Le contrôle interne du système d'information des organisations

Vendredi 13 mars 2009

Ouverture par le Président de séance : Claude Cargou

Jusqu'à présent, nos deux associations (dont l'une – le CIGREF – fêtera ses 40 ans l'an prochain, et l'autre – l'IFACI – a 44 ans) n'avaient eu pratiquement aucun point de rencontre. En 2007, le président du CIGREF d'alors, Didier Lambert, et moi-même sommes tombés très rapidement d'accord sur le fait que le contrôle des systèmes d'information était un sujet insuffisamment documenté. Nous en avons discuté avec nos conseils d'administration respectifs, et avons signé un protocole d'accord, dont l'objet était d'unir nos forces et de travailler sur ce contrôle des systèmes d'information, sujet plutôt nouveau pour nos deux associations professionnelles.

Dans quel contexte avons-nous pris cette décision ? Au début de l'année 2007, l'AMF avait rendu publics des travaux réalisés par un groupe de place, et qui avaient abouti à la définition d'un cadre de référence pour le contrôle interne. Chaque entreprise était priée de mettre en œuvre ce cadre, ou de justifier de sa non mise en œuvre. Ce cadre comportait un guide d'application et des questionnaires, dans lesquels les systèmes d'information occupaient une place déjà importante. On en parlait déjà comme d'un facteur-clé de contrôle interne pour les organisations.

Le CIGREF était déjà positionné depuis un certain temps sur les systèmes d'information en tant que facteurs de création de valeur et d'innovation. Il est clair aujourd'hui que le système d'information est la colonne vertébrale des entreprises et des organisations, et que le contrôle des systèmes d'information est devenu primordial. Pour bâtir ce contrôle, il fallait rapprocher deux directions qui, jusqu'à présent, avaient peu l'habitude de travailler ensemble : la direction du système d'information, garante de l'utilisation optimale des systèmes d'information, et la direction de l'audit interne qui a beaucoup évolué ces dernières années, et se positionne sur des sujets de plus en plus stratégiques. Une étude récente faite au niveau mondial montre qu'il y a deux sujets sur lesquels l'audit interne doit mieux se positionner : l'audit de la gouvernance des entreprises et l'audit des systèmes d'information.

Les travaux ont été lancés en 2007, entre le CIGREF, l'IFACI, des responsables des systèmes d'information et des responsables de l'audit interne d'un certain nombre d'organisations. Cela a pris beaucoup plus de temps que prévu pour deux raisons. D'abord parce que le sujet était difficile et inexploré ; ensuite parce qu'il a fallu rapprocher un certain nombre de points de vue qui n'étaient pas toujours concordants au départ. Mais, au total, il y a eu un véritable enrichissement mutuel. Aujourd'hui, tout le monde est convaincu qu'aucune des deux directions ne peut réussir dans l'entreprise si elle ne s'appuie pas sur l'autre. Il n'est pas possible que les systèmes d'information vivent sans un environnement de contrôle adéquat. Il n'est pas possible que les fonctions de contrôle et d'audit interne se développent sans les systèmes d'information.

Un véritable point d'enrichissement est celui de l'urbanisation. Pour les informaticiens, l'urbanisation des systèmes d'information est un sujet connu depuis longtemps. Ce concept a été repris pour le contrôle interne. Aujourd'hui, système d'information et contrôle interne ne peuvent pas se concevoir sans une démarche globale d'urbanisation.

L'univers d'audit doit incorporer les systèmes d'information. Les DSI doivent intégrer au plus tôt les contrôles dans les systèmes d'information. Trop souvent, on a trouvé des fonctions informatiques un peu isolées dans l'entreprise. Sans doute pour deux raisons : parce qu'elles

ont de multiples implications au sein de l'entreprise, et parce que le contrôle exercé sur elles, était embryonnaire. Les directions de l'audit interne, quant à elles, doivent faire une démarche d'initiation pour comprendre le fondement des systèmes d'information. On peut rêver du jour où la direction des systèmes d'information et la direction de l'audit interne travailleront ensemble pour définir le système d'information et de contrôle de l'entreprise. Peut-être ce chantier se développera-t-il dans le futur.

Le président Lambert et moi-même, à l'époque, voulions des livrables à la fois pratiques et réalistes. Pas de théorie, mais des échanges entre professionnels, avec des pratiques simples à mettre en œuvre, et qui apportent des résultats concrets. Nous voulions également des référentiels. Il nous a paru pertinent de travailler le sujet sous deux angles : le contrôle de la direction des systèmes d'information, et le contrôle du système d'information qui sous-tend les processus métiers. Ce sont deux aspects indissociables et complémentaires.

Je tiens à souligner l'énorme travail qui a été fait, et je félicite toutes les équipes, les présidents et les délégués généraux des deux associations, qui se sont beaucoup impliqués pour donner naissance à un très bon document.

Avant de passer la parole aux deux présidents, je voudrais formuler un dernier souhait : celui de voir nos associations poursuivre leurs travaux. Je pense que notre collaboration a été très fructueuse, avec un livrable tangible et pratique.

Je vais donner la parole à Bruno Ménard. Depuis 2001, il est vice-président des systèmes d'information chez Sanofi Aventis. Il a été élu président du CIGREF en octobre 2008.

Sommaire

Discours introductif : contexte et objectifs du guide opérationnel 5
1 – Restitution des travaux des deux sous-groupes..... 8
1.1 - Le contrôle interne du Système d'information de l'entreprise 8
1.2 - Le contrôle interne de la DSI 10
2- Le contrôle interne du système d'information, élément-clé d'une bonne maîtrise des activités 15
Questions / Réponses..... 26
Discours de clôture..... 32

Discours introductif : contexte et objectifs du guide opérationnel

Bruno Ménard, *Président du CIGREF, Vice-président Systèmes d'information, Sanofi Aventis*

Le CIGREF est une association de grandes entreprises représentées par ses DSI. Le CIGREF a accompagné l'informatisation des entreprises et des organisations depuis le début des années 1970. La mission du CIGREF est de « …*Promouvoir l'usage des systèmes d'information* – et le mot "usage" est très important – *comme facteur de création de valeur et source d'innovation pour l'Entreprise…. »*-Le partenariat avec l'IFACI - signé en octobre 2007 lors de notre AG statutaire - a été une étape très importante entre nos deux associations.

Un peu plus d'un an après les recommandations de l'AMF, nous sommes aujourd'hui en mesure de présenter un guide opérationnel. Je voudrais remercier ceux qui y ont participé, les Délégués généraux, mais également les deux pilotes qui se sont beaucoup investis, au-delà même de leur fonction opérationnelle, pour rédiger ce guide et animer le groupe de travail : Régis Delayat et Farid Aractingi. Je voudrais aussi remercier particulièrement Gérard Rameix, Secrétaire Général de l'Autorité des Marchés Financiers qui prononcera tout à l'heure le discours de clôture.

Parler de contrôle interne aujourd'hui ne peut pas se faire sans réfléchir à ce qui s'est passé depuis quelques mois. Est-ce à dire qu'il s'agit d'une crise de contrôle interne ? Probablement pas ; ce n'est pas par défaut de contrôle interne que nous sommes dans la situation d'aujourd'hui. En revanche, il est naturel de se poser des questions sur l'identification et l'analyse des risques, et ce que met en valeur la crise actuelle, c'est un défaut ou un manque de vigilance sur l'identification des risques. Pour les années à venir et le développement du contrôle interne, elle met en valeur un principe-clé, qui est le principe de réalité. Le contrôle interne est toujours confronté à une limite de moyens. Et si nous voulons que nos systèmes de contrôle interne soient réellement pertinents et efficaces, il faut qu'ils soient adossés à une analyse des risques aussi fine que possible.

Quelles sont les fonctions dans l'entreprise les plus à même d'identifier les risques qui leur sont propres ? Pour les managers, les entrepreneurs, le risque est inévitable. On ne peut pas développer une activité, se battre sur les marchés mondiaux, avec des acteurs venus de l'ensemble de la planète, sans « prendre des risques ». Que ce soit dans une entreprise privée, une entreprise de services, une administration, lorsqu'on veut gérer des changements, le risque est présent. Ces risques doivent être pris certes, mais il convient d'abord de parfaitement les identifier, et surtout de faire en sorte qu'ils soient l'objet de la mise en place de pratiques de contrôle permettant de les encadrer ; le rôle des opérationnels est de ce fait très important. Le guide opérationnel que nous proposons se veut dès lors, très pratique, car il a vocation à sensibiliser tous les acteurs, à commencer par les Dirigeants, et les responsables de centres de profits et de départements, parce que l'identification et l'analyse des risques reposent beaucoup sur eux.

Ayant pris conscience de l'importance des pratiques de contrôle, les DSI se sont mobilisées autour du rôle des systèmes d'information dans les grandes organisations car nous avons conscience que le SI est à la fois objet et outil du contrôle interne. Historiquement, on plaçait les DSI du côté des fonctions support. Je crois que cela ne reflète plus du tout la réalité. Les DSI, aujourd'hui, sont plus des directions opérationnelles, avec des activités assez

proches de directions industrielles. Ce que nous gérons, ce sont des usines à informations, des usines à transactions, une vraie *supply chain* de services extrêmement sensible, notamment parce que, par différence avec le métier industriel, elle n'a pas de stocks, et elle produit et fournit en temps réel. Notre mobilisation, pour mettre en place des pratiques d'analyse de risques et de contrôle interne, va s'amplifier. L'avenir économique, en France et dans les grands pays développés, est probablement plus dans une économie tertiaire, une économie de services, une économie d'innovation. Mais qui dit économie tertiaire, plus immatérielle, dit présence encore plus forte des systèmes d'information, des opérations qui se passent de manière virtuelle, avec des puissances de calcul qui peuvent parfois dépasser l'entendement humain. L'analyse des risques, dans ce contexte, devient un enjeu essentiel de gouvernance d'entreprise.

Claude Cargou

Je vais maintenant donner la parole à Claude Viet, président de l'IFACI depuis un an. Il est aujourd'hui conseiller du président et directeur de l'audit groupe de La Poste.

Claude Viet, *Président de l'IFACI, Directeur de l'audit groupe, La Poste*

Je voudrais rappeler les différentes étapes qui nous amènent aujourd'hui à ce colloque entre le CIGREF et l'IFACI. Tout d'abord, en liaison avec Gérard Rameix, l'IFACI a assuré le secrétariat du groupe de place institué par l'AMF en avril 2005, pour proposer un référentiel de contrôle interne, qui constitue un outil de gestion au service des entreprises. Un an plus tard, un colloque a été organisé par l'IFACI pour définir et valider les principes généraux adoptés par le groupe de place. Dans la foulée, un guide d'application de ces principes généraux de contrôle interne aux procédures relatives à l'élaboration et au traitement de l'information financière, a été présenté en février 2007, lors d'un colloque organisé en partenariat avec la Compagnie nationale des commissaires aux comptes. Aujourd'hui, pratiquement 73 % des entreprises utilisent ce cadre de référence, si l'on en croit les rapports LSF qui engagent les entreprises, leurs présidents et les conseils d'administration. Dans le prolongement des travaux menés en lien étroit avec l'AMF, nous avons souhaité, avec Monsieur Ménard, prolonger ces travaux par un partenariat actif avec le CIGREF. Un accord a été signé le 9 octobre 2007. Ce partenariat a permis de déboucher sur une réflexion qui se concrétise aujourd'hui par un guide d'application et ce colloque.

À l'instar des autres métiers de l'entreprise, le système d'information doit mettre en place un environnement de contrôle favorable, renforcer les dispositifs de maîtrise de ses activités, pour contribuer à la réalisation des objectifs de l'organisation. On sait que maintenant, le système d'information véhicule et diffuse les principes du contrôle interne dans toutes les activités de l'organisation. Et à l'évidence, c'est un outil de prévention de surveillance des risques et des défaillances.

J'ouvre une parenthèse. Nous avons adopté la même démarche avec l'Institut français des administrateurs (IFA). Dans quelques semaines, nous allons organiser un colloque sur l'audit interne et la gouvernance, ces questions étant de plus en plus à l'ordre du jour. Concernant la crise financière, je pense que les responsabilités étaient d'abord stratégiques ou politiques en matière de régulation, en particulier aux États-Unis. Nous devons, à notre échelon, mettre tout en œuvre, avec les pouvoirs politiques, européens et mondiaux, pour participer

à l'effort de régulation indispensable pour redresser une situation qui a totalement dérivé en quelques années.

Cette parenthèse étant fermée, je reviens à notre sujet. Les travaux entre le CIGREF et l'IFACI ont débouché sur un guide d'application, qui s'est voulu opérationnel. C'est un outil destiné à la fois aux responsables de systèmes d'information et aux auditeurs internes. C'est un travail de longue haleine, avec un engagement très fort de la part des personnes qui y ont participé, notamment Farid Aractingi qui a piloté la partie contrôle interne de la DSI, et Régis Delayat qui a piloté le contrôle interne du SI de l'entreprise. Je voudrais aussi saluer l'implication des délégués généraux : Jean-François Pépin et Louis Vaurs ; sans oublier les chargés de mission : Stéphane Rouhier et Béatrice Ki-Zerbo.

Le guide d'application va vous être maintenant présenté.

1 – Restitution des travaux des deux sous-groupes

1.1 - Le contrôle interne du Système d'information de l'entreprise

Régis Delayat, *DSI, Scor*

Nous allons faire avec Farid une présentation à deux voix. Nous allons restituer ces travaux qui ont occupé une vingtaine d'entreprises et une trentaine de personnes pendant quinze mois. Je vais d'abord vous présenter le contrôle interne du système d'information de l'entreprise, en tant qu'instrument du contrôle des activités, des métiers de l'entreprise. Farid enchaînera avec le contrôle interne de la DSI, de l'activité informatique des entreprises, et conclura.

Avant d'aborder le contrôle interne des systèmes d'information, il faut le replacer dans le contrôle interne général de l'entreprise dont il fait partie intégrante. Le contrôle interne de l'entreprise, on en parle beaucoup en ce moment. Je me suis essayé à reprendre un certain nombre d'extraits d'articles de presse ou de rapports qui parlaient du contrôle interne sur les quatre derniers mois. Quand on regarde tout ce qui se dit ou s'écrit aujourd'hui autour du rôle central que doit jouer le contrôle interne dans le bon fonctionnement des entreprises, et quand on entend combien les failles de ce contrôle interne expliquent la crise que l'on traverse actuellement, le constat est assez sombre. La tentation pourrait être de jeter le bébé avec l'eau du bain, alors qu'en fait, la crise actuelle est globale, systémique, et dans un tel environnement, le contrôle interne des entreprises était relativement impuissant. Pour autant, c'est vrai qu'il a révélé un certain nombre de failles. Il est donc important d'améliorer ces dispositifs de contrôle interne, de s'assurer qu'ils existent, qu'ils sont adaptés, qu'ils sont suffisants, qu'ils fonctionnent, qu'ils sont efficaces, pour le bon fonctionnement de l'entreprise.

Je vais juste extraire deux ou trois citations qui me paraissent importantes et lourdes de sens. "Il convient de repenser l'articulation entre régulation et surveillance, entre régulation et contrôle interne." Très certainement. "Il est important que chaque entreprise décline ces régulations et les exigences de ces régulations au sein de son activité, dans son contexte." "Trop de contrôle tue le contrôle." C'est une réalité. On a parfois poussé les choses trop loin, parfois fait preuve d'intégrisme dans le développement des contrôles au sein de l'entreprise. Il y a une proportionnalité, un côté raisonnable à respecter, en fonction des contextes. "Le développement d'une culture de contrôle au sein des entreprises" est un élément essentiel, parmi d'autres.

Nos travaux se sont inscrits dans le cadre de la charte CIGREF-IFACI qui a été présentée et signée en octobre 2007, elle-même faisant suite au cadre de référence AMF et à son guide d'application sur l'information financière diffusé en janvier 2007. Une lecture approfondie du cadre de référence AMF montre qu'il traite – surtout dans son guide d'application, quand il déroule les différents processus métiers qui contribuent à la production d'information financière – quasi en permanence de systèmes d'information : «Des dispositifs de sécurité physique et logique des systèmes et des données » ; on mesure tout ce que cela veut dire. « Des contrôles clés (bloquants, non bloquants, seuils d'alerte, rapprochements automatiques…) » ; on voit là aussi le sens que cela peut avoir dans le développement de nos applications. Derrière chacun des processus métier, il y a des systèmes d'information.

Convaincre les dirigeants des enjeux du contrôle interne et de la maîtrise des systèmes d'information au sein de l'entreprise, est bien l'objet principal de nos travaux.

Quels sont les objectifs poursuivis ? Une sensibilisation de tous les acteurs ; un enrichissement de la dimension système d'information du cadre AMF, en le reliant aux référentiels existants ; l'élaboration d'un guide d'application pratique, aussi concret que possible, avec des listes de bonnes pratiques. Nous nous sommes beaucoup appuyés sur les référentiels existants – Farid y reviendra très largement tout à l'heure –, CobiT notamment pour la fonction informatique.

Dans notre démarche, nous avons très vite identifié **deux sujets, deux parties complémentaires**. D'une part, **les métiers de l'entreprise**, avec pour chacun d'entre eux, les processus, les risques, les contrôles. D'autre part, **la DSI**, que l'on isole, mais qui est bien sûr un des métiers de l'entreprise, avec ses processus, ses risques, ses contrôles. L'ensemble compose le système d'information. Les deux grandes catégories de contrôle, baptisées contrôles généraux informatiques et contrôles applicatifs, sont produites grâce au système d'information.

Nous avons représenté l'entreprise comme une chaîne de valeur. Toute entreprise, quelle que soit son activité, définit une stratégie, conçoit ses produits, les fabrique, les vend, en assure le support, la maintenance, et bien sûr, gère et contrôle. Pour ce faire, elle s'appuie sur des ressources : un capital ; des éléments du capital immatériel ; ses salariés et ses savoir-faire ; ses processus ; et bien sûr son système d'information qui décline les différents processus. Elle s'appuie également sur un certain nombre de partenaires : actionnaires, fournisseurs, autorités de contrôle, marchés financiers, presse, lesquels jouent leur rôle dans le fonctionnement de l'entreprise.

Nous nous sommes basés sur l'identification des processus de l'entreprise. Nous les avons recensés, cartographiés, sans prétendre avoir été exhaustifs : processus de direction, processus opérationnels, processus de support, dont l'activité Informatique. Le système d'information irrigue l'ensemble de ces processus, l'ensemble de ces métiers et activités de l'entreprise. De même pour les risques : chaque entreprise doit avoir sa cartographie des risques. Nous les décomposons en trois grandes catégories : les risques financiers, les risques opérationnels, les risques de conformité. Le message est clair : il est indispensable de construire l'approche de contrôle interne sur l'identification des processus et des risques. Il est également important d'identifier les acteurs du risque, à chaque étape de traitement de ces risques. Les directions métiers sont propriétaires de leur système d'information, sont responsables de leurs risques et de leur contrôle interne, et de l'ensemble des étapes de traitement des risques.

Pour chaque processus, il y a identification des étapes – des sous-processus en quelque sorte –, **des acteurs, des risques et des contrôles à intégrer dès la conception des applications**. Nous avons ensuite réalisé une illustration de cette démarche sur trois processus communs à la majorité des entreprises : les achats, les ventes et la consolidation financière. Nous avons cherché en permanence à nous caler sur le cadre de référence AMF.

Le cadre de référence AMF, et notamment son guide d'application, identifie 14 processus d'entreprise qui contribuent à la production de l'information comptable et financière. Pour chacun de ces processus, le cadre indique un certain nombre de points d'analyse, de points de contrôle. Nous avons repris dans notre démarche le lien entre le processus et le point de contrôle AMF.

Quand on parle de développement de la mise en place d'un contrôle interne du système d'information de l'entreprise, il est important d'intégrer la composante de contrôle dès la conception d'une application, d'un nouveau système, quelle que soit la manière dont on va y répondre, que ce soit au travers d'un développement interne, au travers du déploiement d'une solution de marché. La dimension contrôle doit accompagner chacune des fonctions : réflexion sur les obligations du contrôle interne, identification des objectifs et des activités de contrôle, gestion des accès logiques, spécification des états de contrôle pour améliorer la surveillance des opérations, spécification des contrôles « embarqués » bloquants ou non bloquants, qui permettront d'automatiser un certain nombre de ces éléments de contrôle interne, et contrôles généraux IT sur lesquels Farid reviendra longuement.

Nous allons maintenant faire un gros plan sur le processus achats et les différentes composantes que l'on trouve dans le livrable. Nous avons représenté les sous-processus, et les étapes du processus achats. Deux étapes, asynchrones, sont détachées de la chaîne de commande : la recherche (référencement) des fournisseurs et la gestion des comptes fournisseurs. Les autres étapes sont : définition des besoins ; sélection des fournisseurs en fonction des besoins identifiés ; contractualisation et commandes ; réception et pilotage du fournisseur ; processus de paiement. Pour chaque étape, nous identifions les directions métiers, les acteurs impliqués : direction des achats, prescripteurs métiers, direction juridique, direction comptable… Nous identifions ensuite les risques associés à chacune de ces étapes : achats faits auprès de fournisseurs non autorisés, risques de dépendance, solidité financière non contrôlée, fraude, collusion… Etape suivante : nous relions les risques aux points de contrôle AMF. Pour la fonction achats, 11 points de contrôle ont été listés. Dernière étape : le rapprochement entre points de contrôle et exemples de contrôle. Nous avons identifié, pour chacun des points de contrôle AMF, un certain nombre de contrôles, la plupart pouvant être automatisés, embarqués dans une application achats, permettant de sécuriser le fonctionnement.

Le même exercice peut être réalisé pour l'ensemble des processus métiers de l'entreprise.

Claude Cargou

Je vais maintenant donner la parole à Farid Aractingi. Il est directeur de l'audit et du management des risques chez Renault depuis 2007.

1.2 - Le contrôle interne de la DSI

Farid Aractingi, *Directeur audit et management des risques, Renault*

En guise de préambule au contrôle interne de la DSI, j'ai repris une planche que nous avions présentée en juin dernier, à mi-parcours.

En effet, quand notre groupe d'experts « bénévoles », issus du CIGREF ou de l'IFACI, s'est réuni pour la première fois à la fin de 2007, nous n'avions sur la table, en guise de spécifications, que la charte CIGREF-IFACI. Si on la lit bien, on comprend que les objectifs sont :

- ✓ d'optimiser la coopération entre les fonctions audit interne et système d'information ;
- ✓ d'évaluer, par une approche systématique et méthodique, le processus de management des risques ;

- ✓ de formuler des recommandations aussi concrètes que possible.

Nous avons collectivement réalisé que le système d'information n'est plus une fonction de support quelconque, mais au contraire est devenu un processus opérationnel de l'entreprise, un métier global et transversal à toute l'entreprise, qui, du fait de sa complexité, est encadré par un certain nombre de référentiels existants. Ces référentiels, d'origine anglo-saxonne, nous avons voulu les respecter, en tout cas dans leur esprit, tout en les adaptant à notre contexte hexagonal.

Par ailleurs, notre souci a toujours été de produire un livrable concret, utile à la DSI et à l'audit interne. L'ouvrage comporte donc un nombre considérable de *flowcharts*, de « RACI » et de matrices, qui permettent à des auditeurs, des contrôleurs internes ou des informaticiens, d'y puiser une véritable valeur ajoutée pour leur travail quotidien.

La planche suivante présente notre démarche. Nous avons utilisé comme point de départ le référentiel CobiT, en identifiant 6 processus clés. Nous avons confié chacun des six processus sélectionnés à des binômes ou des trinômes d'individus faisant partie du groupe de travail – ce que nous avons appelé les sous-groupes. Chaque sous-groupe a travaillé de façon autonome, sachant qu'il y avait un pilotage bimestriel, et parfois mensuel, pour faire le point, créer un peu d'émulation interne, et recadrer les équipes.

Pour chacun de ces six processus, nous avons produit d'abord un *flowchart* ou ordinogramme, décomposant fonctionnellement l'activité en processus et sous-processus et décrivant leur interaction. Nous avons ensuite déterminé une matrice des responsabilités de type RACI, en prenant soin de préciser le Réalisateur, l'Approbateur final, les experts Consultés, et enfin les personnes ou les fonctions devant être Informées. Nous avons voulu en particulier distinguer entre la personne qui fait ou qui réalise, et celle qui, in fine, approuve – car la sémantique anglo-saxonne (R = Responsible, A = Approver) nous paraissait totalement occulter le réalisateur, ou le « doer » en américain.

Enfin, nous avons rédigé une matrice où pour chaque sous-processus, nous avons listé les objectifs de contrôle, risques, activités de contrôle, et meilleures pratiques.

Le résultat forme un guide opérationnel, mais pas une norme intangible : chaque entreprise, chaque administration publique, chaque entité, pourra l'adapter à son environnement. Je profite de ce que je viens de dire pour reprendre le titre global de ce guide : il comporte le mot *organisations* à la fin, car c'est « le contrôle interne du système d'information des organisations ». Nous avons eu un très long débat pour savoir s'il fallait mettre ce mot. Ne fallait-il pas dire simplement « le contrôle interne du système d'information » ? Fallait-il privilégier les entreprises, et appeler le guide « le contrôle interne du système d'information des entreprises », et oublier le contrôle interne des systèmes d'information de tout le secteur public ? Nous avons donc décidé, de façon consensuelle, grâce au mot « organisation », d'inclure tous ceux qui contribuent à la création de valeur en France, qu'ils soient dans le système marchand ou qu'ils soient dans le système public.

Les processus sélectionnés – et ceux qui ne l'ont pas été ! – forme le programme de la planche suivante. Nous avons choisi six processus :

- ✓ gestion des compétences – de la DSI s'entend,
- ✓ projet et développement,
- ✓ maintenance et gestion des changements,
- ✓ gestion des incidents,

- ✓ sécurité logique et accès physiques – et donc pas toute la sécurité physique,
- ✓ gestion de la sous-traitance.

Pourquoi ceux-là ? Parce que nous avons considéré qu'ils jouaient un rôle important, souvent essentiel, dans la gestion d'une DSI. Pourquoi d'autres n'ont-ils pas été retenus ? Nous avons certes eu de la peine à renoncer à certains processus qui nous paraissaient extrêmement importants, comme la gouvernance, et à l'alignement métier. Et aussi à ce qui va bien avec l'alignement métier, c'est-à-dire la planification de la DSI. Nous avons eu de la peine à renoncer aussi à la continuité d'exploitation. Mais si nous nous y sommes résolus, c'est pour de (bonnes) raisons matérielles. Nous avions une équipe finie en nombre, experte mais non professionnelle – au sens où elle était bénévole –, mobilisable pendant un espace-temps délimité : choisir de publier un document opérationnel en 2009, c'était donc pour nous renoncer à être exhaustif.

Permettez-moi quelques mots sur chacun de ces processus. Sur la **gestion des compétences**, nous avons distingué les compétences critiques des compétences clés. Nous avons considéré comme critiques les ressources essentielles au bon fonctionnement de la DSI, pour ce qu'elle veut conserver au cœur de son métier de DSI, comme processus clés. Et nous avons considéré comme clés les compétences critiques et rares sur le marché.

Sur le **projet et développement**, nous avons commencé par une partie concernant l'alignement métiers, c'est-à-dire ce qui va permettre réellement de définir les projets à développer dans leur perspective de valeur ajoutée ou de transformation par rapport aux enjeux des métiers opérationnels de l'entreprise – métiers opérationnels autres que ceux de la DSI. Une focalisation particulière est portée sur la gouvernance du projet en tant que tel et les normes de standardisation en matière d'architecture.

La **maintenance et la gestion des changements** ont été traitées dans un chapitre différent, car c'est bien un processus à part. Nous avons cependant utilisé le même *flowchart* que le processus de projet et développement, et je vous le présenterai en détail tout à l'heure. Tout ne s'applique pas évidemment sur la partie maintenance, tout ne s'applique pas non plus sur la partie projet. Nous avons retenu la maintenance, car bien que manquant de prestige, c'est quand même l'activité qui, dans la vie réelle d'une DSI, absorbe une très grande partie de son énergie et de son budget : cela consiste, quand même, à faire fonctionner et optimiser un patrimoine applicatif considérable.

La **gestion des incidents** est le point d'entrée, non pas des métiers, mais des utilisateurs finals. A l'intérieur de la DSI, c'est un processus transversal qui va alimenter, soit l'exploitation, soit la maintenance, soit le support aux postes de travail.

On ne peut pas faire du contrôle interne ou de l'audit de systèmes d'information sans parler de **sécurité**. C'est sur ce sujet qu'un auditeur informatique va commencer à acquérir sa compétence, et à s'aguerrir, et d'ailleurs c'est toujours sur ce thème que traditionnellement, sur une mission générale, un auditeur même non informatique trouvera de nombreux dysfonctionnements, quelle que soit l'entité auditée. Nous n'avons pas traité la totalité de la sécurité physique, par manque de temps, mais nous avons inclus toute la sécurité logique, c'est-à-dire la confidentialité, la disponibilité et l'intégrité, ainsi que les accès physiques et les autorisations d'accès.

Enfin, parce que c'est devenu un sujet de plus en plus important et aussi transversal que la gestion des compétences – vous pouvez le voir à travers les différents points d'interaction

entre processus –, nous avons choisi la **gestion de la sous-traitance**. Aujourd'hui, de plus en plus, la sous-traitance est fondée sur des objectifs de résultats, et son pilotage est donc une activité critique. Nous avons de plus particulièrement focalisé nos travaux sur les contrats pluriannuels, appelés aussi l'infogérance.

Les planches suivantes donnent un exemple de *flowchart,* celui des activités d'études (projet et développement, et maintenance et gestion du changement). On a commencé par la gouvernance en général, en particulier à travers les comités d'entrée de charge concentrés sur la question suivante : comment décider de faire, ou non, l'investissement. Ensuite vient le travail de développement, qui commence par les spécifications du côté maîtrise d'ouvrage et du côté maîtrise d'œuvre. Enfin, on termine par les tests et recettes, et, si tout va bien, la mise en production.

Tout cela implique un partage des meilleures pratiques, et nous en montrons un exemple à travers la matrice Risques, Contrôles, Meilleures pratiques du processus de gestion des incidents. Nous sommes donc partis du processus et des sous-processus, tels qu'identifiés dans les *flowcharts*. De façon assez classique, pour chacun des sous-processus, nous avons décrit les objectifs de contrôle, les risques associés, les activités de contrôle – qui sont parfois une réécriture de l'objectif de contrôle, mais parfois, au contraire, une information réellement distincte – et surtout les bonnes pratiques. Pour y parvenir, nous avons mis à profit l'expérience individuelle des contributeurs et celle des entreprises que ceux-ci représentaient dans le sous-groupe de travail, soit grâce à notre connaissance théorique, accumulée au fil du temps.

En guise de synthèse, je reprendrai quelques éléments déjà évoqués avant moi. Nous considérons que le contrôle interne du système d'information est un élément intrinsèque du contrôle interne (général) de l'entreprise ou de l'administration. Pourquoi ce travail spécifique sur le système d'information par rapport aux travaux généraux effectués par le groupe de place il y a deux ans ? J'espère vous en avoir un peu convaincu, ainsi que Régis Delayat : c'est la spécificité transversale du système d'information, comme sa technicité, qui justifient ce supplément spécialisé et très utile. D'ailleurs, dans de nombreuses organisations, il y a aujourd'hui des auditeurs informatiques spécifiques : soit dans un secteur d'audit informatique au sein de la direction de l'audit interne, soit même directement de petites équipes d'audit informatique au sein de la DSI – ce qui peut être considéré comme hérétique, mais ça existe, même dans une entreprise du CAC 40 ! Si tant d'organisations, d'entreprises, d'administrations ont considéré qu'il était indispensable, compte tenu de la complexité du sujet, de mettre en place un audit informatique spécifique dans ou à côté de l'audit interne « classique », c'est bien la raison pour laquelle nous avons rédigé un livre sur le contrôle interne du système d'information.

Cet ouvrage a aussi pour objectif de sensibiliser les dirigeants aux enjeux, et de fournir des pistes opérationnelles aux praticiens, qu'ils soient dans la direction de l'audit interne ou dans la direction des systèmes d'information, qu'ils soient contrôleurs internes ou utilisateurs du système d'information. Nous avons donc adapté le cadre de référence de l'AMF au système d'information. En tant qu'élément clé de l'excellence opérationnelle et du contrôle interne, le système d'information, in fine, est non seulement un objet du contrôle interne, mais aussi un moyen du contrôle interne.

Je terminerai en rappelant les cinq principes du contrôle interne.

- ✓ Premièrement, le contrôle interne n'est pas un sujet pour des spécialistes du contrôle interne déconnectés de la réalité opérationnelle. C'est un sujet qui doit d'abord être pris en charge par le management opérationnel : le premier acteur du contrôle interne, c'est le management. C'est à lui qu'incombe la responsabilité de le mettre en place, de même qu'il lui appartient aussi d'instaurer la culture et la dynamique du contrôle.
- ✓ Le contrôle interne doit être intégré dans les processus de l'entreprise, dans les gènes des processus de l'entreprise, aussi en amont que possible. Il est consubstantiel aux processus de l'entreprise.
- ✓ Les systèmes d'information jouent un rôle clé dans la mise en place d'un système de contrôle interne, car ils permettent d'embarquer, selon le jargon des DSI, les contrôles dès la conception des projets de transformation.
- ✓ Un principe de proportionnalité et de granularité doit s'appliquer, car on ne peut pas contrôler de façon exhaustive et tatillonne.
- ✓ C'est pourquoi, il faut toujours rester conscient de la non-exhaustivité du dispositif de contrôle et de ses limites. On ne peut pas contrôler tout, et le « «zéro risque » n'existe pas, et c'est à leur capacité de jauger des enjeux et des risques, et des mesures pour mettre ceux-ci sous contrôle, qu'on mesurera le succès des patrons qui réussissent – pas à la chance !

2- Le contrôle interne du système d'information, élément-clé d'une bonne maîtrise des activités

Table ronde animée par **François Renault,** *Président de l'AFAI, Associé Deloitte,*

avec

Pierlaurent Barbieri, *Directeur de l'audit interne groupe, Adecco*

Georges Épinette, *Directeur Général, STIME*

Marie-Noëlle Gibon, *Directrice Générale, Certinomis*

Patrick Lefas, *Conseiller-Maître à la Cour des Comptes*

François Renault

L'AFAI, dont je suis président, est une organisation de personnes intéressées dans l'identification, la promotion, la diffusion des meilleures pratiques autour du contrôle de la gouvernance des systèmes d'information. L'AFAI est la benjamine des associations représentées aujourd'hui puisqu'elle aura 27 ans au mois de juin prochain.

Cette jeunesse ne nous a pas dispensé de nous poser la question du contrôle interne il y a déjà assez longtemps, puisque nous avons écrit un document à la fin des années 1990 sur le contrôle interne et les systèmes d'information. Plus récemment, nous avons monté un groupe de travail pour le moderniser, et en juillet dernier, nous avons rédigé, avec un certain nombre de représentants d'entreprises, un nouveau document sur le contrôle interne et les systèmes d'information. Cette initiative s'est faite parallèlement à l'initiative CIGREF-IFACI. C'est vous dire si ces temps-ci, la convergence est forte entre les organisations, les institutions à l'échelon français mais également international, pour mettre plus de contrôle interne, une meilleure gouvernance dans les organisations, et constater que les systèmes d'information sont indispensables.

Le guide opérationnel réalisé par le CIGREF et l'IFACI arrive à point nommé. Très pragmatique, il incorpore les meilleures pratiques, comme le CobiT qui a été évoqué tout à l'heure. C'est une théorie qui a fait ses preuves, mais qui reste de la théorie. Quelle peut être la mise en pratique ? Pour le savoir, nous avons demandé à un certain nombre d' « entreprises » (dans les domaines des services, de l'industrie, du commerce, du secteur public) de venir témoigner ici.

Marie-Noëlle Gibon, directrice générale de Certinomis, était auparavant DSI de l'activité courrier de la Poste. Elle pourra donc apporter un double témoignage.

Georges Épinette, administrateur du CIGREF, est directeur général de STIME qui est la filiale informatique du groupement des Mousquetaires. Il pourra intervenir en tant que directeur général d'une organisation dans laquelle il est directement confronté avec les problématiques de contrôle interne des processus métiers de l'entreprise, et de ses propres processus métiers au sein de la DSI.

Adecco, société de services, est représentée par Pierlaurent Barbieri, directeur de l'audit interne groupe.

Patrick Lefas est conseiller maître à la Cour des comptes. Il est responsable de la certification des comptes de l'État.

Je passe la parole à Madame Gibon qui va nous parler de son expérience à la Poste.

Marie-Noëlle Gibon

Avant d'entrer dans le vif du sujet, je voudrais attirer votre attention sur le fait que le contrôle interne à la Poste n'est peut-être pas aussi vieux que la création de la Poste sous Louis XI, mais avant même que la Poste ne change de statut (en 1991), un certain nombre de personnes effectuaient des contrôles d'activité dans les établissements de la Poste : c'était les inspecteurs principaux circonscriptionnaires, les anciens du contrôle interne. Cette tradition et cette culture du contrôle interne sont prégnantes dans les organisations d'aujourd'hui. Il existe, au sein de la Poste, une direction de l'audit de groupe rattachée au président ; une direction des contrôles des risques qui rapporte au directeur général ; et cette organisation est répliquée au sein des métiers. En ce qui concerne la direction du courrier, il y a une direction du contrôle général et de l'audit.. Trois instances de gouvernance assurent le pilotage du contrôle interne au sein du Groupe La Poste : le comité contrôle interne du groupe qui regroupe tous les responsables de contrôle interne ; le conseil contrôle interne du groupe et de l'audit, qui suit les évolutions du système et du dispositif de contrôle interne ; le comité d'audit, émanation du conseil d'administration, et qui regroupe quatre administrateurs. Dans cet écosystème plutôt favorable, les DSI se sont sentis investis d'une mission qui visait à apporter leur contribution au contrôle des processus métier. C'est ce dont nous allons parler maintenant.

Nous avons mis en œuvre une démarche qui intègre la gestion des risques SI à la gestion des risques métiers. Quelles sont les préoccupations des DSI ? Gérer les risques dans la conduite des projets, gérer les risques concernant leurs propres entités, et enfin gérer les risques *business* que l'usage du système d'information fait courir aux métiers. Cinq objectifs sont poursuivis dans notre démarche appelée MRB, (comme Maîtrise des Risques *Busines) :* MRB est un dispositif de prévention qui doit permettre de systématiser l'évaluation de la criticité des processus métier et des ressources SI, clarifier le rôle des acteurs impliqués dans la gestion des risques SI, suivre les arbitrages et les risques résiduels non couverts, vérifier la mise en œuvre effective des dispositifs de réduction des risques retenus, et enfin organiser et adapter les systèmes d'information du courrier au regard de la criticité des activités métier. La finalité de la démarche MRB est de contribuer et de vérifier que les contrôles et les sécurités sont bien en place, et que les résultats des dispositifs sont bien atteints. Autrement dit, faire de la prévention en ce qui concerne l'utilisation du SI ; ce qui va nécessiter d'adapter l'offre de services informatiques pour répondre aux impératifs de la gestion de l'information véhiculée par les processus métiers. Ces derniers, en effet, s'appuient sur le système d'information pour fonctionner au quotidien, et satisfaire les objectifs de l'entreprise qui sont que ces activités fonctionnent en permanence et de façon optimale.

Quand utiliser MRB ? C'est une démarche, et la question est opportune. Il faut l'utiliser – c'est ce que nous avons préconisé au niveau des métiers – à partir du moment où le système d'information va traiter des informations pour lesquelles le manque de disponibilité, de confidentialité, d'intégrité, pourrait entraîner un grand nombre de contentieux ; ou serait susceptible d'empêcher la Poste de respecter ses obligations légales ; ou pourrait causer un

dommage financier supérieur à 100 000 euros, etc. Il convient d'utiliser cette démarche pour couvrir tous ces risques. Pour faciliter la tâche, la DSI a mis en place un questionnaire qui permet à un métier de mesurer l'éligibilité de son application par rapport à MRB, de savoir s'il doit entrer dans la démarche ou non. **Cette démarche s'articule autour de trois phases et six étapes**. **La première phase** est l'expression des exigences métiers. MRB s'appuie sur un processus documenté. Il y a trois acteurs majeurs : le métier, son représentant qui est la maîtrise d'ouvrage, et la maîtrise d'œuvre. Il est important, dans cette phase, de qualifier la sensibilité des processus métiers à l'usage des systèmes d'information et au regard d'un certain nombre de critères, qui sont les critères définis par CobiT sur le traitement de l'information : DICP, disponibilité, intégrité, confidentialité, preuve, auxquels se rajoute efficacité, évolutivité, conformité et fiabilité. C'est au regard de ces critères que l'on va définir l'information qui sera véhiculée dans les systèmes d'information pour faire fonctionner les processus au quotidien, le niveau de service exigé pour assurer une disponibilité à 100 %, une conformité par rapport au règlement de 100 %, etc. Ensuite, les métiers sont travaillés sur les risques et les événements pouvant avoir un impact sur leur processus.

Une fois ces exigences définies, on entre dans **la deuxième phase** qui consiste à répondre aux exigences des métiers. On va projeter la sensibilité des processus métier sur les ressources qui vont supporter l'activité au quotidien de l'entreprise. Les ressources sont les ressources au sens CobiT du terme : les installations, les technologies, les applications, les données et les hommes. On va évaluer cette sensibilité par rapport à l'information qui doit être véhiculée, et on va classifier les ressources système d'information. Ensuite, on va faire un état des lieux des dispositifs de sécurité et de qualité mis en œuvre pour chacun des huit critères dont nous avons parlé. On va évaluer le niveau de service offert pour le système d'information, pour chacun de ces critères, sur une échelle de 1 à 4. Et l'on va identifier les zones de risques résiduels, en mesurant les écarts entre le niveau de service exigé, tel que défini dans la phase 1, par les métiers, et le niveau de service offert par le SI.

La troisième phase ne sera pas la plus facile, même s'il n'y a qu'une activité. Il s'agit de décider et de choisir quel plan de réduction des risques mettre en œuvre, de définir ce que l'on va faire des risques résiduels : va-t-on les transférer ? Va-t-on prendre une assurance pour couvrir certains risques ? Va-t-on les refuser ? Va-t-on optimiser ces risques ou les accepter ? La phase importante est l'acceptation d'un risque résiduel que l'on ne va pas couvrir, de la part des métiers qui doivent les valider.

L'avantage de cette méthode est de structurer un dialogue entre l'ensemble des acteurs. J'ai parlé des acteurs métiers maîtrise d'ouvrage et maîtrise d'œuvre. Je voudrais citer les experts qui sont dans les pôles de l'audit, dans les pôles de la gestion des risques, dans le juridique, et qui vont apporter leur expertise dans la démarche et dans les différentes étapes de cette démarche. Si je résume, le métier exprime ses besoins, approuve le plan de réduction des risques, s'exprime sur les risques identifiés et valide les risques résiduels. La maîtrise d'ouvrage va réaliser tous les inventaires nécessaires, ce qui n'est pas une tâche aisée. Elle va notamment regarder, en termes fonctionnels, les incidents majeurs que ces processus ont connus, et le rôle du système d'information dans ces incidents, construire les plans d'action, assurer la cohérence de l'ensemble des métiers de l'entreprise. La maîtrise d'œuvre réalisera l'inventaire et la classification des ressources ; apportera son expertise dans l'analyse des risques techniques, et proposera le plan de réduction des risques. Chacun fournit des livrables.

Il est important que l'ensemble des acteurs soit sensibilisé, et il faut reconnaître que la Poste a mis tous les atouts de son côté. Il existe un site intranet dans le groupe sur le contrôle interne et la maîtrise des risques. Il existe un intranet pour l'activité courrier sur la partie du contrôle interne. Il y a enfin, à la DSI du groupe, un intranet sur les risques et le contrôle général.

Pour conclure, je reprendrais ce que disait Confucius, au VIème siècle avant J.-C. : « celui qui ne prévoit pas les choses lointaines s'expose à des malheurs prochains ». C'est pour cela que nous avons mis en place la démarche MRB.

François Renault

On voit que vous avez de la méthode et des outils. De manière opérationnelle, comment les métiers ont-ils reçu cette approche et comment faites-vous pour dialoguer avec eux ?

Marie-Noëlle Gibon

L'approche et la conversion ont pris un certain temps puisque nous avons mis à peu près un an pour élaborer l'ensemble du cycle et le pratiquer au moins une fois avec des métiers volontaires. Avant de généraliser cette méthode et les pratiques, la difficulté a été souvent le fait d'un manque de connaissance du lien entre l'information, les données et les besoins des processus. Nous avons mis en place, après quelques mois de pratique, un cycle de formation de trois jours, pour les métiers, afin de leur permettre de s'approprier la méthode, et de leur donner des outils pour faire le lien qu'ils ne faisaient pas naturellement.

Georges Épinette

Je me présente aujourd'hui comme Directeur Général de la STIME, et la STIME étant une SSII, je suis amené à aller de temps en temps sur les plates-bandes du système d'information. À ce stade, les préoccupations telles qu'elles ont été décrites ce matin sont vraiment les miennes. On va voir de quelle façon je peux les appréhender.

Il y a **quatre fondamentaux** pour moi :

- maintenir la pérennité des activités de l'entreprise ;
- assurer la protection, la sauvegarde du patrimoine, et la qualité de l'information ;
- veiller à l'application des directives du management ;
- favoriser l'amélioration des performances.

Avant de poursuivre, je voudrais souligner que dans la vraie vie, les deux derniers points, c'est-à-dire la directive managériale et les améliorations de performance, ne sont pas toujours exercés dans une logique positive. Il s'agit souvent de bon sens, qui doit dépasser la simple obligation réglementaire. On aura beau tout documenter, tout procédurer, le risque de faute humaine existera toujours, puisque c'est normalement l'homme qui pilote et maîtrise l'outil.

Les bénéfices, à la STIME comme partout ailleurs, passent d'abord par l'évaluation de l'application et de l'adéquation des procédures de l'entreprise. Optimiser ces procédures ainsi que les processus fonctionnels de l'IT à travers les gains de productivité à réaliser, cela veut dire que l'on aura préalablement identifié les processus et leur contrôle, et les

opportunités de réduction de coûts : il s'agit là de l'identification des réductions des coûts associés au dispositif de contrôle, tant au niveau des processus fonctionnels que des processus purement IT. Ces missions chez nous sont menées par un administrateur de processus. Cette fonction existait dans les directions métiers, mais pas dans ma SSII. Au final, il s'agit de disposer d'un contrôle interne adapté à l'entreprise, fiable, et au juste prix. Le juste prix, c'est de faire en sorte que le ratio de dépenses lié au contrôle soit raisonnable : ni trop ni trop peu. Cette notion de contrôle interne fiable et à un juste prix, prend toute sa mesure à travers l'automatisation d'un maximum de contrôles. Se pose tout de suite la question : faut-il tout cartographier ?

Le contrôle interne, ce n'est pas spontané. Du fait des contraintes qu'il engendre, il y a souvent des résistances à son application, même si au niveau managérial, la plupart des équipes sont d'accord pour en passer par là. Dès que l'on arrive dans les couches inférieures du management, c'est plus difficile. Chez nous, le contrôle interne se déploie essentiellement par une organisation des méthodes et des procédures. Une direction de l'organisation a été créée, qui est vraiment considérée comme le point-clé, le point d'entrée : ce sont les gardiens du temple. Il faut bien reconnaître que le personnel ignore souvent les méthodes et les procédures, et ce dans beaucoup d'entreprises.

A la STIME, il y a une fonction de risk manager, un RSSI, un administrateur et un gestionnaire de patrimoine applicatif. La connaissance des processus, des fonctions, peut se faire via par exemple un plan d'occupation des sols, une démarche d'urbanisation, et des applications comme la gestion du portefeuille applicatif. C'est vraiment indispensable dans le cadre d'une SSII, pour tirer les gains de productivité et la réduction des coûts attendus. Nous sommes actuellement en train de plancher sur une extension de ces thèmes à la cartographie des outils logiciels et des matériels du parc informatique. Pour faire cela, il faut connaître l'existant et savoir l'optimiser en le simplifiant, et en automatisant les contrôles.

Dans le cas particulier d'une SSII, le SI est à la fois l'instrument et l'objet du contrôle interne. Les exemples de gestion de mise en production et des évolutions applicatives, on les trouvera dans n'importe quelle organisation ; gestion de portefeuille applicatif ; gestion des relations contractuelles avec les fournisseurs, sur laquelle je m'étendrai un peu plus longuement. J'aurais pu vous parler de la gestion des compétences, sur laquelle nous avons beaucoup travaillé depuis quelques mois, dans le cadre d'une démarche de capital immatériel. Dans une gestion de mise en production, dans la gestion des changements, les failles se situent souvent aux frontières et il convient d'être attentif aux risques et à la jonction de plusieurs processus ; de même lorsque les applications transversales sont sous la responsabilité de plusieurs directions. Le dispositif LENA permet de contrôler le processus IT avec une vision de bout en bout de la gestion des changements. C'est là que se joue la fameuse séparation de fonctions entre les études et la production. Et nous avons une vision permanente et constante, avant, pendant et après le changement.

Un autre point délicat est la gestion du patrimoine applicatif qui comporte de grands enjeux. Il faut d'abord s'assurer d'avoir les bons interlocuteurs. On peut définir les endroits les plus pertinents pour cibler les contrôles sur les chaînes applicatives, par exemple lors des contrôles fiscaux. On explique le système d'information de manière simple aux parties prenantes, faisant ainsi gagner beaucoup de temps à tout le monde, et notamment aux commissaires aux comptes. Et sur cette gestion du patrimoine applicatif, on est en mesure de positionner des indicateurs et des restitutions de suivi et de contrôle.

Nous avons mis en place un système pour une meilleure gestion des relations contractuelles. Avec le référentiel eSCM, on va un peu plus loin dans la relation avec le fournisseur, en industrialisant le processus de suivi des contrats. Par exemple, en centralisant tous les contrats de la société, en ayant la possibilité d'avoir une vue globale sur l'activité contractuelle, en s'assurant de la capacité de tous les acteurs à répondre aux attentes, en analysant l'utilisation des processus de gestion des fournisseurs, leurs performances, et en lançant les alertes contractuelles : contrats qui arrivent à échéance, prestations non conformes. Ce système d'information fournisseur, propre à une SSII, peut être valable pour n'importe quelle entreprise, et permet d'entretenir une bonne gestion de la relation. Il permet à tous les acteurs internes de contribuer à l'enrichissement des informations, tout en disposant d'indicateurs aptes à rectifier la prestation, dès lors que celle-ci tend à déraper. La non maîtrise de ces relations est devenue un point de risque majeur pour l'entreprise, et donc un thème relevant du contrôle interne.

Sont suivis en permanence, l'alignement de la prestation par rapport au business, qui passe par deux points forts, la gestion de projet et la politique fournisseurs ; la gestion du risque ; l'analyse de la performance fournisseurs. Les comités de pilotage, les comités techniques, les comités stratégiques, font l'objet de comptes rendus prénormalisés, qui permettent d'entrer immédiatement dans une base de données et de pouvoir se référer à des actions, à des moments, à des temps forts qui ont marqué cette relation d'une manière directe. D'autre part, se déroule le cycle de vie contractuelle, avec la gestion des licences, tout ce qui concerne le suivi du contrat, les clauses de propriété intellectuelle, l'assurance, les responsabilités, les contentieux, et le suivi budgétaire. Tout cela permet de créer un véritable écosystème de la relation client-fournisseur, et d'être en mesure de montrer rapidement au contrôle interne comment l'ensemble est géré et contrôlé.

Dans le cycle des achats sept étapes sont concernées, selon les critères de l'AMF. J'ai regardé s'il y avait un *mapping* harmonieux avec le référentiel eSCM. Effectivement, l'utilisation du référentiel est un moyen pour le contrôle interne, et aussi pour les CAC, de vérifier très rapidement les pratiques en vigueur, avec toutes les mesures des risques prises via la mise en place des dites bonnes pratiques.

François Renault

Est-ce que la recherche permanente de la mesure du coût de la valorisation a un impact sur le contrôle interne. Est-ce qu'il a fallu démontrer une sorte d'héroïsme du contrôle interne aux maîtrises d'ouvrage au sein de l'entreprise ? Est-ce que l'on mesure l'efficacité en termes de coût du contrôle interne ?

Georges Épinette

C'est le grand débat, c'est notre leitmotiv au CIGREF. On voit que dans la crise, on tend à confondre trois notions, tout au moins chez les dirigeants. Ce sont les réductions des frais généraux, la création de valeur en tant que telle et l'amélioration de la performance. Ces trois notions sont mal comprises. La création de valeur nécessite un rôle d'éducation permanent, puisqu'on voit que, dès que l'entreprise est sous tension, tout ce qui concerne la création de valeur générée par les SI passe à la trappe du fait de la réduction des budgets. Quant à la performance, son amélioration, à mon avis, tient d'une part à l'environnement –

d’un ordinateur plus puissant qu’un autre, on dira qu'il est plus performant – d’autre part au processus global, où l'élément le plus faible tire en arrière la performance dudit processus. Ces trois notions sont à marteler auprès de nos dirigeants. Je m'y emploie mais ce n'est pas toujours simple.

François Renault

Je vais passer la parole à Pierlaurent Barbieri, responsable de l'audit interne groupe chez Adecco. Il est confronté à un système d'information qui évolue à grande vitesse. Il aimerait bien que le contrôle interne suive.

Pierlaurent Barbieri

J’explique rapidement ce qu’est Adecco et les différences de cette société par rapport aux autres sociétés ici représentées. De manière très générale, le « business model » d’Adecco est d' « acheter et de vendre » des heures de travail ce qui se traduit, d’un point de vue de contrôle, par l’absence de contrôles d'inventaire. Deuxièmement, en 2003 et 2004, Adecco a eu de gros problèmes aux États-Unis parce que les auditeurs externes n’étaient pas d’accord de certifier les résultats ; nous avons donc créé une structure basée sur SOX pour améliorer les contrôles. Chez Adecco, le management est troisièmement très jeune et le *Board of Directors* prend toutes les décisions importantes.

L’entreprise a grandi très rapidement en multipliant les acquisitions. Nous avons plus de 60 *brands*. En France, on peut en citer Adecco, Altedia, Adia et Datavance. Par conséquent, notre système informatique est très complexe et très décentralisé : chaque pays (*business unit*) a son système informatique. Ceci implique aussi qu’il est presque impossible de faire des audits standard ou des investigations sur les fraudes depuis le siège international.

Comme on le voit dans l’example, le Groupe Adecco possède quatre divisions opérationnelles qui utilisent quatre applications différentes de *front office*. L’objectif est la mise en œuvre de processus métiers « *front office* » standardisés et communs pour toutes les divisions ainsi qu’un système informatique unique pour les fonctions de facturation et de paiement (chose qui n’est pas si simple, notamment en période de récession mondiale).

Comme je vous l’ai dit auparavant, nous étions dans une structure de contrôles basés sur SOX aussi parce que nous étions côtés au NYSE. On s’y est délisté il y a deux ans, mais on reste listé en France et en Suisse.

Nos contrôles IT se basent sur *Control Framework*. On utilise par exemple *Records and Information Management*. Il y a d'autres contrôles plus liés au *Business Control*, c'est-à-dire les achats ou les ventes d’heures, et qui suivent les *Group Policies*.

SOX demandait si les *Group Policies* étaient appliquées ou pas appliquées, mais ne se préoccupait pas de la qualité des résultats Après ma nomination, mon premier objectif consistait ainsi dans la « restructuration » des contrôles en fonction des risques.

Au lancement de chaque projet - qui doit être approuvé ensuite par un *Steering Committee* où, au siège de la compagnie, par le CIO du groupe -, l’Audit Interne Group revoit l'organisation, la planification, la gestion des risques, la qualité, le contrôle des changements, etc.

Une fois le projet terminé, les recommandations de l'audit interne sont suivies. Ensuite, des revues sont effectuées à des points-clés, c'est-à-dire avant la signature du contrat, pendant la phase de conception (afin de s'assurer que les contrôles des processus métiers sont bien pris en compte) et durant la phase pilote (pour s'assurer que les contrôles informatiques généraux sont bien pris en compte).

François Renault

On voit que dans un univers éclaté, décentralisé, l'audit interne joue un rôle important dans la partie contrôle interne. Est-ce à dire que c'est l'audit qui est devenu propriétaire, maître d'ouvrage, responsable, garant, du contrôle interne ? Ou les métiers sont-ils aussi impliqués ?

Pierlaurent Barbieri

Pour l'instant, ce sont encore les différents pays qui font leurs contrôles de conformité. Nous allons ensuite vérifier que ce travail est fait. Dans l'avenir, tout passera par l'audit interne groupe. Aujourd'hui, je suis le responsable face à l'*Audit Committee* et au *Board of Directors*. C'est ma responsabilité de dire si les différents pays qui rendent compte au DAF local ont fait leur travail ou non.

François Renault

Nous allons maintenant quitter le monde de l'entreprise pour aborder le monde de l'Administration, avec une problématique de contrôle interne que Monsieur Lefas va nous décrire. C'est vrai que l'État a des structures de contrôle depuis très longtemps, et des principes de séparation de fonctions qui remontent à plusieurs siècles. L'État, ce sont aussi des systèmes d'information qui ont grandi chacun de leur côté, et Il est maintenant confronté à un véritable défi dont va nous parler Patrick Lefas.

Patrick Lefas

La matière du système d'information de l'État est extraordinairement variée et complexe. Le point de vue que j'ai choisi, c'est celui de mon métier en tant qu'observateur attentif des conditions dans lesquelles l'ensemble des administrations maîtrise les risques métiers, les risques financiers et comptables ; c'est un point de vue parmi d'autres.

Le système d'information financière et comptable de l'État : financière et comptable, sont deux objectifs tout à fait essentiels à distinguer. Chez nous, financier signifie budgétaire. Le Parlement vote les lois de finances, et il donne des enveloppes de crédit. Il faut s'assurer que ces enveloppes de crédit ont été exécutées conformément à l'ensemble des dispositions législatives et réglementaires, à commencer par la loi organique relative aux lois de finances (LOLF), qui est la constitution financière de l'État depuis 2001 ; et aussi conformément aux dispositifs réglementaires, puisque dans l'organisation de l'État, il y a une séparation stricte des responsabilités entre les ordonnateurs, ceux qui vont prendre la responsabilité de l'engagement de la dépense, et les comptables qui vont en vérifier la sincérité et s'assurer que l'ensemble des dispositions législatives et réglementaires ont été respectées.

Le système d'information pour l'État représentait un enjeu absolument essentiel, qui était d'être partagé, faute de quoi il n'est pas possible de restituer des informations en deux comptabilités : la comptabilité budgétaire, puisque c'est la manière de vérifier le respect des autorisations parlementaires, et la comptabilité générale ; c'est la nouveauté de la loi organique qui débouche sur un exercice de certification des comptes assumé par la Cour des comptes, collectivement. C'est une différence importante avec les commissaires aux comptes dans les entreprises, qui signent eux-mêmes, en tant qu'associés, leur rapport de certification. Chez nous, la démarche est collégiale et collective. On passe d'un système morcelé à un système intégré, avec un mot-clé qui est Chorus, dont vous avez certainement entendu parler. L'enjeu pour l'État, choisissant un progiciel de gestion intégrée, c'est de bénéficier de l'ensemble des avantages de cet outil, c'est-à-dire d'avoir son cœur comptable. Chorus est au centre du dispositif. Mais chaque ministère a de nombreuses applications, et à ces applications se rajoute l'application maîtresse qui est le tableau Excel ; en fait, beaucoup de choses se passent encore sur Excel, mais je crois que ce n'est pas une caractéristique de l'État.

L'objectif est bien d'unifier. Les applications étaient anciennes, et pas du tout adaptées aux dispositions de la loi organique. Il a fallu, après l'échec d'Accord 2 en 2004 – puisque l'appel d'offre a été annulé sur décision du ministre de l'époque, Nicolas Sarkozy –, bâtir en catastrophe un dispositif de remplacement en attendant de refaire un appel d'offre qui a donné lieu au projet Chorus, qui maintenant se déploie progressivement avec plus ou moins de difficultés. Mais au départ, des applications anciennes ont été développées en dehors d'une démarche de contrôle interne, ce qui ne veut pas dire qu'il n'y avait pas de contrôle ; il y avait un contrôle a priori, et pas du tout dans une logique de maîtrise des risques. Le dispositif comportait beaucoup de contrôles, souvent très redondants. Et comme les supports papier étaient dominants, les contrôles informatisés étaient très limités. On est donc face à un système qui ne fonctionne pas de manière optimale et il est évident qu'il faut progressivement le changer. Un des gros problèmes est la volumétrie considérable de la comptabilité générale de l'État, qui est de 40 millions d'écritures, là où un grand groupe comme EDF en fait 3 ou 3,5 millions. En outre, le pourcentage d'écritures manuelles reste très élevé, même s'il s'est substantiellement réduit du fait des efforts de la direction générale des finances publiques.

Pourquoi le Système d'information ne joue-t-il pas son rôle ? D'abord parce que le système n'est pas suffisamment intégré. Ensuite, parce qu'il n'y a pas de référentiels uniques et partagés ; or, c'est évidemment essentiel. Enfin parce que les outils de contrôle et de pilotage sont en fait très faibles. De ce fait, on en déduit qu'il n'y a pas de pistes d'audit facilement exploitables ; qu'il y a des retraitements manuels de données considérables, et que la bureautique est dominante, avec tous les avantages et les inconvénients qu'elle représente. On a donc des schémas d'écritures comptables non homogènes, point essentiel quand on cherche à bâtir une comptabilité de tiers. On n'a pas de base nationale tiers. C'est vrai aussi bien pour la gestion de l'impôt aujourd'hui – il y a 827 bases différentes – que pour la rémunération des personnels de la fonction publique et assimilés – plus de 2,5 millions de fonctionnaires – où il y a un éclatement de base. Et c'est vrai aussi pour la liquidation de pensions. Il est évident que ce sont des faiblesses considérables. On arrive à les pallier par des infocentres. Ça a été l'enjeu de l'infocentre INDIA LOLF. Mais ces infocentres sont des substituts. Il y a peu de contrôles automatisés, en tout cas pas suffisamment, et il n'y a pas

de lettrage des écritures ; retrouver des écritures dans des délais très cours est très compliqué.

D'où la nécessité de faire évoluer le système vers un système intégré. C'est l'objectif de Chorus, qui est de mettre en œuvre toutes les dispositions de la LOLF, donc d'introduire la logique de performance, qui n'existait pas préalablement. Maintenant, le budget de l'État s'exécute par programmes. L'objet est voté par missions, qui se décomposent en programmes, une mission formant une politique publique. Et chaque programme a une stratégie, des objectifs, des indicateurs. Tout ceci doit normalement être restitué au Parlement dans des rapports annuels de performances. C'est la première disposition. La deuxième, c'est de tenir une comptabilité générale digne de ce nom, de façon à ce que les comptes soient certifiés ; sincérité, régularité, fidélité des comptes de l'État.

Chorus devait apporter une amélioration du pilotage de la gestion publique, de bout en tout, étant un outil partagé. Il fallait aussi – et c'était, pour le certificateur que je suis, un enjeu essentiel – renforcer la traçabilité et l'auditabilité des données financières de l'État, et contribuer à la simplification des processus financiers. C'est une des raisons pour lesquelles Accord n'a pas correctement fonctionné : on n'avait pas fait le travail préalable de remise à plat des processus. On a donc été confronté à la nécessité de prendre un progiciel mais il fallait faire des développements spécifiques. Qui dit développements spécifiques dit nécessairement problèmes avec l'éditeur au bout d'un certain temps pour la version suivante, puisqu'il ne peut pas garantir la modification des développements spécifiques ; donc, cela coûte très cher et ce n'est pas performant.

Le choix qui a été fait avec Chorus était de dire : nous nous situons résolument dans le cadre d'un progiciel auquel nous adaptons des spécificités très limitées. Il y a très peu de développements spécifiques. C'est une force de la direction qui a piloté le projet jusqu'à présent, l'AIFE, de résister aux tentations de faire du spécifique. Mais en contrepartie, cela incitait à la remise à plat des processus, et donc à se poser les bonnes questions en matière de contrôle interne. Il fallait déployer l'ensemble progressivement dans l'ensemble des administrations. Nous avons commencé le 1er juillet 2008, et l'objectif est de terminer le déploiement en 2011. Le projet présente plusieurs avantages. D'abord, d'avoir, à l'échelon déconcentré comme à l'échelon central, le même outil, ce qui n'est pas le cas aujourd'hui : des administrations déconcentrées vont engager la dépense sur une application extrêmement ancienne, qui date du début des années 1980 et qui de ce fait, n'a pas les possibilités de raffinement qu'on peut avoir dans un progiciel de gestion intégrée. Ensuite, Chorus a vocation à remplacer le maximum d'applicatifs ministériels. Il faut bien dire que nous sommes un peu au milieu du gué. Comme il y a eu des retards dans les versions successives, les administrations ne veulent lâcher leurs applications que si elles sont sûres que l'application interministérielle aura les mêmes qualités, et même apportera davantage. Ce n'est pas encore définitivement acquis. Nous nous étions fixé comme objectif de supprimer une centaine d'applications ministérielles, et, pour le moment nous sommes autour de quatre-vingts. Remplacer les applications, renforcer les capacités de restitution et d'analyse, et plus largement rénover l'ensemble du système d'information, à une exception près : la recette fiscale ne fait pas partie de l'exercice. La recette fiscale dépend d'un autre projet, le projet Copernic, qui va donner lieu aux comptes uniques du contribuable, qui se met en place en fonction de la nouvelle organisation de l'établissement de l'assiette et du recouvrement pour l'ensemble des impôts. Mais Chorus comprend tout le reste : la dépense,

les recettes non fiscales et les différentes comptabilités : budgétaire, comptable, analyse des coûts, même si cette dernière n'a pas encore vraiment décollé.

Ces dispositifs doivent nous apporter, du point de vue de la certification, une meilleure auditabilité. Ils remplissent normalement toutes les fonctions prévues par la LOLF, et améliorent la qualité du contrôle interne. Ce contrôle interne s'est mis progressivement en place, sous la forte incitation du certificateur et du directeur général des finances publiques. Actuellement, on certifie les comptes de l'Etat avec des réserves assez lourdes, dont une réserve sur le système d'information et une réserve sur le contrôle interne. Le contrôle interne, progressivement, se déploie dans les différents ministères. Chaque ministère a maintenant une organisation du contrôle interne qui descend dans les services déconcentrés, avec une cartographie des risques, un plan d'action ministériel, qui se décline souvent en plans d'action par direction – les PAD, les plans d'action directionnels. De ce point de vue, les ministères financiers sont plus en avance que le reste de l'Administration. Le contrôle interne s'améliorera au fur et à mesure que les contrôles manuels seront remplacés par des contrôles bloquants, des contrôles généraux informatiques. Tout ceci doit se faire entre la maîtrise d'ouvrage et la maîtrise d'œuvre, de manière coordonnée, concertée, d'où l'importance du pilotage interministériel.

Le contrôle interne est bien au centre du système d'information, mais la route est sans doute encore longue. Tant que le projet Chorus ne sera pas complètement déployé, on sera sous l'empire de l'ancien système avec les inconvénients que j'ai décrits.

François Renault

Merci pour cette impressionnante présentation. On assiste là à une véritable révolution du système d'information. J'ai lu dans la presse que le projet Chorus était le plus gros déploiement de SAP à l'échelle européenne ; certains avancent même à l'échelle mondiale. On est face à un cas d'école extraordinaire. On voit que l'Administration est en train de déployer les meilleures pratiques en la matière. Cela s'accompagne d'une révolution culturelle. Pour vous, en tant que certificateur des comptes de l'État, j'imagine que l'impact de Chorus sur vos méthodes de travail pour cette certification va être très important.

Patrick Lefas

En tant que certificateur – sur la partie contrôle de gestion, retour sur investissement, c'est une autre problématique et ce n'est pas l'objet de la table ronde – il est essentiel de s'assurer de l'auditabilité, de la possibilité de pouvoir rapprocher facilement l'ensemble des fichiers ; d'avoir du lettrage, de disposer de tous les éléments afférents à la tenue d'une comptabilité générale moderne. Nous avons le souci de faire passer aux administrations le message qu'au travers de l'exigence de maîtrise des risques comptables, ce qui se joue, c'est la maîtrise plus large des risques. Et de ce point de vue, en accord avec la direction générale des Finances publiques, nous avons veillé à avoir une approche qui puisse marier la maîtrise des risques métiers et la maîtrise des risques comptables et financiers. Nous nous sommes référé au cadre de définition du contrôle interne.

Questions / Réponses

Claude Cargou

Nous allons maintenant répondre à quelques questions de la salle.

La première question concerne les différentes données traitées par les entreprises. Si les données qui sont structurées et traitées par les ERP, traitées dans des bases de données, semblent plutôt bien maîtrisées, que faites-vous dans vos entreprises pour toutes les données qui ne sont pas structurées, et que l'on retrouve dans des logiciels comme Excel, Access, Mail. Est-ce que vous avez des procédures, comment faites-vous pour les gérer, et quel genre de risques engendrent-elles ? A quel coût parvenez-vous à gérer ces données non structurées ?

Pierlaurent Barbieri

Nous avons plus de 200 systèmes et outils informatiques différents (Excel est l'un des plus importants). Nos résultats financiers sont publiés presque un mois après la fin du dernier mois considéré, parce qu'on doit rapprocher des données et effectuer les contrôles. Du point de vue du contrôle, on travaille avec les personnes qui gèrent les systèmes. La première chose que l'on fait est d'étudier ces systèmes informatiques et leur impact financier. Par exemple, s'il appartient à un pays qui réalise 0,2% du chiffre d'affaire du groupe, l'audit interne ne vérifie pas. Par contre, si dans un outil sont consolidés toutes les données, notre travail est de vérifier qui exactement peut mettre ses mains sur cet outil et comment sont traitées les données. Nous faisons ce genre de travail avec les auditeurs externes. A la fin de l'année, nos résultats et leurs résultats doivent donner à l'*Audit Committee* la certitude que tous les outils ont été utilisés correctement.

Patrick Lefas

Du point de vue de l'État, comme vous l'avez compris, il y a beaucoup de données non structurées. Dans des ministères aussi complexes que le ministère de la Défense, on travaille essentiellement sur des fichiers d'inventaire qui sont des tableurs Excel. Heureusement maintenant Excel a progressé, et on peut aller jusqu'à un million de lignes. C'est un peu mieux, mais cela reste très compliqué. L'élément clé, en présence de données non structurées, est d'être au clair sur l'organisation. Les données non structurées doivent se retrouver dans la cartographie des applications et dans la cartographie du contrôle interne. Ensuite, il faut que tout soit documenté, et que l'on puisse conserver les tableaux puisque ce sont des éléments de preuve ; c'est l'enjeu de la traçabilité : qui a fait quoi et où c'est stocké, ces éléments doivent être dans des dossiers de contrôle, qui d'ailleurs peuvent être informatisés. Aujourd'hui, en ce qui concerne l'Etat, on ne peut pas dire que l'on est à un seuil optimal.

Claude Cargou

Avec le développement des outils de gestion des risques, des logiciels de formalisation des processus, des modèles de contrôle interne et de toutes les couches qu'on est en train de

rajouter, ne risque-t-on pas de s'intéresser plus à la mise en œuvre des processus qu'à la substance ?

Marie-Noëlle Gibon

Si l'on s'intéresse à la mise en œuvre des processus, c'est bien. Par contre, si l'on pense que l'outil va résoudre l'analyse interne et le travail de "jus de crâne" qu'il faut faire, alors on fait fausse route ; de même si l'on pense que l'outil va sauver le système d'information.

Farid Aractingi

Excel n'a jamais transformé un individu qui n'est pas très bon analyste en excellent analyste. En revanche, un bon analyste va pouvoir utiliser Excel pour décupler, avec un véritable effet de levier, toutes ses capacités d'analyse. C'est également vrai pour tous les outils de gestion des risques et de cartographie des processus, et d'ailleurs pour tout ce qui est autour de la gouvernance, y compris la partie gestion de l'audit. L'outil permet de créer des références à peu près automatiques, depuis le processus vers le référentiel de contrôle interne, du référentiel de contrôle interne vers la cartographie des risques, depuis la cartographie des risques vers les plans de réduction de ces risques, ainsi que vers le plan d'audit, les missions d'audit, les recommandations d'audit, les plans d'action en réponse aux recommandations d'audit. Le système d'information, c'est un effet démultiplicateur, un levier de performance absolument considérable, mais la mise en place d'un système d'information ne se fait pas sans efforts.

Pierlaurent Barbieri

Je ne pense pas que la question soit : se mettre sur les processus ou pas ? Je suis convaincu que c'est mieux de passer du temps sur les processus que sur le système informatique. Tout dépend des données entrées dans les systèmes informatiques parce qu'à la fin, c'est comme disent les anglais : « garbage in – garbage out ». C'est donc le processus qui est important.

Régis Delayat

Il n'y a pas d'exclusivité entre la structuration de cette gestion processus/risques et la matière. Je pense que l'on a besoin de plus de structuration de ces cartographies de risques et de processus. On en a besoin parce qu'il faut rendre compte. On en a besoin pour nous rassurer sur le fait que tout est bien géré. Mais en aucun cas, cela ne doit empêcher de travailler sur la matière, sur le fond du besoin des métiers d'aujourd'hui et de demain.

Claude Cargou

Quelles sont vos bonnes pratiques pour gérer les risques liés à la sous-traitance, sachant que l'on a de plus en plus recours à la sous-traitance, et que l'on est souvent face à des sous-traitants de sous-traitants, auquel cas on risque de perdre le fil ?

Farid Aractingi

Les bonnes pratiques sont dans le guide. Toutefois, elles n'y sont peut-être pas toutes.

Marie-Noëlle Gibon

C'est bien parce que c'est un sujet majeur pour la plupart des DSI, qu'a été créé le référentiel ISCM qui vise à définir les bonnes pratiques entre un client et un fournisseur, sachant qu'il n'y a pas de bons fournisseurs si le client est mauvais. Et pour que le client soit bon, il faut qu'il ait mis en place chez lui une réflexion sur la nécessité ou pas de sous-traiter. L'avantage de ce référentiel qui a été développé par l'université de Carnegie Mellon, c'est de mettre chacun en face de ses responsabilités, pour faire en sorte que les objectifs que l'on s'est fixés soient tenus. Et pour les tenir, un certain nombre de bonnes pratiques sont définies, et, parmi elles, celles qui relèvent de la gestion des risques liés à la sous-traitance. Il y a 95 bonnes pratiques pour les clients et 84 pour les fournisseurs. On aborde bien cette problématique de gestion des risques, puisqu'il y a un avant, un pendant, et peut-être un après.

Régis Delayat

La sous-traitance au sein des DSI est de plus en plus encadrée. Tout se fait très souvent dans le cadre d'un référencement d'un certain nombre de fournisseurs partenaires à qui, de plus en plus, on impose un contrat – on a au moins réglé les aspects contractuels – un contrat interne SCOR pour ce qui nous concerne. Tout cela avant l'engagement des missions. Ensuite, quand on engage les missions, on détermine un certain nombre de standards internes auxquels doivent se conformer les prestataires, les fournisseurs que l'on fait intervenir. Le respect de ces standards est contrôlé et fait partie de la responsabilité des chefs de projet et de leurs équipes, qui intègrent des prestataires. On fait très largement appel à la prestation. A la SCOR, à titre d'exemple, on n'a quasi aucune force de développement. On capitalise sur nos forces de conception. On considère que c'est là que l'on apporte de la valeur à l'entreprise, parce qu'au-delà de la compétence pour mener des projets et de la compétence informatique, on apporte aussi de la compétence métier. Nos chefs de projets, a priori – et c'est ce qu'on veut – sont de bons interlocuteurs pour les métiers. Par contre, les forces de développement, on les trouve sur le marché du service et bien sûr, cela impose de définir très précisément l'encadrement dont je parlais.

Farid Aractingi

On peut ajouter quelques bonnes pratiques. Il y a le fait de faire des revues de performance du fournisseur régulières a posteriori ; l'analyse du niveau de dépendance de l'entreprise et du fournisseur l'un par rapport à l'autre ; le fait (quand on fait de l'infogérance) de faire des exercices de fin de l'infogérance, de reprise de réversibilité ; le fait (quand on fait de l'infogérance), si l'on pousse au maximum le partenariat et que l'on confie tout à un seul fournisseur, de se retrouver dans une situation où l'on est un peu dépendant, car quitter ou changer devient un exercice difficile. Et il y a une *best practice* que tout le monde connaît qui est de ne pas lancer une prestation avant d'avoir signé le contrat ; mais tout le monde a déjà lancé des prestations sans avoir signé des contrats.

Claude Cargou

Une question concerne la localisation géographique ou hiérarchique des auditeurs informatiques. Est-ce qu'il vaut mieux, pour le contrôle du système d'information, avoir des auditeurs informatiques dans la direction des systèmes d'information ou à l'intérieur de la direction de l'audit interne ?

Farid Aractingi

Au nom de l'indépendance, nous considérons que le lieu où doivent se trouver tous les auditeurs, y compris les auditeurs informatiques, c'est dans une direction aussi centrale que possible de l'audit interne. Compte tenu de la complexité des sujets, je crois qu'il est très important qu'il y ait un alignement métier ; puisqu'on a parlé d'alignement métier en ce qui concerne la DSI, il faut qu'il y ait un alignement au niveau de la direction de l'audit interne. Notre choix a été de créer des secteurs d'audit par métier de l'entreprise Renault. L'un d'eux est le secteur d'audit informatique. Il organise des réunions, au minimum trimestrielles, avec la direction des systèmes d'information, pour pouvoir comprendre au mieux les enjeux.

Patrick Lefas

Pour l'État, le principe est le même. Les auditeurs internes sont tous au même endroit. Nous avons le souci que l'audit interne soit implanté partout, dans tous les ministères, avec une dimension d'audit informatique. Et du point de vue de l'audit externe, de la certification des comptes de l'État, nous travaillons de plus en plus en mettant en équipe les auditeurs informatiques et les auditeurs financiers. C'est absolument indispensable parce qu'il y a une telle imbrication entre les processus métiers, les problématiques comptables et les problématiques d'audit des systèmes d'information, que l'on gagne énormément de temps, que l'on optimise le diagnostic, à travailler en équipe. Dans tous les grands cabinets d'audit, c'est ce vers quoi l'on va.

Claude Cargou

L'acceptation des risques ne relève-t-elle pas de la gouvernance de l'entreprise plutôt que des seuls métiers ?

Marie-Noëlle Gibon

Tout dépend de quels risques il s'agit. C'est pour cela que les plans de management de risques sont faits au niveau des entités. En outre, il y a un plan de management des risques du groupe, avec toute une échelle de risques que l'entreprise doit couvrir. Mais on ne peut pas couvrir tous les risques, les coûts seraient prohibitifs. Donc, il faut choisir, et choisir, c'est renoncer.

Régis Delayat

On l'a dit en présentant le rapport, on ne peut pas s'intéresser à tous les risques. On ne peut pas imaginer de pallier la totalité des risques. On est obligé de choisir, et bien sûr, les choix se font en fonction des enjeux que représentent ces risques pour l'entreprise. Là encore, c'est le fruit d'un dialogue entre les métiers et la direction des risques groupe. Mais, il est important de savoir qu'on ne pourra pas tout traiter et qu'il faut choisir.

Patrice Lefas

La réponse est bien aux deux niveaux. Il est essentiel d'avoir un pilotage au niveau des directions générales. Chez nous, ce sont les secrétaires généraux des ministères qui ont le pilotage, de façon à veiller à ce que les cartographies des risques reflètent bien la totalité des risques auxquels le ministère est confronté. C'est une matière évolutive, et une information très éclatée, avec les niveaux d'éclatement qui dépendent de l'organisation. Le ministère de l'Éducation nationale est par essence même complètement déconcentré. C'est au niveau des rectorats, des inspections d'Académie et des universités que tout se joue. Des ministères plus petits sont beaucoup plus concentrés. Le reporting doit être piloté par le sommet, avec un travail d'animation sous la responsabilité du secrétaire général. Et je pense qu'il est essentiel que ceci donne lieu à l'établissement d'un document annuel. De ce point de vue, les bonnes pratiques prévoient la production d'un rapport de contrôle interne. L'État, depuis 2006, établit un rapport de contrôle interne dont on espère que progressivement, il va se démultiplier dans chacun des ministères.

Pierlaurent Barbieri

Je dépasse un peu la limite franco-française. Selon le droit suisse, chaque société cotée doit faire un Entreprise Service Management. Il n'est pas du ressort de l'audit, mais du CFO. Toutefois, il est clair que le plan d'audit doit en tenir compte. En revanche, je ne vois pas comment – pour dépasser la partie IT traitée ici – l'audit pourrait auditer la sécurité environnement. Personnellement, je ne peux que m'assurer que les règles soient appliquées, mais je ne pourrai jamais savoir si elles sont bonnes ou pas.

Claude Cargou

Le guide existe en français. Existera-t-il en anglais ?

Envisagez-vous de balayer les autres processus des systèmes d'information dans la suite de vos travaux ?

Vous avez bien indiqué avoir eu du mal à renoncer à certains processus et vous avez notamment cité l'alignement stratégique et la planification. Écarter ce processus ne risque-t-il pas de privilégier le court terme au détriment de l'évolution moyen-long terme des systèmes d'information dans les organisations ?

Farid Aractingi

C'est vrai que le choix a été extrêmement difficile. J'ai eu beaucoup de mal à abandonner le sujet de la gouvernance. Il a été assez difficile d'abandonner gouvernance et alignement métier, alignement stratégique. Ce qui finalement nous a permis malgré tout d'y renoncer,

c'est le fait qu'il est explicitement mentionné, dans la page introductive du processus : projet et développement. Dans l'introduction, on dit : "afin de garantir l'alignement stratégique des projets sur les métiers, la politique informatique et sa déclinaison en plans stratégiques doivent être décrites et communiquées, et les projets priorisés selon leurs enjeux, investissements et risques, par un comité de gouvernance, avant d'être lancés." Certes, ce n'est qu'une phrase introductive. Il n'empêche que jusque dans la façon dont on a décrit le processus et ses sous-processus, on a tenu à rappeler l'existence de ce comité de gouvernance qui est au niveau de la direction générale, puisque la direction générale doit se positionner par rapport à où elle gère, sauf pour ceux qui ont la chance d'avoir des systèmes d'information dont le budget est porté par la business unit et non pas de façon centrale. Sauf pour ceux-là, dès lors que le budget est tenu pour l'ensemble de l'entreprise, il faut que l'entreprise puisse se positionner en conséquence. Cela dit, compte tenu du fait que nous sommes en plein dans la crise, je crois qu'il y a beaucoup d'entreprises – la mienne en fait partie – dans lesquelles, de facto, on est en train de faire ce qu'il faut faire pour pouvoir être vivant dans un an, et non de se positionner sur ce qu'il conviendra de faire dans dix ans. C'est la réalité d'aujourd'hui. Quand nous serons sortis de la crise, nous repenserons à des problèmes plus stratégiques.

Régis Delayat

L'alignement stratégique recherche l'adéquation entre les besoins de l'entreprise et le système d'information. Nous y avons travaillé au sein du sous-groupe de travail qui s'est occupé du contrôle des processus métiers. Quand on décrit les processus, quand on décrit les risques associés, on traite bien sûr ce qui existe, mais on traite aussi ce qui devra exister demain pour sous-tendre le développement de l'entreprise.

François Renault

Pour le guide en anglais, la question reste en suspens. Je pense qu'il y aura une discussion ultérieure sur ce point.

Claude Cargou

Je passe maintenant la parole à Gérard Rameix.

Discours de clôture

Gérard Rameix, *Secrétaire Général, Autorité des Marchés Financiers*

Mesdames, Messieurs, je voudrais vous dire mon très grand plaisir de participer à ce colloque, et la grande responsabilité que vous m'avez confiée en me demandant de le clore. Je remercie pour leur invitation les présidents de l'IFACI et du CIGREF, Monsieur Claude Viet et Monsieur Bruno Ménard. J'ai été très sensible au fait qu'il y avait, dans le travail très important qui a été présenté ce matin, une filiation directe avec des travaux auxquels j'ai eu l'occasion de participer, et même de lancer quelque peu, avec le groupe de place dont je parlerai tout à l'heure. Le travail présenté ce matin comble pour partie une lacune, puisque les travaux du groupe de place (le référentiel) avaient été relativement sobres sur le sujet majeur des systèmes d'information.

Je ne peux, en toute rigueur, parler ici en tant que secrétaire général de l'AMF puisque je ne le suis plus depuis quelques jours. Je suis en ce moment conseiller, pour quelque temps, auprès de mon successeur, et je rejoindrais la Cour des comptes au début du mois d'avril. Néanmoins, depuis onze ans et demi, à la tête des services de la COB, puis de l'AMF, j'ai beaucoup traité des questions de la qualité de l'information financière sur les marchés, et vu, tant en temps réel, lors des opérations financières, tant à l'occasion d'enquêtes, à quel point la qualité des contrôles internes des entreprises était importante pour le marché. C'est pourquoi je souhaiterais, non pas ajouter à tout ce que les techniciens vous ont dit très clairement, mais profiter de la clôture de ce colloque pour retracer les grandes étapes de cette soudaine accélération de l'histoire qu'a connue le contrôle interne depuis quelques années en France.

Il faut se reporter aux scandales financiers du début des années 2000, survenus principalement lors de l'éclatement de la bulle aux États-Unis, avec en particulier la trop célèbre affaire Enron, qui concernait, de mémoire, la 7e capitalisation mondiale, qui a perdu toute sa valeur en très peu de mois, mais aussi avec des grandes sociétés françaises de médias ou de télécommunications, dont les comptes ou l'activité ont été d'un seul coup remis en cause. Tous ces événements ont montré que quelques dérives pouvaient aggraver dans l'esprit du public un à-coup conjoncturel qui à l'époque était déjà tout à fait sévère, et provoquer une perte générale de confiance du public dans les marchés financiers, détruire de la valeur, peser sur la croissance économique. C'est cette situation qui a débouché aux États-Unis sur la loi Sarbanes-Oxley, communément appelée SOX, et sur la Loi de Sécurité Financière (LSF) d'août 2003 dans notre pays. L'une, l'américaine, très exigeante et coûteuse, aux dires de ceux qui l'ont pratiquée, obligeant les dirigeants des sociétés américaines à multiplier les *due diligences*, les engagements de responsabilité personnelle, les attestations d'auditeurs externes pour garantir la conformité de leur système d'information et de leur contrôle interne en matière financière et comptable. L'autre, la nôtre, plus pragmatique, plus progressive, mais fondée sur le même constat, qui était alors nouveau, de la nécessité d'une implication au plus haut niveau de l'entreprise sur les sujets de contrôle interne. Avant d'aller plus loin, je souhaite d'emblée écarter un doute majeur qui a d'ailleurs été évoqué à plusieurs reprises, en particulier par Monsieur Ménard si je me souviens bien, à propos des événements que nous vivons. Certes, nous devons nous interroger de façon approfondie sur les raisons qui ont fait que cette priorité donnée au contrôle interne dans plusieurs pays majeurs depuis 5-6 ans, n'a pas permis d'éviter la crise des *subprimes*, celle de ces produits structurés surnotés, qui sont devenus subitement incessibles parce que sans marché et sans

personne pour les acheter ; celle aussi des scandales Madof et Stanford. Il y a là un paradoxe. Ce n'est pas mon propos aujourd'hui d'apporter ni même d'esquisser une réponse à ce sujet. Mais je veux dire clairement qu'il faut résister à la tentation du fatalisme, à celle qui consisterait à jeter le bébé avec l'eau du bain et à considérer que cette démarche de contrôle interne est devenue inopérante et qu'on peut l'abandonner, l'alléger, ou la remettre au second plan des préoccupations. Ma conviction est exactement inverse. Certes, il faut centrer les procédures sur l'essentiel et non les multiplier pour se donner bonne conscience ou pour se protéger juridiquement, ce qui est toujours une tentation. Mais l'idée de base qu'il faut évaluer ses risques, définir une politique permettant de les gérer, diffuser dans toute l'entreprise une culture de contrôle interne, de respect des règles, d'utilisation de reporting précis et fiable ; l'idée aussi qu'il faut, au plus haut niveau de l'entreprise, s'assurer de la culture que l'on diffuse et de la bonne coordination de l'ensemble des acteurs du contrôle interne, ces idées restent pour moi essentielles. Elles ont déjà produit des résultats malgré ce qu'on peut penser dans le pessimisme ambiant d'aujourd'hui, et elles doivent être un des fils directeurs pour sortir de la crise actuelle et restaurer un peu de confiance. Et de ce point de vue-là, j'ai été heureux de voir que c'était le sentiment qui semblait vous animer.

Si l'on refait un peu d'histoire, en 2003, notre législateur a exigé que le président du Conseil d'administration, ou de surveillance, rende compte dans un rapport joint au rapport de gestion, des conditions de préparation et d'organisation des travaux du Conseil, ainsi que des procédures de contrôle interne mises en place par la société. Cette même loi a demandé que les commissaires aux comptes présentent dans un rapport joint à leur rapport général leurs observations sur ce rapport du président, pour celles des procédures du contrôle interne relatives à l'élaboration et au traitement de l'information comptable et financière. Ni la loi ni les travaux parlementaires préparatoires ne définissaient alors cette notion de contrôle interne qui était nouvelle dans notre corpus législatif, même s'il était déjà utilisé par beaucoup de praticiens. L'obligation nouvellement posée de faire un rapport soumis à l'œil critique des commissaires aux comptes et au regard de l'ensemble des investisseurs, et donc susceptible de provoquer des réactions de marché, constituait alors un redoutable défi pour les dirigeants d'entreprise. Cette obligation, d'abord énoncée de façon générale, fut très vite concentrée sur les sociétés cotées. Dès la promulgation de la loi, l'AMF prend l'initiative de mettre en place un premier groupe de réflexion pour assister les émetteurs et les commissaires aux comptes pour la première application de ces obligations. Ceci aboutit à la publication en 2004 par l'AMF de simples orientations, qui permettent aux émetteurs de connaître les modalités de publication des informations prévues par la loi, et surtout à la publication par les associations représentatives des émetteurs, l'AFEP et le MEDEF, de premières lignes directrices, mais qui étaient à l'époque très générales, pour aider les premiers rédacteurs des rapports. A la différence des Américains, nous avions prévu une application immédiate de ces dispositions dans la loi française. Parallèlement commençait à s'ouvrir un débat de fond qui allait nous occuper quelques années, sur la question de savoir si ce type de rapport peut rester purement descriptif ou s'il doit comporter des éléments d'évaluation. Ce débat semble un peu dépassé aujourd'hui, avec la transposition de la directive sur l'audit qui nous a conduit à imposer au comité d'audit de s'assurer de l'efficacité des systèmes de contrôle interne et de gestion des risques. Petite précision : l'ordonnance prévoit que c'est au comité d'audit de s'assurer du suivi et de l'efficacité de ces systèmes de contrôle interne et de gestion des risques, mais on n'a pas modifié les termes de la loi sur la manière dont le président doit rendre compte. Toutefois, nous avons tendance à l'AMF à considérer que la transparence n'est pas neutre, qu'elle doit avoir un

impact vertueux sur la mise en place ou l'application des règles. Et nous avons toujours rappelé qu'un émetteur était tenu par les règles générales à communiquer au marché des défaillances ou des insuffisances graves de contrôle interne, et donc maintenant de la gestion des risques, qui auraient été révélées par une évaluation, et tout particulièrement lors de la préparation de ce rapport.

Vous le voyez, même si les textes évoluent un peu, et dans le bon sens, ma philosophie personnelle n'a pas changé. J'ai toujours considéré que ce débat sur le caractère évaluatif ou descriptif était un faux débat. Lorsqu'on instaure une obligation légale d'une telle portée, rendre compte publiquement des procédures de contrôle interne, quand on voit tout ce que les spécialistes que vous êtes mettez derrière, on a forcément pour objet de permettre au marché, à l'ensemble des analystes, des investisseurs ou des futurs investisseurs, de disposer d'une information responsable sur le fait de savoir si l'entreprise cotée est ou n'est pas dotée de procédures opérationnelles de contrôle interne, correspondant plus ou moins à ce qu'on peut appeler l'état de l'art. Ce qui ne veut pas dire – car il y avait dans ce débat des considérations juridiques importantes – que tout chef d'entreprise s'engage de façon absolue sur la fiabilité du système, et d'une façon telle qu'il puisse être jugé responsable de toute défaillance. Vous avez à plusieurs reprises rappelé ce matin – et vous avez raison – que tout système de contrôle repose sur un certain arbitrage, qu'il repose sur la qualité des données prises en compte, et qu'il ne saurait en aucune façon constituer une sorte d'obligation de résultat. La seule manière qui nous a paru bonne pour sortir de ce débat un peu stérile, était de chercher à se doter d'un référentiel de place autour duquel pourrait s'ordonner la présentation des procédures demandées.

C'est pourquoi l'AMF a pris l'initiative de rassembler les différents acteurs, émetteurs, auditeurs internes, auditeurs externes et nous, les régulateurs, en vue d'élaborer un référentiel à l'usage des sociétés françaises soumises à cette obligation légale. La démarche est d'emblée pragmatique. Nous sommes au début 2005 ; la recherche du consensus, la prise en compte de la très grande hétérogénéité des sociétés cotées, vont primer sur la sophistication technique. Dans le même temps, les spécialistes, sous l'égide en particulier de l'IFACI et de Louis Vaurs, apporteront un cadre méthodologique et veilleront à la rigueur de notre démarche par rapport aux techniques de contrôle interne, à la qualité des concepts utilisés, mais ils admettront que la situation ne se prête pas à chercher véritablement à bâtir ce qu'on peut appeler un référentiel complet. Le produit final sera plutôt un cadre de référence exprimant les principes généraux de la démarche de contrôle interne, complété par deux annexes comprenant un questionnaire relatif au contrôle interne comptable et financier, et un autre questionnaire sur l'analyse et la maîtrise des risques ; nous avons tenu – certains partenaires étaient un peu réticents sur cette approche – à les insérer. L'ensemble fournit une excellente base pour une démarche progressive de l'amélioration de leur contrôle interne par des entreprises très diverses dans leur taille, les risques de leur activité, et leur degré de maturité en matière de contrôle interne. Cette démarche est aussi parfaitement compatible avec le référentiel COSO que certains émetteurs cotés français sont obligés d'appliquer, ainsi qu'avec les 4e et 7e directives européennes. C'est pourquoi je tiens particulièrement à saisir l'occasion de cette séance de travail pour rendre hommage à ce groupe de travail, dont les travaux ont duré deux ans. Ils ont été parfois longs et difficiles, mais ils ont finalement débouché sur un outil qui a rencontré l'adhésion d'un grand nombre d'émetteurs et les a véritablement incités à s'engager dans une démarche dynamique d'amélioration de leurs procédures. Il faut saluer les présidents de ce groupe, Jean Cédelle et

Guillaume Gasztowtt, Michel Léger qui a présidé un sous-groupe très important, les équipes de l'AMF, celles de l'IFACI. Je crois que tous ceux qui ont travaillé à cette époque – on a un peu de mal à s'en rendre compte aujourd'hui – ont réalisé une œuvre tout à fait positive.

L'autre apport de l'outil ainsi construit, c'est de permettre une plus grande homogénéité des concepts sous-tendant la rédaction des rapports – c'était l'objectif modeste mais important que nous avions fixé au départ –, et de faciliter la lecture pour les investisseurs. Preuve en est qu'aujourd'hui, dans le dernier rapport que nous avons établi à l'AMF sur les rapports de contrôle interne, plus de 73 % de l'échantillon étudié déclarent se référer au cadre de référence AMF, les trois quarts l'utilisant comme référentiel exclusif, et les autres en complément du COSO. Parallèlement, 84 % des sociétés de l'échantillon, contre 60 % et 34 % les années précédentes, précisent dans le rapport qu'elles inscrivent leur dispositif de contrôle interne dans le cadre d'une amélioration continue, dans des termes plus ou moins précis. C'est massif pour les grandes entreprises qui sont dans le compartiment A d'Euronext, mais c'est à 70 % pour les petites et moyennes, qu'on appelle maintenant les VaMPs dans notre jargon. 47 % des sociétés de notre échantillon précisent avoir réalisé au cours de l'exercice une évaluation de leur procédure, et pour 70 %, il s'agit d'une évaluation menée en interne. Il y a certes des disparités dans ces chiffres, puisque la plupart des sociétés font simplement état des différents plans d'action menés par la direction de l'audit interne, alors que d'autres soulignent la mise en place d'un processus spécifique d'évaluation. Mais au final, l'évolution générale est positive et montre une volonté des émetteurs d'aller plus loin dans leur réflexion. Et l'on voit que les entreprises – et c'était notre but en tant que régulateur, et le but du législateur – ont compris qu'il ne s'agit pas là d'un simple exercice de conformité, mais bien d'une démarche active de progrès dans la maîtrise de leurs risques.

Les dernières évolutions législatives, avec la transposition de plusieurs directives européennes à la fin de l'année dernière, ont confirmé la pertinence des orientations qui avait été prises par le groupe de place, puisque aujourd'hui la démarche s'étend à la gestion des risques, qui devient une dimension explicite, alors qu'elle ne l'était pas auparavant. On comprend ainsi que le législateur confirme sa conception d'un cadre global de contrôle interne, qui appréhende l'ensemble des risques susceptibles d'affecter l'entreprise, même s'il invite les émetteurs à détailler plus précisément pour le marché financier les procédures relatives à l'élaboration et au traitement de l'information comptable et financière. Pour compléter cette démarche, le comité d'audit fait son entrée officielle dans notre droit des sociétés, à l'occasion de la transposition de la directive sur le contrôle légal des comptes. Il est très important qu'en sus de ses attributions classiques en matière d'information financière ou de contrôle des comptes, le comité d'audit soit explicitement chargé de suivre l'efficacité des systèmes de contrôle interne et l'efficacité de la gestion des risques. On a là je pense une réponse partielle, ou même de principe, très importante, à certaines des questions qui ont été posées. L'entreprise au plus haut niveau, par son management, par son comité d'audit qui a une certaine indépendance, une responsabilité directe, doit mettre en œuvre cette politique. Bien entendu, elle ne peut pas appréhender tout dans le détail. Mais les principaux risques et les principales procédures doivent être calés au plus haut niveau du management.

Au total, je crois qu'on peut dire que par petites touches successives, notre pays, qui était réputé cultiver une certaine conception régalienne du chef d'entreprise, le tout puissant PDG, a mis en place les éléments d'une gouvernance plus équilibrée, plus responsable et

plus soucieuse surtout de rechercher un équilibre entre d'un côté l'initiative, l'innovation, la recherche du résultat, qui sont des dimensions majeures de l'entreprise, et l'appréhension et la maîtrise des risques. Certains penseront peut-être que tout cela est bien mais que ce n'est pas l'essentiel, que les temps que nous vivons appellent des remises en cause plus radicales du système d'économie de marché globalisé dans lequel nous vivons. Et bien sûr, les sujets ne manquent pas : le marché de crédits non régulés pour des dizaines de trillions de dollars qui s'est développé dans une certaine forme de liberté, tenant presque de l'anarchie ; les centres *off shore* ; les *hedge funds*, pour n'en citer que quelques-uns, qui sont évidemment à traiter au plan international pour restaurer un système financier plus stable. Mais je tiens à réinsister sur le fait que les sujets de gouvernance et de contrôle des risques sont des sujets de longue haleine, qui impliquent une mobilisation continue des acteurs et que les faire passer pour secondaires alors que tant reste à faire serait une grave erreur. C'est pourquoi, pour revenir sur les échanges que vous avez eus ce matin, votre initiative de compléter, d'approfondir, de travailler spécifiquement sur les systèmes de contrôle et de remontée de l'information me paraît tout à fait importante et opportune. Je crois que votre travail – je l'avais déjà constaté à la lecture, j'en ai été encore plus persuadé en vous écoutant – s'articule parfaitement avec la démarche de régulation et la démarche législative. Je ne saurais donc trop vous encourager à accentuer ces travaux de réflexion entrepris sur les systèmes d'information qui sont au cœur de tous les processus métiers, et qui irriguent bien sûr toute l'organisation de l'entreprise. Et je suis sûr – et je vous engage à le diffuser – que le guide opérationnel d'application que vous avez bâti va constituer un outil supplémentaire, qui va s'ajouter au cadre des références pour les entreprises qui avancent dans cette démarche de contrôle interne.

Voilà quelques réflexions que je voulais partager avec vous. Je profite de l'occasion pour remercier tous les participants de ce groupe de travail, et singulièrement l'IFACI, son président et son délégué général, pour l'appui qu'il a apporté aux régulateurs, en articulation parfaite entre les entreprises et les commissaires aux comptes, pour nous faire avancer globalement sur ces sujets, et pour nous fournir une base dont l'immense mérite a été, encore une fois, de permettre à chacun, à son niveau, de pouvoir y trouver une démarche de progrès. Je n'ai qu'un vœu, c'est que vous poursuiviez sur d'autres thèmes, par exemple sur la gestion des risques.