs de contrôle interne se trouvant dans son système d'information. C'est actuellement un cas d'école. Par contre il est possible que certaines entreprises ressentent le besoin de rendre ces dispositifs moins contraignants et moins lourds.

contrôle interne.

- rapprocher l'analyse des processus et les systèmes informatiques en place. Il faut s'attacher à :
  - revalider les documents existants d'analyse des processus et des systèmes informatiques ; une attention particulière doit être portée à la conformité de l'application informatique et des procédures par rapport aux besoins, au cahier des charges et à la documentation,
  - si c'est nécessaire remettre en cause certaines parties de processus, notamment si on a le sentiment qu'il existe des défauts graves. Il ne faut pas hésiter à les corriger.

- établir un tableau de bord des indicateurs de performance pour chaque processus, et un tableau de synthèse pour les principaux processus : c'est l'outil de gestion indispensable pour maîtriser les flux, détecter les engorgements, mesurer la dégradation des délais, … Ce n'est pas a priori un outil de contrôle interne, mais cela permet de s'assurer que les processus sont sous contrôle, et le cas échéant d'identifier les zones de risques.

Ces trois points sont la base d'une démarche d'amélioration de maîtrise des processus et donc du contrôle interne.

12.2 Identifier les domaines à fort niveau de risques

Trop souvent on contrôle là où « il y a de la lumière » et on laisse de côté les zones d'ombres. Cette démarche est coûteuse et peu efficace. Il est de loin préférable de choisir les domaines à mettre sous contrôle en fonction d'une évaluation des risques. L'effort sera plus adapté et le résultat plus sûr.

Parmi toutes les fonctions et tous les processus, certains supportent des niveaux de risques particulièrement importants alors que d'autres bénéficient de niveaux nettement plus faibles. Il est dans ces conditions nécessaire de s'assurer que les principaux risques sont sous contrôle et que des parades ont été mises en place afin de les maîtriser. Pour identifier ces domaines à haut risque, différentes approches peuvent être utilisées :

- chaque incident constaté doit être enregistré dans un journal par le responsable des risques et le responsable de la sécurité informatique, qui décrivent sa cause, ses impacts et les parades adoptées.

- les domaines à risques des systèmes d'information doivent avoir été identifiés : impact financier potentiel, confidentialité des données, règles d'accréditation, risques de fraude, ….

- des analyses de risques doivent être effectuées notamment en ce qui concerne la sécurité des systèmes informatiques. Ceci concerne aussi les PC, les serveurs, le réseau, les logiciels, …. Il est nécessaire que ces évaluations soient périodiquement effectuées. On doit s'assurer que des mesures sont prises pour diminuer l'impact de ces risques.

- les résultats des audits internes et externes précédemment effectués doivent être pris en compte.

A la fin de ces travaux, une cartographie des risques est établie qui présente les risques majeurs ainsi identifiés. Ils doivent être périodiquement réévalués.

12.3 Évaluer les dispositifs de contrôle interne de l'entreprise

Pour réduire ces risques, il est nécessaire de s'assurer du niveau de maîtrise par le management de l'entreprise des dispositifs de contrôle interne, en évaluant les différents dispositifs actuellement en place :

- analyser les documents définissant les dispositifs de contrôle interne de l'entreprise et leur mise en œuvre, en se concentrant sur les différents composants du système d'information : équipements informatiques, applications, données et sécurité.

- s'entretenir avec quelques dirigeants de l'entreprise pour évaluer leur niveau de connaissance des dispositifs de contrôle interne et notamment du rôle des systèmes d'information dans le contrôle. Leur demander les instructions qu'ils ont données dans ce domaine à leurs collaborateurs et aux développeurs informatiques.

- en cas de doute, effectuer des audits permettant d'évaluer la qualité des contrôles et des dispositifs de sécurité mis en place, notamment :
    - o les données saisies,
    - o l'intégrité et le contenu des bases de données,
    - o les traitements effectués,
    - o les sorties : éditions et consultations,
    - o les règles et les modalités de la conservation des données,
    - o la disponibilité du système.

- s'assurer que le personnel de l'entreprise partage un savoir commun à la démarche de contrôle interne. Il faut un tronc commun et un langage commun destinés à toutes les personnes concernées par le contrôle interne de l'entreprise. C'est à la fois un problème d'organisation et de contrôle interne.

A l'issue de ces travaux une charte de contrôle interne doit être établie et on doit s'assurer qu'elle comprend le système d'information.

12.4 Maîtriser l'approche par les processus

Le développement des mesures de contrôle interne repose en grande partie sur le renforcement des processus de l'entreprise et notamment la mise en place de contrôles plus puissants et plus efficaces. Il faut pour cela :

- repérer les processus ayant un niveau de risque élevé. On va pour cela s'attacher à identifier :
  - les applications informatiques mises en œuvre dans le processus.
  - les données et particulièrement leur qualité et leur fiabilité.
  - l'efficacité de l'organisation en place.

- s’assurer de la qualité de la documentation des processus et des contrôles mis en place. Si c’est nécessaire il faut la faire compléter. L'absence de documentation des processus est un facteur de risque important. On doit homogénéiser l'ensemble des documentations des procédures, les compléter et, si nécessaire, les mettre en cohérence.

- évaluer la maturité de l'ensemble des processus de l'entreprise. Cette évaluation doit être faite par un expert compétent et indépendant. Il doit en particulier s'attacher à apprécier la pertinence des dispositifs de contrôle interne mis en œuvre.

- nommer un responsable de chaque processus, chargé de surveiller en permanence son fonctionnement, de détecter des dysfonctionnements et le cas échéant de prendre des mesures permettant d'améliorer l'efficacité des dispositifs de contrôle interne.

- s'assurer qu'un membre du comité de direction a la responsabilité de l'ensemble des processus. Il doit s'assurer du fonctionnement régulier et efficace de l'ensemble des processus. Il a pour mission d'organiser la coopération des différentes personnes concernées, internes ou externes, comme les comptables, les contrôleurs de gestion, les auditeurs internes, les responsables qualité,…

- faire auditer les principaux processus par des experts indépendants ou par des auditeurs. Ceci concerne les

processus métiers mais aussi les processus informatiques. L'objectif est de détecter des fragilités et des contrôles insuffisants.

Comme on le voit, ces démarches demandent un premier niveau de maturité. Pour réussir cette étape il est nécessaire d'avoir parfaitement maîtriser l'étape n°1 : Développer l'approche par les processus.

12.5 Mettre en place des mesures a minima concernant l'activité informatique

Un certain nombre de mesures simples peuvent être prises sur les activités informatiques elles-mêmes pour renforcer les dispositifs de contrôle interne, comme par exemple :

- renforcer les sauvegardes et vérifier qu'elles sont exploitables. En cas de doute demander qu'une simulation de redémarrage soit faite sur le site de secours.

- s'assurer que toutes les transactions sont enregistrées (existence d'un log), notamment les créations ou les mises à jour des bases de données, et qu'il est possible de redémarrer après un incident avec des bases de données à jour.

- pour les applications stratégiques ou à fort enjeu, s'assurer que les conditions de la continuité de service sont garanties :
  - les matériels sont redondants, y compris les disques,
  - les bases de données sont simultanément mises à jour,
  - les liaisons de télécommunication sont doublées,
  - les alimentations électriques ne sont pas branchées sur le même réseau et il existe une alimentation de secours,
  - ...

- améliorer les mesures d'activité, et établir un tableau de bord des principales fonctions informatiques :
  - les études,
  - les projets critiques,
  - l'exploitation,
  - la maintenance,
  - le help-desk,
  - …

- définir un tableau de bord par application, rassemblant des indicateurs tels que :
  - les volumes à traiter (par mois, par jour, par heure, par minute,…),

  - les temps de réponse,
  - la disponibilité,
  - les coûts de l'application,
  - les effectifs utilisant l'application,
  - la productivité (comme le nombre de dossiers par jour et par personne),
  - la charge de maintenance,
  - …

- enregistrer toutes les anomalies détectées dans une base de données spécifique. Les analyser systématiquement et rechercher leurs causes. C'est le meilleur moyen de comprendre les fragilités du système d'information et ses risques potentiels. Il est sur cette base possible de prendre des mesures afin de corriger ces défauts.

- périodiquement, tous les mois par exemple, effectuer une synthèse de ces anomalies et diffuser un bref compte rendu des problèmes détectés.

Ces mesures sont nécessaires afin d'assurer un niveau de contrôle minimum. Si elles ne sont pas appliquées il est recommandé de remonter une alerte à la direction générale car l'entreprise est probablement en situation de risque majeur.

12.6 Renforcer les dispositifs de contrôle intégrés

Pour aller plus loin dans la mise en place de mesures de contrôle interne, il faut s'intéresser aux contrôles automatisés embarqués dans les programmes permettant de s'assurer que les opérations se déroulent normalement. Ils concernent :

- les données saisies : les contrôles mis en place par les programmeurs sont-ils suffisants ? Faut-il les renforcer ?
- les données se trouvant dans les bases de données, qui doivent être vérifiées pour s'assurer qu'elles ne comprennent pas d'erreurs, d'oublis ou d'informations inutiles,
- le contrôle des traitements pour s'assurer qu'il ne survient aucune erreur, ni oubli ni doublon : ceci concerne surtout les traitements batch mais on peut aussi effectuer ces contrôles sur les traitements transactionnels,
- le contrôle des éditions et des consultations d'informations : il faut s'assurer que l'ensemble des états édités est complet et qu'aucun document ne manque. C'est notamment le cas de l'édition de la paie, de la facturation, ….

On s'attachera en particulier aux actions suivantes :

- établir la liste des contrôles existants et définir les contrôles à mettre en place. Il est nécessaire de disposer d'un document de

référence recensant tous les types de contrôles possibles : on décide ensuite les contrôles qui doivent être mis en œuvre en fonction du niveau de risque constaté.

- tous les contrôles internes figurant dans les programmes alimentent automatiquement une base de données spécifique quels que soient leurs statuts (positif ou négatif). Périodiquement, tous les mois par exemple, une analyse des contrôles effectués au cours de la période est réalisée et un compte-rendu synthétique est rédigé.

- définir et mettre au point des programmes de contrôle des principales bases de données pour s'assurer de la qualité des informations qu'elles contiennent. Il est pour cela possible d'utiliser des progiciels d'aide à l'audit. Ces programmes analysent une à une toutes les occurrences de la base et s'il y a des liaisons entre bases ils analysent chaque chaînage. Chaque zone doit être contrôlée.

- tous les contrôles de données doivent être faits au moment de la saisie. Dans les traitements ultérieurs des anomalies peuvent être constatées. Il faut dans ce cas gérer ces rejets et les recycler pour ne pas perdre d'information.

- prévoir des contrôles globaux pour s'assurer de l'intégrité des données au cours de la période, et notamment qu'aucune donnée n'a été perdue au cours des traitements, que toutes les données ont été saisies et que les bases de données ont été mises à jour.

Ceci correspond à une évolution des systèmes de contrôle. Voir Chapitre 10 : "Importance des contrôles continus".

12.7 Mettre en place un système d'information dédié aux contrôles et au suivi des anomalies

Pour s'assurer de l'efficacité des dispositifs de contrôle mis en place, il est nécessaire de développer des outils de suivi des contrôles effectués, permettant de garder trace des anomalies constatées :

- s'assurer que tous les contrôles prévus dans les applications et sur les bases de données sont réellement effectués. Pour cela, au fur et à mesure qu'ils s'exécutent, on alimente une base de données des contrôles effectués, et lorsque des anomalies sont détectées on enregistre les codes d'anomalies correspondants. Périodiquement cette base est analysée et une statistique des types d'anomalies est établie.

- mettre en place un tableau de bord des contrôles en place permettant de détecter rapidement une dégradation du système

d'information.

- mettre en place un test de non-régression pour s'assurer que tous les contrôles définis sont effectivement en place et fonctionnent de manière correcte.

- effectuer périodiquement un traitement de contrôle des principales bases de données en contrôlant tous les items et tous les chaînages entre bases.

- créer des bases de données (datawarehouse) alimentées par les grands processus : achats, ventes, production, … A l'aide de logiciels d'audit, il sera possible d'effectuer des analyses du contenu, de la qualité et de la complétude de ces données.

12.8 Évaluer la qualité et l'efficacité des contrôles en place

Il est nécessaire de régulièrement s'assurer que les contrôles en place sont suffisants et efficaces. Si on constate une multiplication des incidents dus à des défauts de contrôle, il faudra renforcer les contrôles en place.

- effectuer périodiquement une analyse des incidents dus à des défauts de contrôle. Les premiers concernés sont les utilisateurs. Dès qu'ils constatent une anomalie, ils doivent la signaler et la décrire. Elles sont normalement analysées et les défauts constatés sont corrigés. Parmi ces anomalies, les défauts de contrôle doivent être particulièrement pris en compte. Cette revue peut être conduite dans un domaine applicatif donné ou pour l'ensemble de l'entreprise.

- dans le cas où un domaine ou un processus a rencontré des défauts de contrôle récurrents, il est recommandé d'effectuer un audit. C'est le meilleur moyen d'apprécier la qualité et l'efficacité des contrôles en place. L’audit va faire apparaître les points faibles et des points forts permettant de dégager des recommandations.

- effectuer tous les 2 ou 3 ans une évaluation de tous les processus de l’entreprise dans le cadre des audits d'applications.

12.9 Renforcer les processus informatiques

Il est nécessaire de :

- s'assurer que le service informatique connaît et applique CobiT. Ceci peut se faire de différentes manières et notamment en vérifiant que les principaux objectifs des processus CobiT sont appliqués. Si nécessaire, évaluer leur degré de maturité.

- vérifier qu'il existe un système de management par la qualité conforme à un référentiel tel que la norme ISO 9001 : 2000.

- mettre en place à l'exploitation le référentiel ITIL et si on constate des fragilités d'exploitation, améliorer les pratiques.

- mettre en place aux études le référentiel CMMi et si on constate des fragilités dans le domaine des projets, améliorer les pratiques.

- élever le niveau des exigences et des spécifications de contrôle interne en regard du niveau des performances attendues. La démarche consiste à augmenter progressivement le niveau des standards, de façon à améliorer le niveau de contrôle interne. La référence est CobiT, mais on peut aussi s’appuyer sur ITIL et CMMi.

13 Annexes

Annexe 1 : Application du cadre de l'AMF aux systèmes d'information

Annexe 2 : Le COSO appliqué aux systèmes d'information

Annexe 3 : Bibliographie

1 - Application du cadre de l'AMF aux systèmes d'information

Les systèmes d'information participent aux 5 composantes du contrôle interne telles que définies par le cadre de l'AMF (Chapitre 4 "Le contrôle interne en environnement informatique : le rôle du cadre de l'AMF"). Le tableau ci-après indique, pour chacun des thèmes abordés dans le cadre de l'AMF, les recommandations faites par AFAI précisant la façon dont ces thèmes peuvent être pris en compte.

Cadre de l'AMF	Composante système d'information à prendre en compte
Composante Organisation	
« Une organisation… s'appuyant sur des systèmes d'information appropriés …. des systèmes d'information adaptés aux objectifs actuels de l'organisation et conçus de façon à pouvoir supporter ses objectifs futurs. Les systèmes informatiques…doivent être protégés efficacement tant au niveau de leur sécurité physique que logique afin d'assurer la conservation des informations stockées »	C'est le thème de la gouvernance des systèmes d'information (alignement entre les systèmes d'information et les besoins utilisateurs, prise en compte des besoins futurs)
« leur continuité d'exploitation doit être assurée au moyen de procédures de secours »	Sécurité des systèmes d'information (protections logiques et physiques des systèmes informatiques, continuité d'exploitation / plan de secours)
« les informations relatives aux analyses, à la programmation et à l'exécution des traitements doivent faire l'objet d'une documentation »	Qualité des processus informatiques (documentation des processus de « développement » et de « production », ainsi que les procédures de « gestion des modifications »)
« des procédures ou modes opératoires qui précisent la manière dont devrait s'accomplir une action ou un processus »	Fiabilité des opérations supportées par le système d'information (description des processus et modes opératoires – lien étroit avec les systèmes d'information)
« des outils ou instruments de travail (bureautique, informatique) qui doivent être adaptés au besoin de chacun et auxquels chaque utilisateur devrait être dûment formé »	Fiabilité des opérations supportées par le système d'information (formation des utilisateurs aux outils)
DIFFUSION D'INFORMATION	
« La diffusion en interne d'informations pertinentes, fiables, dont la connaissance permet à chacun d'exercer.. »	Sécurité des systèmes d'informations (le système d'information est le principal circuit de diffusion des informations au sein d'une organisation, à travers l'infrastructure existante et les outils mis en place. Ces éléments doivent répondre à des objectifs de fiabilité, de confidentialité et de disponibilité – la traçabilité est également importante). Des dispositifs de contrôle des flux de

	données permettent de s'assurer de l'exactitude et l'exhaustivité (intégrité) des données en entrée et en sortie du système d'information. Ces contrôles ne sont pas nécessairement inclus dans les dispositifs de sécurité.
	Gestion des autorisations (la diffusion d'information nécessite de mettre en place des mécanismes d'accès et d'autorisation dont la gestion incombe généralement aux métiers)
GESTION DES RISQUES	
« un système visant à recenser, analyser les principaux risques identifiables au regard des objectifs de la société et à s'assurer de l'existence de procédures de gestion des risques »	Risk Management des systèmes d'information (« Recenser, Analyser et gérer les risques » doit se décliner au niveau des systèmes d'information : le risque informatique — sous toutes ses formes — reste une préoccupation forte ; les points à régler font encore débat : où faut-il localiser la fonction, quelle méthode, quel référentiel choisir ? Le risque informatique n'est pas encore assez bien pris en compte)
ACTIVITES DE CONTROLES	
« des activités de contrôles proportionnés aux enjeux propres à chaque processus et conçus pour s'assurer que les mesures nécessaires sont prises en vue de maîtriser les risques susceptibles d'affecter la réalisation des objectifs. Les activités de contrôles sont présentes partout dans l'organisation, à tout niveau et dans toute fonction qu'il s'agisse de contrôles orientés vers la prévention ou la détection, de contrôle manuels ou informatiques ou encore de contrôles hiérarchiques. En tout état de cause, les activités de contrôle doivent être déterminées en fonction de la nature des objectifs auxquels elles se rapportent et être proportionnées aux enjeux de chaque processus. Dans ce cadre, une attention toute particulière devrait être portée aux contrôles des processus de construction et de fonctionnement des systèmes d'information »	Fiabilité des opérations (activités de contrôles automatisées : contrôles inhérents au système d'information, contrôles paramétrés dans le système d'information, contrôles fondés sur des informations fournies par le système d'information, autorisations)
SURVEILLANCE	
« Une surveillance permanente portant sur le dispositif de contrôle interne ainsi qu'un examen régulier de son fonctionnement »	Surveillance mise en œuvre par la Direction Générale sur les systèmes d'information grâce à : - l'audit interne informatique, - l'assurance qualité faite par la direction qualité de la DSI, - la surveillance exercée par le Comité d'Audit.

Figure 9 - Recommandations de l'AFAI sur le cadre de référence de l'AMF

2 - Le COSO appliqué aux systèmes d'information

En octobre 1985, la *Treadway Commission* (*5*) a constitué aux USA un groupe de travail réunissant les grandes entreprises, les cabinets d'audit et les associations professionnelles afin d'établir les règles de contrôle financier interne efficaces et d'améliorer la qualité des reportings financiers.

Le COSO, (*Committee of Sponsoring Organizations of the Treadway Commission)* est le nom donné à ce groupe de travail et qui, sur la base de ses recommandations, a rédigé le « COSO Framework » ou référentiel COSO publié en 1992.

L'importance accordée à ce référentiel s'est accrue lorsque la loi américaine Sarbanes Oxley (SOX Act) a été adoptée en juillet 2002 par le Congrès. SOX ne fournit pas de directives spécifiques quant à la définition du contrôle interne approprié, ce dernier pouvant varier sensiblement d'une entreprise à l'autre.

Cependant, dans ses règles édictées en juin 2003, la SEC a identifié l'infrastructure de contrôle interne COSO en tant qu'infrastructure répondant à ses critères en matière de recommandations pour l'évaluation et le développement des contrôles**.**

Par ailleurs, le COSO donne peu d'informations concernant les contrôles spécifiques du système d'information. Par conséquent, nombreuses sont les entreprises qui ont choisi CobiT (6) comme étant la meilleure voie pour rendre le système d'information conforme aux exigences du COSO.

Le cube COSO

Le référentiel COSO a donné naissance à un cube dont les 3 faces visibles représentent les 3 objectifs, les 5 composants et les activités de l'entreprise.

Dans cette approche en « cube », chaque activité contribue à la réalisation des 3 objectifs. Pour chacune d'elle, et pour chacun de ces 3 objectifs, il s'agit d'analyser les 5 composantes du contrôle interne.

---

5 - Treadway est le sénateur qui a dirigé la commission. Il a été membre de la Securities and Exchange Commission et le premier président du COSO.

6 - Voir « IT Control Objectives for Sarbanes-Oxley » publiées par l'IT Governance Institute. Ce document reprend les éléments du COBIT et du COSO, dans le but de répondre aux exigences du SOX Act.

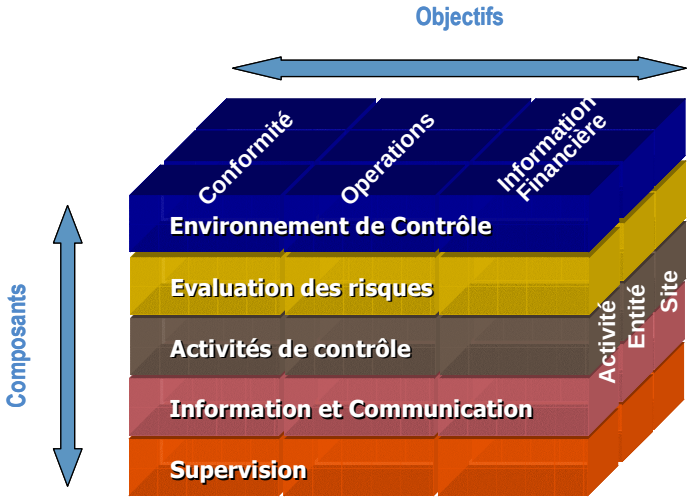

Figure 10 - Le cube du COSO, 1ére version 1

La combinaison des trois objectifs, des cinq composants et des différentes activités de l'entreprise, vue comme trois axes d'analyse distincts, donne la base des évaluations à réaliser: « Evaluer dans toute entité et pour toute activité la façon dont chacun des 5 composants du contrôle interne participe à chacun des 3 objectifs ».

Les trois objectifs

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

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

Les cinq composants

Les cinq composants ont pour objectif l'amélioration du système du contrôle interne de l'organisation et ils sont interconnectés. Il s'agit de :

- l'environnement de contrôle,
- l'évaluation des risques,
- les activités de contrôle,
- l'information et la communication, qu'il s'agit d'optimiser,
- la surveillance, c'est-à-dire le « contrôle du contrôle » interne.

L’environnement de contrôle et le système d’information (SI)

Ce composant constitue le fondement de tous les autres composants du contrôle interne ; il établit «the tone at the top». L'environnement du contrôle contient notamment l'intégrité et les valeurs éthiques d'une organisation, la philosophie et le style de la direction, la manière dont les compétences et les responsabilités sont attribuées.

Le contrôle interne informatique s’appuie sur l’environnement de contrôle de l’organisation et concerne l'attribution de l'autorité et de la responsabilité des activités. Les solutions de gestion des identités et des accès sont un élément essentiel du dispositif.

Compte tenu des caractéristiques intrinsèques du système d’information, une attention particulière est portée à l'alignement métier du système d’information, aux rôles et responsabilités, aux politiques et procédures et aux compétences techniques. Par exemple, les points de vigilance à adresser sont :

- le système d’information est souvent considéré comme une organisation séparée des métiers ce qui conduit, à tort, à établir un environnement de contrôle séparé.

- il est complexe, non seulement en ce qui concerne ses composants techniques, mais aussi en termes d’intégration dans le système de contrôle interne de l’organisation.

- il peut exposer l’organisation à des risques spécifiques qui exigent des activités de contrôle adéquates pour réduire les risques.

- il exige des compétences spécialisées qui peuvent être rares.

- il peut conduire à un niveau de dépendance significatif sur la sous-traitance dans le cas où des processus ou des composants du système d'information seraient externalisés.

Evaluation des risques et le système d’information

Toute organisation s'expose à une multitude de risques tant externes qu'internes. L'analyse de risques est le processus qui identifie et évalue ces risques par rapport aux objectifs de l'organisation et forme dès lors la base pour le contrôle des risques.

La multiplication des risques lié au contrôle interne est probablement plus importante en ce qui concerne les systèmes d'information que dans d'autres secteurs de l'organisation.

L’évaluation des risques intervient :

- au niveau de l’organisation avec des campagnes d’évaluation des risques des systèmes d'information couvrant le management, la sécurité des données, et le développement.

- au niveau de chaque activité : l'exploitation des infrastructures, les processus de modification d’une application,…

Activités de contrôle et système d’information

Les activités de contrôle répondent au besoin de politiques, de procédures et d'actions spécifiques pour s’assurer que les objectifs métiers sont atteints. Elles sont mises en œuvre pour traiter les risques. Le COSO imposant la matérialisation factuelle des contrôles.

Il s'agit ici d’activités à tout les niveaux de l'organisation : approbations, compétences, vérifications, réconciliations, évaluations de prestations opérationnelles, surveillance de l'actif et séparation des fonctions.

COSO identifie deux grands groupes d’activités de contrôle informatique : les contrôles généraux et les contrôles applicatifs (7).

Les contrôles généraux se rapportent au contrôle interne appliqué à la fonction informatique. Ils concernent les points suivants :

- la planification et l'organisation générale de l'activité informatique,

- la conception et le développement des applications (les procédures de documentation, les revues, les tests et l'approbation des systèmes ou des programmes et des changements qui y sont apportés),

- la maintenance des applications et des systèmes,

- les accès aux ressources matérielles et informationnelles (données et programmes),

- les autres contrôles de données et les procédures affectant les opérations informatiques globales.

Les contrôles applicatifs sont les contrôles automatisés relatifs à des tâches réalisées par le système d'information. Associés aux contrôles manuels, les contrôles applicatifs apportent une assurance que les enregistrements, les traitements et le reporting des données sont correctement réalisés.

7 - GLEIM Partie III

Information- communication et système d'information

Ce composant vise à assurer que l'information pertinente est identifiée, recueillie et diffusée dans les délais appropriés afin que l'ensemble du personnel puisse assumer ses responsabilités.

Pour cela, les systèmes d'information doivent garantir que toutes les informations importantes sont collectées de manière fiable et ponctuelle et diffusées convenablement.

Par exemple, le système d'Information intervient en support pour identifier et communiquer des événements significatifs à l'aide du courrier électronique ou des systèmes d'aide à la décision.

Surveillance et système d'information

Les systèmes de contrôle interne doivent être supervisés pour évaluer leur qualité et leur performance dans le temps.

C'est le « contrôle du contrôle », qui couvre différents types de suivi : le contrôle continu, les évaluations séparées ou une combinaison des deux.

Le contrôle continu correspond à la supervision « normale » du management opérationnel. La nécessité de conduire des évaluations séparées (tant en ce qui concerne le contenu que la durée) dépend des résultats de l'analyse de risques et des activités de surveillance continue.

Deuxième version du COSO

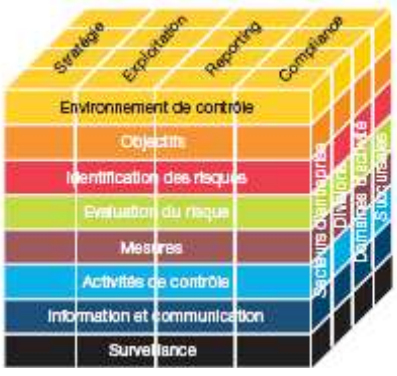

Figure 11 - Le cube du COSO, 2ème version

Publié en 2004, le «COSO II Enterprise Risk Management Framework » tient lieu de standard dans le cadre de la gestion des risques d'entreprise. Le «cube COSO» visualise la gestion du risque en trois dimensions : du point de vue des objectifs de l'entreprise tels le contrôle interne, les

composantes de la gestion du risque à l'échelle de l'entreprise et l'organisation de l'entreprise.

Selon le COSO II (8), le management des risques traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Il se définit comme suit :

> *Le management des risques est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation.*
>
> *Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque(9). Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.*

La gestion des risques doit être considérée dans une optique de pilotage : quels risques veut-on absolument éviter, quels risques sont inutiles, quels risques est-on prêt à prendre pour profiter de quelles opportunités ou conserver quel avantage ?

8 - www.coso.org : Le management des risques de l'entreprise - Cadre de Référence

9 - Appétence au risque : niveau de risque souhaité pour atteindre les objectifs de l'entreprise

3 - Bibliographie

1. CobiT : Gouvernance, Contrôle et Audit de l'Information et des technologies associées – ITGI – édition française AFAI Version 4.1 Mars 2008 : www.isaca.org et www.afai.fr

2. Val IT : Création de valeur pour l'entreprise : la gouvernance des systèmes d'information – ITGI - édition française AFAI Version 4.1 2006 : : www.isaca.org et www.afai.fr

3. IT control Objectives for Sarbanes-Oxley – Version 2 septembre 2006- Ce texte est téléchargeable à partir du site : www.itgi.org et www.isaca.org

4. Prise en compte de l'environnement informatique et incidence sur la démarche d'audit - Compagnie Nationale des Commissaires aux Comptes (avec la participation de l'AFAI)

5. Approche et méthode de la mission de diagnostic du contrôle interne ou comment répondre aux obligations de la loi sur la sécurité financière – Conseil Supérieur de l'Ordre des Experts Comptables (encours avec la participation de l'AFAI)

6. La nouvelle pratique du contrôle interne – Traduction du COSO Report (version 1) – IFACI. Editions d'organisation. 1994

7. Le management des risques de l'entreprise - Cadre de Référence – Techniques d'application – Traduction du COSO II - IFACI. Editions d'Organisation. 2005

8. Le dispositif de contrôle interne : Cadre de référence AMF (Autorité des Marchés Financiers) – Édité par l'IFACI et disponible sur le site de l'AMF : www.amf-france.org

9. An audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements Auditing Standard N°2– PCAOB (The Public Compagny Accouting Oversight Board) – Août 2007 : www.pcaobus.org

10. An audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements Auditing Standard N°5– PCAOB (The Public Company Accounting Oversight Board) – Juin 2007 : www.pcaobus.org

11. Japan SOX : On the Setting of the Standard and Practice

Standards for Management Assessment and Audit concerning Internal Control Over Financial Reporting - Business Accounting Council – Février 2007

12. Mise en oeuvre d'un contrôle interne efficace via un ERP : LSF, SOX, 8e Directive européenne, US GAAP, IFRS - Pascal Kerebel – AFNOR

13. Contrôle interne - Frédéric Bernard, Rémi Gayraud, Laurent Rousseau – Maxima, 2006

14. Livre blanc "Sécurité Financière et Système d'Information" - Jean-Yves Galley, Pierre Bernassau

15. L'approche processus mode d'emploi- Éditions Organisation - Septembre 2006 - 2ème édition

16. Audit 2ème édition. Gestion des risques d'entreprise et contrôle interne. Hamzaoui - Pearson Education France.

17. Sarbanes-Oxley IT Compliance Using Open Source Tools, 2nd Edition – 2007 - Christian B. Lahti, Roderick Peterson- ISACA

18. Sarbanes-Oxley Guide for Finance and Information Technology Professionals, 2nd Edition - Sanjay Anand - 2006- ISACA

19. Manager's Guide to Sarbanes-Oxley Act: Improving Internal Control to Prevent Fraud - Scott Green – 2004- ISACA

20. IT Control Objectives for BASEL II: The Importance of Governance and Risk Management for Compliance - IT Governance Institute – 2007 – ISACA

21. Information Technology Audits - Lynford Graham, Xenia Ley Parker– 2007 – ISACA