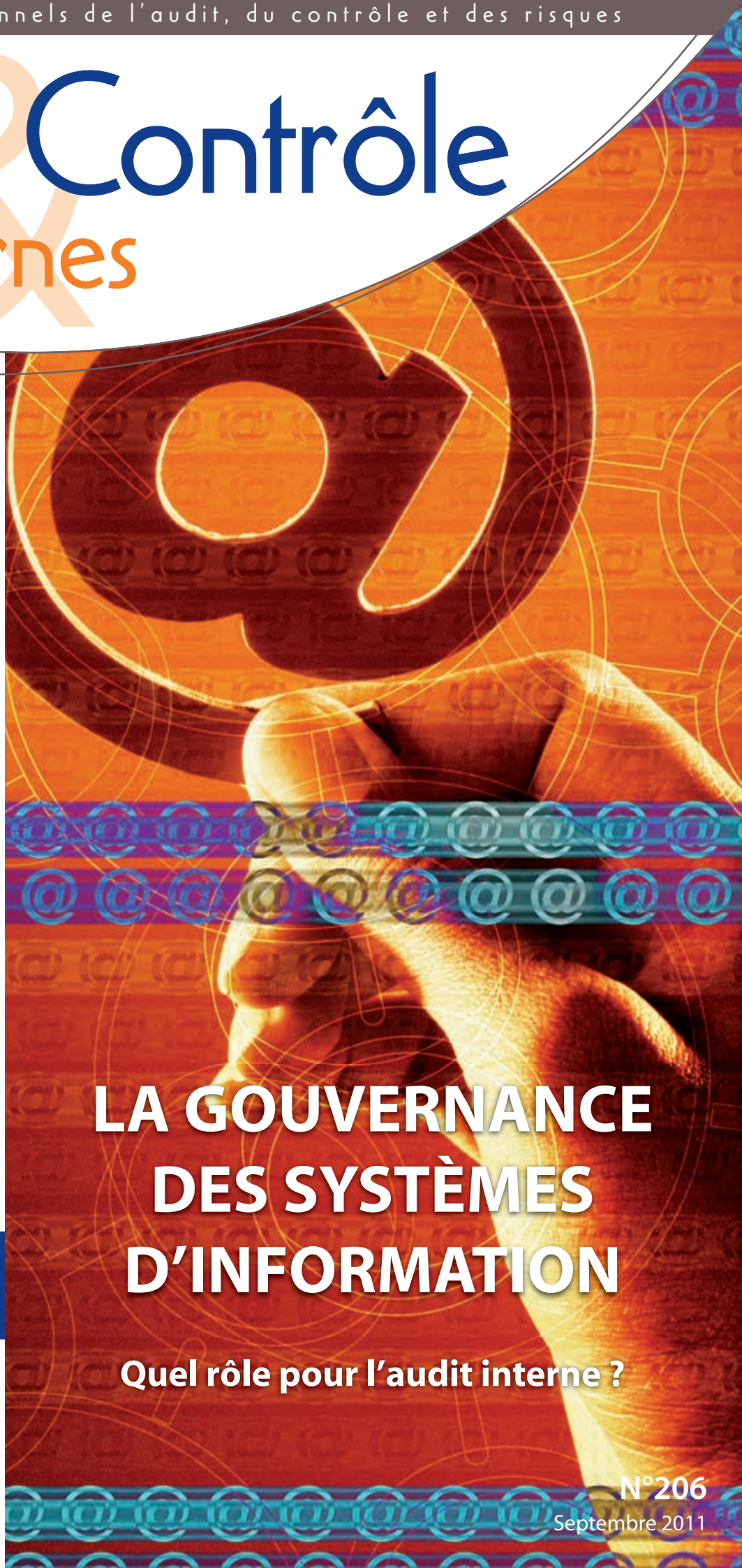
la revue des professionnels de l'audit, du contrôle et des risques

Audit & Contrôle internes



LA GOUVERNANCE DES SYSTÈMES D'INFORMATION

Quel rôle pour l'audit interne ?

ifaci
institut français de l'audit et du contrôle internes

N°206
Septembre 2011

Les Trophées du Contrôle Interne

Face aux nombreuses failles révélées ces derniers mois, il est indispensable pour les grands groupes de se doter d'un dispositif global de gestion des risques et de contrôle interne performant : un dispositif au service des opérationnels pour faciliter la prise de décision, protéger l'entreprise, et garantir l'atteinte de ses objectifs.

Les lauréats 2010

Aussi, cette nouvelle édition des **Trophées du Contrôle Interne**, organisée par l'IFACI et le cabinet de conseil BearingPoint, a pour objectif d'analyser et de récompenser le **meilleur dispositif global de Gestion des Risques et de Contrôle Interne.**

Pourquoi participer ?

- Pour comparer votre degré de maturité à plus de 300 entreprises, **en répondant à l'enquête en ligne***, et pour bénéficier d'une analyse et d'un panorama des grandes tendances sur le sujet.
- Pour concourir aux Trophées venant récompenser les meilleures pratiques et facteurs clés de succès de votre entreprise.
- Pour échanger avec vos pairs lors d'une soirée de prestige.

4 Trophées seront décernés par un jury d'experts au cours d'une cérémonie qui se tiendra le **8 décembre prochain** à l'hôtel George V (Paris) :

- Meilleure démarche de cartographie des risques.
- Meilleure démarche en matière de contrôle interne.
- Meilleure contribution de l'audit interne.
- Grand Prix du Jury.

** Les directeurs de l'audit interne, du contrôle interne, de la gestion des risques seront contactés par courriel pour participer à l'enquête en ligne. Cette enquête (20 minutes environ) nous permettra de présélectionner les projets qui seront soumis au jury chargé d'élire les lauréats des Trophées.*

Pour tout renseignement, contactez Aurélia Le Bour (alebour@ifaci.com - Tél. : 01 40 08 48 12)

ifaci
institut français de l'audit et du contrôle internes

BearingPoint. Management & Technology Consultants

Audit & Contrôle internes

La revue des professionnels de l'audit, du contrôle et des risques

n°206 - septembre 2011

EDITEUR
Institut Français de l'Audit et du Contrôle Internes (IFACI)
Association Loi 1901
98 bis, boulevard Haussmann
75008 Paris (France)
Tél. : 01 40 08 48 00
Mel : institut@ifaci.com
Internet : www.ifaci.com

DIRECTEUR DE PUBLICATION
Claude Viet

RESPONSABLE DE LA RÉDACTION
Philippe Mocquard

RÉDACTEUR EN CHEF
Louis Vaurs

RÉDACTION - RÉVISION
Jean-Loup Rouff - Béatrice Ki-Zerbo

SECRÉTARIAT GÉNÉRAL
Eric Blanc - Tél. : 01 40 08 48 02
Mel : eblanc@ifaci.com

RÉALISATION / PUBLICITÉ
EBZONE Communication
32, avenue de Beauregard
94500 Champigny-sur-Marne
Tél. : 01 48 80 00 56
Mel : ebzone@ebzone.fr

IMPRESSION
Imprimerie de Champagne
Rue de l'Etoile de Langres - ZI Les Franchises
52200 Langres

ABONNEMENT
Elsa Sarda - Tél. : 01 40 08 48 04
Mel : esarda@ifaci.com

Revue bimestrielle (5 numéros par an)
ISSN : 2117-1661
CPPAP : 0513 G 83150
Dépôt légal : septembre 2011
Crédit photos : © Fotosearch

Prix de vente au numéro : 22 € TTC

Ce document est imprimé avec des encres végétales sur du papier issu de forêts gérées dans le cadre d'une démarche de développement durable.

ifaci
institut français de l'audit et du contrôle internes

Pour une bonne efficience de l'audit interne

Pour être efficient, l'audit interne ne doit se complaire ni dans une profonde thébaïde qui le déconnecte de la vie de l'organisation, ni dans ses certitudes à même de décrédibiliser à tout jamais la fonction.

Rouage essentiel du bon fonctionnement de l'organisation, l'audit interne doit y être parfaitement intégré et s'y sentir pleinement légitime. Il doit, pour ce faire, connaître le ou les métiers de l'organisation, bien se coordonner avec les fonctions qui lui sont proches et répondre aussi bien que possible aux attentes de ses parties prenantes.

Ces objectifs sont au cœur des préoccupations de l'IFACI. Citons à titre d'exemples :

- prise de position d'octobre 2008 « L'urbanisme du contrôle interne : Comment en améliorer l'efficacité ? Quelle place pour l'audit interne ? » ;
- cahier de la Recherche (avril 2010) « Pour un urbanisme de contrôle interne efficient » dans le secteur bancaire ;
- premiers trophées du contrôle interne et de la gestion des risques réalisés avec Bearing Point (décembre 2010) ;
- prise de position IFA (Institut Français des Administrateurs) / IFACI (avril 2009) « Le rôle de l'audit interne dans le gouvernement d'entreprise » ;
- colloque du 14 septembre 2010 « 4ème, 7ème et 8ème directives : impact des recommandations de l'AMF pour les entreprises et les acteurs du contrôle interne » ;
- colloque du 17 mai 2011 « Risk managers, auditeurs internes… comment les acteurs du contrôle interne contribuent-ils ensemble à la valeur ajoutée des organisations ? ».

Dans le cadre d'un partenariat signé en octobre 2007 entre le CIGREF (Réseau des grandes entreprises utilisatrices des systèmes d'information) et l'IFACI, un premier groupe de travail mixte a publié deux ans plus tard un imposant document ayant pour titre « Le contrôle interne du système d'information des organisations : guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne ». Tout récemment, un deuxième groupe de travail comprenant cette fois-ci des représentants de l'AFAI (Association française de l'audit et du conseil informatique) a publié au premier semestre 2011 un « Guide d'audit relatif à la gouvernance du système d'information ». Ce guide a été présenté lors du colloque du 23 juin dernier. Vous trouverez dans ce numéro la retranscription de quelques bonnes pages de ce colloque.

Vous y trouverez également un article sur le « *cloud computing* » dont on parle beaucoup ces temps-ci. Le journal Les Echos du 21 septembre dernier annonçait d'ailleurs que l'Etat investirait 135 millions d'euros dans l'alliance française pour le *cloud computing*, société qui sera créée le 1er novembre prochain entre l'Etat, Orange, Thales et Dassault Système. ●

Louis Vaurs - Rédacteur en chef

ifaci Certification

La Certification par l'IFACI : la bonne pratique d'évaluation externe de l'Audit Interne

La Certification IFACI, régulièrement mentionnée dans les rapports du Président sur le Contrôle Interne, atteste que les activités d'Audit Interne sont conduites conformément aux Normes Professionnelles Internationales et contribuent à créer de la valeur ajoutée.

La Certification IFACI permet à l'Audit Interne :

- de **légitimer l'évaluation interne**, indépendante et objective, qu'il délivre sur l'efficacité des systèmes de gestion des risques et de contrôle interne ;
- de souligner sa capacité à **délivrer des prestations de qualité** et donc à **apporter de la valeur** à son organisation ;
- de **renforcer la confiance** que les parties prenantes placent en lui.

« L'Audit Interne est une profession très organisée, qui a mis en place des dispositifs de certification et de formation. Il convient de tirer vers le haut d'abord les administrateurs, mais aussi d'encourager les partenaires du Comité d'audit à enrichir et à améliorer constamment leurs pratiques. Tout ce qui permet de ***renforcer le professionnalisme*** *des uns et des autres va certainement dans la bonne direction. »*

Daniel Lebègue, Président de l'Institut Français des Administrateurs

« Je pense que l'Audit Interne doit présenter constamment un niveau élevé de professionnalisme : cela passe normalement par le respect de ses propres règles et standards de pratique, puis par une certification qui ***rend compte de manière objective de ce respect.*** *»*

Guylaine Saucier, Présidente du Comité d'Audit, Danone *(DAI certifiée en 2009)*, Areva *(DAI certifiée en 2006)*

*« L'évaluation externe objective et méthodique de l'Audit Interne, par des personnes qui disposent d'une vue d'ensemble professionnelle, est une démarche extrêmement précieuse. Dans ce monde tellement changeant, bénéficier des avis et conseils du certificateur est un facteur d'****augmentation de la capacité et de la qualité de travail*** *de l'Audit Interne. »*

Alexandre Lamfalussy, Président du Comité d'Audit, CNP Assurances *(DAI certifiée en 2008)*

« J'ai demandé que les auditeurs certificateurs nous présentent leurs conclusions sur notre Audit Interne pour deux raisons. Tout d'abord, nous avons souhaité entendre ce qu'ils avaient identifié sans biais et sans filtre. Nous avons aussi voulu apprendre ce qu'ils pensaient de ***la qualité et de la profondeur des audits*** *: ce sont des choses que je ne peux voir que très indirectement. »*

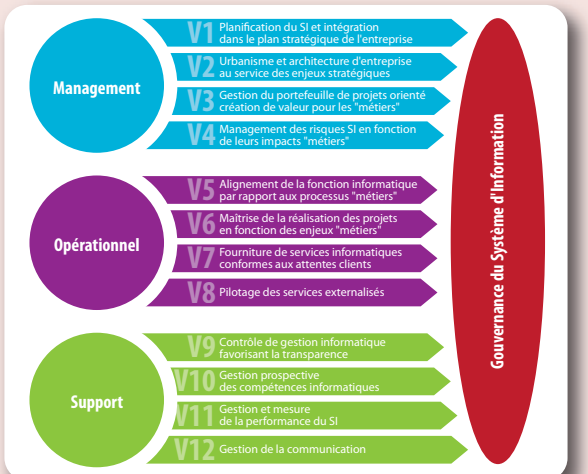
Hervé Saint-Sauveur, Président de LCH Clearnet SA *(DAI certifiée en 2008)*

« Le Comité des Comptes a toujours examiné avec attention l'activité de l'Audit Interne. Mais comment s'assurer que les méthodes utilisées et l'organisation retenue sont parfaitement adaptées ? La Certification par l'IFACI a été choisie, d'un commun accord pour répondre à cette question. Cette procédure a engendré pas mal de travail, mais nous a également beaucoup apporté. Enfin, si tant est que j'en avais besoin, ***la Certification m'a tranquillisé.*** *»*

Bruno Flichy, Président du Comité des Comptes, EIFFAGE *(DAI certifiée en 2007)*

IFACI Certification - 98 bis, boulevard Haussmann - 75008 Paris
Contact : Jean-Baptiste Gamas - Tél. : 01 40 08 48 10 - Mel : jbgamas@ifaci.com

SOMMAIRE



Risques commerciaux : Que nous apprend la crise des subprimes ?

Antoine de Boissieu - Associé-gérant, **OSC Solutions**

Plusieurs banques, surtout américaines, sont actuellement accusées d'avoir trompé leurs clients sur les produits qu'elles leur ont vendus ces dernières années, notamment lors de la crise des subprimes.

Paradoxalement, un auditeur ou contrôleur interne qui aurait fait une analyse des risques en 2007 aurait pu conclure que ce type de risques était peu probable. Trois éléments semblaient en effet aller dans ce sens :

1- Un secteur réglementé et surveillé

Le secteur bancaire est particulièrement réglementé et contrôlé. Des fonctions de contrôle interne, de conformité, de gestion des risques, y existent depuis longtemps et sont obligatoires. On estime qu'elles regroupent 1 à 1,5% des effectifs totaux, soit largement plus que dans n'importe quel autre secteur d'activité. Ces directions et leur fonctionnement sont de plus audités tous les ans par les autorités de tutelle. On pouvait donc penser que, dans ces conditions, les banques n'avaient pas la possibilité de vendre massivement des produits financiers en trompant leurs clients sur leur niveau de risque véritable.

2- Un audit interne indépendant

Les faits concernent en majorité des banques obligées par la loi d'avoir une direction de l'audit interne rattachée au comité d'audit (issu du conseil d'administration). On pouvait penser que l'audit interne aurait identifié ce type de risques et aurait pu les évaluer correctement. Apparemment, 6 à 7 ans après les affaires Enron et Worldcom, plusieurs grandes directions de l'audit interne n'ont pas su correctement identifier un risque majeur. A moins que les comités d'audit de ces banques n'aient volontairement pas réagi.

3- Un intérêt évident à ne pas prendre ce type de risques

La banque est un secteur où la fidélisation du client est un axe essentiel de la stratégie ; le but d'une banque n'est pas de vendre un produit, mais de fidéliser le client pour lui vendre, sur la durée, l'ensemble des produits dont il peut avoir besoin. Pour cela, l'image de marque, la respectabilité, la confiance du client sont des éléments essentiels. On pouvait donc penser que ce secteur était particulièrement enclin à la transparence vis-à-vis de ses client et que la hiérarchie, à tous les niveaux, était particulièrement vigilante face à ce type de risques.

Ces trois éléments se sont avérés insuffisants. Quels sont donc les facteurs de risque qu'il aurait fallu prendre en compte pour corriger cette première appréciation ?

1- Un contexte particulier

L'analyse ci-dessus est vraie de manière générale, dans des conditions normales. Le risque s'est cependant matérialisé dans des **conditions exceptionnelles :** les prix de l'immobilier avaient augmenté fortement pendant plusieurs années, beaucoup plus vite que le pouvoir d'achat des ménages, et la situation des marchés s'était brusquement dégradée, ou menaçait de le faire.
Les risques ont également concerné un type de produits **spécifique** (des produits structurés, adossés à des créances hypothécaires), et relativement **nouveau** à l'époque.

2- Des pratiques généralisées

Le mouvement a sans doute été amplifié parce que les banques incriminées ont considéré que le risque était acceptable puisque les autres banques faisaient pareil. Il est ainsi probable que les principales banques actives aux Etats-Unis savaient que leurs consœurs dissimulaient des informations sur leurs produits structurés. On imagine mal en effet que 17 banques aient eu en même temps l'idée de mentir à deux de leurs principaux clients (Freddy Mac et Fanny Mae) sur la qualité des crédits immobiliers auxquels étaient adossées les obligations qu'elles leur vendaient. Ce mimétisme a sans doute donné une fausse impression de normalité et de sécurité.

3- Des bonus extrêmement élevés

Les dirigeants des banques avaient annoncé des niveaux de profits élevés. De l'atteinte de ces résultats à court terme dépendait le versement de milliards de dollars de bonus aux dirigeants et cadres des grandes banques. Cette pression pour l'atteinte des résultats a sans doute poussé certaines lignes hiérarchiques à prendre des risques pour garantir l'atteinte des objectifs à court terme.

Quels sont les enseignements que peuvent en tirer auditeurs et contrôleurs internes ?

1. Le contexte reste primordial pour l'analyse des risques. Une analyse des risques valable un ou deux ans plus tôt peut être complètement dépassée. Il faut donc être très prudent avant de réutiliser tels quels des référentiels d'audit ou des cartographies des risques.

2. Les risques se sont matérialisés sur des produits spécifiques et relativement nouveaux. Les auditeurs et contrôleurs internes doivent donc bien auditer et contrôler les spécificités et les nouveautés.

3. Le fait d'avoir un dispositif de contrôle interne formalisé, audité, certifié, ne suffit pas pour maîtriser les risques. Ces dispositifs peuvent multiplier les contrôles de conformité sur des points de détail, mais très mal couvrir certains grands risques. L'audit interne conserve donc tout son rôle dans l'évaluation du dispositif de contrôle interne, notamment en s'assurant que les risques les plus importants y sont bien envisagés et couverts.

4. L'environnement de contrôle interne est essentiel pour l'analyse des risques. L'audit et le contrôle interne doivent vérifier qu'il n'y a pas une pression excessive pour atteindre les résultats, et envisager la possibilité que le montant des bonus distribués incite une ligne hiérarchique à prendre des risques inconsidérés. Dans le cas présent, ils auraient dû faire leur analyse des risques en en tenant compte, et se concentrer sur les dispositifs de contrôle capables d'empêcher ces éventuelles dérives. ●

Saisies immobilières

Plusieurs grandes banques américaines sont visées par une enquête en cours, les soupçonnant de n'avoir pas respecté les procédures de saisies immobilières. Les saisies se sont multipliées depuis la crise des subprimes. Les analystes estiment le montant probable des amendes à **20 milliards de dollars.** Indépendamment du volet financier, **14 banques** américaines ont déjà accepté de modifier leurs procédures internes.

Obligations garanties

17 banques sont poursuivies par la Federal Housing Finance Agency, organisme public américain, qui les accuse d'avoir dissimulé des informations sur le niveau de risque des obligations garanties par des créances immobilières vendues aux organismes para-publics Freddy Mac et Fanny Mae. La Federal Housing Finance Agency réclamerait **30 milliards** de dollars.

Obligations garanties et assurance crédit

D'autres investisseurs ou assureurs portent des accusations similaires. Bank of America a déjà accepté de payer 8,5 milliards de dédommagements à un groupe d'investisseurs, et a provisionné **5,5 milliards** supplémentaires. AIG lui réclame cependant **10 milliards** dans une autre affaire. Les autres banques n'ont pas rendu public le montant des litiges en cours.

Auditer l'éthique d'entreprise

Sridhar Ramamoorti et **R. Luke Evans**

Pour détecter et prévenir les fraudes commises par les dirigeants, les auditeurs internes doivent avoir une solide compréhension des comportements humains.

En théorie, les dirigeants d'une entreprise conçoivent et mettent en œuvre des systèmes de contrôle interne fiables, puis doivent également exercer une surveillance afin de confirmer que ceux-ci demeurent efficaces dans la durée. Pourtant, cette surveillance – souvent considérée comme le talon d'Achille du contrôle interne – est de plus en plus souvent négligée, comme le montrent les deux études sur les fraudes, réalisées en 1998 et en 2010 par le COSO *(Committee of Sponsoring Organizations of the Treadway Commission).* Lorsque celui qui est censé surveiller devient celui qui commet la fraude, comment les actionnaires peuvent-ils se protéger ? Pour citer le poète satirique latin Decimus Juvénal : *« Mais les gardiens, eux, qui les gardera ? ».*

Les équipes d'audit externe, qui remplissent la fonction de surveillance, examinent les états financiers pour le compte des actionnaires et du conseil d'administration et donc, indirectement, évaluent les performances des dirigeants. Cependant, la complexification du monde des affaires, et le fait que les états financiers ne soient que des « indicateurs de performance et de risque a posteriori » semblent remettre sérieusement en question la pertinence de cette surveillance. L'audit interne, qui agit en gardien de l'organisation, tel un bouclier contre les menaces qui pèsent sur sa mission et ses objectifs, est probablement la fonction la mieux à même de surmonter ces obstacles en réalisant des audits d'éthique.

Un audit d'éthique a pour objectif d'identifier les éventuels comportements à risques, notamment en matière d'intégrité de données. Lorsque l'on parle de risque lié à l'intégrité des données, on fait référence tant aux risques liés aux informations à proprement parler (incomplètes, inexactes, incohérentes, périmées ou peu fiables), qu'aux risques liés à l'intégrité de celui qui les manipule (falsification intentionnelle, altération, camouflage ou manipulation des données afin d'entraîner une distorsion). Un risque élevé d'atteinte à l'intégrité des données finit tôt ou tard par sonner le glas du gouvernement d'entreprise.

Prévenir, détecter et analyser les fraudes commises par la direction d'une entreprise requiert une lecture fine des risques d'atteinte à l'intégrité des données d'un point de vue comportemental. Compte tenu de l'augmentation des actes frauduleux commis par les dirigeants, il apparaît clairement que les auditeurs internes doivent aujourd'hui, non seulement être compétents techniquement mais également savoir décrypter les comportements. D'autant plus qu'un gouvernement d'entreprise se fonde en grande partie sur des valeurs culturelles et éthiques, paramètres qui s'insèrent difficilement dans un cadre analytique prédéfini.

On fait souvent référence au *« Tone at the top »* - l'exemplarité des dirigeants - pour évaluer notamment la qualité de l'environnement de contrôle. Cette base d'évaluation reste floue, extrêmement contextuelle, et ne saurait par conséquent constituer un indicateur fiable des actions futures de la direction d'une société. Le gouvernement d'entreprise peut varier considérablement selon les conditions du marché, c'est pourquoi il est important de se concentrer sur le comportement des personnes occupant des postes clés dans l'organisation. Comme le soulignait Luther Hodges, secrétaire américain au Commerce dans les années 1960, *« la question du comportement éthique et moral dans les affaires ou dans un gouvernement revient à apprécier une série de situations personnelles ».*

En outre, quel que soit le bien-fondé des lois et des réglementations, il est généralement reconnu que l'on ne peut légiférer sur l'éthique et l'intégrité. Les lois sont conçues pour réglementer le comportement humain, pas la pensée humaine. Elles reposent sur un raisonnement sensé, qui vise à préserver le bien ou la vertu. De la même façon, un code de conduite formel, transmis à tous les employés, accompagné d'une formation des responsables et du personnel clé, ne suffisent pas à garantir la conformité. En effet, les lois, les réglementations et les codes professionnels ne font qu'établir des normes de comportement et les sanctions applicables.

Les auditeurs internes peuvent utiliser les techniques d'analyse comportementale afin de mesurer si certains comportements peuvent porter préjudice à l'intégrité des informations. Il est nécessaire

dans ce cas d'apprécier les schémas de comportement (styles éthiques) ainsi que les facteurs qui favorisent ces comportements (objectifs éthiques) ; il est question ici de culture d'entreprise et de dynamique comportementale. Les auditeurs internes qui possèdent ces compétences sont capables de mener des entrevues comportementales, de reconnaître ces schémas et facteurs particuliers et peuvent auditer avec succès la dimension éthique de la culture d'entreprise. Ils tentent ainsi de prévenir les comportements indésirables, en haut de la hiérarchie et à tous les échelons de l'organisation.

Depuis qu'il existe, on dit du service d'audit interne qu'il est les « yeux et les oreilles » de la direction. Son rôle est le suivant : déterminer les objectifs des dirigeants et la façon dont la fonction audit peut les aider à atteindre ces objectifs.

Aujourd'hui, l'intérêt d'un audit interne indépendant et objectif est reconnu au sein des entreprises tournées vers l'avenir.

Lorsque le responsable de l'audit interne rend compte au président du comité d'audit, on dit de l'audit interne qu'il est « les yeux et les oreilles, mais aussi les bras et les jambes » du comité d'audit. Cette expansion du rôle de la fonction d'audit interne pourrait s'illustrer en parlant, non plus d'« audit pour la direction », mais d'« audit pour et de la direction ». Ce type d'audit cherche à mettre en lumière les risques d'atteinte à l'intégrité des informations découlant de comportements inappropriés parmi les hauts dirigeants de l'entreprise, y compris des conflits d'intérêts cachés, des vides éthiques, des informations ou déclarations erronées ou trompeuses, ou des activités immorales ou illégales susceptibles de salir la réputation de l'entreprise.

Pour pouvoir faire leur travail correctement, les équipes d'audit interne doivent être objectives, compétentes, crédibles et suffisamment indépendantes du reste de l'organisation. Les auditeurs internes doivent gagner le respect de tous les collaborateurs afin de pouvoir approcher ces derniers sans réserve et avoir accès à toutes les informations leur permettant d'établir les faits.

Ils doivent faire preuve d'un « scepticisme naïf » et chercher sans relâche les signes de comportements inappropriés. Ils doivent également s'armer de patience et de ténacité afin de pénétrer au cœur même des affaires de la société.

Évaluer l'efficacité de la gestion des risques, des contrôles et des processus de gouvernance au sein d'une organisation, c'est avant tout appréhender la nature et le comportement des hommes

Pour mener à bien sa mission complexe d'évaluation du risque d'atteinte à l'intégrité des informations dans la culture d'entreprise et au niveau des dirigeants, l'audit interne doit comprendre avant tout qu'il convient de savoir appréhender la nature et le comportement des hommes. Comme l'explique Lynn Mc Gregor dans *The Human Side of Governance* (2004), « *les organisations qui survivent et prospèrent dans la durée sont celles qui mesurent toute l'importance du facteur humain dans le processus de gouvernance* ». Les services d'audit interne, en jaugeant la sensibilité éthique de l'entreprise et en évaluant les risques liés à l'intégrité des données, constituent une ligne de défense essentielle pour le conseil d'administration et la direction qui seront ainsi avertis de tout « risque humain » nécessitant une attention particulière. Agir vite et bien dans ce domaine peut éviter une véritable catastrophe.

Dans son ouvrage *In the New World of Business: Ethics and Free Enterprise in the Global 1990s* (1994), Robert Solomon défend avec conviction la nécessité d'effectuer un audit d'éthique intelligemment conçu, en arguant que l'éthique d'entreprise réside avant tout dans le fonctionnement interne de la société, c'est-à-dire la manière dont les hauts dirigeants, les responsables et les employés interagissent. Ainsi, les valeurs éthiques de l'entreprise sont souvent un des principaux éléments qui incitent les collaborateurs à travailler et à rester dans l'entreprise.

Dès lors, il semble pertinent de poser une question fondamentale : « Vous êtes-vous déjà senti contraint par votre entreprise d'agir à l'encontre de votre sens moral ? ». Si la réponse est « oui », un audit d'éthique très approfondi s'impose : Quels types de pression avez-vous subi ? Ces pressions sont-elles réelles ou imaginaires ? Cela vaut-il la peine de rester dans cette entreprise ? La situation doit-elle être signalée au conseil d'administration voire à un organisme extérieur ? Même si la réponse est « non » ou « très rarement », l'audit d'éthique peut tout de même être révélateur, puisqu'il soulève une question existentielle primordiale : « Suis-je la personne que je voudrais être ? ».

L'audit d'éthique est une première étape du processus qui consiste à déterminer dans quelle mesure les dirigeants et les responsables opérationnels épousent, diffusent, appliquent et renforcent la culture, les valeurs et l'éthique de l'entreprise. À l'instar de toute étude visant à mesurer les fondements éthiques d'une organisation, l'audit d'éthique doit être pensé avec soin et mis en œuvre à l'échelle internationale, de façon efficace et rentable. Comme le souligne Robert Solomon dans son livre, sans un cadre et des connaissances de base solides, il est peu probable que les auditeurs internes soient en mesure de fournir une évaluation exhaustive des risques d'atteinte à l'intégrité des informations parmi les membres de la direction et au sein de la culture d'une entreprise. ●

Vous pouvez approfondir ce sujet en assistant au colloque :

Les enjeux de l'éthique appliqués en entreprise : le rôle de l'auditeur et du contrôleur internes

Jeudi 1er décembre 2011

Pour consulter le programme complet du colloque et vous inscrire, rendez-vous sur le site www.ifaci.com

Article initialement paru dans la revue « The Internal Auditors » (The IIA)

La gouvernance des systèmes d'information

Quel rôle pour l'audit interne ?

Guide d'audit de la gouvernance du système d'information

Messages clés

Jean-Pierre Bouillot

VP Information System Audit,
Risk Committee Project Leader,
Sanofi

C'est un lieu commun de dire que les entreprises sont devenues au fil du temps de plus en plus dépendantes de leur informatique.

Il est moins communément admis qu'un lien de dépendance existe également en matière de gouvernance et que de façon corrélative **la qualité de pilotage du système d'information est souvent le reflet de la maturité de la gouvernance globale de l'entreprise.**

Cette dimension est en toile de fond de ce guide d'audit et chaque thème abordé prend en compte la qualité de l'implication de l'ensemble des acteurs de l'entreprise dans la gouvernance du SI dont les directions informatiques ne peuvent désormais exercer seules la responsabilité.

On peut, bien entendu, constater aujourd'hui que la gouvernance des SI a poursuivi une montée en maturité au sein des entreprises et des organisations et que celle-ci s'est traduite par la création et la mise en place de multiples référentiels de bonnes pratiques et de méthodologies spécialisées.

Mais parallèlement, la complexité des systèmes d'informations (multi-couche technologique, obsolescence accélérée, couverture de processus métiers transverses intégrés…) s'est accrue, et la difficulté à évaluer les risques d'une défaillance des SI sur l'activité de l'entreprise et jusqu'où investir pour s'en prémunir sont devenus une source de préoccupation majeure pour les dirigeants.

En réponse, les grandes entreprises et organisations, disposant de moyens importants, ont parfois multiplié le nombre d'instances de décision ou d'arbitrage dont le haut niveau de positionnement ne peut totalement pallier les lacunes des dispositifs de collaboration opérationnelle en place.

Ce contexte, illustré par les difficultés effectivement rencontrées pour maîtriser de vastes programmes de transformation (perçus comme trop longs, trop chers, trop lourds…) a conduit certaines directions opérationnelles à ne pas intégrer la stratégie SI en support de la Stratégie d'Entreprise, mais à recourir à un « pilotage par les coûts », comme seul indicateur tangible et commun à l'ensemble des acteurs.

La conviction des associations réunies pour l'élaboration de ce guide d'audit est que les lacunes des dispositifs de pilotage des SI, dits de « Gouvernance », ne peuvent se résoudre de manière indépendante du reste de l'entreprise par l'empilement de référentiels connus et compris par la fonction SI seule ; **un effort de partage et de pédagogie est nécessaire pour refonder les bases d'un pilotage partagé où les métiers de l'entreprise, clarifiant leur stratégie et leurs besoins, réinvestissent leur domaine de responsabilité dans la construction du système d'information qui les supporte** (notion d'alignement).

En effet, les missions réalisées sur le terrain par les équipes d'audit interne montrent très fréquemment que la Gouvernance des SI est un miroir des difficultés de gouvernance de l'ensemble de l'entreprise et qu'**il s'agit bien de déployer un modèle de co-gouver-**

nance DSI/métiers pour sortir de schémas de fonctionnement où la responsabilité est diluée ou indument transférée.

Pourquoi ce guide ?

Ce guide, fruit de la collaboration d'une trentaine de professionnels de terrain issus des métiers du système d'information, de l'audit interne et du conseil, se veut donc être une illustration d'une collaboration renouvelée entre deux fonctions transverses que sont la DSI et l'audit interne.

Trois associations professionnelles se sont mobilisées pour son élaboration : le CIGREF, réseau de grandes entreprises utilisatrices de système d'information, l'IFACI, institut français de l'audit et du contrôle internes, et l'AFAI, association française de l'audit et du conseil informatiques.

Leur principal objectif a été de mettre à disposition des auditeurs et des DSI un guide pratique d'audit abordant, sous un angle managérial et non pas technique, la **problématique globale de la gouvernance du SI** par l'entreprise ou l'organisation.

Il permet ainsi aux directions de l'audit interne de répondre aux questions que se pose la direction générale à propos du niveau de maîtrise de son SI et de fournir aux autres fonctions de l'entreprise ou de l'organisation **une assurance raisonnable que leurs processus métiers sont bien soutenus par des systèmes d'information de qualité.**

Cette évaluation de haut niveau de la gouvernance permet de **mettre en évidence des points de vigilance par rapport à des pratiques de management du SI, qui peuvent être de nature opérationnelle, économique ou stratégique**, mais qui doivent toutes être sous contrôle pour que la gouvernance du système d'information de l'entreprise ou de l'organisation puisse être considérée performante.

Toutefois, même si la gouvernance du SI s'évalue de façon globale, celle-ci a été décomposée, pour des considérations pratiques, en 12 vecteurs distincts (cf. schéma 1), suffisamment autoporteurs pour pouvoir faire l'objet de missions individualisées par vecteur ou groupe de vecteurs.

En fonction de leur nature, **les points de vigilance ainsi mis en évidence pourront contribuer à l'élaboration du plan d'audit du SI, voire du plan d'audit général de l'entreprise ou de l'organisation**, puis être éventuellement suivis de missions d'audit plus approfondies utilisant des référentiels adaptés tels que COBIT, Val IT, Risk IT, ou autres… selon le sujet à traiter.

Cet outil se veut également pédagogique pour **démystifier la gouvernance du SI en évitant le jargon technique**, qui prévaut généralement dès lors qu'il est question d'informatique.
La communication de la DSI vers la direction générale et les directions « métiers » s'en trouve ainsi facilitée et renforcée.

Son périmètre

Le périmètre de ce guide couvre les processus de gouvernance du SI par l'entreprise, qui associent étroitement la direction générale, les métiers et la DSI.

A contrario, et malgré leur importance, il ne couvre pas les aspects opérationnels du management de l'informatique, tels que le développement des projets, la production récurrente de services, dès lors que ceux-ci sont entièrement placés sous la responsabilité de la DSI et donc moins en interaction avec le reste de l'organisation.

Ces aspects opérationnels sont traités par ailleurs et notamment dans les « contrôles généraux informatiques » de l'audit.

Comment l'utiliser ?

L'ambition de ce guide est de mettre à disposition du lecteur un outil pratique pour réaliser un audit permettant d'obtenir une assurance raisonnable de la

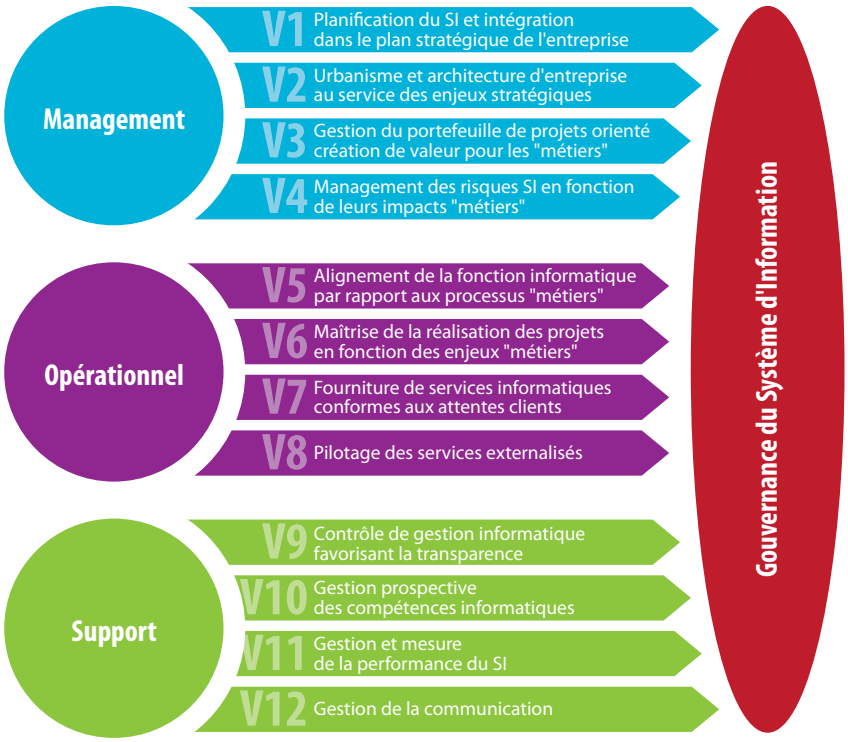


Schéma 1

qualité des processus de gouvernance du SI. Dans un second temps et en fonction du résultat obtenu, ce premier audit permettra d'identifier les risques et insuffisances potentielles afin, si cela est nécessaire, de lancer un audit plus approfondi.
Lors de la préparation de son programme d'audit, l'auditeur pourra sélectionner le ou les vecteurs correspondants au périmètre de la mission dans le cadre du plan d'audit annuel.
Il est donc tout à fait possible de réaliser un audit ciblé sur un ou plusieurs vecteurs.
Bien entendu, en fonction du périmètre de l'audit, il peut être pertinent de sélectionner plusieurs vecteurs qui seraient complémentaires.

Modalités d'évaluation retenues

Une fois le ou les vecteurs choisis, en fonction des objectifs et du périmètre de l'audit que l'on souhaite effectuer, il s'agit de passer en revue l'ensemble des bonnes pratiques des vecteurs à auditer. Pour chacune de ces bonnes pratiques, il faut évaluer le niveau de maîtrise de chacun des critères concernés.
Les critères d'une même pratique expriment parfois une progressivité dans le niveau de maîtrise. Il n'y a cependant pas de pondération à appliquer et chaque critère peut s'évaluer indépendamment des autres critères.
Pour évaluer une bonne pratique, il convient donc d'examiner l'ensemble des critères de la bonne pratique concernée. Éventuellement, un critère peut être « non applicable » au contexte de l'organisation, **l'auditeur devant naturellement exercer son jugement professionnel.**

Pour chacun de ces critères, le niveau de maîtrise s'évalue par couleur :

- couleur rouge : faible,
- couleur jaune : insuffisant,
- couleur verte claire : satisfaisant,
- couleur verte foncée : bon,
- couleur blanche + N/A : Critère « Non Applicable » au contexte de l'organisation évaluée.

Cette grille exclut tout recours à un système d'évaluation chiffré.

Comme toujours en matière d'audit interne, il est bien sûr recommandé de recueillir des preuves (documentation, tableaux de bord, indicateurs, méls, etc.) permettant de conforter l'évaluation du niveau de maîtrise constaté.

Modalités de restitution

Une fois l'ensemble des critères évalués, pour toutes les bonnes pratiques du vecteur examiné, il est alors possible de positionner l'ensemble des résultats sous la forme d'un « mur de couleurs » (cf. schéma 2).

peut ainsi donner son appréciation sur l'ensemble du vecteur.
L'auditeur veillera dans son évaluation finale à identifier des points de vigilance et proposera éventuellement un audit approfondi.

Structure de chaque Vecteur

L'intitulé de la plupart des vecteurs est rédigé de façon à donner l'orientation principale ayant conduit à la sélection de bonnes pratiques en support de cette dernière.
Exemple : vecteur 4 « Management des risques SI en fonction de leurs impacts métiers »

Exemple d'évaluation globale du vecteur 4
Management des risques SI en fonction de leurs impacts « métiers »

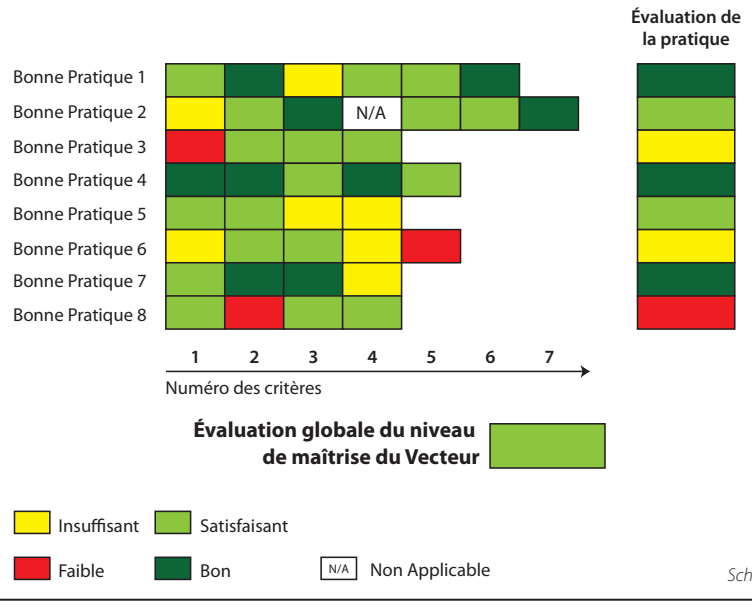


Schéma 2

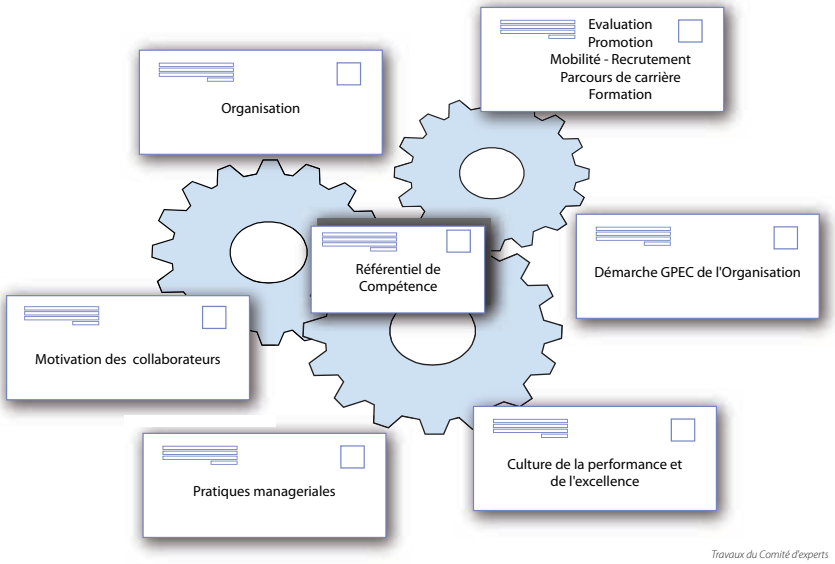
Modalités d'appréciation

Sur la base de la restitution ci-dessus, l'auditeur est en mesure de porter un jugement sur le niveau de maîtrise globale de chaque bonne pratique en leur attribuant la couleur correspondante (colonne « Évaluation de la bonne pratique »). Bien entendu, ce jugement tiendra compte des poids attribués aux critères d'évaluation en fonction du contexte de la mission.
À la suite de cette opération, l'auditeur

Ensuite, à titre d'introduction, s'enchaînent deux paragraphes : le premier expose les enjeux qui sont à couvrir, le suivant décrit les risques auxquels l'organisation pourrait avoir à faire face si les bonnes pratiques décrites s'avéraient non maîtrisées.

Chaque bonne pratique est décrite sous forme d'un intitulé complet, complété par une moyenne de 5 critères d'évaluation dont le descriptif est parfois enrichi d'un commentaire explicatif.

La démarche GPEC : Gestion Prospective des Emplois et Compétences



Travaux du Comité d'experts

Schéma 3

Enfin certains vecteurs disposent d'un schéma illustré devant faciliter une compréhension rapide et commune.

Exemple : vecteur 10 (cf. schéma 3).

* *
*

Vous l'avez compris ce guide n'a pas pour vocation à se substituer aux nombreux référentiels experts existants pour réaliser l'audit des systèmes d'information.

Il constitue une plateforme commune DSI / audit interne pour réaliser un premier niveau d'évaluation donnant une visibilité globale et intelligible pour les autres acteurs de l'entreprise.

Il peut permettre aux directions de l'audit interne, sans recours à des auditeurs experts en système d'information, de réaliser en toute légitimité leurs évaluations et d'identifier si le système d'information de l'entreprise est piloté au travers d'un processus de décision structuré impliquant l'ensemble des parties prenantes.

Il s'agit bien entendu de **veiller à dépasser l'aspect formel des choses et la simple conformité**, et de s'assurer de l'efficacité des instances et dispositifs de gouvernance en place, en évaluant si **la mise en œuvre des décisions est bien le reflet d'une compréhension commune et d'une prise de responsabilité « éclairée » et partagée.**

Il est rassurant, en définitive, de constater qu'au-delà des technologies et de l'accumulation des savoirs, c'est la qualité de collaboration des hommes et des femmes de l'entreprise qui reste une condition clé pour nous conduire au succès. ●

Le guide d'audit sur la gouvernance du système d'information est téléchargeable (accès réservé aux adhérents de l'IFACI) et en vente sur le site internet de l'IFACI (www.ifaci.com).

*Diplômé en Etudes Comptables Supérieures et titulaire d'une maîtrise de Gestion, **Jean-Pierre Bouillot** a occupé des postes très variés durant sa carrière. Elle se répartit globalement par tiers : 1/3 en finance opérationnelle, un autre tiers en système d'information et enfin un dernier tiers à l'audit interne.*

En Finance tout d'abord, en charge des systèmes d'information finance du Groupe, puis de la direction comptable corporate.

En DSI ensuite, en charge du secrétariat général de la fonction SI du Groupe, couvrant l'assurance qualité des SI, la RH, les achats et la finance.

Enfin, depuis 2005 à l'audit interne, Jean-Pierre Bouillot est en charge de la direction de l'audit des systèmes d'information, département qu'il a créé lors de la fusion de Sanofi avec Aventis.

Il est également en charge, depuis octobre 2010, de la direction d'un projet de mise en place d'un ERM (Enterprise Risk Management) au niveau du groupe.

Gouvernance des SI : de la fiction à la réalité

Antoine Gourevitch

Partner & Managing Director,
Responsable mondial du centre d'expertise Gouvernance et Organisation SI,
BCG

J'ai une passion pour les projets informatiques. J'en ai croisé beaucoup, mais rares sont ceux que j'ai vu réussir, notamment parmi les plus importants. En cas d'échec, il est facile d'incriminer l'IT, mais il convient de se pencher également sur le rôle du *business*. Je suis, en effet, convaincu que les entreprises ont l'IT qu'elles méritent.

Je voudrais faire un point sur l'histoire de la gouvernance des systèmes d'information et sur ce que nous rencontrons aujourd'hui, puis passer un peu de temps à évoquer le futur. Pour ma part, je considère que l'arrivée du numérique obligera les DSI à se transformer sous peine de disparaître.

Voici une histoire que j'ai vécue. Le président d'une entreprise du CAC 40 nous a un jour demandé d'intervenir sur un projet représentant 50 millions d'euros et qui commençait, au bout de sept mois, à présenter des signes de faiblesse. Ce projet avait été accepté en comité exécutif. Deux mois plus tard, une petite crise était survenue. Il serait impossible de livrer tout ce qui avait été prévu. Le comité exécutif avait alors décidé d'abaisser ses objectifs de 10 %. Après cette réduction d'ambition, avait suivi, comme souvent, une période de répit que l'on pourrait intituler « Jusqu'ici, tout va bien ». Tout le monde pensait alors que le projet serait livré. Dans ce genre de situation, une nouvelle crise survient au bout d'un an. Le dernier comité de pilotage avait validé un projet dans lequel tous les signaux étaient dans le vert. Le comité suivant finit par expliquer que le projet était dans le rouge. Seuls 20 % des objectifs seraient atteints, avec six à huit mois de retard.

Nous sommes intervenus dans la période de répit, parce que certaines personnes avaient des doutes. Nous avons donc audité le projet et conclu qu'il ne délivrerait jamais ce qui avait été prévu. Nous l'avons par conséquent restructuré. En effet, de nombreux points étaient problématiques. Par exemple, l'une des justifications du chantier était que les systèmes en place ne permettraient pas de tenir la charge. Je n'ai, pour ma part, jamais vu de systèmes qu'il est impossible de faire évoluer pour tenir la charge. Certains clients m'ont même expliqué, il y a dix ans, qu'ils vivaient sur des grenades dégoupillées. Aujourd'hui, leur entreprise fonctionne toujours avec le même système.
Le projet en question consistait à remplacer un *front office* de commandes-livraisons de biens industriels. Son coût de développement était de 50 millions d'euros et il ne pouvait engendrer que 3 millions d'euros d'économies, ce qui représentait un retour sur investissement très long. A l'époque, le directeur Europe nous avait indiqué que jamais un projet informatique initié par l'entreprise n'avait été à l'origine d'un quelconque retour sur investissement. Je lui avais répondu que c'était peut-être la raison pour laquelle ils avaient tous échoué.

A la fin de notre intervention, le président du Groupe nous a convoqués. Il était content que nous ayons redimensionné le projet mais souhaitait savoir comment la décision de lancer un tel projet avait pu être prise. Nous avons donc poursuivi l'audit. En réalité, la décision avait été prise parce qu'un jour, le directeur Europe et le directeur informatique étaient venus ensemble au comité exécutif en expliquant qu'ils étaient d'accord sur un nouveau projet. Le comité exécutif avait alors accepté en quelques secondes ce projet à 50 millions d'euros. J'ai demandé au président ce que représentaient 50 millions d'euros pour l'entreprise. Il m'a répondu que cette somme représentait une toute petite usine ou une nouvelle technologie. Pour ce type d'investissement, six

mois de discussions étaient nécessaires au sein du comité exécutif. Je lui ai expliqué que dans le cas de son projet de système informatique, le temps de décision nécessaire n'ayant pas été pris, l'opération était vouée à l'échec.

Encore aujourd'hui, l'informatique fait peur. Les membres des comités exécutifs ne rentrent pas dans le sujet comme ils rentrent dans celui du *business*. Je suis toujours fasciné de voir que tout le monde a un avis sur une campagne à quelques millions d'euros, et personne sur un projet informatique. C'est l'une des raisons pour lesquelles la gouvernance est problématique dans ce domaine. L'un des rôles importants du DSI est de faire en sorte d'exister au sein du comité exécutif afin de faire prendre conscience des enjeux aux autres membres.

Il existe quatre types de dysfonctionnement dans un projet, liés au choix des bonnes priorités, des bonnes solutions, de la bonne gouvernance et de la bonne capacité d'exécution. On se focalise souvent sur les solutions. J'ai rarement vu des projets échouer parce que le DSI avait choisi une technologie plutôt qu'une autre ; tout comme il est rare que l'on ne puisse pas trouver, dans l'entreprise ou en dehors, de personnes capables d'aider le projet en termes d'exécution. En revanche, les projets échouent parce que la gouvernance est défaillante, qu'il n'existe pas de contrepouvoir utile ou parce que les priorités sont mal définies.

Je me suis inspiré de Fernand Braudel et de sa citation « *Le présent sans passé n'a pas d'avenir* ». Avant de nous pencher sur l'avenir du numérique, il est important de nous demander d'où nous venons en termes de gouvernance et de projet, et quelles sont les bonnes pratiques aujourd'hui. L'informatique est une matière extraordinaire permettant une sorte d'homothétie entre organisation et matière. Il y a plus de quarante ans, l'informatique a commencé avec les *mainframes*, dans une époque bénie pour les DSI, qui s'appelaient alors les DOSI, ou directeurs de l'organisation des systèmes d'information. Tout était alors centralisé. Il était donc facile de gérer les équipes, qui travaillaient à côté des centres de calcul, sur des machines assez grandes. La période était moins favorable aux utilisateurs dans la mesure où toute modification était compliquée et demandait du temps.

Avec l'arrivée du PC et des systèmes client-serveur dans les années 1985-1990, la vie des utilisateurs a été révolutionnée mais la situation est devenue cauchemardesque pour les DSI. Dans les banques d'investissement, les premiers à utiliser les PC ont été les *traders*, dont le métier s'est envolé dans ces années-là. Leur centre de calcul était sous leur bureau. Il consistait en un PC et un serveur dans lequel tournaient des bases de données importantes, à savoir les clients de la banque et de nombreuses transactions représentant beaucoup d'argent. On était de ce fait très réactif. Les publicités des magazines destinés aux *traders* vantaient alors les derniers systèmes d'exploitation ou les dernières bases de données, censés tourner plus vite que les autres. Le client était alors très proche de l'informaticien.

L'arrivée d'internet a, par la suite, donné un rôle tout particulier aux DSI, notamment aux Etats-Unis, où la vague a commencé en 1995 et a eu un impact très rapide. Les informaticiens étaient alors très recherchés. Nombre d'entre eux, en charge de la transformation de l'entreprise vers le numérique, sont entrés dans les comités exécutifs mais cette ascension a été suivie d'une grande déception. En effet, de nombreuses entreprises ont monté des projets qui n'ont pas abouti. Peu de *start-up* ont du reste véritablement réussi, même si 1995 a vu la fondation d'Amazon, Yahoo et eBay.

En 2001, avec l'explosion de la bulle des télécoms, les directeurs généraux ont compris que le développement d'internet serait plus long que prévu, et estimé que les directeurs informatiques n'avaient pas joué leur rôle. Ces derniers ont donc perdu leur place au sein des comités exécutifs, au bénéfice d'une ère glaciaire de rationalisation des systèmes d'information. Il s'agissait de nettoyer la période des PC sous les bureaux et de la prolifération des applications dans les entreprises en consolidant les centres de calcul externalisés.

Depuis quelques années, la période numérique ou web 2.0, a commencé, avec Apple, Google, Amazon ou Microsoft. Aujourd'hui, tout particulier peut bénéficier d'une qualité de système d'information au moins aussi élevée que dans son entreprise, voire meilleure, notamment en termes de sauvegarde de ses informations dans le cloud.

La période récente, période d'industrialisation, a connu quatre changements importants :

- consolidation des centres de calcul ;
- standardisation des méthodes et des pratiques ;
- mise en place d'une gestion de *process* avec des techniques comme Six Sigma, CMMI, CobiT ;
- arrivée de l'*offshoring* et de l'*outsourcing*.

Avant 2000, les dépenses informatiques d'une entreprise typique augmentaient sans être remises en question, autant pour le *change*, part allouée aux projets, que pour le *run*, part allouée à la main-

tenance, aux centres de calcul et aux postes de travail. Les coûts étaient alors rarement un problème. En 2001, les directeurs généraux ont décidé de réduire les budgets. Les directeurs informatiques ont donc réduit en priorité la part des projets mais cette solution n'a fonctionné qu'un temps. Très vite, une nouvelle augmentation des budgets des projets a été nécessaire afin de permettre aux entreprises de continuer à se développer. Les directeurs généraux ont accepté, tout en refusant d'augmenter du même coup les budgets informatiques, ce qui manifeste leur manque de confiance vis-à-vis de la DSI, réduite à faire des efforts en termes de productivité au sein d'un budget contrôlé par la direction.

Chaque année, le *Standish Group* publie le *Chaos Report*, rapport sur l'ensemble des projets informatiques et leur vitesse d'évolution. La situation s'améliore année après année, mais reste problématique. Deux tiers des projets sont jugés insatisfaisants par les utilisateurs, tandis que 60 % d'entre eux sont en retard ou hors budget, et 40 % ne couvrent pas leurs coûts. Dans un système de gouvernance bien pensé, on peut imaginer que les résultats seraient meilleurs.

Je suis convaincu que la gouvernance fait partie d'un système. L'informatique est d'abord au service d'un *business* et d'une stratégie. Elle doit donc être organisée en fonction des objectifs de l'entreprise. Si elle cherche à réduire les coûts, l'informatique doit être centralisée et fonctionner à l'aide de structures partagées. Si elle est en plein développement international, elle doit au contraire envisager de la décentraliser dans les métiers afin de favoriser l'agilité. Il est ensuite important de s'interroger sur la vision de l'informatique cultivée par l'entreprise. Est-elle un *business partner* ou un preneur d'ordres ? Enfin, la partie gouvernance, qui correspond à la prise de décision, s'appuie sur un système structuré autour d'une ligne hiérarchique. Quels sont les talents qui la composent ? Comment les gérer dans le cadre du *sourcing*, en interne et en externe ? Quels sont les processus de management, à la fois en termes de conception de projets et d'exploitation ?

Il est important que la gouvernance soit cohérente. J'ai trop souvent vu de directeurs informatiques boucs émissaires devant décider des budgets ou centraliser, alors que l'entreprise elle-même n'était pas en phase de centralisation. Dans ce type de cas, la durée de vie du DSI est faible.

L'informatique ne crée de valeur que si elle gère des tensions. C'est la raison pour laquelle la gouvernance est primordiale. Les gens ont souvent peur des conflits. Pourtant, ils sont importants au sein d'une entreprise et doivent pouvoir s'exprimer. Dans le domaine de l'informatique, ils peuvent être de deux ordres :

- **Conflit entre les métiers et l'informatique**
  Un bon projet doit pouvoir rester six mois devant le comité exécutif afin que le métier puisse exprimer son envie, et l'informatique ses contraintes et ses idées. Un projet bien dimensionné d'un point de vue métier et technique, que j'appelle le 80/20, voit le jour parce que les architectes informatiques, qui connaissent bien leur matière, peuvent proposer des idées, mais aussi parce que les gens du *business* s'intéressent à la matière technique et exposent leurs attentes. Lorsque ce conflit s'exprime bien, les projets sont souvent excellents.

- **Conflit entre les personnes chargées d'exploiter le projet et celles qui l'ont fabriqué**
  Souvent, l'exploitation des projets informatiques apparaît comme moins noble que leur conception. Je pense le contraire. La vérité d'un projet se trouve dans la production. On y voit comment le code a été développé ou comment il interagit avec le *business* au fur et à mesure de son développement. Les personnes travaillant à la production veulent des environnements stables qui évoluent peu. Celles concevant les projets sont à la recherche d'innovation. Ils veulent les dernières versions de SAP, d'Oracle ou de Salesforce. Si un conflit permet aux points de vue de s'exprimer, le meilleur des deux mondes viendra nourrir le projet. Dans le cas contraire, son architecture deviendra vite chère et compliquée.

La gouvernance est une occasion de s'assurer que l'on sait traiter les conflits nécessaires. Le rôle du DSI consiste à « *do the right things* » et « *do the things right* », à savoir d'une part s'assurer qu'entre le métier et l'IT, les bonnes ressources soient allouées aux activités à valeur ajoutée, et choisir d'investir et d'innover sur les bons endroits, et d'autre part, aller dans la bonne direction le plus efficacement possible. La question se pose donc souvent aujourd'hui entre une IT Groupe en charge de synergies et de services partagés, et une IT située dans les métiers, les *business units* ou les géographies, en charge de réactivité. Un projet informatique doit offrir à la fois une bonne réactivité et une bonne industrialisation. De nombreux groupes ont rencontré des problèmes parce qu'ils sont allés très loin dans l'industrialisation au détriment de leur activité métier.

Comment gouverner ? J'ai eu de longues discussions à ce sujet avec le co-auteur de mon ouvrage, Eric Baudson, directeur informatique de la partie banque d'investissement d'une grande banque française. A l'origine, Eric Baudson n'est pas informaticien mais vient du métier, à savoir le *back office* d'une importante salle des marchés, où il a ensuite été nommé directeur de l'ensemble du *back office*. Il est devenu directeur informatique après s'être intéressé à un très grand projet n'ayant pas donné les résultats escomptés.
Pour lui, la gouvernance exige quatre éléments :

- **La transparence**
  L'informatique a trop souvent tendance à s'enfermer afin de conserver

ses marges de manœuvre vis-à-vis du métier, mais le métier doit pouvoir évaluer l'acquis. Au-delà des enquêtes clients sur le taux de service, Eric Baudson a mis en place un système dans lequel chaque projet est évalué par son sponsor métier à l'aide des indicateurs vert, orange et rouge. Tous les mois, une discussion se tient sur le projet. J'ai, pour ma part, trop souvent rencontré des directeurs informatiques qui ne souhaitaient pas noter rouge un projet de peur d'entrer en conflit avec le directeur commercial.

- **La formalisation**
  Une fois que des outils favorisant la transparence ont été mis en place, il est nécessaire de pouvoir s'exprimer dans un comité important, à savoir celui présidé par le directeur général de la société, réunissant le directeur informatique et les principaux métiers et dévolu aux revues de projets, allocations de portefeuilles projets ou arbitrages sur les ressources. Ce comité de haut niveau doit faire preuve de transparence quant aux points positifs et négatifs découlant de ses décisions.
  Aujourd'hui, dans les entreprises, on fait trop souvent remonter à la direction générale que tout va bien. L'audit est l'une des dernières fonctions de l'entreprise à dire la vérité. Tout ne doit pas être normalisé, avec un rouge qui devient orange et un orange qui devient vert. Je suis toujours surpris lorsque je travaille sur des projets de transformation d'entreprise. Au bout d'un mois, tout est vert. J'explique aux personnes concernées qu'il est impossible pour une entreprise de se transformer en n'ayant que des indicateurs positifs. Pourtant, des comités entiers valident des projets qui vont bien. La vie est faite de problèmes à résoudre. Il est important de les formaliser pour les faire apparaître.

- **Le partage de la prise de décision**
  Entre l'IT et le *business*, la répartition des rôles est compliquée. Certaines décisions, comme les choix techniques ou les propositions en termes de portefeuille de produits et de services, relèvent du directeur informatique. D'autres, comme le choix des projets, reviennent au *business*. J'ai remarqué que lorsque le système de gouvernance d'une entreprise est défaillant, on demande au DSI de choisir les projets de l'entreprise. Normalement, s'il peut participer à la prise de décision ou éclairer le débat, choisir entre un système d'information logistique ou un système de CRM n'est pas de son ressort.

- **Le pouvoir de dire non**
  J'ai longtemps cru que mon rôle, en tant que consultant, était d'aider les entreprises à mener à bien leurs projets. Je me rends compte aujourd'hui que je suis plus utile à mes clients lorsque je les aide à dire non. On accepte en effet trop de dire oui à tout. Dans le cas du projet à 50 millions d'euros que j'évoquais tout à l'heure, le comité exécutif aurait dû dire au bout d'un mois, à partir d'une analyse simple de grille sur le niveau de risque des projets, que le projet n'irait pas à son terme. L'équipe aurait dû être dissoute, et le projet repensé.

« Tout le monde a un avis sur une campagne à quelques millions d'euros, et personne sur un projet informatique »

Je connais une entreprise informatique qui gère ses projets avec le temps pour seule métrique. Pour un projet de six mois, vous disposez d'un mois et demi pour proposer une conception fonctionnelle satisfaisante. Si vous n'y parvenez pas, le projet est arrêté et l'équipe est dissoute. Cette gestion de la transparence, de la formalisation, de la prise de décision et de la capacité à dire non relève d'une bonne gouvernance mais exige une organisation fluide permettant de gérer les personnels dans un pôle de ressources.

Le rôle du DSI est souvent d'assurer une standardisation importante des fonctions. Souvent, ce mandat leur est du reste imposé par leur directeur général. Pourtant, dans un modèle décentralisé ou fédéral fonctionnant avec un IT centralisé, il est très difficile de favoriser une standardisation des fonctions. La gouvernance de l'IT ne doit jamais être supérieure à la gouvernance de l'entreprise. De nombreux DSI se sont fait évincer au moment où ils ont tenté de prendre du poids au sein de la gouvernance de l'entreprise, ce qui n'est pas possible.

Dans le cadre des pratiques de gouvernance actuelles, il me semble important que les DSI ne se fassent pas instrumentaliser. Leur rôle n'est pas de choisir les projets à la place des métiers mais de faire émerger les conflits en assumant la transparence et les difficultés. Par ailleurs, leur *leadership* doit s'exercer sans qu'ils sortent du cadre de leur mandat. Les DSI qui y parviennent sont ceux qui obtiennent de bons résultats dans le *Standish Report*.

Aujourd'hui, quatre tendances apparaissent. Deux d'entre elles touchent les gens ; les autres, la technologie et l'écosystème.

Les gens

Les attentes des personnes entrant dans le monde de l'entreprise en termes d'informatique sont très différentes de par le passé. Les trentenaires n'ont plus peur de l'informatique. Ils peuvent discuter avec les informaticiens, pratiquent la programmation chez eux et ont un bon niveau de connaissance. C'est encore davantage le cas chez les plus jeunes. Ceux qui entreront dans les entreprises dans les années à venir poseront de nombreux problèmes aux

informaticiens dans la mesure où leur installation informatique personnelle sera souvent de meilleure qualité que celle de leur lieu de travail.
Une bataille des talents est donc ouverte. Il s'agit pour les informaticiens de réussir à faire venir les bonnes personnes dans leur entreprise, ce qui est plus facile aux Etats-Unis, où l'informatique est vue comme un vecteur de développement de la société. Lorsque l'on est doué en sciences, on fait naturellement de l'informatique puis l'on rentre facilement dans les directions informatiques des grands groupes. En France, la situation est plus compliquée dans la mesure où les personnes douées en informatique partent aux Etats-Unis. Il devient donc difficile de trouver de bons techniciens pour aider les DSI.

La technologie

J'ai choisi d'illustrer cette partie avec la galaxie Apple, mais j'aurais pu choisir l'image d'une voiture avec contrôle moteur ou d'un système électrique à puces présent dans toutes les maisons et toutes les entreprises. Aujourd'hui, l'informatique devient le produit, ce qui représente une révolution fondamentale. Mais les DSI sont-ils prêts à développer le contrôle moteur des voitures ? Ils ont besoin de trouver un positionnement par rapport aux métiers.

L'écosystème

Les directeurs généraux continuent à développer l'*offshoring* et l'*outsourcing* parce qu'IBM, Accenture et les autres les y exhortent. On parle du reste aujourd'hui beaucoup du *cloud*. Pourtant, les DSI n'ont pas attendu Amazon, IBM et Microsoft pour entamer une politique de réduction des coûts. Ils pratiquent en effet la virtualisation depuis cinq à dix ans. Dans ce domaine, l'apport du *cloud* est donc tout relatif dans les grandes entreprises, qui ne sont pas prêtes à y placer l'ensemble de leurs applications.
En revanche, le *cloud* est en passe de changer le monde des grandes entreprises dans le domaine du *business*. On est aujourd'hui capable de mieux partager l'information et de mieux gérer les écosystèmes, ce qui permet d'imaginer des *business models* différents avec les fournisseurs et les clients, puis la création de nombreuses applications nouvelles. Quel est le rôle du DSI au regard de ces évolutions ?

Le CIO avait autrefois une place importante dans le graphique sur la frontière de communalité. Il est aujourd'hui pris en étau entre le métier qui décide de développer seul l'IT, les services digitaux ou les réseaux sociaux, et IBM ou Accenture qui prennent en charge les opérations, la paie ou la compta. Il est donc délesté à la fois des *process* et des systèmes d'information, si bien que son rôle disparaît. Le CIO a alors deux options : changer de rôle pour monter vers le métier en devenant plus proche des *process* et de l'information ou devenir directeur des achats pour gérer l'ensemble des fournisseurs externes. Créer un mur autour de sa direction est en revanche rarement une option.
Aujourd'hui, il est nécessaire de changer de positionnement. Une matrice à deux dimensions permet de matérialiser la répartition des rôles entre l'organisation IT et le *business*.

L'exemple le plus frappant serait celui d'une multinationale spécialisée dans les biens de consommation courante. Sur leurs 10 000 informaticiens, ils en ont *outsourcé* 5 000, à savoir ceux qui s'occupaient des opérations et du code. Ils ont en contrepartie chargé 5 000 personnes du *business* de s'occuper des *process*.

Leur ancien directeur ventes monde, devenu DSI, ne vend plus d'applications mais des produits et des services comme des systèmes de fidélité ou des systèmes logistiques. Il est également responsable de la *supply chain*, seul poste d'observation de l'information au commerce, à la finance et dans les usines. Il a du reste expliqué au comité exécutif que tant que les bases de données du marketing, de la finance et du *manufacturing* calculeraient des stocks différents, les prévisions de vente seraient erronées. En effet, la finance ajuste ses chiffres en fonction des résultats à faire pour le trimestre, le commerce fait des prévisions de vente en fonction de ce que les clients sont supposés attendre et le *manufacturing* souhaite faire plus ou moins 2 % par rapport à l'année précédente afin de favoriser la stabilité des usines. Le DSI a donc décidé de créer une seule base de données, ce qui a demandé au comité exécutif une séance de travail de trois heures par mois pendant un an afin de déterminer quelles informations l'entreprise souhaitait partager. Aujourd'hui, l'entreprise en question est la seule entreprise à avoir une seule base de données et un système SAP mondial. Les comités exécutifs qui parviennent à mener ce type de travail font monter leur entreprise. Les autres empêchent la leur de rester en haut.

Il existe plusieurs types de DSI. Je me suis inspiré d'un graphique d'Alain Deschênes, directeur informatique d'une grande banque française, classant les DSI selon leurs objectifs, leur habitat, leurs prédateurs et leurs outils. L'objectif du « DSI Bouc-émissaire » est de survivre, son habitat est sous le bureau, ses prédateurs sont tout le monde et ses outils, les rapports et les incidents. L'objectif du « DSI Central » est de mettre en place des standards. Il travaille au siège, ses prédateurs sont les seniors VP qui l'entourent et ses outils sont Gartner et PowerPoint. Le « DSI Ego Maximus », capable de poser un veto, peut approuver ou désapprouver les projets. Grâce à sa capacité à dire non, il commence à avoir beaucoup de pouvoir dans l'entreprise. Ses prédateurs sont les responsables métier, qui veulent que les projets soient approuvés, et il travaille avec une équipe faisant de la faisabilité projet. Le « DSI *Back office* » est chargé par le DG de réduire les coûts. Les revues budgétaires constituent son habitat. Ayant du budget, il commence à faire peur dans l'entreprise. Ses prédateurs sont les *outsourceurs*, les directeurs financiers et les métiers. Ses budgets lui permettent d'établir un tableau de *benchmark* important. ●

Quel modèle de gouvernance du SI pour « l'entreprise numérique » ?

Table ronde animée par **Claude Cargou,** ancien président de l'**IFACI** et du **CIGREF**

Pascal Antonini, associé, **Ernst & Young,** président, **AFAI**

Pascal Buffard, directeur général, **AXA,** vice-président, **CIGREF**

Harry Guez, directeur Groupe de l'audit informatique, **Vivendi**

Denis Pétonnet, directeur du système d'information des fonctions Groupe, **Orange-France Télécom**

Claude Cargou : *Quels sont les fondamentaux d'une bonne gouvernance dans vos entreprises respectives ? Où souhaitez-vous faire porter vos efforts afin que cette gouvernance atteigne les objectifs que vous vous êtes assignés ?*

Claude Cargou

Pascal Buffard : Voilà dix ans que le CIGREF s'interroge sur le terme « bonne gouvernance » et sur les relations à tisser entre la DSI, les directions métiers et la direction générale pour créer de la valeur pour l'entreprise. Avec McKinsey, nous avons publié trois livres blancs sur cette question en 2002, 2004 et 2008. Ils sont accessibles sur notre site internet. Nous avons également, compte tenu de la numérisation toujours croissante du monde et de nos entreprises, produit des démonstrations statistiques qui ont abouti à la publication, fin 2009, d'un quatrième livre blanc avec Capgemini Consulting. Nous y tentions, à travers des questionnaires en face-à-face et *on line*, de quantifier les fondamentaux mis en évidence au cours de nos années de travail scientifique sur le sujet.

Toutes les entreprises n'en sont pas au même niveau de maturité en termes de création de valeur par les systèmes d'information, même si des progrès substantiels ont pu être observés ces dernières années. Je vais donc m'attacher à vous parler du niveau de maturité le plus élevé, dans lequel se retrouvent 42 % – déjà ou seulement – des grandes entreprises françaises.

Dans ces entreprises, les fondamentaux de la fonction SI sont maîtrisés, ce qui signifie qu'on fait ce que l'on dit, et qu'on le fait bien. On livre donc les projets dans les délais en tenant à la fois la qualité de service, les coûts et les budgets. Ce point est essentiel.

Par ailleurs, les DSI y ont mis en œuvre, de concert avec la direction générale et les directions métiers, des partenariats forts.

Dans ce cadre, nous avons développé de nouvelles compétences. Nous savons aujourd'hui mesurer la valeur du système d'information, ce qui aboutit à mettre en œuvre des systèmes de gouvernance intégrés avec les grands métiers de l'entreprise nous permettant de garantir un alignement stratégique et la valeur attendue des investissements. Nous sommes, de ce fait, plus agiles et adaptables aux évolutions de l'environnement.

Claude Cargou : *Harry Guez, en tant qu'auditeur informatique, comment voyez-vous une bonne gouvernance ?*

Harry Guez : Vue de la fenêtre Vivendi, une bonne gouvernance implique que la direction générale et la DSI partagent une vision commune de l'entreprise numérique, de ses fondamentaux, de

son écosystème et de ses risques. Au sein des DSI de notre Groupe, nous observons que le numérique a bousculé la façon d'aborder les systèmes d'information et d'appréhender les services qui y sont liés, notamment avec l'émergence de nouvelles directions telles que des directions de l'innovation, de l'expérience client ou de l'internet vivant à côté des directions marketing et pouvant faire appel à des compétences informatiques. Ces nouvelles directions sont amenées à fournir des écosystèmes lorsque la DSI est déconnectée des problématiques métiers ou perçue comme un frein en raison de ses *process* et de ses cycles de décision ou de priorisation, jugés parfois trop contraignants.

Compte tenu de ce virage numérique, la gouvernance doit être renforcée et redéfinie afin que la DSI reprenne la main,

Harry Guez

avec l'appui des directions métiers, sur un système d'information qui lui échappe parfois. Aujourd'hui, lorsque les directions marketing veulent commercialiser un produit sur internet, elles font appel à des *web agencies*. Ces agences développent, par exemple, un site marchand dont le développement, hors des standards SI imposés par l'entreprise et faute de concertation avec les entités compétentes, peut finir par poser des difficultés en termes de continuité et de sécurité. Lorsqu'on est face à un réel problème, on fait alors appel à la DSI, qui s'aperçoit un peu tardivement qu'elle a été court-circuitée.

Comment renforcer la gouvernance pour que la DSI ait sa place et puisse garantir les actifs qui sont sous sa responsabilité ? La gouvernance doit faire en sorte que les organisations, les *process* et les hommes deviennent de plus en plus agiles.

Enfin, pourquoi parle-t-on de « gouvernance SI » et non de gouvernance de la *supply chain* ou de gouvernance RH ? La gouvernance du SI est devenue un enjeu à part entière parce que les DSI n'ont pas bénéficié de l'écoute suffisante, ou œuvré dans ce sens, leur permettant d'accomplir leur tâche dans un environnement favorable. Elle doit cependant être appréhendée dans le cadre d'une gouvernance plus globale de l'entreprise. En conclusion, faire comprendre à nos dirigeants que les SI sont une source d'innovation et de création de valeur est un combat de tous les jours.

Claude Cargou : *Denis Pétonnet, France Télécom partage plusieurs terrains concurrentiels avec Vivendi. Vous devez vivre vous aussi le développement de nouveaux écosystèmes numériques.*

Denis Pétonnet : Je partage la déclaration d'Harry Guez, même si des interrogations sont permises quant à la responsabilité des DSI. Je considère moi aussi que la gouvernance IT n'existe pas. Elle s'intègre à une gouvernance globale de l'entreprise. Nous avons récemment lancé l'offre quadruple *play Orange Open*, qui réunit sur un seul tuyau la voix, la télévision et internet. Ce projet est passé en comité d'investissements Groupe. Il a nécessité une gouvernance globale dans la mesure où il impliquait des investissements pour les boutiques, le marketing, le réseau et l'IT.

Je répondrais tout de même à Harry Guez que lorsque le métier rencontre des difficultés, il trouve souvent plus commode de rejeter la faute sur l'IT. Une relation de sincérité et de transparence, voire le travail sur une plateforme commune ou en équipes intégrées, sont donc nécessaires. Les petits jeux politiques sont derrière nous. Nous essayons aujourd'hui de progresser ensemble pour l'entreprise.

Je rejoins par ailleurs les propos de Pascal Buffard. Le DSI n'est crédible que s'il sait maîtriser les fondamentaux de son IT, qui comprend, d'une part, la base installée des actifs logiciels et matériels et, d'autre part, les projets correspondant aux questions d'innovation. On ne fera appel au DSI pour cette deuxième partie que s'il est exemplaire sur la première. Dans le cas contraire, le marketing fera appel à une *web agency*.

Enfin, concernant les projets, les processus de décision doivent être clairs. Les communautés IT et *business* doivent donc faire preuve d'une certaine obstination afin que la répartition des rôles soit respectée, sous peine que certains pôles de décisions ne partent à la dérive. La discipline est essentielle au sein de l'entreprise. Dans cette perspective, le *top management* doit être impliqué et afficher les règles.

L'une des missions fondamentales de la DSI dans le cadre des projets développés avec le business est par ailleurs d'expliquer la valeur ajoutée apportée par ces projets afin d'éviter que l'IT reste considéré comme un centre de coûts. Développer un site en ligne ou fournir des informations en temps réel aux personnels, des *call centers* en ligne avec les clients, apportent une valeur ajoutée immédiate. Certains managers pensent encore que l'IT sert à automatiser les processus et à réduire les coûts mais aujourd'hui, le rôle de l'IT est bien plus important.

Claude Cargou : *Pascal Antonini, vu de votre poste d'observateur et d'intervenant, où pensez-vous qu'il reste des progrès à faire ?*

Pascal Antonini : J'interviens régulièrement en tant qu'auditeur externe, notamment dans le cadre de la certifica-

tion des comptes des entreprises, ce qui me permet d'avoir un regard sur bon nombre de systèmes d'information. Jean-Pierre Bouillot a parlé de « soxisation ». Je crois comme lui que l'écueil à éviter serait de se reposer sur des dispositifs de contrôle interne uniquement fondés sur le fait de cocher des *checklists*. Il est impératif de se reposer les bonnes questions. Le rôle des auditeurs internes et externes, pas mal représentés à l'AFAI, est d'aiguillonner l'organisation et la DSI pour les remettre sur la bonne voie.

Pascal Antonini

Aujourd'hui, la mobilité et l'usage du *cloud* posent la question du périmètre du système d'information. Les entreprises les plus matures ont peut-être pris en compte ces éléments, apparus sous l'impulsion des directions métiers, mais nombre d'entre elles ne les ont pas développés en cohérence avec le reste de leur organisation. Des efforts restent à faire afin que des règles claires permettent d'atteindre les objectifs de la gouvernance, à savoir la création de valeur et la maîtrise des risques dans un environnement de coûts maîtrisés.

Le sujet de la gouvernance n'est pas au cœur de la préoccupation du commissaire aux comptes, mais lorsque l'on vérifie que l'information comptable et financière est exacte, la question de la maîtrise du système d'information se pose. Dans le cas d'entreprises numériques, les forces de vente passent des contrats depuis un site externe. Les éléments liés au système d'information doivent de ce fait être pris en compte. La gouvernance du système informatique concerne donc également les auditeurs externes.

Pascal Buffard : Pour illustrer ce que je considère comme une gouvernance intégrée dans le cadre d'un partenariat fort avec les métiers, je voudrais reprendre l'exemple du site web confié par la direction marketing à une *web agency*. Je considère que nous sommes responsables de cette situation. Si nous en sommes là c'est que nous n'avons pas su répondre correctement à l'attente de cette direction, notamment en termes d'agilité, par exemple lorsqu'il s'est agi de mettre rapidement en ligne sa dernière campagne de publicité. Ces difficultés sont récurrentes. Nous avons toujours répondu de manière ad hoc lorsque de telles questions nous ont été posées. Nous n'avons par conséquent jamais été compétitifs, en termes de coûts, ni en termes de délais.

Chez Axa, je viens de mener une réflexion sur ce point au niveau mondial. Nous avons créé des *turnkey websites*, ou « sites web sur l'étagère », qu'il faut quinze jours et 20 000 euros pour rendre exploitables. Nous sommes tout à coup devenus très intéressants pour les directions marketing dans la mesure où nous étions plus compétitifs que les *web agencies* et en conformité avec les standards de l'entreprise, à la fois au niveau informatique et en termes de préservation de l'image.

Aujourd'hui, nous montons des partenariats avec nos directions marketing au niveau mondial, mais il ne suffit pas, pour créer de la valeur, de mettre cette information en ligne. Les internautes doivent aussi avoir envie d'y accéder. C'est la raison pour laquelle nous investissons également en matière de *Web analytics* et de *Search Engine Optimization*.

Pascal Antonini : Il y a quelques années, je suis intervenu dans une entreprise qui avait contacté sa DSI pour mettre en place un site web. Celle-ci lui avait indiqué ne pas être capable de le faire dans les délais. La décision avait donc été prise de faire appel à une *web agency*. A l'époque, les aspects de maîtrise des risques et de gestion de la sécurité n'avaient pas été bien conçus. Un incident a affecté l'entreprise et nécessité un audit qui a mis en évidence des carences significatives en matière de sécurité et de contrôle interne. L'internalisation n'est pas toujours la meilleure des solutions mais lorsqu'on externalise, il est nécessaire de se poser les bonnes questions au bon moment.

Claude Cargou : *J'ai retenu de nos discussions l'importance du principe de réalité. Parler de mettre en place une bonne gouvernance n'a de sens que si les fondamentaux sont respectés. La question du périmètre du système d'information se pose également. Aujourd'hui, des écosystèmes se développent de plus en plus et créent de la valeur. Comment appréhendez-vous l'évolution du périmètre des systèmes d'information dans vos entreprises ?*

Harry Guez : Dans l'entreprise numérique, nous percevons que la différence entre l'informatique personnelle et professionnelle se réduit de plus en plus. Certains sites de nos métiers offrent la possibilité, via des liens Facebook ou Twitter, de donner un avis au vu de tous sur les contenus diffusés ou d'interagir en direct. Ces frontières sont de plus en plus difficiles à gérer ainsi que les risques associés. On parle aujourd'hui d'e-réputation. Comment manage-t-on l'information véhiculée ? Dans nos métiers, nous mettons en œuvre les moyens nécessaires à créer et diffuser du contenu accessibles n'importe quand et sur n'importe quel média. Comment protéger les contenus métiers diffusés ? Et par ailleurs, comment collecter l'information associée à l'usage de ces contenus, disséminée sur de petits et de grands sites webs comme sur le poste même de l'utilisateur ? Les frontières entre informatique professionnelle et

personnelle tendent à s'estomper. Tous les commerciaux peuvent d'ores et déjà accéder à leur base clients via leur BlackBerry ou leur ordinateur portable connecté. Comment continuer, au niveau des DSI, à maîtriser un écosystème qui évolue sans cesse.

Pascal Buffard : Nos entreprises sont sorties de leurs limites physiques depuis des années, avec une architecture métiers de plus en plus ouverte. Par exemple, lorsque vous êtes client d'Amazon, vous ne l'êtes pas vraiment mais l'entreprise veille à garder sa *customer intimacy* et à assurer la qualité et la compétitivité du service fourni. Dans le monde de l'assurance des biens, nous ne nous contentons plus d'indemniser nos assurés. Nous prenons en charge les problèmes qui leur causent un stress

Pascal Buffard

afin de les en dégager en mobilisant un réseau de partenaires dans un écosystème large. Leurs problèmes seront résolus sans qu'ils n'aient eu besoin de payer le moindre euro.

Pour sortir de ses frontières naturelles, l'entreprise doit mettre en œuvre des systèmes d'information multiples, qu'elle ne connaît pas toujours, et dont la gouvernance exige une vision intégrée avec les directions métiers. Les partenariats d'offre et de distribution sont devenus une réalité dans de nombreuses entreprises avec la « servicisation » du produit. Dans la chaîne de valeurs de SFR, l'interaction avec le client est au moins aussi importante que l'appel téléphonique, même s'il se doit d'être de qualité. L'élément de différenciation réside dans l'alignement parfait entre les métiers et la DSI en termes de gouvernance.

Claude Cargou : *Toutes nos entreprises sont soumises à des contrôles plus contraignants depuis quelques années. Les règlements visant à s'assurer que l'intérêt des parties prenantes est bien protégé s'alourdissent d'année en année. Parallèlement, des référentiels et des méthodologies ont été publiés comme le CobiT, Val IT, Risk IT, ITIL ou le guide d'audit « Gouvernance du système d'information » publié conjointement par le CIGREF, l'IFACI et l'AFAI. Comment vivez-vous l'augmentation du poids du contrôle ? Les outils de contrôle sont-ils trop nombreux, et risquent-ils d'annihiler les développements envisagés à l'intérieur des entreprises ?*

Pascal Antonini : Il faut éviter d'en arriver aux dérives liées à certains projets SOX qui ont conduit à la mise en œuvre de dispositifs trop lourds, mais disposer de différents référentiels n'impose pas de devoir tous les appliquer à la lettre. Ils sont des guides auxquels se référer. Il faut adapter l'utilisation des référentiels à la culture de l'entreprise dans une approche très pragmatique. Dans certains cas, des raccourcis peuvent être opérés. Concernant la certification, elle relève d'un choix de l'entreprise et doit lui apporter un avantage compétitif.

Harry Guez : Je partage l'avis de Pascal Antonini, mais jusqu'à quand les référentiels se développeront-ils ? Vu de ma fenêtre, j'ai l'impression qu'on ajoute des référentiels aux référentiels. Ils doivent être perçus comme des guides ; leurs utilisateurs doivent toujours garder à l'esprit ce qu'ils en attendent. Parfois, on peut se demander pourquoi certains tiennent absolument à les suivre à la lettre. La certification ISO 27001 telle que parfois déployée, peut notamment consister à élaborer de très nombreuses

***Pascal Antonini** est président de l'AFAI et associé au sein de l'activité Advisory d'Ernst & Young. A ce titre, il conduit des missions de conseil sur les risques informatiques dans de nombreuses organisations. Il intervient également dans les systèmes de gouvernance auprès des DSI.*

***Pascal Buffard** travaille chez Axa depuis plusieurs années. Il a été CIO puis COO et secrétaire général d'Axa France. Il est désormais directeur général d'Axa Group Solutions, une entité qui développe les applications de convergence du Groupe. Il supervise également AXA Technology Services qui regroupe tous les moyens d'exploitation et de télécommunications pour l'ensemble des sociétés du Groupe. Pascal Buffard est par ailleurs vice-président du CIGREF.*

***Harry Guez** a rejoint le Groupe Vivendi en 2005 en tant que directeur Groupe de l'audit informatique. Il y coordonne tous les plans d'audit IT, en France comme à l'étranger. Il est également impliqué dans des projets spéciaux d'ordre présidentiel comme les acquisitions ou les évaluations de programmes de transformation.*

***Denis Pétonnet** est DSI des fonctions corporate à France Télécom après y avoir occupé plusieurs postes, dont des fonctions opérationnelles de direction. Il a également travaillé, au sein du Groupe, sur la gouvernance des systèmes d'information.*

procédures. Pourtant dans la pratique, et malgré la certification, la sécurité souffre bien souvent de lacunes importantes. Les fondamentaux opérationnels n'y sont pas correctement appréhendés.

Pascal Buffard : On a trop souvent confondu les moyens et l'objectif des référentiels, qui peuvent nous aider à progresser dans la maîtrise des risques opérationnels. Je considère, en tant que DSI, que CMMI n'est pas une fin en soi. Elle peut en revanche permettre de s'intéresser aux meilleures pratiques dans un environnement déterminé. La certification n'en sera que la conséquence. Vouloir obtenir la certification pour elle-même fait prendre le risque de passer à côté de sa valeur. Il est donc nécessaire de faire preuve de bon sens et d'humilité. Les référentiels sont des leviers nous permettant de progresser dans la compréhension de sujets que nous souhaitons mieux maîtriser.

Denis Pétonnet : Le grand danger des référentiels est en effet leur application dans un esprit strictement technique comme un jeu de procédures. N'oublions pas que nous avons des obligations de sécurité vis-à-vis des clients qui nous confient leurs données personnelles en ligne. J'ai pour ma part travaillé sur la conformité des systèmes IT de France Télécom avec SOX. Nous avons rencontré des difficultés pour rappeler le sens de ce référentiel en amont et faire le tri entre l'indispensable et ce qui pouvait être reporté. Nous faisions très régulièrement des points entre les auditeurs et le projet opérationnel afin de s'assurer que nous étions bien en ligne.

Denis Pétonnet

Aujourd'hui, des questions similaires se posent lorsque nous parlons de la sécurité des paiements, avec les recommandations de nos partenaires, comme PCI DSS. S'il s'agit d'appliquer 250 pages de recommandations, il est nécessaire de revenir au sens global, à savoir qu'un client payant en ligne doit être certain que ses données ne seront pas corrompues ou volées. Souvent, la mise en place de mesures opérationnelles doit venir compléter ce que préconise la norme.

Lorsque l'activité informatique est externalisée, le fait que le prestataire soit conforme aux normes est un confort, mais il est souvent nécessaire d'accompagner le partenariat d'accords contractuels imposant des visites dans ses infrastructures et ses sites ou des revues bilatérales.

Claude Cargou : *Imaginez que je suis votre directeur général. Vous disposez de trois minutes pour me formuler des recommandations afin que je réussisse la mise en place d'une bonne gouvernance.*

Harry Guez : Je vous recommanderais d'abord de me recevoir plus souvent ! Une communication plus fluide entre le DSI et les plus hautes instances de l'entreprise est fondamentale. Le DSI doit pouvoir s'exprimer, échanger, proposer. Si ce canal n'est pas mis en place, comme on l'observe souvent, une évolution sera difficile. Au sein du Groupe Vivendi, les DSI ont des positions très diverses. Chez SFR, où l'informatique est un élément clef, le DSI est un directeur général en prise directe avec la direction. Ailleurs, il est parfois beaucoup plus difficile de se faire entendre.

Pascal Antonini : La communication me semble être un point central. Il est donc essentiel de mettre en place des points réguliers entre la DSI et sa direction. Je vous dirais également que j'ai participé à un colloque très intéressant organisé par le CIGREF, l'IFACI et l'AFAI. Je vous demanderais alors de lancer un audit sur la gouvernance du SI parce que je suis persuadé qu'en appliquant les recommandations contenues dans le guide de l'AFAI, l'audit interne ou externe peut constituer un véritable catalyseur pour faire progresser l'entreprise en matière de gouvernance. En effet, les remarques passent souvent mieux lorsqu'elles sont formulées par quelqu'un de l'extérieur.

Denis Pétonnet : Je vous demanderais, pour ma part, quel modèle d'entreprise vous souhaitez obtenir. Par exemple, dans le Groupe France Télécom, chaque filiale est autonome, avec ses propres dépenses informatiques, ses propres infrastructures et son propre *data center*. Dans le cadre d'un grand projet de mutualisation des infrastructures, il sera nécessaire de discuter en amont de ce que l'on trouve dans le compte d'exploitation des pays. Achètent-ils directement leurs serveurs chez les fournisseurs, ou sont-ils achetés par le Groupe ? Ces interrogations dépendent également du caractère local ou global du marché.

Je vous dirais également que le *business* doit être responsabilisé dans ses projets à composante informatique. Lorsqu'il souhaite transformer ses agences commerciales, une réflexion sur l'évolution des processus doit être menée. Dans le domaine des fonctions support, si la comptabilité envisage de changer son système comptable, choisira-t-elle de mettre en place un service partagé ? Ces principes doivent être actés par le *business*.

Pascal Buffard : Le monde et sa maturité sur ces sujets ont beaucoup évolué. Il n'existe pas de réponse unique, mais des réponses adaptées au contexte de l'entreprise. L'étude que nous avons menée en 2009 avec Capgemini Consulting a montré que 42 % des grandes

entreprises françaises étaient arrivées à maturité dans le domaine de la gouvernance du SI. Nous avons également découvert que 12 % seulement d'entre elles se trouvaient dans un niveau de maturité « très faible ».

Un tel retard de maturité imposera au directeur général de s'impliquer fortement dans l'évolution de sa gouvernance dans le domaine informatique. Il devra en particulier favoriser la prise de conscience des métiers, qui sont en partie responsables de la situation. On a l'informatique qu'on mérite. Si le DSI a changé, qu'une nouvelle gouvernance des fondamentaux est en marche et qu'un dialogue s'est instauré, l'entreprise est arrivée au second niveau de maturité sur les systèmes d'information et leur contribution à la réalisation d'une stratégie. 46 % des grandes entreprises sont dans cette situation.

Enfin, un jour, les entreprises atteignent le niveau de maturité où la DSI parle *business*, enjeux métiers et gestion du changement avec les métiers dans les enceintes de pilotage. En tant que DSI, je vous demanderais de me laisser développer ces compétences. Si vous refusiez, je m'adresserais au DRH de l'entreprise afin de tenter d'aller au bout des investissements pour en tirer un véritable bénéfice. Il m'est, pour ma part, arrivé, il y a très longtemps, d'assister à un comité de direction générale avec un collègue en charge d'une branche très importante de l'assurance. Ce dernier a expliqué : « *Avec Pascal, nous avons construit un extranet pour nos courtiers qui nous donne plusieurs années d'avance sur la concurrence* ». Je l'en remercie encore, mais il a ensuite ajouté : « *L'ennui, c'est que personne ne l'utilise* ». Nous dépensions tous les jours de l'argent pour exploiter un extranet qui ne produisait aucune valeur.

Claude Cargou : *Nous avons beaucoup parlé de gouvernance des systèmes d'information et du lien entre gouvernance et direction générale. Nous n'avons pas évoqué le lien avec les conseils. Je suis moi-même président de deux comités d'audit. Nous ne l'avons pas évoqué aujourd'hui, mais les questions de gouvernance des systèmes d'information remontent déjà à ces comités, notamment sous la forme du rapport sur le contrôle interne que le président doit présenter à l'Assemblée générale et qui doit être contrôlé par les commissaires aux comptes. Dans le secteur financier, il existe un lien direct entre les capitaux propres exigés et la maîtrise des risques incluant les risques opérationnels. L'impact sur la profitabilité est réel en matière de gouvernance ; peut-être serait-il souhaitable de faire remonter plus d'informations ciblées au niveau des conseils.* ●

L'informatique dans les nuages !

Christine Garcia, directeur de l'audit informatique, direction de l'audit interne, **Renault**

Sylvie Sadones, directeur enterprise architecture, direction des systèmes d'information, **Renault**

Le *Cloud Computing* est un concept qui consiste à utiliser des ressources banalisées, distantes ou non pour effectuer des traitements informatiques. Véritable rupture technologique et organisationnelle, le *Cloud Computing* est désormais une réalité et un levier technique et financier au service des entreprises.

Les différents types de *Cloud*

On peut définir trois types de *Cloud* :

- ***Cloud* public :** une même ressource, banalisée et localisée chez un fournisseur, est partagée par plusieurs entreprises utilisatrices ;
- ***Cloud* privé externe :** la ressource est dédiée à une entreprise utilisatrice. Cette ressource est localisée en externe chez un fournisseur ;
- ***Cloud* privé interne :** la ressource est localisée dans le *DataCenter* et gérée par l'entreprise utilisatrice elle-même (cas des entreprises disposant d'une capacité informatique importante, qui peut être optimisée en appliquant les principes du *Cloud*, sans besoin de mutualisation avec l'externe).

Les niveaux de services proposés

Trois niveaux de service progressifs sont distingués, de la simple fourniture de matériel, à la mise à disposition d'une application complète opérationnelle :

- **IaaS –** « *Infrastructure as a service* » : mise à disposition de moyens (serveurs, stockage…) que l'entreprise utilise comme une extension de ses propres moyens techniques.

  Pour offrir des ressources à la demande, de manière quasi-instantanée, les principes consistent à :
  - standardiser des capacités physiques,
  - déployer des serveurs virtuels,
  - orchestrer le déploiement et le retrait des serveurs virtuels sur les infrastructures.

  Ce type de service est utilisé par environ 5 % des entreprises françaises.

- **PaaS –** « *Platform as a service* » : mise à disposition d'une plateforme complète (matériel et logiciel), utilisée par l'entreprise pour développer et installer ses propres applications.
  Son utilisation est encore marginale.

- **SaaS –** « *Software as a service* » : mise à disposition d'un service applicatif complet = abonnement à une application.
  Cette offre est apparue dès le début des années 2000, sous l'appellation d'ASP.
  Ce service est désormais bien développé et est utilisé par environ 25 à 30 % des entreprises françaises.

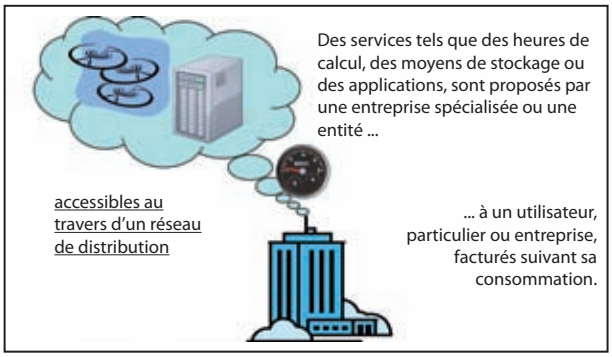


Schéma 1

Le « *Cloud Computing* »

Les principes du « *Cloud computing* » sont assimilables à ceux qui régissent la distribution d'une ressource telle que l'eau ou l'électricité (cf. schéma 1).

Pour les particuliers, l'usage du *Cloud* est déjà banalisée au travers de comptes personnels qui permettent à chacun, par internet, d'accéder, dans le monde entier et à partir de n'importe quel ordinateur, à sa messagerie, à ses données, photos, vidéos, à des jeux en ligne, applications diverses, etc.

Pour les entreprises, il s'agit de disposer de ressources à la demande, sans projet lourd de déploiement d'infrastructures, ce qui permet de considérer les matériels et logiciels comme des « services » loués suivant le besoin.
Mais le modèle économique est encore fluctuant ; les offres des fournisseurs de *Cloud* sont très disparates et doivent être travaillées avant d'arriver à une offre explicite comme celle de l'eau ou l'électricité.

Dans la suite de l'article, seul le point de vue des entreprises est abordé.

Les avantages du *Cloud*

Pour une entreprise, les points forts du *Cloud*, par rapport à une informatique plus traditionnelle, sont :

- une baisse des coûts par la mutualisation des infrastructures et la standardisation / banalisation des applications : les dépenses d'investissements (CAPEX) sont réduites et remplacées par un coût à l'usage (OPEX), au juste nécessaire ;
- une meilleure flexibilité et évolutivité par la mise à disposition rapide des services et l'adaptation en continu au niveau de besoin ;
- une disponibilité des dernières technologies, rapidement et sans nécessité d'investir, en moyens et en compétences.

Les risques du *Cloud*

Cependant, le déploiement du *Cloud* est freiné par un certain nombre de risques, pour l'entreprise utilisatrice :

- risques pour la gouvernance informatique :
  - perte de maîtrise des normes et technologies mises en œuvre par le fournisseur ;
  - difficultés d'intégration entre services disponibles en interne & sur le *Cloud* et entre diverses briques de *Cloud* de fournisseurs différents ;
- risques de dépendance vis-à-vis du fournisseur et de difficulté de réversibilité ;
- risques juridiques, en particulier :
  - non-maîtrise de la localisation des données ;
  - non-destruction de données au-delà des délais légaux de conservation (sauvegardes, archives, …) ;
- risques sur la sécurité des données :
  - disponibilité : perte de maîtrise du système d'information et manque de visibilité sur les dysfonctionnements ;
  - intégrité : risque de perte, de destruction, d'altération par erreur ou malveillance ;
  - confidentialité : risque d'intrusion, d'usurpation ou de non-étanchéité entre les différents utilisateurs ;
  - traçabilité des données et des accès difficile, voire impossible.
- risques liés aux changements d'organisation et à la nécessité de faire évoluer les compétences et les processus.

Le *Cloud Computing* chez Renault

Renault dispose dans son centre informatique d'infrastructures physiques, supportant des systèmes et des *middlewares* et intégrant des applications.
Le mode opératoire permettant de mettre à disposition ces ressources est encore aujourd'hui largement manuel et l'offre proposée est orientée ressource et non pas service.
Afin d'améliorer ses coûts et de diminuer ses délais, des offres assimilables à du *Cloud Computing* ont été abordées dès 2000 par la direction des systèmes d'information de Renault.

Les premières expériences

- **Standardisation et Virtualisation**
  En 2007, le choix d'une plateforme standard X86 et de la virtualisation a permis une rationalisation de la puissance informatique, une accélération des processus de mise à disposition des infrastructures et une focalisation des expertises.
  Au-delà de la virtualisation des serveurs, c'est également la virtualisation du stockage qui a permis à Renault une optimisation réelle de ses ressources.

- **Conception des véhicules (service de type SaaS)**
  En 2008, achat d'heures de calcul à l'extérieur pour les véhicules en développement.
  Limites de cette approche :
  - coût du service au final non différenciant par rapport à un coût interne,
  - assurance de confidentialité insuffisante,
  - service trop spécialisé limitant la flexibilité du nombre d'heures achetées.

- **Messagerie (service de type SaaS)**
  En 2007, messagerie fournie « clef en main », facturée en fonction du nombre de boîtes mises à disposition, avec un objectif de 75 000 boîtes.
  Abandon après une phase pilote limitée à 5 000 boîtes.
  - Essentiellement pour des raisons de confidentialité : réticences internes vis-à-vis du stockage des messages à l'extérieur de l'entreprise.
  - Le coût en interne est peu différent.

- **Hébergement d'un site internet (service de type IaaS puis SaaS)**
  Développement fait par l'informatique Renault en 2000 et exploité sur une infrastructure externe, pour bénéficier de la rapidité de mise à disposition de l'infrastructure.

Christine Garcia *dépend de la direction de l'audit interne du groupe Renault et est en charge de l'audit des systèmes d'information. Ingénieur INSA de Lyon, elle a effectué toute sa carrière au sein de la direction informatique du groupe Renault, avant de rejoindre l'audit interne en 2010.*

Sylvie Sadones *dépend de la direction des systèmes d'information de Renault et est en charge de la direction enterprise architecture. Ingénieur civil des Mines Saint-Etienne et titulaire d'un Master of Science de McGill, elle a effectué la majorité de sa carrière à la direction informatique du groupe Renault. Les missions de la direction enterprise architecture sont de définir et promouvoir les politiques IS/IT, les méthodes et outils architecture, de contribuer à la construction des schémas directeurs et des plans triennaux.*

L'application est transférée en 2007 à un autre fournisseur pour l'évolution et l'exploitation, afin de bénéficier de l'évolutivité de la plateforme, du savoir-faire métier et technologique du fournisseur et d'une rapidité de déploiement dans tous les pays. La responsabilité et la gouvernance sont complètement assurées par le métier Marketing Client.
Quantification : 60 millions de visiteurs annuels pour le site renault dans le monde et 10 millions pour le site Dacia.
Réflexions sur l'évolution du contrat de service :
- difficulté pour appliquer la répartition des responsabilités entre Renault et le fournisseur, telle que définie contractuellement ;
- difficulté pour trouver l'équilibre entre les besoins spécifiques Renault, en termes d'image sur Internet, et la fourniture d'un service standard ;
- difficultés de rapprochement des données gérées en SaaS et en interne.

Les premiers succès

Les expériences précédentes ont permis de définir les conditions de réussite, dans le contexte Renault, et de réunir les conditions favorables pour d'autres applications.

- Accélération de la virtualisation des serveurs (50% du patrimoine des systèmes distribués à fin 2010).

- Externalisation d'environnements de développement (service de type PaaS)

- Achat de services, en particulier dans le domaine RH (service de type SaaS) Exemple : gestion du plan de formation et des évaluations des collaborateurs à partir d'une plateforme *Cloud* RH partagée par plusieurs centaines d'entreprises.
  Pour Renault : environ 20 000 utilisateurs depuis 2005.

- Logiciels embarqués à bord des véhicules : fourniture de services aux clients de Renault (service de type SaaS) :
  - par Carminat Tom Tom et depuis 2009 : accès en temps réel à partir du véhicule à des services tels que l'info trafic, les alertes Sécurité Routière, la recherche locale avec Google, la météo… ;
  - plus d'un million de véhicules Renault sont équipés dans le monde ;
  - pour les véhicules électriques, s'ajouteront entre autres la localisation de stations de recharge, la consultation à distance du niveau de charge des batteries.

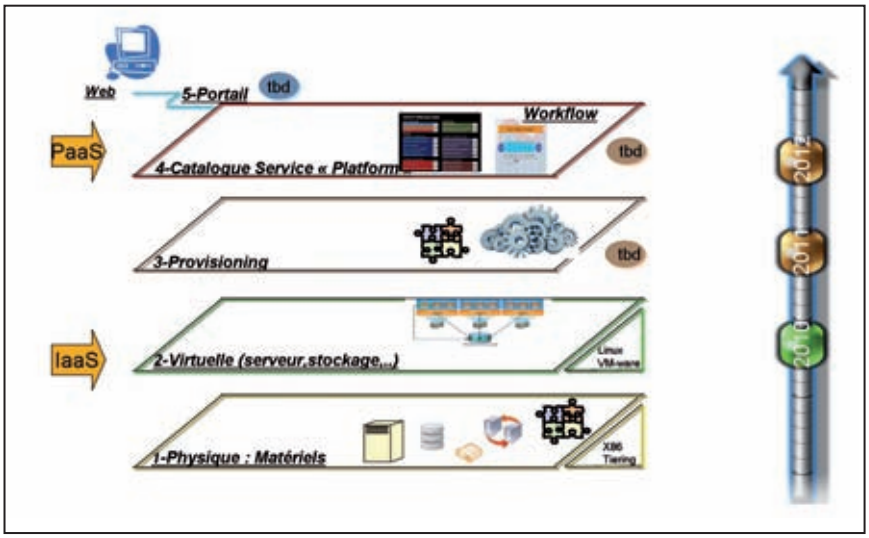


Schéma 2

La généralisation, la stratégie et ses enjeux

Suite à ces premiers bilans positifs, un projet de *Cloud* IaaS à grande échelle a été lancé début 2011.

Son objectif est de réduire le délai de mise à disposition des ressources en offrant la possibilité, via un portail sur l'intranet Renault, de commander des services, soit IaaS, soit PaaS, grâce à une forte standardisation et à de l'automatisation.
Avantages attendus :
- infrastructure flexible masquant le physique et allocation dynamique des ressources sur l'ensemble de la capacité installée ;
- accès automatisé à des services « plateforme » standards et robustes ;
- visibilité sur le délai de fourniture du service et sur le coût de son usage ;
- standardisation des compétences techniques nécessaires ;
- gain sur les licences par optimisation du nombre de serveurs physiques ;
- informatique plus écologique *(« Green IT »)*, par optimisation de la consommation électrique.

La prise en compte des risques liés à la sécurité physique et logique et des risques technologiques conduit à s'orienter dans un premier temps vers un ***Cloud* privé interne**.

Les étapes de mise en œuvre (2010 - 2013)

1. Optimiser les infrastructures actuelles :
   - Réduire le nombre de serveurs : consolidation.
   - Migrer vers la cible (réalisé à 50 % à ce jour).
2. Virtualisation des serveurs et du stockage : 50 % aujourd'hui, 90 % en 2013.
3. Allocation automatique de ressources *(« provisionning »)*.
4. Mise en place d'un catalogue de services « *Platform* », à disposition de l'informatique interne. Chaque service correspond à la mise à disposition d'une plateforme (matériel, logiciel,

supervision …) « clef en main » pour installer ensuite une application d'un type donné (SAP, portail, réseau social, calcul …).

5. Mise à disposition d'un portail et d'un *workflow* pour gérer les demandes.
(Cf. schéma 2).

Positionnement de Renault en 2011 sur la matrice de maturité du **cabinet IDC** et cible Renault en 2013 sur un *Cloud* privé interne

2011 → 2013

Phase / Impact	Pilot	Consolidation	Assured Computing	Private Cloud
Staff Skills	Little or no expertise	Hands on expertise; some formal training	Formal training; certification desirable	Certification required
Technology & Tools	Simple static partitions	Simple Mobility: Manual & Off-hours Matched application pairs	Portable Applications: Automated Failover CMDB Implemented	Policy based automation; Service management; Lifecycle Mgmt; Self Service Delivery
Financial Impact	No substantial financial impact	Measurable Hard Cost Savings: Consolidation Power/Real Estate	Justified TCO savings: Business Continuity	Variable costs recognized or charge back models established
IT Process & Policies	Skunk Works	Ad hoc	Partially Integrated; Partially Standardized	Fully Integrated Fully Standardized
Line of Business	Hidden	Revealed	Transparent	Engaged in Governance Process
Application Usage	Test Development	Production: Non-critical	Production: Business Critical	Production: Service Profiles & Catalogs
% of Customers	15%	55%	25%	5%
Average VM Density	4	6	10	35
Experience	9-12 months	9 months - 2 years	1.5 - 3 years	3-5 years
% Virtualized Servers	<10%	25%	50%	80%

Suite aux premières expériences effectuées au sein de l'entreprise, il apparaît que la vigilance lors d'un audit doit être renforcée sur certains points :

- la sélection du fournisseur et la contractualisation (clarté des responsabilités du fournisseur, nature des livrables, le pilotage de la performance (SLA), clause d'audit, réversibilité…) ;
- la capacité de l'entreprise à formaliser ses besoins et la réalité des gains informatiques et *business* ;
- la transparence des processus de contrôle interne du fournisseur ;
- la gestion des données, en particulier la localisation, la confidentialité et la traçabilité, en conformité avec les législations ;
- la sécurité logique et la gestion des accès, la garantie de moyens contre les brèches de sécurité, la détection et la gestion des éventuelles intrusions ;
- l'intégration entre services *Cloud* et applications internes.

* *
*

La politique technique de Renault, et son déploiement depuis 2007, ont permis d'atteindre le niveau de consolidation et de maturité nécessaires pour permettre la dernière étape vers le ***Cloud* privé interne** à l'horizon 2013. Tout cela pour obtenir bien sûr les gains économiques, mais surtout pour fournir des services et des systèmes d'information aux métiers de l'entreprise dans des délais optimisés, et avec une flexibilité et une qualité supérieures.

Le choix de solutions **SaaS** est étudié et mis en œuvre pour les fonctions de l'entreprise pour lesquelles les risques énumérés plus haut sont faibles et contractuellement traités.

Des études du modèle PaaS sont en cours, mais il ne doit pas interférer avec la politique technique définie. ●

NDLR : Comme annoncé dans Les Echos du 3 août 2011, un protocole aurait été signé entre l'Etat, et Orange, Thales et Dassault Systèmes avec pour objectif de créer un « Cloud Computing » à la française.

L'informatique Renault en quelques chiffres

Entretien avec Lord Smith of Kelvin

Propos recueillis par **Alice Hoey**

« De par sa position unique au sein de l'entreprise, l'auditeur interne est dans une situation idéale pour évaluer les risques liés à la culture d'entreprise », affirme Lord Smith of Kelvin.

« J'ai eu l'occasion et le privilège d'observer de près la fonction d'audit interne et d'influer sur la manière dont elle s'intègre dans le gouvernement d'entreprise. Depuis la publication de mon rapport[1], en 2002, à la suite du scandale Enron, l'audit interne a fait du chemin, et quel chemin ! Il fait désormais partie intégrante de toutes les grandes organisations et contribue à fournir une assurance sur la maîtrise des activités. L'attitude des dirigeants face à l'audit interne a également changé, tandis que les relations entre les comités d'audit et l'audit interne se sont structurées.

Cependant, les auditeurs internes ont encore beaucoup de chemin à parcourir pour apprendre à « se glisser dans la peau » de l'entreprise, c'est-à-dire comprendre son style de management, ses enjeux et les stimuli culturels qui sous-tendent son fonctionnement et sa stratégie. Car c'est ce qui compte réellement.

L'affaire Enron a marqué un tournant dans l'histoire de l'audit interne, de l'audit externe et du gouvernement d'entreprise. Elle a donné lieu à des mesures politiques et réglementaires qui ont renforcé le rôle de l'audit interne, tandis que les entreprises se sont efforcées de prendre en compte l'importance fondamentale de cette fonction.

La crise financière a tout autant compté dans l'évolution de l'audit interne, notamment en conduisant les professionnels à faire un travail d'introspection qui, aussi loin que je m'en souvienne, n'avait jamais été aussi poussé. Cette crise a créé un espace idéal au développement de l'audit interne, lui permettant d'élargir le champ de ses interventions aux risques stratégiques de l'entreprise. Si les professionnels savent saisir l'occasion, le métier et son rôle de conseiller de confiance vont continuer à s'imposer. Le lien déjà solide entre comités d'audit et auditeurs internes n'en sera alors que plus fort.

S'interroger, toujours

Il est important de comprendre que ce n'est pas l'inadéquation des contrôles ou une fraude qui peut causer la perte d'une société. Ces événements peuvent exacerber une situation de crise ou porter le coup de grâce en cas de problème, mais ils ne seront pas la cause de la faillite de l'entreprise. Ce qui cause véritablement la perte d'une société, ce sont les comportements inadaptés découlant de sa culture de management – la cupidité, l'orgueil, l'intimidation ou la dissimulation, qui débouchent sur des perspectives de croissance faussées et des prises de décision mal fondées. Comme le dit le dicton, « le poisson pourrit toujours par la tête ».

Un bon comité d'audit doit, par conséquent, comprendre non seulement le fonctionnement, la stratégie et les transactions de la société, mais également ce qui les sous-tend, ce qui en est à l'origine et comment les décisions sont mises en œuvre. Il doit s'efforcer d'intégrer toutes les facettes de la culture de l'entreprise. Nous ne pourrons peut-être pas empêcher une autre crise, mais telle doit être notre ambition. Lorsque tout va bien, il est difficile de se poser régulièrement la question « Et si ? », mais la fonction d'audit interne est justement là pour ça. Les auditeurs internes se doivent d'être sceptiques, tout en fournissant l'assurance que les risques sont connus et mesurés.

*Actuellement président du Groupe Weir et de Scottish and Southern Energy, **Lord Smith** a également été président ou administrateur indépendant de plusieurs grandes entreprises publiques britanniques au cours des dix dernières années. C'est en occupant ces fonctions qu'il a pu mesurer toute l'importance de l'audit interne pour les entreprises.*

En 2003, Lord Smith a rédigé le rapport Smith Guidance, *qui a depuis été incorporé aux directives publiées dans le code de gouvernement des entreprises britanniques. Ces directives ont fait l'objet de révisions en 2008 et en 2010. Elles sont fondées sur l'idée que les qualités personnelles des membres du comité d'audit sont plus importantes que leurs compétences techniques et financières.*

©mentalrai - Fotolia.com

En étant toute l'année dans l'entreprise, qui donc mieux que vous peut se forger une opinion objective sur la finalité économique des activités exercées par l'entreprise, et pas seulement sur les contrôles qui les entourent ? Les auditeurs internes doivent délibérément se mettre en quête des risques non maîtrisés, se poser la question « Et si ? » et être en mesure de décrire la réalité économique des produits et services offerts par leur société. Voilà la véritable opportunité de sortie de crise. Mais pour comprendre ce que vous auditez, vous avez besoin de personnes de grande qualité, qui ont accès aux bonnes informations, qui prennent part aux bonnes discussions et qui disposent des moyens de travailler en toute objectivité.

Les équipes dirigeantes doivent intégrer les équipes d'audit interne dans leurs discussions stratégiques et dans le processus de développement de produit, afin de bénéficier de leur vision globale et de savoir quel niveau de maîtrise des risques doit être atteint. Les auditeurs internes, quant à eux, doivent mesurer l'appétit pour le risque, la qualité globale du gouvernement d'entreprise et le levier financier de l'entreprise.

La prochaine génération

Les services d'audit interne sont probablement une des clés d'un gouvernement d'entreprise et d'une gestion des risques efficaces. Leur position au sein de l'entreprise est unique et ils peuvent couvrir des domaines de risques bien plus larges que ne pourrait le faire une équipe d'audit externe.

Même si elle est rémunérée par l'entreprise qu'elle contrôle, l'équipe d'audit interne occupe un espace à part, le *no man's land* entre l'organe de direction et les administrateurs non exécutifs. Dans le cas des sociétés cotées, c'est la passerelle qui relie les représentants des actionnaires à ce qui se passe concrètement dans la société. Ce rôle requiert de la subtilité et un véritable courage.

Quand je regarde les dix dernières années, je suis extrêmement fier de la façon dont l'audit interne a évolué. La qualité des personnes qui choisissent cette profession, l'interaction entre les comités d'audit et les équipes d'audit interne, la valorisation du statut et du rôle de l'audit interne au sein des entreprises sont des signes rassurants. Toutefois, pour passer à la vitesse supérieure, nous devons concentrer notre attention sur les aspects comportementaux et la culture de l'organisation. Cela ne doit pas se faire au détriment du processus d'audit en tant que tel bien sûr, mais nous savons tous que l'application consciencieuse des procédures n'a pas aidé les banques à éviter la crise de 2008. Nous devons progressivement comprendre quelles sont les motivations intimes qui sous-tendent les projets et les opérations menées par les entreprises.

C'est en cela que les administrateurs ont besoin de l'audit interne. Ils ont besoin de son objectivité et de son intégrité. Vous pouvez lire les informations destinées aux comités d'audit, comprendre les activités et la stratégie de l'entreprise, ou encore voir les cours monter ou descendre en fonction des risques, tout bon comité d'audit se doit aussi de comprendre comment tout cela survient. La crise financière fournit aujourd'hui les conditions idéales à l'élargissement du rôle de la profession. » ●

[1] *Smith Guidance for audit committees.*

Article initialement paru dans la revue « Audit & Risk » (IIA UK)

Vous pouvez approfondir ce sujet en assistant au colloque :

Les variables culturelles du contrôle interne

Lundi 17 octobre 2011

Pour consulter le programme complet du colloque et vous inscrire, rendez-vous sur le site www.ifaci.com

Des relations commerciales de plus en plus cadrées par des contrats

Beatriz Sanz Redrado - Directrice de l'audit interne, **Groupe Galeries Lafayette**

Diplômée d'ICADE, de l'université de Humberside et détentrice des certifications DPAI, CIA et CFE, ***Beatriz Sanz Redrado*** *est en charge de la direction de l'audit interne du Groupe Galeries Lafayette qui regroupe, entre autres, les enseignes Galeries Lafayette, BHV, Monoprix, Laser Cofinoga et Louis-Pion Royal Quartz.*

Bien que la formalisation des échanges entre deux parties ne soit pas obligatoire d'un point de vue légal, il est très courant (et fortement recommandable) de formaliser les droits et engagements entre l'organisation et ses partenaires. Deux avantages sont incontestables :

- l'impossibilité pour une des parties de modifier le contrat de façon unilatérale, et
- servir comme preuve en cas de désaccord lors de la mise en application du contrat.

Ainsi, sans formalisation, les malentendus peuvent apparaître facilement : quelle qualité livrer, quelle mesure utiliser, quelles analyses réaliser, qui prend en charge les assurances lors du transport des marchandises, quels indices utiliser pour la révision des prix…

L'audit des directions juridiques commence à figurer dans les plans d'audit des sociétés françaises. Toutefois, dans la quasi-totalité des missions d'audit réalisées, la vérification de certains contrats, ou d'un certain nombre de clauses, est partie intégrante des missions. En effet, avec la judiciarisassion des affaires, les pratiques entrepreneuriales sont de plus en plus sécurisées via des contrats.

Qu'il s'agisse d'achat ou de vente de marchandises ou de prestations intellectuelles, les contrats tendent à cadrer les relations commerciales et les auditeurs et/ou contrôleurs internes doivent connaître les principaux risques et les réflexes clés pour bien maîtriser la tâche qui leur est confiée dans la lettre de mission.
Le service juridique des organisations dispose souvent des modèles pour les différents types de contrats que l'organisation pourrait être amenée à signer. Il est très utile de se procurer un exemplaire et de discuter avec ce service des clauses qui doivent faire l'objet d'analyses et de vérifications dans toute mission d'audit. D'autres organisations, sans avoir des modèles standardisés, disposent de clausiers avec l'ensemble de clauses permises et les points d'attention à observer. Ce document sera également précieux pour l'auditeur interne lorsqu'il faudra auditer le contrat et/ou vérifier son application sur le terrain.

Bien que l'audit interne intervienne la plupart du temps dans le cas des contrats déjà signés et en application dans l'organisation, les constats identifiés permettront de mettre en place des plans d'actions visant à sécuriser les opérations et les recommandations proposées et pourront permettre par la suite de ne pas s'engager dans des aventures hasardeuses.

La négociation et la contractualisation sont les clés nécessaires au bon déroulement des opérations commerciales

Comme dans tout audit, il est important de comprendre l'organisation en place pour la négociation et formalisation des contrats. Pour cela, les organigrammes, les délégations de pouvoir et habilitations de signature, les procédures en vigueur, les tableaux de bord ou indicateurs existants sont autant d'informations à collecter et analyser pour mener à bien la phase de prise de connaissance avant la finalisation du programme de travail et le début de la phase terrain.

D'un point de vue pratique, il est utile de lire les conditions générales de vente (et les conditions particulières dans le cas de l'audit d'un seul contrat). Par la suite, il est nécessaire d'identifier et rencontrer les acteurs clés pour comprendre l'environnement, les besoins et particu-

larités. Rappelons que le but de l'enquête préliminaire est une première démarche qui permet de voir plus clair, savoir ce qui est fait et dans quelles conditions. En plus du service juridique, il faut à minima rencontrer le prescripteur, l'acheteur ayant mené la négociation depuis la définition du besoin à la signature du contrat sans oublier bien sûr l'utilisateur.

Avoir des connaissances du système d'information en place pour la gestion contractuelle et pour réaliser les achats contribuera à la réalisation aisée des points de contrôle autour de la sécurité logique de la mission.

Prenons l'exemple d'un audit opérationnel sur la mise en place et l'application des contrats cadres. Pour être en mesure de donner une assurance raisonnable à la direction générale et au comité d'audit de l'adéquation du contrôle interne sur ce domaine, l'auditeur devrait s'attacher à vérifier les points énumérés ci-après.

La décision de contracter doit être cohérente avec la stratégie de l'organisation et ses objectifs

Sur la base d'un échantillon, il s'agit de comprendre quel était le besoin initial, la nature et la durée souhaitée de la relation commerciale envisagée (partenariat long terme versus achat ponctuel), les obligations réciproques et les flux financiers souhaités.

Il ne faut pas oublier qu'il est courant que les besoins évoluent pendant la négociation du contrat mais l'identification, la formalisation et la validation par le prescripteur restent des éléments clés pour la réussite du contrat.

Ainsi, la demande d'achat émanant du prescripteur devrait contenir un cahier des charges fonctionnel (et parfois technique) détaillant le besoin, les modalités d'exécution, le planning prévisionnel, le volume, le budget prévu et une fiche de risques produit, si besoin.

La sélection des fournisseurs et la formalisation des contrats cadres doivent respecter les principes de contrôle interne

Même si la mission d'audit porte exclusivement sur l'application des contrats cadres, il est fondamental de comprendre comment les contrats ont été préparés, négociés et formalisés. Pour cela, il faudra réaliser des contrôles clés rencontrés dans les missions d'audit des achats, notamment en ce qui concerne la méthode de sélection des fournisseurs (appel d'offres ? consultation ? approche directe sans mise en concurrence ?). Selon la méthode utilisée, le rapport de forces et la marge de négociation sont différents. Il s'agit dans cette phase de s'assurer que les dés n'étaient pas pipés avant même la contractualisation.
Ainsi, la sélection des fournisseurs doit pouvoir se justifier par des critères éthiques, économiques, objectifs, constants et cohérents avec l'activité de l'organisation. Ces critères doivent être formalisés.
L'association des fonctions expertes (juridique, sécurité, technique, financière, assurances…) dans la négociation et la rédaction des contrats avec les acteurs clés (prescripteur, acheteur et utilisateur) peut rassurer quant à l'indépendance du processus de sélection des fournisseurs. L'existence des panels ou des comités d'achat au dessus d'un certain montant, et d'une liste des critères de sélection avec la pondération associée à chaque critère sont également indicateurs d'un processus « objectif de sélection ».
S'agissant de la formalisation des contrats, il faut s'assurer que les différentes clauses contractuelles sont en ligne avec les pratiques de l'organisation : des modèles types peuvent exister, des clausiers peuvent être à la disposition des acheteurs et certains contrats peuvent faire l'objet d'une validation formelle du service juridique (contrats stratégiques, au dessus d'un montant intégrant ou excluant des clauses standards de l'organisation…).
L'auditeur devra également vérifier que les délégations de

pouvoirs sont adéquates et cohérentes avec les seuils autorisés et la fonction occupée par le délégataire et que seuls les collaborateurs dûment habilités signent les contrats et les bons de commandes associés.

Pour qu'un contrat soit appliqué, il doit être facile à comprendre

Pour cela les clauses doivent être précises, cohérentes, complètes et disponibles pour l'ensemble des collaborateurs concernés.
Il faut donc veiller à la mise à disposition des opérations des copies des contrats ou, tout au moins, des clauses les concernant.
Lorsque des contrats locaux existent, il est nécessaire de vérifier qu'ils répondent à un réel besoin et qu'ils n'ont pas été mis en place pour contourner certaines clauses des contrats centraux (par exemple, que les conditions négociées avec les fournisseurs sont respectées, que la politique de l'organisation en termes d'application des pénalités de retard figure au contrat…), ou favoriser un fournisseur local.

L'application des contrats cadres doit être conforme aux procédures et aux principes de contrôle interne

Cet objectif de contrôle, assez général, consommera la plupart du temps de la mission. Des éléments clés pour sécuriser le processus devront être analysés, tels que :

- le respect des seuils fixés pour la validation des contrats ;
- le respect du principe de séparation des tâches, qu'il soit au niveau opérationnel ou au niveau des systèmes d'information (sécurité logique du processus) ;
- la désignation du lieu de livraison[1] et/ou de l'incoterm lors des échanges, notamment transnationaux ;
- la vérification du flux des opérations ;
- les modalités de calcul des prix, notamment lorsqu'il est déterminable à chaque commande (par exemple, dans le cas des matières premières) ;
- les modalités de révision des prix, leur fréquence et les indices ou formules utilisés ;
- les mesures pour l'acceptation des biens/services ;
- la vérification de la présence des clauses dites « protectrices » :
  - accord de confidentialité,
  - clause d'audit,
  - cautions et garanties bancaires (caution de restitution d'acompte, de bonne fin, garantie à première demande…),
  - début et période de garantie,
  - transfert de propriété[2] et assurance des biens/prestations,
  - pénalités prévues (techniques, retard…) ;
- la gestion des mainlevées ;
- l'intervention en amont de l'émission du bon de commande du contrôle budgétaire. ;
- le paiement des biens/prestations après la présentation de justificatifs dûment approuvés.

D'autres objectifs périphériques à l'audit de la contractualisation et de son application peuvent être inclus dans la mission, tels que l'audit du processus financier associé au contrat (de l'enregistrement de la facture au paiement sans oublier la gestion des acomptes et des soldes par exemple).
L'utilisation de techniques assistées par ordinateur pour analyser le respect des contrats et des principes de contrôle interne facilite grandement le travail des auditeurs. Par ailleurs, l'utilisation de ces outils permet d'analyser de grandes quantités de données et ainsi d'être en mesure de mettre en évidence des résultats fiables et sur la totalité de la population. Quelques exemples de contrôles pouvant être effectués :

- identification des trous dans la séquence des bons de commande ;
- identification des doublons dans les numéros de commande ;
- identification des commandes n'ayant pas donné lieu à réception ;
- réceptions n'ayant pas donné lieu à facturation ;
- écart entre les réceptions reçues après le nombre de jours contractualisés donnant droit à l'application de pénalités rapprochés du fichier des pénalités ;
- réceptions en quantité ou poids négatif ou nulles ;
- date de commande < date de réception < date de facture < date de paiement.

Celui qui commande est différent de celui qui réceptionne
Ceux qui commandent ou réceptionnent ne font pas le rapprochement entre commande / réception / facture
Ceux qui commandent ou réceptionnent ne mettent pas en paiement les factures
S'assurer que seuls les utilisateurs autorisés à passer des commandes ont réalisé ces transactions (idem avec les profils informatiques donnés au personnel en charge de la réception, de la validation et de la mise en paiement)

La performance des contrats (et commandes passées dans les contrats cadres) doit faire l'objet d'une analyse régulière pour alimenter le retour d'expérience

Le principal élément utilisé pour le retour d'expérience est la base qualitative de données des contrats qui trace tout au long de sa durée les difficultés rencontrées et permet également d'anticiper les périodes de renouvellement ou de dénonciation des contrats. Ces informations (qui doivent être tangibles et mesurables) seront contrastées avec les résultats des tests d'audit (taux de commandes reçues avec retard, acceptées avec réserves ou rejetés…) pour conclure sur la fiabilité des informations contenues dans l'outil.

Le nombre de litiges est également un indicateur clé. Il peut signaler des contrats non adaptés aux besoins ou contraintes opérationnelles ou des fournisseurs/prestataires sous-dimensionnés par rapport aux besoins de l'organisation. Pour calculer le taux de litiges, il faut prendre en compte la totalité des cas possibles :

- les litiges en cours ;
- les saisies au Tribunal de Commerce, qui reste la clause la plus courante pour régler les différends ;
- les cas de médiation (procédure non obligatoire par laquelle un intermédiaire neutre, le médiateur, aide les parties en litige à trouver une solution mutuellement satisfaisante) ;
- les cas d'arbitrage (procédure par laquelle le litige est soumis à un ou plusieurs arbitres qui rendent une sentence qui lie les parties).

Il sera également intéressant de prendre en compte l'analyse des précontentieux ayant donné lieu à des accords transactionnels sans toutefois avoir déclenché un litige.

Le retour d'expérience ne doit pas faire abstraction des besoins initiaux par rapport aux résultats escomptés, notamment en matière de qualité, délais, prix et/ou gains attendus (financiers, parts de marchés…), respect des budgets, etc.

Enfin, il ne faut pas oublier de prendre en compte la veille réalisée sur les fournisseurs sur des critères additionnels tels que la fiabilité, la stabilité, la santé économique et la réputation des fournisseurs ainsi que leur niveau de dépendance économique vis-à-vis de l'organisation. Ces informations peuvent conditionner le renouvellement du contrat ou la réalisation d'un nouvel appel d'offres.

En réalisant ces contrôles on s'aperçoit que la valeur ajoutée d'un tel audit est non seulement l'identification des risques et/ou dysfonctionnements, mais le travail des auditeurs peut également aboutir dans la prise en compte de certaines décisions visant à sécuriser davantage les relations commerciales en anticipant notamment les risques juridiques et réduire à terme les cas de litiges avec les fournisseurs. ●

---

[1] Selon l'article 1603 du Code civil (il a deux obligations principales, celle de délivrer et celle de garantir la chose qu'il vend), le vendeur doit délivrer la chose et l'acheteur doit en prendre possession. Délivrer la chose consiste à la remettre en possession de l'acheteur. Mais un contrat peut prévoir des conditions d'acceptation (analyses indépendantes réalisées en attestant la qualité de la chose, calibre ou poids minimal accepté, écart maximum toléré…).

[2] En principe, le transfert de propriété et le transfert de risques ont lieu dès que le vendeur et l'acheteur se sont mis d'accord sur la chose et le prix, même si le prix n'est pas payé et la chose n'est pas livrée. Dans la réalité, les parties prenantes peuvent décider autrement : livraison, acceptation de la marchandise…

A propos d'un éditorial …

Jacques Renard

Le n°205 de la revue « Audit & Contrôle internes » nous a gratifié d'un remarquable éditorial sous la signature de Louis Vaurs.
Texte remarquable en ce qu'il énonce clairement le défi posé aux responsables d'entreprises par la survenance d'événements « imprévisibles ». Mais texte également remarquable en ce qu'il met en lumière la responsabilité des risk managers et auditeurs internes, curieusement désarmés alors qu'ils devraient donner l'alerte.

Mais on peut progresser dans la maîtrise de ces situations paroxysmiques à la double condition d'affiner le regard des intéressés et d'évaluer autrement les risques à venir.

Certes, ainsi qu'il est fort justement souligné dans l'éditorial, de nombreux risques sont imprévisibles.

Mais sont-ils pour autant inimaginables ? Et alors qui peut être en mesure de les imaginer ?
Le risque imprévisible c'est celui dont on ne peut prévoir la survenance, en général estimée si lointaine qu'on finit par l'oublier.

Mais les acteurs directs, ceux qui sont au plus près des évènements, ceux-là peuvent imaginer les signes précurseurs et y porter remède, c'est à dire atténuer les conséquences à venir. On ne pouvait prévoir la crise financière mondiale mais les banquiers américains pouvaient imaginer la crise des subprimes. On ne pouvait prévoir la catastrophe de la plateforme pétrolière dans le golfe du Mexique – aucun accident de cette nature ne s'étant jamais produit – mais les ingénieurs sur le site pouvaient imaginer un sinistre majeur.
Et il appartient au risk manager de réveiller les imaginations de chacun et de pousser à envisager l'impensable. Et de même à l'auditeur interne de poser les bonnes questions.
Mais encore faut-il envisager autrement l'évaluation du risque.

On connait l'analyse classique des commentateurs et exégètes sur l'évaluation du risque. Ce dernier comprend deux composantes, la fréquence et l'impact ; d'où l'on déduit :

- Fréquence importante et impact important = risque grave
- Fréquence faible et impact faible = risque faible
- Fréquence importante et impact faible= risque moyen
- Fréquence faible et impact important = risque moyen

Or, dès l'instant où l'on s'efforce d'imaginer le risque catastrophe il est évident que cette dernière égalité est fausse. Et non seulement elle est fausse mais elle transforme l'imaginable en inimaginable, d'où l'absence de réactions.

Or, lorsque l'impact est important, le risque doit toujours être considéré comme un risque grave et être traité comme tel. Peu m'importe que la fréquence soit estimée à une fois par siècle ou davantage : ce peut être demain !

Dans leur démarche d'identification des risques imprévisibles, les responsables seront donc attentifs à la notion d'impact. C'est à partir de là qu'ils estimeront les mesures jugées nécessaires ou considéreront que l'on peut attendre. Et c'est l'auditeur interne qui va sécuriser les mesures prises par son appréciation de la situation.

On perçoit bien que dans cette double démarche : interrogation sur les risques précurseurs imaginables et appréciation de l'impact possible, le rôle du risk manager est essentiel. C'est lui qui, en premier, va inciter le manager à explorer le domaine des possibles et élargir ce faisant le champ d'investigation de l'auditeur interne.

Ce rôle charnière ne peut que se développer et il est souhaitable qu'il se développe. « *La montée en puissance de la gestion des risques* », soulignée par Louis Vaurs, est la réponse indispensable aux incertitudes. ●

Evénements

La mise en œuvre des recommandations : comment faire adhérer les audités et les dirigeants aux recommandations ?

Réunion mensuelle du 20 septembre 2011

La valeur ajoutée de l'audit interne est dans la mise en œuvre des recommandations, volet primordial de toute mission d'audit. Ces recommandations sont également source de valeur ajoutée pour les audités qui doivent se les approprier. Pour cela, un certain nombre de critères doivent être retenus : les recommandations doivent être réalistes et pertinentes ; précises (sans apparaître comme des directives) et adaptées au contexte et aux spécificités de l'organisation ; consensuelles, partagées et hiérarchisées ; il faut évidemment tenir compte de la faisabilité et des coûts.

Les facteurs clés de succès impliquent une communication permanente auprès des directions, sur le terrain en cours de mission et lors de la réunion de clôture. Le rapport final sera utilisé pour le suivi des plans d'action, lesquels doivent être détaillés et précis : désignation d'un responsable, fixation de la date d'échéance.

Pour émettre des recommandations opportunes, et renforcer l'écoute des audités et du *top management*, l'audit doit disposer de ressources et de compétences crédibles. Une équipe idéale est composée d'éléments venant d'horizons divers permettant de couvrir un large spectre des activités auditées : profils variés, avec des compétences techniques différentes et des parcours professionnels antérieurs multiples ; des compétences clés dans la finance, la comptabilité, les systèmes d'information. Cela passe aussi par une exigence de formations continues individuelles et collectives.

Les recommandations devant contribuer à minimiser les risques, à corriger les dysfonctionnements et à améliorer l'efficacité, il est conseillé d'affecter les meilleurs auditeurs aux missions les plus exposées.

L'auditeur est responsable de la qualité de ses recommandations ; il est jugé sur sa capacité à proposer des recommandations innovantes et adaptées et ce, en toute indépendance. Un manque d'indépendance ou d'impartialité nuit à la crédibilité de l'audit et peut même affaiblir l'image de l'ensemble du département. Il y a risque de perte d'indépendance en cas de pression de la part de l'exécutif, de liens trop forts entre l'audit et la fonction auditée, d'audit décentralisé dépendant hiérarchiquement du management local, ou encore lorsque l'auditeur souhaite évoluer vers la fonction auditée.

La mise en œuvre des recommandations s'inscrit dans le cadre d'une amélioration continue des processus, ce qui suppose un « partenariat » entre l'audit et la direction générale. Le taux de mise en œuvre des recommandations est un indicateur de performance de la fonction audit. ●

Les prochains rendez-vous

PARIS

>> **mercredi 12 octobre 2011**
Réunion mensuelle - **L'audit des sujets sensibles**

>> **lundi 17 octobre 2011**
Colloque - **Mieux appréhender l'environnement et la culture de contrôle de l'organisation pour un dispositif de contrôle interne plus efficace**

AQUITAINE (Bordeaux)

>> **Jeudi 3 novembre 2011**
Réunion - **Résultats de l'Enquête CBOK IIA France : Evaluez vos pratiques au regard des tendances européennes et mondiales**

>> **Mercredi 14 décembre 2011**
Réunion - **La multiplication des démarches de maîtrise des risques et le positionnement de l'audit interne**

Renseignements complémentaires et inscription : www.ifaci.com

Publications IFACI

Bon de commande

Le « Manuel d'Audit Interne - Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques » est l'ouvrage international de référence sur le métier d'auditeur interne. Élaboré sous l'égide de la fondation pour la recherche de l'IIA, il est le fruit de la collaboration de trois professeurs et de quatre praticiens. Son adaptation aux contextes européen et français a été réalisée par des universitaires et praticiens français réunis par l'IFACI, ce qui en fait l'outil idéal pour les auditeurs internes, les étudiants en audit interne et leurs enseignants.

Ce manuel est organisé en deux sections : « concepts fondamentaux de l'audit interne » et « conduire une mission d'audit interne ». Il reflète les dernières évolutions de la profession, en particulier dans les domaines suivants :

- normes internationales de l'audit interne ;
- gouvernance, contrôle interne et management des risques ;
- éléments clés liés aux systèmes d'information et références aux guides GTAG et GAIT diffusés par l'IIA et par l'IFACI ;
- risques de fraude ;
- missions de conseil.

La première édition de ce manuel, traduite en espagnol et en japonais a été adoptée par de nombreux pays de par le monde. Nous sommes convaincus que cette adaptation française de la seconde version ajoutera encore à ce succès et contribuera efficacement à la formation des étudiants et à la professionnalisation des auditeurs internes.

AUTEUR : The Research Foundation (The IIA) / IFACI - **Prix HT : 61,61 €** (65 € TTC)
Septembre 2011 - Format : 17 x 24 cm - ISBN : 978-2-915042-33-7

Bon de Commande

Société : .....

Nom : ..... Prénom : .....

Adresse : .....

Code postal : ..... Ville : ..... Pays : .....

Tél. : ..... Fax : ..... Mél : .....

TITRE	PRIX HT	QUANTITÉ	TOTAL
Manuel d'audit interne	61,61 €		
		Total HT	
		TVA 5,5 %	
		Net à payer TTC*	

PAIEMENT PAR :

- ○ Chèque bancaire ou postal (à l'ordre de l'IFACI)
- ○ Virement à la banque HSBC agence centrale
  Compte IFACI n°30056-00148-01485415521-72
- ○ Carte de crédit :
  N° .....
  Date d'expiration : .....

DATE : ..... SIGNATURE :

(*) Hors frais de port et d'emballage.

Bon de commande à retourner à :
Marie-Thérèse Tran - IFACI
98 bis, bd Haussmann - 75008 Paris
Tél. : 01 40 08 48 00 - Fax : 01 40 08 48 20
Mel : mtran@ifaci.com - Internet : www.ifaci.com

Règlements :
Une facture pro forma vous sera adressée par courriel dès réception de votre commande.
Chèque : libellé en euros tiré sur une banque française.
Virement : les virements émis à partir d'une banque hors de France doivent être nets de tous frais bancaires pour l'IFACI.

FICHE TECHNIQUE

Audit & Contrôle internes

GTAG 11 – Elaboration d'un plan d'audit des SI

José Bouaniche - auditeur interne, **Caisse des Dépôts et Consignations**

Réaliser un plan d'audit est désormais une condition indispensable à l'activité des directions d'audit interne. Mais quelle est la place de l'audit informatique dans la conception du plan d'audit ?

L'enquête CBOK 2010 de l'IIA rapporte que *« 94% des répondants formalisent les missions d'audit dans le cadre d'un plan annuel et, dans 79% des cas, cette planification est réalisée à partir d'une analyse de risques »*. De plus, la mise en place d'un plan d'audit plus réactif et plus flexible, basé sur les risques, figure parmi les 10 impératifs d'amélioration résultant de cette étude (cf. http://www.ifaci.com/Bibliotheque/Bibliotheque-en-ligne-telecharger-la-documentation-professionnelle/Enquetes-154.html).

L'élaboration d'un plan d'audit présente un intérêt indéniable

Les avantages de la réalisation d'un plan d'audit sont indéniables. Comme le rappelle Sawyer[1], elle :

- donne l'assurance de couvrir les fonctions clés à intervalles planifiés ;
- simplifie le travail d'affectation des missions ;
- implique l'encadrement supérieur, approbateur du plan, et facilite donc la bonne réalisation des missions ;
- prémunit contre des demandes de missions qui ne relèvent pas de l'audit ;
- justifie du bien fondé de l'existence du service d'audit ;
- optimise les travaux des commissaires aux comptes et en diminue, par conséquent, les coûts.

A ceci, ajoutons que c'est un exercice qui fournit l'occasion de contacts et d'un dialogue riche entre audit interne et management des fonctions (prise de connaissance et échanges ouverts sur les objectifs, enjeux clés, contextes, risques). Plus encore, il permet au DAI et à son équipe de profiter de l'expérience et des connaissances de chacun pour bâtir une vision commune et partagée, gage d'efficacité du service. Rappelons ici que l'expérience et la connaissance directe, le bon sens et le jugement professionnel sont les éléments essentiels pour construire un plan d'audit. Les outils, techniques et méthodes demeurent des aides accessoires.

Le particularisme du plan d'audit informatique et le GTAG 11

Alors même que les évolutions normatives et réglementaires renforcent le rôle essentiel des SI dans la conduite de l'entreprise et en imposent

une connaissance certaine aux auditeurs, des équipes ont encore du mal à intégrer de manière raisonnée les S.I. dans leur réflexion, en laissant souvent l'initiative aux commissariats aux comptes.
En effet, l'environnement S.I. se distingue par :

- une forte complexité de chacun de ses éléments ;
- des activités diversifiées et très spécialisées ;
- une forte propension des incidents à générer des effets « domino ».

De ce fait, dans la suite du document, nous avons voulu mettre l'accent sur ce qui particularise un plan d'audit des systèmes d'information, notamment la prise en compte de l'activité.

Plan d'audit intégré ou non ?

A cette question, le GTAG 11 répond sagement qu'il faut prendre en compte « *la fonction d'audit interne ainsi que le personnel, la taille, la répartition géographique et le mode de management de ce service* » et 3 différents niveaux d'intégration :

- un plan d'audit faiblement intégré, où la part des systèmes d'information dans les audits non spécifiquement informatiques est inexistante ;
- un plan d'audit partiellement intégré où, lors des audits non informatiques, des revues d'application sont réalisées. En effet, auditer les applications en même temps que les processus qu'elles supportent, permet d'obtenir une assurance sur toute la suite des contrôles, automatisés ou manuels ;
- un plan d'audit fortement intégré, « *dans lequel les activités d'audit des systèmes d'information font partie intégrante des missions portant sur les processus de l'organisation* » et dont la conception, par conséquent, est réalisée par les auditeurs toutes spécialités confondues.

La nécessaire prise en compte des objectifs de l'entreprise

Il faut noter que la conception du plan suit des phases successives, mais que plusieurs itérations du cycle entier peuvent être nécessaires pour obtenir des résultats satisfaisants.
Le plan d'audit S.I. ne se conçoit pas à partir des objectifs donnés à l'informatique, mais bien à partir des objectifs d'entreprise (voir la Figure 1 et l'article sur la gouvernance des S.I.).
Plus exactement, la norme 2010 fait découler le plan d'audit des objectifs d'entreprise par l'entremise de l'analyse des risques (voir Figure 2).
Il faut bien noter que le dialogue avec les parties prenantes est un élément important de cette prise en compte des objectifs de l'organisation. Ces objectifs alimentent chacune des 4 phases de la démarche d'établissement du plan d'audit IT (voir Figure 3).

La prise en compte des objectifs des S.I. doit être prudente

Si des objectifs ont été assignés à la fonction informatique, il serait mal venu de ne pas les prendre en compte. Mais il convient de les utiliser après coup, à l'issue d'au moins une itération du cycle de conception du plan. Ceci a plusieurs avantages :

- donner l'assurance au service d'audit d'avoir bien couvert les risques d'entreprise ;
- ne pas déléguer à d'autres la réalisation d'une approche critique de l'IT par rapport aux objectifs d'entreprise ;
- inclure la conception des objectifs IT dans l'univers d'audit, sans présupposer de sa qualité.

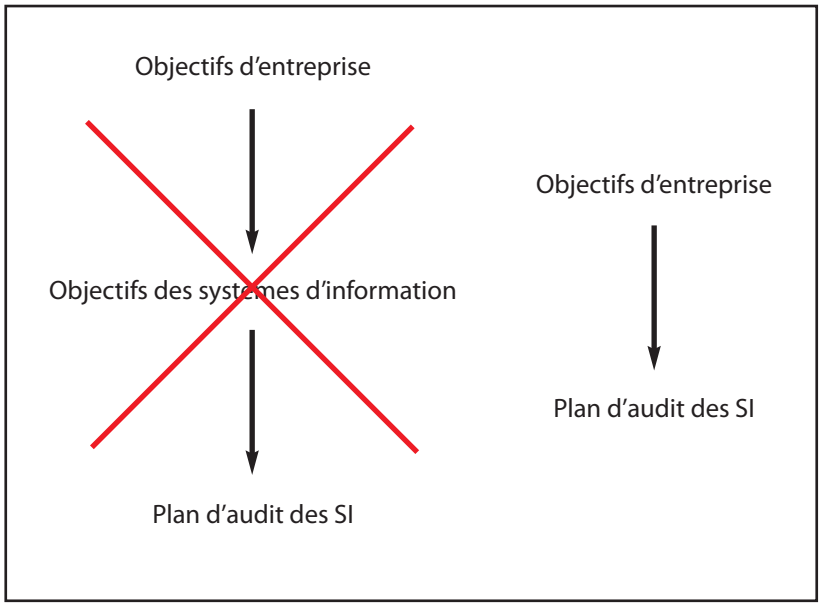


Figure 1 : Le plan d'audit des S.I. découle directement des objectifs de l'entreprise

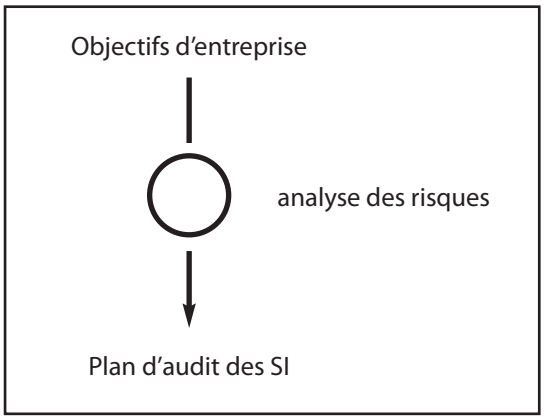


Figure 2 : Le plan d'audit découle des objectifs d'entreprise via l'analyse des risques

La prise en compte de l'activité est fondamentale

Première phase de la démarche de conception du plan d'audit des systèmes d'information, la prise en compte de l'activité procède ainsi d'une démarche descendante : elle part des objectifs, stratégie et modèles d'activité de l'entreprise qui sont les fondamentaux qui permettront d'identifier les processus clés *« par lesquels l'organisation réalise ses objectifs premiers »*, sans oublier les processus supports indispensables à leur fonctionnement (voir Figure 4) ainsi que les applications importantes et les infrastructures informatiques critiques.

L'environnement informatique doit venir compléter l'appréciation globale de l'activité. Huit éléments sont à prendre en compte :

1. Le niveau de centralisation (géographique ou fonctionnelle), car : *« il faut veiller à aligner les différents audits sur la fonction de direction qui est, in fine, responsable de ce domaine. »*
2. Les technologies déployées, dont le degré de diversité *« déterminera l'ampleur des connaissances techniques requises au sein du SAI ainsi que le nombre de domaines spécifiques qu'il faudra examiner »*. En effet, pour le GTAG 11, chaque couche de structuration du S.I. (du programme d'application au câblage des salles machines) induit des risques propres en termes de sécurité (disponibilité, confidentialité, intégrité). Or, le niveau de risque est fonction, d'une part *« du degré d'importance pour l'organisation du domaine d'activité concerné par les moyens technologiques en cause et, d'autre part, de leur configuration comme de leur déploiement. »*
3. Le degré de personnalisation des logiciels standards, car plus l'entreprise développe ses

Prendre en compte l'activité	Définir l'univers des SI	Procéder à une évaluation des risques	Formaliser le plan d'audit (programme de missions)
• Identifier les stratégies et objectifs de l'organisation • Prendre en compte ce qui présente un profil de risque élevé pour l'organisation • Prendre en compte la façon dont l'organisation structure ses opérations • Prendre en compte le modèle de fonctionnement de la DSI comme support de l'activité de l'entreprise	• Analyser les fondamentaux de l'activité • Identifier les applications importantes qui concourent au traitement des opérations de l'organisation, en tenant compte du rôle des moyens technologiques intervenant dans ce traitement • Identifier l'infrastructure critique pour les applications importantes • Identifier les grands projets et initiatives • Définir des thèmes d'audit réalistes	• Mettre au point des processus d'identification des risques • Évaluer les risques spécifiques au SI et classer les thèmes d'audit à partir des facteurs correspondants	• Sélectionner les thèmes d'audit retenus et les grouper en missions d'audit distinctes • Définir le cycle d'audit et sa fréquence • Ajouter des missions répondant aux demandes de la direction ou constituant des opportunités pour remplir une mission de conseil • Valider le plan avec la direction

Figure 3 : Les 4 phases de la démarche de conception du plan d'audit des S.I. (extrait GTAG 11)

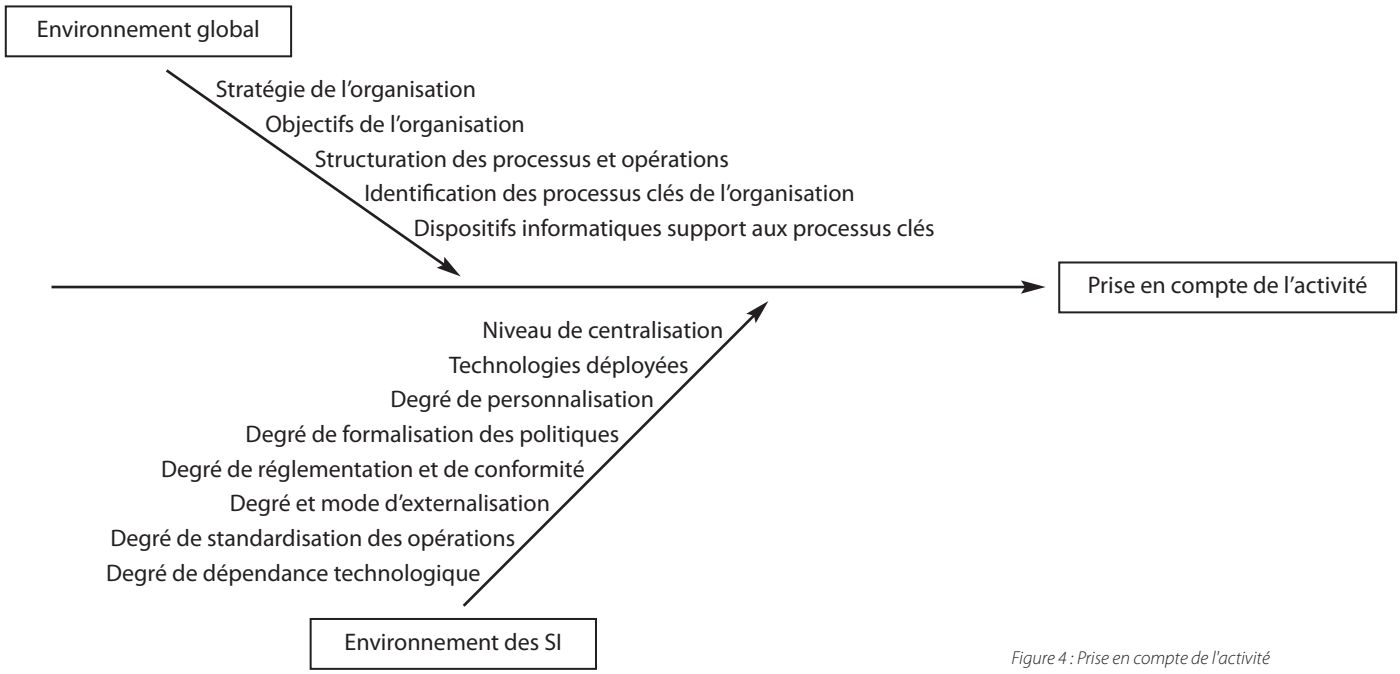


Figure 4 : Prise en compte de l'activité

propres spécificités, plus la maintenance des S.I. s'avère complexe, fragilisant d'autant la sûreté de fonctionnement.

4. Le degré de formalisation des politiques et référentiels des S.I. Le GTAG 11 distingue :
   - les politiques qui « *fournissent les directives émanant de la DG sur des thèmes concernant les droits attachés à la propriété intellectuelle, le respect de la vie privée, […] , afin de garantir la conformité aux lois et règlements* » ;
   - les référentiels qui « *décrivent un processus ou une procédure obligatoire et donnent des orientations plus précises sur la manière de se conformer aux principes fondamentaux auxquels ils se réfèrent* ».

   Le GTAG 11 souligne aussi la nécessité de définir « *un processus de mise à jour continue de toutes les directives et de tous les référentiels que la réglementation impose* ».

   Ces politiques et référentiels contribuent d'autant plus à instaurer un environnement de contrôle efficace que « *ces politiques et référentiels sont communiqués, compris, pilotés, surveillés et actualisés par la direction générale* ».
5. Le degré de réglementation et de conformité.
6. Le degré et le mode d'externalisation (voir le GTAG 7 sur l'infogérance). « *Les principaux facteurs qui interviennent sont :*
   - *la manière dont la DG envisage son rôle de supervision et de pilotage ;*
   - *la maturité du dispositif d'externalisation ;*
   - *les risques spécifiques au pays ;*
   - *la complémentarité des plans de continuité d'activité (PCA) de l'entreprise et de son prestataire* ».
7. Le degré de standardisation des opérations. Le GTAG11 conseille l'usage du référentiel ITIL.
8. Le degré de dépendance technologique, car il est évident que « *plus la dépendance aux SI est importante, plus une forte gouvernance et de solides processus opérationnels internes sont nécessaires* ».

Définir ce qu'il convient d'auditer : l'univers d'audit des S.I.

Après avoir réalisé la prise en compte de l'activité, il est possible de définir l'univers d'audit : « *ensemble fini et exhaustif des domaines d'audit* » qui représente « *la plus grande exposition au risque* » sans oublier « *ceux qui représentent un enjeu majeur pour les auditeurs dans l'apport qu'ils constituent en matière de valeur ajoutée à l'organisation* ».

Ainsi, « *les auditeurs auront conscience des audits qui peuvent être réalisés avant d'effectuer une évaluation et une hiérarchisation des risques aboutissant à un programme d'audit* ». (Cf. figure 5).

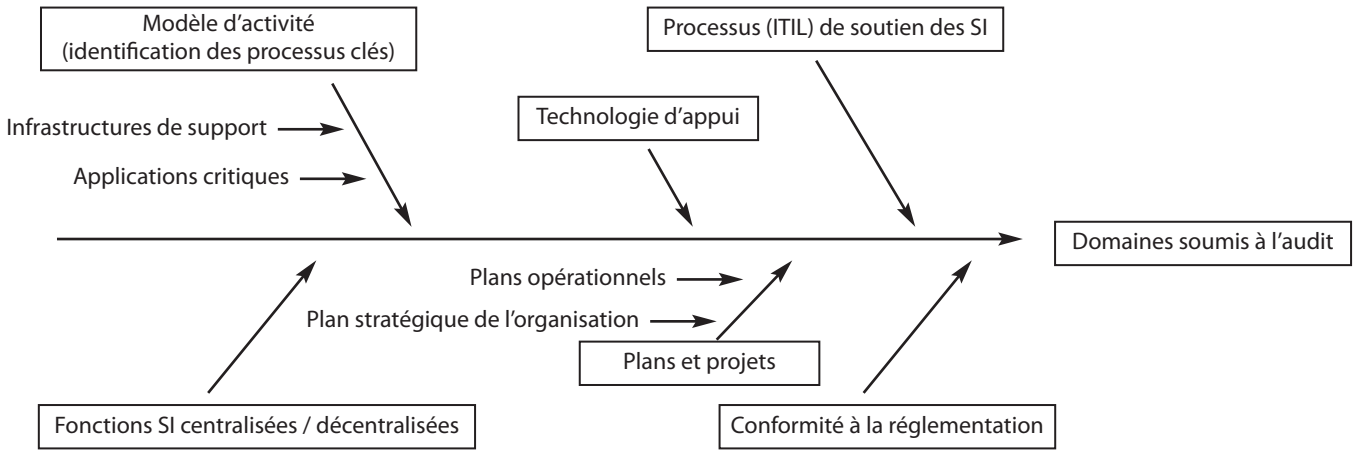


Figure 5 : définir les domaines soumis à l'audit

Procéder à une évaluation des risques

L'évaluation des risques va permettre, à partir de l'univers d'audit (phase précédente) et des connaissances traitées lors de la première phase de prise en compte de l'activité, d'identifier les missions éligibles au plan d'audit (voir Figure 6).

Cette démarche se fera en deux étapes :

1. L'évaluation des risques qui repose sur la prise en compte des objectifs de l'entreprise (cf. MPA 2010-1) et de la stratégie relative aux systèmes d'information. Lors de cette étape, il est capital de *« cerner les domaines de l'environnement du système d'information susceptibles d'entraver fortement la réalisation des objectifs de l'organisation »*.
2. La hiérarchisation des risques, qui consiste à valoriser les éléments de l'univers d'audit des systèmes d'information. Au cours de cette étape *« les auditeurs détermineront les dysfonctionnements susceptibles d'intervenir pour chaque catégorie et en quoi l'organisation en sera affectée si les contrôles visant à gérer ou à atténuer ces dysfonctionnements ne sont pas appliqués correctement ou ne fonctionnent pas correctement »*. Pour ce faire, outre les facteurs de risque objectifs ou historiques, il faut tenir compte des facteurs subjectifs car *« il faut mobiliser à la fois de l'expertise, des compétences, de l'imagination et de la créativité. Cet accent placé sur les mesures subjectives est corroboré par la pratique. En effet, bien des unités auditables évoluent tellement entre deux audits que l'historique des audits antérieurs n'apporte pas grand-chose. En conséquence, le jugement sensé mais subjectif d'un praticien chevronné est tout aussi valide que n'importe quelle autre méthode »*.

Lors de la construction de la première itération du plan, nous préconisons de ne pas partir d'une typologie pré établie, mais de la déduire a posteriori des travaux réalisés. Dans un deuxième temps on pourra s'inspirer des propositions du GTAG 11 (qui scinde l'univers d'audit en 3 : infrastructure S.I., exploitation informatique et applications), ou de la procédure sur la mesure du risque de l'ISACA[2] et affiner, si nécessaire, la typologie déduite. A noter que cette procédure de l'ISACA propose des exemples variés suivant le degré d'intégration du plan d'audit des S.I. au plan d'audit global de l'organisation, notion que nous avons abordée précédemment.

Prise en compte du management des risques dans la planification de l'audit interne

Doit-on prendre en compte les risques identifiés par le management des risques de l'organisation ? Si le GTAG 11 ne répond pas à cette question, la MPA 2010-2 y est consacrée. Cette dernière indique sans ambiguïté que : *« la planification de l'audit interne doit s'appuyer sur le processus de management des risques de l'organisation lorsque celui-ci a été déployé »*.

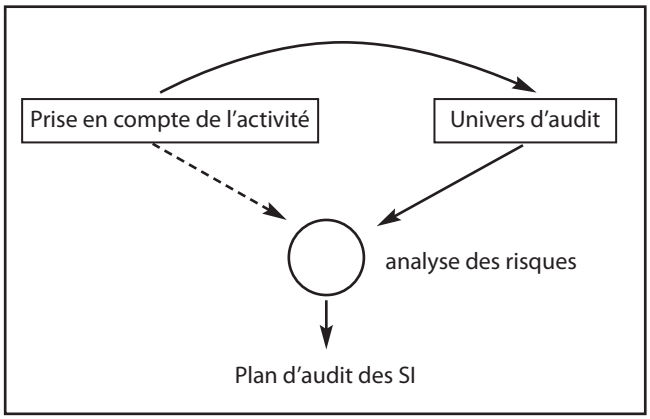


Figure 6 : Enchaînement des phases

Mais « *s'appuyer sur* » ne signifie pas, dans ce contexte, « *faire confiance à* ». Ainsi, on ne doit pas se reposer sur les résultats du management des risques mais utiliser ces derniers avec circonspection même si l'on s'est assuré de la fiabilité et de l'efficacité de celui-ci.

Formaliser le plan d'audit

« *Tous les éléments de l'univers d'audit pourraient être examinés périodiquement* » si les ressources étaient illimitées, ce qui n'est jamais le cas. « *Par conséquent, le responsable de l'audit interne doit créer un programme d'audit tenant compte des contraintes du budget opérationnel de la fonction d'audit et des ressources disponibles* ».

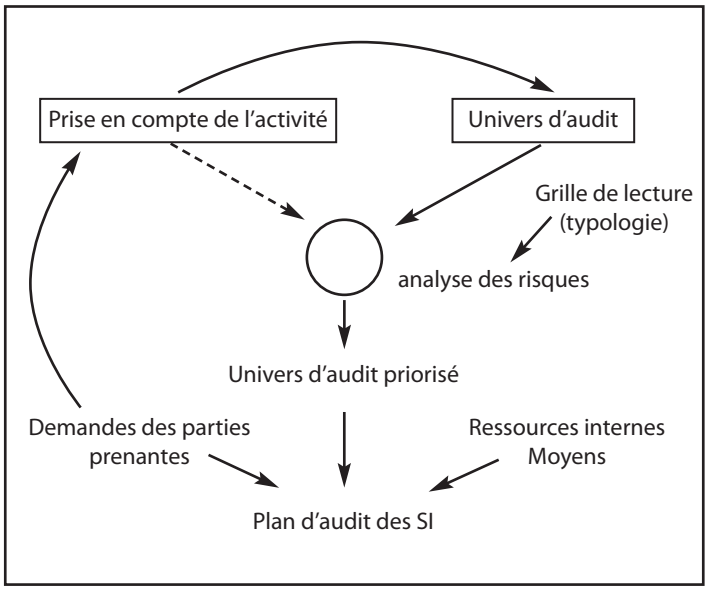


Figure 7 : Formaliser le plan

C'est ici une démarche classique, tenant compte des demandes des parties prenantes (voir Figure 7).

Le GTAG 11 considère que le rythme de changement des S.I. est plus rapide que celui des autres activités, par exemple avec l'adoption de nouvelles technologies à risque, les changements majeurs dans les applications ou encore avec l'émergence de nouvelles menaces de piratage. « *En conséquence, il faut périodiquement réexaminer les priorités du programme d'audit des S.I. et, au besoin, en rendre compte au conseil d'administration et à la direction générale plus fréquemment que pour d'autres domaines d'audit plus classiques et plus statiques* ».

* *
*

Le GTAG 11 s'inscrit parfaitement dans les impératifs d'amélioration identifiés par le CBOK 2010. On peut ainsi rappeler quelques points forts de ce GTAG :

- le plan d'audit des systèmes d'information découle directement des objectifs de l'organisation ;
- il repose sur une analyse des risques avec une démarche descendante ;
- il est élaboré par une équipe d'auditeurs (spécialistes en systèmes d'information ou équipe mixte, suivant le degré d'intégration du plan d'audit des systèmes d'information) et le DAI ;
- il ne s'enferme pas dans un cadre rigide : priorité au jugement professionnel, échanges avec les parties prenantes, dialogue tout au long du cycle de conception, remise en cause permanente des priorités, implication du management de l'organisation, etc.

Il s'intègre aux évolutions les plus récentes de la profession en termes de gouvernance des systèmes d'information, de valeur ajoutée de l'audit des systèmes d'information[3] ou encore de capacité d'assurance. ●

[1] *Saywer's internal auditing : The practice of modern internal auditing, 5th ed. / Lawrence B. SAWYER ; Mortimer A. DITTENHOFER ; James H. SCHEINER. - IIA, 2003*
[2] *Au chapitre des « IT audit and assurance tools and techniques » des normes de l'ISACA, la procédure 1 « IS risk assessment mesurement procedure P1 ».*
[3] *Voir par exemple l'article d'Edward Hill « the relevant IT audit » dans Internal Auditor de juin 2011.*

ifaci
institut français de l'audit et du contrôle internes

Calendrier 2012

SESSIONS	Durée	Tarifs adhérents	Tarifs non adhérents	janvier	février	mars	avril	mai	juin	juillet	sept.	octobre	nov.	déc.
SE FORMER AU CONTRÔLE INTERNE														
S'initier au contrôle interne	2 j	950 €	1 125 €	5-6	2-3	8-9	2-3	2-3	11-12	2-3	5-6		8-9	
Cartographie et management des risques	3 j	1 675 €	1 875 €	11-13	6-8	12-14	4-6	9-11	13-15		10-12	8-10		3-5
Mettre en œuvre le dispositif de contrôle interne	2 j	1 200 €	1 350 €	16-17	9-10	15-16		14-15	19-20	4-5	13-14		15-16	
Piloter et faire vivre le dispositif de contrôle interne	2 j	1 200 €	1 350 €	19-20	15-16	19-20		23-24	21-22		18-19		22-23	
Le contrôle interne des systèmes d'information	2 j	1 200 €	1 350 €	24-25		22-23			27-28			3-4		
SE FORMER À L'AUDIT INTERNE														
Les fondamentaux de l'audit interne														
S'initier à l'audit interne	2 j	950 €	1 125 €	5-6	1-2	8-9 29-30		15-16	7-8	2-3	6-7	4-5	8-9	6-7
Conduire une mission d'audit interne : la méthodologie	4 j	1 950 €	2 150 €	10-13	6-9	12-15	3-6	21-24	11-14	2-5	10-13	9-12	12-15	10-13
Maîtriser les outils et les techniques de l'audit	3 j	1 625 €	1 775 €	16-18	13-15	19-21	10-12	29-31	18-20	9-11	17-19	15-17	19-21	17-19
Maîtriser les situations de communication orale de l'auditeur	2 j	1 050 €	1 150 €	19-20	13-14	22-23	10-11	21-22	21-22	12-13	20-21	18-19	22-23	20-21
Réussir les écrits de la mission d'audit	2 j	1 050 €	1 150 €	23-24	16-17	26-27	12-13	23-24	25-26	12-13	24-25	22-23	26-27	20-21
Exploiter les états financiers pour préparer une mission d'audit	3 j	1 525 €	1 675 €	25-27		26-28		29-31			26-28			3-5
Désacraliser les systèmes d'information	3 j	1 525 €	1 675 €			28-30			4-6		26-28			12-14
Détecter et prévenir les fraudes	2 j	1 050 €	1 150 €			29-30			28-29		24-25	24-25		6-7
Le management														
Piloter un service d'audit interne	2 j	1 300 €	1 450 €	30,31				10-11				11-12		
Manager une équipe d'auditeurs au cours d'une mission	1 j	685 €	770 €			21				4			14	
L'audit interne dans les petites structures	1 j	685 €	770 €			7			29			19		
Balanced Scorecard du service d'audit interne	1 j	685 €	770 €		10				25				28	
Le suivi des recommandations	1 j	685 €	770 €	6			11		26		7		21	
Préparer l'évaluation externe du service d'audit interne	2 j	1 300 €	1 450 €		13-14			15-16					29-30	
L'audit interne, acteur de la gouvernance	1 j	685 €	770 €				12					26		
Audit interne, contrôle interne et qualité : les synergies	1 j	685 €	770 €		15			25				5		
Les audits spécifiques														
Audit du Plan de Continuité d'Activité - PCA	2 j	1 300 €	1 450 €			8-9			27-28				26-27	
Audit de la fonction Comptable	2 j	1 300 €	1 450 €				5-6					8-9		
Audit de performance de la gestion des Ressources Humaines	3 j	1 525 €	1 675 €				11-13						21-23	
Audit de la fonction Achats	2 j	1 300 €	1 450 €		16-17						27-28			
Audit des Contrats	1 j	685 €	770 €			16						1		
Audit de la fonction Contrôle de Gestion	2 j	1 300 €	1 450 €			5-6							29-30	
Audit de la Sécurité des Systèmes d'Information	2 j	1 300 €	1 450 €			22-23					12-13			
Audit des Processus Informatisés	2 j	1 300 €	1 450 €			27-28							19-20	
Audit de la Législation Sociale	2 j	1 300 €	1 450 €			13-14						17-18		
Audit du développement durable	2 j	1 300 €	1 450 €			7-8						15-16		
SE FORMER DANS LE SECTEUR PUBLIC														
Le contrôle interne dans le secteur public	2 j	1 300 €	1 450 €		2-3			21-22			6-7		12-13	
Pratiquer l'audit interne dans le secteur public	4 j	1 950 €	2 150 €			26-29			4-7			22-25		17-20
SE FORMER DANS LE SECTEUR BANCAIRE ET FINANCIER														
Le contrôle interne dans le secteur bancaire et financier	3 j	1 525 €	1 675 €						6-8		19-21			5-7
Pratiquer l'audit interne dans le secteur bancaire et financier	4 j	1 950 €	2 150 €						11-14		24-27			10-13
SE FORMER DANS LE SECTEUR DES ASSURANCES														
Le contrôle interne dans le secteur des assurances	2 j	1 300 €	1 450 €		8-9			2-3			4-5		8-9	
Pratiquer l'audit interne dans le secteur des assurances	4 j	1 950 €	2 150 €			13-16			26-29			8-11		17-20
SE FORMER DANS LES SECTEURS INDUSTRIE ET COMMERCE														
Audit des processus clés des activités industrielles et commerciales	4 j	1 950 €	2 150 €	23-26			2-5		18-21			15-18		4-7
ACQUÉRIR UNE CERTIFICATION														
Le DPAI														
Préparation au DPAI	2 j	950 €	1 125 €					29-30				11-12	15-16	13-14
Le CIA														
Préparation au CIA - partie I	1,5 j	850 €	1 050 €	16pm-17		12pm-13			12pm-13		10pm-11			3pm-4
Préparation au CIA - partie II	1,5 j	850 €	1 050 €	19pm-20		15pm-16			14pm-15		13pm-14			6pm-7
Préparation au CIA - partie III	1,5 j	850 €	1 050 €	23pm-24		19pm-20			18pm-19		17pm-18			10pm-11
Préparation au CIA - partie IV	1,5 j	850 €	1 050 €	26pm-27		22pm-23			21pm-22		20pm-21			13pm-14

DPAI

Découvrez le pilotage du Contrôle Interne sous un autre angle !

Optimisez la gestion de votre Contrôle Interne grâce à notre progiciel ESPHYNX :

- ✓ Identifiez rapidement les dysfonctionnements,
- ✓ Centralisez vos référentiels,
- ✓ Maîtrisez les risques,
- ✓ Gagnez en productivité.

EXPERTISE :

- Préparation des questionnaires
- Pilotage de campagnes d'évaluation
- Reporting complet
- Suivi des plans d'actions
- ...

Activité des progiciels Cogis-Software :

Audit Interne

Contrôle Interne

Reporting Décisionnel

COGIS SOFTWARE
DYNAMIC GOVERNANCE

www.cogis-software.com

☎ 01.47.82.40.59