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

Audit & Contrôle internes

Dans l'actualité

Stuxnet : une nouvelle ère dans la gestion des risques ?

International

Les anciens de l'audit interne utilisent leurs acquis pour apporter une valeur ajoutée à leur nouvelle profession

Idées et débats

COSO 2013 : Une nouvelle édition du référentiel COSO sur le contrôle interne

Grands projets

L'audit des projets de construction chez GDF SUEZ : une approche intégrée

Les audits métiers

Audit d'un processus informatisé

Fiche technique

>> De l'usage du GTAG 1 chez Sodexo : forces et faiblesses

LA GESTION DES RESSOURCES HUMAINES

Un levier de la performance des services d'audit et de contrôle internes

ifaci
institut français de l'audit et du contrôle internes

N°214
Avril-Mai 2013

ONE WORLD
ONE PROFESSION
ONE DESTINATION

ONE WORLD

Only in Orlando will you have an opportunity to participate in 77 career-spanning educational sessions and pre-conference events focused on current issues and opportunities facing the profession.

Tap into the experience of world renowned keynote speakers including:

MADELEINE K. ALBRIGHT, Former U.S. Secretary of State, and Author of five *New York Times* best-sellers

TOM PETERS, co-author of *In Search of Excellence: Lessons From America's Best-Run Companies*

MODERATOR: PAUL J. SOBEL, CIA, CRMA
Vice President/Chief Audit Executive
Georgia Pacific Corp. LLC

PANELISTS:

MICHELE J. HOOPER, President, Chief Executive Officer, The Directors Council
KAREN MOORE, Vice President, Compliance, Philip Morris International
JAMES M. SYLPH, Executive Director, Professional Standards and External Relations, International Federation of Accountants
BRIAN D. THELEN, General Auditor and Chief Risk Officer, GM Audit Services

ONE PROFESSION

More than 2,500 delegates from 100+ countries will represent every industry at career-level.

ONE DESTINATION

Orlando is one of the world's premier travel destinations, and the Orlando World Center Marriott Resort and Convention Center is offering an exclusive room rate of US $169 per night.

REGISTER BY FEBRUARY 28 AND SAVE UP TO US $600

Register at www.iia2013ic.org using Source Code IA0213.

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
ORLANDO, FLORIDA, USA / JULY 14-17, 2013

Audit & Contrôle internes

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

n°214 - avril-mai 2013

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
Farid Aractingi

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
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 47 84
Mel : esarda@ifaci.com

Revue bimestrielle (5 numéros par an)
ISSN : 2117-1661
CPPAP : 0513 G 83150
Dépôt légal : mai 2013
Crédit photos : © Séverine MARTIN - Fotolia.com

Prix de vente au numéro : 25 € 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

Les articles sont présentés sous la responsabilité de leurs auteurs.

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

La gestion des ressources humaines

Un levier de la performance des services d'audit et de contrôle internes

Bien gérer les ressources humaines des services d'audit interne, comme celles des services de contrôle interne est une absolue nécessité si l'on veut disposer d'un personnel de qualité et à haut potentiel.

Dans le dossier que nous vous présentons, nous avons l'exemple d'organisations représentant quatre grands secteurs d'activité : la finance, l'industrie, les administrations centrales de l'État et les collectivités territoriales. Si les objectifs sont semblables, les approches sont différentes car fortement influencées par la culture de chaque organisation et son niveau de maturité dans les domaines du contrôle et de l'audit internes. Chaque lecteur pourra se rendre compte des difficultés auxquelles se heurtent les services d'audit interne à la maturité en développement, pour constituer et conserver une équipe d'auditeurs internes, mais il pourra aussi s'approprier les pratiques éprouvées des services d'audit interne à la maturité affirmée.

Dans ce numéro, les systèmes d'information sont également à l'honneur : attention, nous dit Antoine de Boissieu, au risque d'attaque informatique malveillante par des virus du type Stuxnet, l'audit interne mais aussi les services de risques et de contrôle doivent s'assurer que l'organisation apporte à ce risque majeur toute l'attention souhaitable ; les processus informatisés sont quasiment partout et doivent pouvoir faire l'objet d'un audit par tout auditeur interne, nous précise Dominique van Egroo ; enfin, la deuxième édition du GTAG 1 vient d'être publiée. Plus didactique que la précédente, elle est, de ce fait, plus à la portée d'un non expert en systèmes d'information, nous indique Alain Rogulski.

Je vous recommande enfin de lire avec attention l'audit des projets de construction chez GDF pour lequel les directions du management des risques, du contrôle interne et de l'audit interne se sont associées pour apporter une offre globale de sécurisation aux directeurs de projets.

Bonne lecture. ●

Louis Vaurs - Rédacteur en chef

ifaci
Certification

Progressez sur des bases solides

Votre engagement pour
+ de bonnes pratiques
+ de performance
+ de légitimité
+ de sécurité

Conception : ebzone communication - Photo : © Jakub Cejpek - Fotolia.com

ifaci

Le label de qualité et de performance Certification IFACI est délivré aux services d'audit interne qui appliquent de façon pérenne les trente exigences pragmatiques du Référentiel Professionnel de l'Audit Interne.

Contactez-nous :
Tél. : 01 44 70 63 00
E-mail : certification@ifaci.com

SOMMAIRE

DANS L'ACTUALITÉ

6 **Stuxnet : une nouvelle ère dans la gestion des risques ?**
Antoine de Boissieu

INTERNATIONAL

8 **Les anciens de l'audit interne utilisent leurs acquis pour apporter une valeur ajoutée à leur nouvelle profession**
Shannon Steffee

IDÉES ET DÉBATS

11 **COSO 2013 : Une nouvelle édition du référentiel COSO sur le contrôle interne**

GRANDS PROJETS

13 **L'audit des projets de construction chez GDF SUEZ : une approche intégrée**
Edouard Bucaille et Catherine Gouverneur

LES AUDITS MÉTIERS

36 **Audit d'un processus informatisé**
Dominique van Egroo

FICHE TECHNIQUE N°44

>> **De l'usage du GTAG 1 chez Sodexo : forces et faiblesses**
Alain Rogulski

DOSSIER

La gestion des ressources humaines

Un levier de la performance des services d'audit et de contrôle internes

p. 17 à 35

18 **Les ressources humaines de l'audit et du contrôle internes : Panorama du contexte français**
Julie Ferré

21 **Le professionnalisme des auditeurs conditionne étroitement l'essor de l'audit interne au sein des ministères**
Hervé Toro

25 **Evolution et transformation d'une équipe d'audit**
Jean-Denis Malpelet

28 **Auditeur, une étape positive pour construire son plan de carrière**
Florence Vincent

33 **Constituer et gérer une équipe d'audit et de contrôle internes dans une collectivité territoriale**
Yannis Wendling

Stuxnet : une nouvelle ère dans la gestion des risques ?

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

La Corée du Sud a été victime le 20 mars dernier d'une attaque informatique spectaculaire. Les trois principales chaînes de télévision (YTN, KPS, MBC) ont vu leur système informatique paralysé pendant près d'une journée. Les agences de deux grands réseaux bancaires (Shinhan et Nonghyup) ont également été touchées. Toutes ces sociétés utilisaient le même type de serveurs (LG Uplus), qui a visiblement été la cible de l'attaque.
Ces incidents font écho à deux affaires survenues en 2010 et 2012 ; en 2010, le virus Stuxnet avait déréglé les centrifugeuses de la centrale nucléaire de Bouchehr et, selon les dires des experts, retardé le programme nucléaire iranien d'un à deux ans. En 2012, un virus très complexe, Flame, avait été identifié sur les ordinateurs de quelques personnes ciblées au Proche-Orient.

Quels enseignements en tirer pour les services d'audit et de contrôle ?

Des cibles pourtant bien préparées

La première observation frappante est que les cibles frappées étaient bien préparées.

1. Dans les deux cas en effet, les organisations impactées étaient parfaitement conscientes du risque. La Corée du Sud avait accusé plusieurs fois ces dernières années la Corée du Nord d'attaques informatiques. L'Iran savait que les Etats-Unis et Israël étaient fermement opposés à ses projets nucléaires, qu'ils étaient prêts à utiliser tous les moyens, et qu'ils disposaient de compétences très poussées en matière de sécurité informatique.

2. Dans les deux cas, les cibles visées étaient bien conscientes de l'imminence du risque. Au moment de l'attaque contre la Corée du Sud, la Corée du Nord était en pleine escalade verbale, menaçant son voisin de représailles (contre une attitude jugée hostile). De même, les Etats-Unis avaient insisté pour durcir les sanctions contre l'Iran à l'ONU, et avaient envisagé ouvertement la possibilité d'actions militaires.

Les cibles touchées étaient donc préparées à faire face à la menace. Elles ont pourtant été prises en défaut.

Un risque en très forte hausse

Le deuxième enseignement de ces affaires est que le risque d'attaque informatique a considérablement augmenté ces dernières années.

Des attaques de plus en plus probables

Il serait tout d'abord illusoire de croire que ce type d'attaques restera longtemps l'apanage d'organisations étatiques. Les réseaux de pirates informatiques et autres *hackers* échappent déjà largement à tout contrôle. Le développement et l'utilisation de virus du type Stuxnet par des acteurs privés (légaux ou non) est donc un risque à considérer très sérieusement. La question n'est pas de savoir si de tels virus pourraient être utilisés par des acteurs non étatiques, mais plutôt de savoir quand leur utilisation se généralisera.

Des effets potentiels dévastateurs

Le deuxième enseignement est que Stuxnet inaugure sans doute une ère nouvelle dans l'histoire des risques informatiques. On savait que des attaques informatiques pouvaient paralyser des systèmes d'information. Stuxnet va beaucoup plus loin, en étant le premier virus connu qui permet de prendre le contrôle de machines pour leur donner des instructions aberrantes. Les conséquences potentielles ne sont plus seulement la paralysie de l'activité, mais le sabotage pur et simple, avec toutes les conséquences imaginables. Ce sont ces conséquences que les entreprises doivent envisager désormais. La question qu'elles doivent se poser est « que se passerait-il si un

acteur extérieur prenait le contrôle de nos systèmes à notre insu, et y injectait des instructions aberrantes ou dangereuses ? ». Pour les sociétés du secteur des transports, de l'industrie lourde, d'exploitation de réseaux (électricité, gaz, eau, télécoms…), les conséquences potentielles peuvent être dévastatrices. Il en est de même pour les sociétés gérant des données complexes (pharmacie, ingénierie…), pour qui la modification frauduleuse de données peut avoir des conséquences majeures.

La protection contre ce type de risques est difficile, comme l'ont prouvé les exemples récents. Comme dans toutes les situations où l'élément générateur du risque n'est pas maîtrisé, il convient de concevoir une stratégie de maîtrise du risque qui agisse à trois niveaux.

Une stratégie de défense à trois niveaux

On peut tout d'abord se protéger contre la **probabilité** d'être touché : les systèmes peuvent être équipés de pare-feux, anti-virus, et autres dispositifs visant à empêcher l'entrée des virus. Ces dispositifs s'accompagnent de politiques de sécurité appliquées aux postes de travail (clefs et périphériques, postes bloqués contre l'installation de logiciels…) et aux réseaux. Il est aussi possible d'isoler les systèmes critiques, afin d'éviter qu'ils soient en communication avec des systèmes extérieurs. C'est d'ailleurs ce qui avait été fait dans le cas de la centrale de Bouchehr. Tous ces dispositifs permettent de diminuer la probabilité d'occurrence du risque, et sont absolument nécessaires. Ils restent cependant vulnérables à une négligence humaine ou à une évolution technique des menaces.

Il faut donc prévoir des dispositifs de contrôle qui permettent de lutter contre **l'ampleur** des attaques une fois qu'elles ont passé les premières défenses. La logique est celle suivie par les autorités sanitaires dans la lutte contre les épidémies. Il faut tout d'abord détecter l'attaque le plus tôt possible : des dispositifs de surveillance et d'identification des anomalies sont donc nécessaires. L'étape suivante consiste à isoler les systèmes infectés, pour éviter qu'il y ait une propagation aux systèmes et composants sains. Il est à noter que cette isolation est d'autant plus difficile que les systèmes sont intégrés et interconnectés, ce qui tend à être de plus en plus le cas. La conception même des systèmes d'information et de communication peut donc être un facteur aggravant du risque.

On peut ensuite se prémunir contre **l'impact** des attaques informatiques. Ainsi, l'existence de procédures de fonctionnement en mode dégradé peut permettre de déconnecter un sous-système sans impacter le fonctionnement de l'organisation. Il est aussi possible de prévoir des systèmes redondants, utilisant des technologies différentes, ce qui diminue la probabilité que les deux soient touchés en même temps. De tels dispositifs sont déjà obligatoires pour des systèmes critiques, par exemple dans l'aéronautique. Il est également important de pouvoir reprendre les opérations rapidement après une attaque : des plans de continuité ou de reprise d'activité bien rodés et régulièrement testés sont pour cette raison essentiels. Enfin, des assurances peuvent permettre de limiter les impacts financiers.

Les services d'audit, de risques et de contrôle doivent donc s'assurer que l'organisation a envisagé le risque d'attaque informatique malveillante par des virus du type Stuxnet, et y apporte une réponse globale, appuyée sur une véritable stratégie de maîtrise de ce risque. Certaines directions générales et comités d'audit ont déjà demandé des audits internes sur le sujet ; les événements récents survenus en Corée vont sans doute accélérer la tendance. ●

Stuxnet

Stuxnet est un ver informatique découvert en 2010. Il a vraisemblablement été développé par les États-Unis et Israël pour s'attaquer à l'industrie nucléaire iranienne. C'est le premier ver découvert qui espionne et reprogramme des systèmes industriels. Il permet de reprogrammer des automates programmables industriels (API) fabriqués par Siemens. Ces automates sont utilisés notamment par les centrifugeuses de la centrale nucléaire iranienne de Bouchehr, mais aussi par d'autres centrales électriques (pas forcément nucléaires), et pour l'exploitation de réseaux d'eau ou d'oléoducs. Stuxnext aurait touché 45 000 systèmes informatiques, dont 30 000 en Iran.

Flame

Flame est un autre un ver informatique, découvert en mai 2012, vraisemblablement de la même origine que Stuxnet. Il infecte les systèmes d'exploitation Windows. Il aurait infecté 1 000 ordinateurs de cibles bien précises, au Proche-Orient essentiellement. Il a des fonctionnalités de cyber-espionnage (interception de mails, de données PDF, Office, enregistrement de conversations…). Le programme, extrêmement complexe, a certainement d'autres applications, mais elles n'ont pas encore été dévoilées.

Les anciens de l'audit interne utilisent leurs acquis pour apporter une valeur ajoutée à leur nouvelle profession

Shannon Steffee - auditeur senior , **Internal Auditor**

La profession d'audit interne est sous les feux de la rampe depuis la chute d'Enron et de WorldCom il y a une dizaine d'années et la mise en place de la loi américaine Sarbanes-Oxley de 2002 qui s'en est suivie. Depuis, l'audit interne est devenu une profession dont le rôle au sein de l'entreprise est largement reconnu pour la valeur ajoutée qu'il apporte globalement à la gestion des risques, à la gouvernance et au contrôle interne. Si beaucoup le voient toujours comme un choix professionnel, l'audit interne est également considéré comme un tremplin et une école de formation pour ceux qui souhaitent que leur carrière évolue rapidement vers des fonctions de management. Souvent, ceux qui ont exercé la profession peu de temps déclarent qu'ils partent vers d'autres horizons avec des compétences précieuses.

Qu'ils aient été intégrés à un modèle de rotation selon lequel les entreprises font évoluer les collaborateurs dans différentes unités opérationnelles ou qu'ils décident de quitter l'audit interne de leur propre chef, bon nombre d'anciens auditeurs ont acquis une solide expérience qui leur est utile dans leurs nouvelles fonctions. Certains cherchent à démarrer une nouvelle carrière, tandis que d'autres déploient leurs compétences dans des rôles à responsabilités au sein de l'organisation. Autrement dit, de nombreux professionnels considèrent l'audit interne comme un tremplin vers d'autres opportunités et objectifs.

Que vous envisagiez de changer de carrière ou que vous l'ayez déjà fait, il est toujours utile d'écouter les conseils et les enseignements de ceux qui en ont l'expérience. Comme le dit un vieux proverbe roumain : « Les sages apprennent de l'expérience des autres ».

Exposition à toutes les facettes de l'entreprise

Les programmes de rotation des organisations qui intègrent l'audit interne ont pour but de former les collaborateurs à un rôle de management. Ceux qui travaillent au sein de l'audit interne gagnent souvent en expérience plus rapidement qu'en prenant directement des fonctions de management car l'audit interne doit comprendre le fonctionnement de l'entreprise.

Pour **Ashley Luft**, c'est le programme de rotation du distributeur mondial Home Depot, basé à Atlanta, qui l'a attirée. Aujourd'hui directrice financière au sein de la société, Ashley Luft travaille chez Home Depot depuis huit ans, dont quatre au sein de l'audit interne. Elle a rejoint Home Depot avec un diplôme d'ingénieur, sans formation comptable ou financière. *« Ayant toujours été curieuse de tout, la taille du programme de rotation de Home Depot et son exposition à toutes les facettes de l'entreprise étaient vraiment attrayantes à mes yeux ».* Tout en déclarant qu'elle ne s'appuie pas au quotidien sur ce qu'elle a appris de l'audit interne, elle reconnaît mieux comprendre le fonctionnement de la société grâce à l'interaction avec différentes unités opérationnelles qu'elle a connue lorsqu'elle faisait partie de l'audit. *« Rétrospectivement, c'est ce qui m'a donné confiance pour travailler avec tant de personnes différentes au sein de l'organisation et m'a permis de nouer de nombreux contacts ».*

Dans le cadre du modèle de rotation existant chez Ford Motor Co., **Brian Schaaf** a été appelé à travailler deux ans en tant qu'auditeur avant de prendre ses fonctions actuelles de trésorier adjoint. Avant cela, il avait exercé différentes responsabilités financières pendant près de

20 ans. Brian Schaal déclare : *« Pour être honnête, j'aurais préféré d'autres postes, parce que je ne connaissais et n'appréciais pas celui d'auditeur. Toutefois, au bout de quelques mois, j'ai vu pour l'équipe d'audit interne de nombreuses opportunités pour contribuer à renforcer la réussite de Ford ».* Selon lui, une meilleure compréhension de la philosophie de contrôle interne de Ford et des exigences et processus de contrôle interne compte parmi les avantages inhérents à la fonction d'auditeur. Son expérience en tant qu'auditeur l'a mieux armé pour poser des questions et donner des conseils sur l'efficacité des contrôles.

Le parcours d'**Andrew Griffith**, qui a commencé à travailler en entreprise, est complètement différent. En tant que responsable des charges au sein d'une société de transport en 2000, Andrew Griffith était constamment confronté à la fraude. Lorsqu'il a découvert que la société ne disposait pas d'une fonction d'audit interne, il s'est documenté et a commencé à réaliser des travaux d'audit interne, outre ses responsabilités de responsable des charges. Lorsque son poste a été supprimé, il a intégré pendant six mois le département commercial jusqu'à ce que le management lui propose de passer à plein temps à l'audit interne. Selon Andrew Griffith : *« Lorsqu'en 2002, la société s'est trouvée en difficulté du fait de problèmes financiers, j'ai vu là une opportunité pour parfaire ma formation ».* Il a acquis plusieurs diplômes et s'est vu proposer un poste d'enseignant après avoir obtenu un MBA. Puis, il a achevé un doctorat en comptabilité tout en enseignant à plein temps. Andrew Griffith intègre aujourd'hui ce qu'il a appris lorsqu'il était auditeur interne dans les cours de comptabilité qu'il dispense à l'Iona College de New Rochelle, dans l'État de New York.

Andrew Griffith explique que l'enseignement tiré de l'audit interne est l'importance du processus. *« Tout comme je l'ai appris quand j'étais auditeur interne, j'encourage mes étudiants à penser de façon moins cloisonnée et plus globale ».* Andrew Griffith, qui travaille par ailleurs comme consultant, déclare qu'il continue de considérer son travail comme une opportunité pour apprendre, et essaye d'identifier des améliorations pour les organisations qu'il conseille. *« Même les politiques de documentation que je continue d'appliquer ont été influencées par mon expérience d'auditeur interne. Si je pense qu'un problème peut provenir d'un scénario ou que les preuves sous-jacentes peuvent ou devraient faire l'objet d'un audit ou d'un examen, je prends soin de le documenter et de le conserver ».*

Formation sur le terrain

Grâce à l'exposition à toutes les facettes de l'entreprise et au temps passé avec les collaborateurs à tous les échelons, un passage à l'audit interne a accéléré l'apprentissage pour certains professionnels et a augmenté leur capacité à travailler avec des équipes transversales. De surcroît, les capacités de réseautage et les autres compétences générales acquises au sein de l'audit interne leur ont été bénéfiques lorsqu'ils ont quitté la profession.

« Quelle que soit la raison pour laquelle on quitte l'audit interne, le temps passé au sein de la profession permet d'acquérir des compétences et une expérience précieuses dans des fonctions ultérieures »

Ashley Luft déclare : *« Avec le recul, je pense que l'audit a sans doute été pour moi l'une des meilleures introductions à la société. Si j'avais rejoint la société à un poste financier, je n'aurais probablement jamais été exposée aux domaines de l'entreprise auxquels j'ai eu accès en travaillant au sein de l'audit ».* Ashley Luft a collaboré avec les équipes de la chaîne d'approvisionnement, des cartes cadeau, des fusions-acquisitions et des achats à l'échelle internationale, ce qui lui a donné l'occasion d'interagir avec des personnes très différentes dans toute l'organisation.

Selon Ashley Luft, un autre aspect concordant avec ses responsabilités financières est la capacité à influencer et persuader en dehors du rôle de propriétaire d'un métier. Lorsqu'elle était auditrice, elle a collaboré étroitement avec d'autres unités opérationnelles afin de mettre en œuvre les changements visant à améliorer l'organisation. Elle précise : *« Maintenant que j'occupe des fonctions dans la finance, je soutiens une unité opérationnelle et je dois bâtir des relations de confiance et influencer ses membres sur la base de mon point de vue en matière financière. J'ai pu établir ce lien plus facilement, de sorte que mon opinion est appréciée ».*

Avec une meilleure compréhension de la philosophie de contrôle interne de Ford, **Brian Schaaf** s'efforce aujourd'hui de démontrer l'importance d'une solide auto-évaluation et de la réactivité pour identifier et corriger les faiblesses de contrôle. Brian Schaaf explique : *« Je ne conteste jamais la nécessité de faire appel à une équipe d'audit interne hautement qualifiée pour obtenir une assurance supplémentaire sur le bon fonctionnement de nos contrôles ».*

Certaines personnes qui quittent la profession ont parfois besoin d'acquérir des connaissances avant de prendre leurs nouvelles fonctions. **Gary Gaugler**, par exemple, a créé puis dirigé pendant plus de 20 ans le service d'audit interne de Victaulic Co., une société du secteur manufacturier dont le siège social est

établi à Allentown, en Pennsylvanie. Lorsque la société lui a demandé de créer un nouveau service de fiscalité en 2009, il est devenu directeur de la fiscalité et du développement. Gary Gaugler explique : *« Bien que je ne sois pas expert en droit fiscal, je connais très bien les activités et les implantations géographiques de la société. Ainsi, par exemple, si j'examine une déclaration fiscale, je peux détecter les chiffres erronés en effectuant un examen des évolutions et une revue analytique des caractéristiques ».* Bien que la courbe d'apprentissage ait été rude, Gary Gaugler a plus que compensé ce déficit grâce à son expérience dans l'audit interne. Et le temps passé à revoir les processus, les procédures et les contrôles internes à l'époque où il faisait partie de l'audit interne l'a préparé à créer le nouveau service.

Jody Whitley, contrôleur chez Florida Fruit and Vegetable Association à Maitland en Floride a également été confrontée à un déficit de connaissances lorsqu'elle a quitté la profession d'audit. Elle a passé 24 ans en tant qu'auditrice interne, principalement dans le secteur bancaire, avant d'évoluer vers ses fonctions actuelles. Selon Jody Whitley, *« Il peut être difficile de sortir de l'audit interne pour évoluer vers un poste dans un secteur différent de celui dans lequel vous travailliez. Les opportunités pour se lancer sont moindres et toute la courbe d'apprentissage est à refaire ».*

Auditeur un jour, auditeur toujours ?

Pour certains anciens professionnels, l'audit interne a totalement modifié leur façon de penser. Les auditeurs cherchent souvent des moyens d'améliorer l'entreprise et cet état d'esprit perdure lorsqu'ils évoluent vers d'autres fonctions. Jody Whitley, par exemple, déclare qu'elle analyse systématiquement les problématiques d'audit interne, même en dehors de son lieu de travail – lors d'émissions télévisées, dans les restaurants et les magasins.

Il en est de même pour **Ashley Luft**. En tant qu'auditrice, elle a dû examiner des domaines dont elle ignorait tout. Elle explique : *« Vous devez apprendre à poser des questions et vous assurer de comprendre les réponses. Lorsque quelque chose paraît étrange, vous devez continuer les investigations. La capacité à aller dans le détail et à effectuer des diagnostics devient une seconde nature ».* Elle a également appris à être d'un optimisme prudent et à exercer un scepticisme salutaire. Cette approche s'avère particulièrement utile dans ses fonctions financières actuelles lorsqu'elle pose des questions telles que *« Quel est le scénario catastrophe ? », « Que se passera-t-il si ce risque se concrétise ? »* et *« Comment notre entreprise réagirait-elle si tel événement se produisait ? ».*

La réflexion analytique et la sensibilisation aux contrôles, aux processus et à l'évaluation des risques acquises à travers l'audit interne deviennent une seconde nature. **Gary Gaugler** indique : *« Tout ce que je propose ou que je mets en œuvre est marqué par mon expérience de l'audit interne. Je me demande quel serait le point de vue d'un auditeur objectif ».*

Pour **Andrew Griffith**, la pratique de l'audit interne a fait de lui un sceptique et il surveille de près les données financières, notamment celles qui concernent son salaire. Il explique : *« Dans la quasi-totalité des sociétés dans lesquelles j'ai travaillé, le service paye commet des erreurs, donc je vérifie systématiquement. J'invite mes étudiants à vérifier que les calculs dans leurs fiches de paye sont exacts et qu'ils sont payés ce qui leur est dû. Et j'ai personnellement détecté des cas où des organismes de prêts étudiants avaient prélevé des intérêts trop importants, ce que les étudiants n'avaient pas remarqué ».*

Et après ?

Quelle que soit la raison pour laquelle on quitte l'audit interne, le temps passé au sein de la profession permet d'acquérir des compétences et une expérience souvent considérées comme précieuses dans des fonctions ultérieures. L'exposition de l'audit interne à toutes les facettes de l'entreprise permet d'acquérir une compréhension des éléments porteurs de valeur et des meilleures pratiques applicables dans n'importe quelle autre fonction. Un auditeur interne efficace maîtrise également des compétences techniques et générales telles que la manière de structurer les rapports et le langage de l'entreprise. Pour **Ashley Luft** : *« En fin de compte, vous pouvez effectuer un travail de qualité et parvenir à des constats pertinents, mais si vous ne savez pas bien les communiquer et vous faire comprendre, vous aurez travaillé pour rien ».*

Selon **Jody Whitley**, il faut aussi parfois être sélectif dans les conseils ou les propositions de modification des processus opérationnels. *« Les recommandations de changement peuvent être interprétées comme une critique des processus existants, qui ont été mis en place par quelqu'un. La capacité à expliquer de façon positive les avantages, les efficiences et les problématiques de contrôle, et à convaincre, peut contribuer à atténuer les frustrations ».*

Étant au cœur de l'entreprise et exposé à un large éventail de compétences et d'expériences, l'audit interne peut être considéré comme un vivier de talents, tant sur le plan du développement de carrière que sur celui de la formation de collaborateurs appelés à devenir des dirigeants. ●

Article paru dans le numéro de décembre 2012 de la revue « Internal Auditor » de l'IIA Global www.internalauditoronline.org.

COSO 2013 : Une nouvelle édition du référentiel COSO sur le contrôle interne

A l'approche de la parution du nouveau référentiel COSO sur le contrôle interne, il convient de s'interroger sur ce qui change par rapport au référentiel d'origine, bien connu depuis plus de vingt ans des organisations de tous secteurs et de toutes tailles qui s'appuient sur celui-ci pour la conception, la mise en œuvre et l'évaluation de leur dispositif de contrôle interne.

Les experts nous donnent un premier aperçu des lignes directrices et de la valeur apportée par le nouveau référentiel dont la prise en compte bénéficierait à toutes les organisations, quelle que soit leur maturité en matière de contrôle interne.

Pourquoi devrais-je m'intéresser à cette mise à jour du COSO ?

La première raison est évidente, si votre organisation y est contrainte par la réglementation. Toute entreprise soumise à la réglementation SOX sera contrainte de s'adapter, mais également toutes celles faisant référence au cadre COSO dans le rapport signé par le président sur le contrôle interne. Ces dernières devront, a minima, analyser l'adéquation de leur dispositif par rapport aux nouveautés du référentiel sur l'ensemble du périmètre réputé couvert par un dispositif conforme aux exigences COSO.

La seconde raison est sans doute plus pertinente quant à l'intérêt de cette mise à jour. Dans de nombreuses organisations, il a été constaté que le contrôle interne pouvait se traduire par un dispositif lourd, à bout de souffle et éloigné des enjeux qu'il doit couvrir. De ce fait, les personnes qui en sont responsables peinent à trouver l'adhésion nécessaire autour du contrôle interne, particulièrement dans le contexte de crise et restrictions actuel. La nouvelle édition a été conçue pour aider les organisations à faire évoluer leur dispositif en fonction de l'environnement toujours plus complexe dans lequel elles opèrent. Les organisations cherchant à renforcer la fiabilité des informations utilisées pour le pilotage et les prises de décision y trouveront également leur intérêt.

Quelles nouveautés dans la version 2013 du COSO ?

Ceux qui étaient familiers du référentiel COSO retrouveront facilement leurs marques dans la version mise à jour. La nouvelle édition conserve notamment la même structure et reprend ainsi la définition du contrôle interne, les cinq composantes du contrôle interne et les critères utilisés pour évaluer l'efficacité des systèmes de contrôle interne. De plus, le nouveau référentiel continue d'insister sur l'importance d'aller au delà de la simple « *check-list* » et sur l'importance de l'implication et de l'appropriation par le management.

Pour autant, cette mise à jour apporte plusieurs nouveautés significatives, notamment la synthèse en 17 principes structurants associés aux différentes composantes, avec des points d'attention sous-jacents qui permettent de guider l'organisation dans l'élaboration ou l'évaluation de son dispositif de contrôle interne.

L'un des principaux contributeurs de la mise à jour du COSO, **Catherine Jourdan,** *directrice chez PwC*[1], nous explique en quoi la nouvelle édition permet d'apporter de la valeur à l'organisation : « *Une application intégrée des 17 principes structurants permet d'assurer un bon ciblage des efforts de contrôle interne et leur évolution en phase avec les évolutions de l'environnement interne et externe. Par exemple, la mise en place d'un centre de service partagé présente souvent de nouveaux risques par rapport aux objectifs opérationnels, de conformité et de reporting, qui demandent une redéfinition des points de contrôle, des flux d'information et du pilotage, pour soutenir la prise de décision et réaiguiller les activités le cas échéant* ». Cette approche dynamique axée sur les 17 principes confère une meilleure réactivité – voire une meilleure anticipation – par rapport aux enjeux de contrôle interne pour l'organisation.

Les évolutions des environnements opérationnels et sectoriels sont également abordées dans cette nouvelle édition. [Un membre du groupe de travail de relecture] souligne qu'« *une évolution importante réside dans l'élargissement des objectifs de la communication financière, afin que ces derniers tiennent compte des attentes croissantes en matière de transparence sur les sujets transversaux tels que le développement durable, l'environnement de*

travail, la sécurité, etc. Une seconde évolution bienvenue est la prise en compte de l'augmentation du recours aux fournisseurs de services externalisés et du besoin d'obtenir l'assurance nécessaire sur les dispositifs de contrôle interne de leurs tiers. Enfin, le référentiel met également en avant l'évolution des technologies, les attentes croissantes concernant le traitement de la fraude et la complexité croissante des modèles opérationnels ».

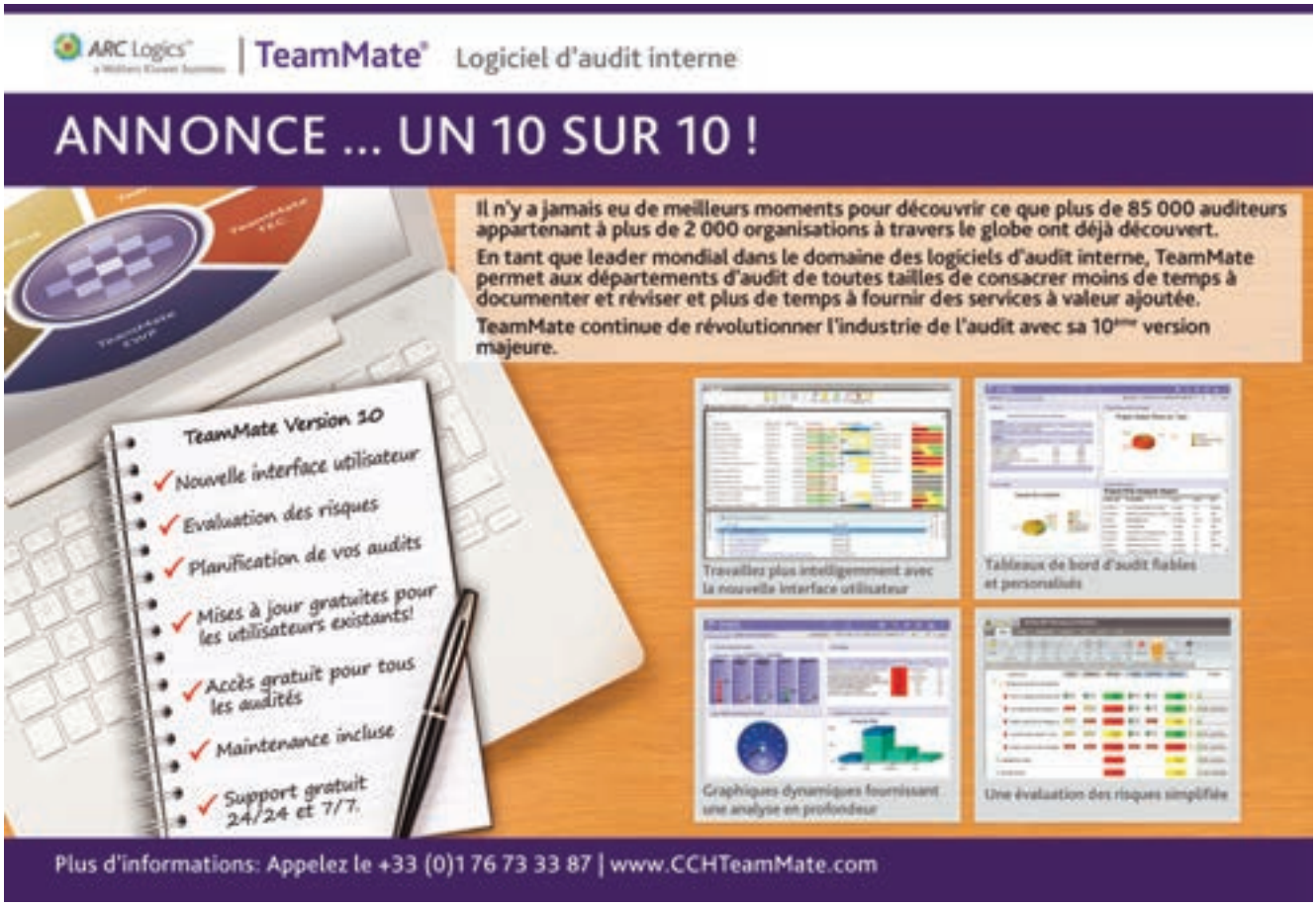
Comment le nouveau référentiel COSO peut-il aider mon organisation ?

Le référentiel mis à jour est destiné à aider les organisations à mettre en œuvre ou affiner des dispositifs de contrôle interne qui répondent aux spécificités de leur modèle opérationnel, de leur activité, de leur environnement externe.

L'articulation cohérente du dispositif de contrôle interne soutient une bonne gestion des risques et une bonne gouvernance de l'organisation. Selon **Jean-Pierre Hottin,** *associé chez PwC, « un exercice de coordination du contrôle est nécessaire pour qu'une organisation évalue les niveaux de risque acceptables et gère les risques, sans pour autant superposer des "couches" de contrôles ».* L'application d'un référentiel commun à un cadre plus large que la seule communication financière, englobant les opérations, la conformité et la communication extra financière, diminuerait le nombre de langages différents, de canaux de communication et de processus utilisés pour mettre en œuvre et évaluer le contrôle interne. Jean-Pierre Hottin précise : *« c'est la réussite d'une approche coordonnée entre les 3 lignes de maîtrise – ligne opérationnelle, fonctions supports et audit interne – qui permettra au dispositif de contrôle interne d'être non seulement efficace mais aussi efficient ».*

Le référentiel COSO a été largement accepté et utilisé depuis 20 ans – illustrant clairement que le contrôle interne n'est pas simplement un effet de mode mais un outil à haute valeur ajoutée pour le management. L'application élargie du contrôle interne à d'autres domaines tels que la qualité, la responsabilité sociétale et environnementale, ou encore la gouvernance, aboutit à une trame de réflexion commune. Cette harmonisation des méthodes fournit une plus grande flexibilité à l'organisation, aujourd'hui requise par les transformations internes et externes qu'elle subit. Ainsi, l'application des nouveautés du COSO 2013 permet la mise en œuvre d'un dispositif plus agile, s'alignant en permanence sur les objectifs de l'organisation et participant activement à l'atteinte de ces derniers. ●

[1] *PwC participe à la révision du référentiel avec le COSO et à sa traduction en Français avec l'IFACI.*



L'audit des projets de construction chez GDF SUEZ : une approche intégrée

Catherine Gouverneur, Conseiller en contrôle interne, **groupe GDF SUEZ**

Edouard Bucaille, Responsable de portefeuille de missions audit interne, **groupe GDF SUEZ**

Le contrôle interne de GDF SUEZ tient un rôle central dans la gestion des projets de construction. Il prend un caractère préventif en s'intégrant dans le pilotage de l'efficacité et de la performance, jouant ainsi pleinement son rôle de deuxième ligne de maîtrise des risques.

Dans la continuité du contrôle interne, l'audit interne tient le rôle de troisième ligne de maîtrise des risques, en s'assurant que la gouvernance et le contrôle interne sont effectifs et efficaces.

Dans le contexte de tension concurrentielle, économique et financière que nous connaissons actuellement, la croissance des grands groupes industriels repose sur leur capacité à développer des projets créateurs de valeur.

Sur la base des expériences acquises ces dernières années, et afin d'assurer le niveau de rentabilité des projets, il importe pour le groupe GDF SUEZ de maîtriser non seulement l'ensemble des risques opérationnels (techniques, environnement, sécurité, budget, contractualisation…), mais aussi de gérer avec le même soin les relations avec l'ensemble des parties prenantes : autorités concédantes, co-investisseurs, fournisseurs, clients, populations locales. Face à la complexité que revêt la gestion de projets de construction, les directions du management des risques, du contrôle interne et de l'audit interne du groupe GDF SUEZ se sont associées pour apporter une offre globale de sécurisation aux directeurs de projets.

Le cycle de vie d'un projet de construction

Dans un premier temps, et afin de donner une réponse adaptée, le management des risques, le contrôle interne et l'audit interne se sont attachés à analyser le cycle de vie des projets de construction. Il se décompose en trois phases clés au cours desquelles les risques majeurs de dysfonctionnement ont été identifiés de manière générique :

- la phase de *Business Development*, au cours de laquelle le projet est défini et caractérisé selon des hypothèses et des critères de rentabilité ;
- la phase de construction, qui consiste en la conception détaillée de l'ouvrage, l'exécution de la construction en soi, la phase de tests, la mise en service et le transfert aux opérations ; et
- la clôture du projet au cours des pre-

*Diplômé de Rouen Business School et d'Expertise Comptable, **Edouard Bucaille** est responsable de portefeuille de missions à l'audit interne du groupe GDF SUEZ depuis septembre 2008. Il a précédemment assuré le commissariat aux comptes de grands groupes industriels et été le directeur exécutif Europe de la gestion des risques dans un cabinet international d'audit externe.*

***Catherine Gouverneur** travaille au sein du Groupe GDF SUEZ depuis 15 ans. Diplômée dans les domaines de l'énergie et de l'ingénierie gazière à l'Ecole des Mines de Nancy et à l'Ecole des Mines de Paris, elle a exercé jusqu'à présent différentes fonctions de management opérationnel de structure et de management de projets au sein du métier Infrastructures du groupe (distribution du gaz, transport / acheminement et stockage). Ce faisant elle a choisi d'enrichir ses expériences opérationnelles par des passages dans les fonctions centrales en accompagnant l'ex groupe Gaz de France dans sa démarche de certification des processus techniques au début des années 2000 et en développant depuis 2 ans le programme de contrôle interne du groupe en matière industrielle.*

miers mois d'exploitation, qui permet de finaliser des détails mineurs de l'ouvrage et de capitaliser le retour d'expérience, notamment sur la véracité des hypothèses du projet et du scénario économique et financier.

Chaque phase fait appel à un ensemble d'acteurs dont les rôles et les missions peuvent évoluer au cours du projet.

L'analyse par la direction du management des risques fait apparaître une dizaine de grands risques génériques de dysfonctionnement pour chacun des 5 processus clés liés au pilotage d'un projet de construction exposés ci-après. Afin de couvrir ces risques, la direction du contrôle interne du groupe GDF SUEZ a élaboré deux référentiels : le premier (STR1 « Gestion des Engagements ») vise à s'assurer que les projets de construction présentés à décision d'engagement sont en phase avec la stratégie, les besoins et les critères de rentabilité du groupe ; le second (IND1 « Management de Projets de Construction Industrielle ») s'adresse aux chefs de projet en charge d'assurer l'exécution des projets dans les conditions retenues lors de la décision d'engagement.

Le rôle central du contrôle interne dans la gestion des projets de construction

GDF SUEZ a axé en priorité ses efforts de contrôle sur les phases amont de Business development et de construction car les retours d'expérience montrent que la phase d'exploitation représente en général moins d'incertitudes lorsque l'ensemble des étapes liées à la définition du projet et à la phase de construction ont été correctement couvertes.

Le référentiel IND1 vise à aider les chefs de projets à s'assurer qu'ils respectent les bonnes pratiques et principes fondamentaux du groupe pour sécuriser toutes les phases du projet. Il se fonde sur une analyse des principales familles de risques par phases et grandes thématiques ainsi que sur le résultat des travaux des communautés de pratiques du groupe mises en place au sein du groupe.

Le référentiel IND1 résulte lui-même de la mise en commun des expertises des activités multiples au sein du groupe, de la comparaison avec nos pairs, des normes internationales en vigueur, mais aussi des conclusions d'audits sur les projets de construction. Il donne les outils de maîtrise de ces projets selon 5 processus : gouvernance, gestion technique, gestion des coûts, gestion des contrats et des achats, et santé, sécurité et environnement. Ainsi le dispositif de contrôle interne prend un caractère préventif en s'intégrant dans le pilotage de l'efficacité et de la performance : le contrôle interne de GDF SUEZ joue pleinement son rôle de seconde ligne de maîtrise des risques.

La couverture globale de l'audit Interne

Dans le groupe GDF SUEZ, et dans la continuité du contrôle interne, l'audit interne assure le rôle de troisième ligne de maîtrise des risques. Sa mission est de s'assurer que la gouvernance et le contrôle interne sont effectifs et efficaces sur l'ensemble du cycle de vie des projets de construction et qu'ils permettent bien d'atteindre les objectifs poursuivis. En conséquence, il peut être amené à revoir tous les domaines couverts par le référentiel de contrôle IND1 sur la phase de construction. L'audit interne intervient aussi sur les étapes d'initialisation du projet et d'exploitation de celui-ci. Ainsi les missions d'audit interne peuvent porter sur les domaines suivants :

- la définition du projet de construction ;
- le transfert de la phase de *Business development* à celle de construction ;
- le pilotage du projet de construction dans différentes configurations contractuelles ;
- la revue de l'organisation du projet ;

Extension du barrage hydraulique de Jirau au Brésil

- la supervision par le management de l'ensemble du processus de construction ;
- la préparation de la phase d'exploitation et de maintenance ;
- le transfert de la phase de construction à celle d'exploitation.

Outre les référentiels de contrôle interne établis par le groupe, tels que IND1 et STR1, l'audit interne s'appuie sur plusieurs dispositifs normatifs internes et externes. Notamment, il travaille dans une optique de conformité avec les procédures spécifiques relatives à la gestion de projets de construction mises en place par les différentes entités du groupe, ainsi qu'avec le PMBOK *(Project Management Book Of Knowledge – Construction Extension of the Project Management Institute)* et le *Construction Audit Guide : Overview Monitoring & Auditing,* publié par l'IIA Research Foundation.

Cibler les thématiques d'audit

Les projets de construction exigent l'intervention de nombreuses parties prenantes internes et externes : ingénieurs, financiers, juristes, autorités administratives, sous-traitants, etc. Ils revêtent donc une complexité d'organisation particulière. Aussi, et notamment dans le cas de grands groupes industriels comme GDF SUEZ, ces projets s'étalent souvent sur plusieurs années, et sont donc sujets aux changements de contexte liés à des facteurs endogènes (stratégiques, commerciaux…) et exogènes (économiques, financiers, environnementaux, sociaux, politiques…). Il convient donc de déterminer avec précision les thématiques qui seront couvertes lors de la préparation de la mission d'audit. En effet, il convient d'adapter les objectifs de la mission à l'environnement dans lequel se situe le projet et aux perspectives que souhaite lui donner la direction générale.

L'audit de projets de construction chez GDF SUEZ couvre un ou plusieurs thèmes parmi les suivants, en fonction du degré d'avancement de ceux-ci :

- la revue de la gestion contractuelle du projet : revue juridique des contrats, des réclamations ;
- la gestion des partenariats : co-investisseurs, concédants, clients, sous-traitants… ;
- l'analyse technique du projet ;
- la rentabilité du projet : financement, retour sur investissement ;
- les dispositions environnementales, sociales et de sécurité autour du projet ;
- la gestion de l'évolution du projet : pilotage, modification du cahier des charges, retards… ;
- la commercialisation du projet : positionnement marketing, vente de la production ;
- l'exploitation des retours d'expérience sur le projet ;
- la gestion des imprévus : incidents et accidents, gestion de crise.

Compte tenu du nombre de sujets en jeu, un auditeur peut être un expert métier sur un domaine particulier, mais ne peut afficher une expertise de référence sur tous les domaines à la fois.

Aussi, les thématiques abordées et diligences requises sont fortement liées à l'état d'avancement du projet étudié. Il

Centrale électrique de ChilcaUno au Pérou

convient donc, pour l'auditeur en charge de la revue de projets de construction, qu'il suive a minima un certain nombre de principes de base : connaître la chronologie des grandes phases du projet, leurs livrables et objectifs principaux puis faire preuve de bon sens et savoir réagir efficacement en fonction des circonstances. Ainsi, l'auditeur est en mesure de mieux percevoir les risques liés au projet tel qu'il est structuré et d'évaluer l'efficacité des mesures de contrôle mises en œuvre pour maîtriser ces risques. A partir de ces principes de base, l'auditeur interne adaptera ses diligences en fonction des particularités du projet et de son contexte.

Quand auditer un projet ?

Un projet de construction peut s'auditer, soit lorsqu'il est terminé, selon une approche a posteriori, soit aux différentes étapes de son développement.

- A posteriori, tous les éléments constitutifs du projet sont connus et disponibles, l'auditeur interne peut plus facilement adopter une approche globalisée du projet et bénéficier des retours d'expérience sur le projet. Ce type d'audit est constitutif d'une boucle d'apprentissage importante dans la gestion des projets de construction.

- En cours de réalisation, les éventuels dysfonctionnements peuvent être corrigés – à moindre coût – avant qu'il ne soit trop tard ; il est aussi important de vérifier que les bonnes pratiques de gestion de projet sont bien appliquées. Ainsi, ce type d'audit permet une implication plus opérationnelle dans la gestion des projets de construction pour une amélioration en temps réel des processus mis en œuvre par les équipes projet.

Chaque méthode d'audit a ses particularités et est adoptée en fonction des objectifs de l'audit et des circonstances. De fait, il n'existe pas de moment plus ou moins adapté pour procéder à l'audit de projets de construction, car chaque méthode suit une philosophie propre et une logique spécifique. L'audit de ces projets s'effectue lorsque les événements le requièrent, un même projet peut d'ailleurs être audité à plusieurs reprises et un programme de construction peut être revu à différents stades de son avancement en fonction des événements : le bon moment pour procéder à cette démarche relève de l'expérience et du jugement professionnels de l'auditeur.

La combinaison des démarches de management des risques, de contrôle interne et d'audit interne constitue un facteur majeur de succès pour optimiser la gestion des projets de construction. ●

La gestion des ressources humaines

Un levier de la performance des services d'audit et de contrôle internes

18 **Les ressources humaines de l'audit et du contrôle internes : Panorama du contexte français**
Julie Ferré

21 **Le professionnalisme des auditeurs conditionne étroitement l'essor de l'audit interne au sein des ministères**
Hervé Toro

25 **Evolution et transformation d'une équipe d'audit**
Jean-Denis Malpelet

28 **Auditeur, une étape positive pour construire son plan de carrière**
Florence Vincent

33 **Constituer et gérer une équipe d'audit et de contrôle internes dans une collectivité territoriale**
Yannis Wendling

Les ressources humaines de l'audit et du contrôle internes : Panorama du contexte français

Julie Ferré - Chargée de projets Recherche, **IFACI**

De l'enquête réalisée en 2012, il ressort que l'on exige de plus en plus de compétences comportementales et techniques tant de la part des auditeurs internes que des contrôleurs internes.
Les motivations des uns et des autres ont également évolué : une vision globale de l'entreprise, une diversité des sujets abordés, c'est une demande des contrôleurs internes ; une bonne gestion de la crise, la pertinence des recommandations, la capacité à anticiper les risques – mais également une vision globale de l'organisation et la diversité des sujets traités, c'est ce que recherchent les auditeurs internes.
Ces exigences ne vont pas sans créer des difficultés de recrutement, car les profils recherchés sont rares sur le marché.

Les responsables d'audit interne et/ou de contrôle interne doivent gérer leurs ressources humaines afin d'apporter de la valeur à leur organisation. Cet objectif primordial est ainsi un des principes du Code de déontologie de l'audit interne, et un élément de la composante « environnement de contrôle » du COSO.

L'IFACI a réalisé une enquête en 2012 sur les métiers de l'audit et du contrôle internes, en partenariat avec le cabinet de recrutement Robert Half, dans le prolongement de celle réalisée en 2008. Les résultats de cette enquête présentés ci-après montrent que l'audit et le contrôle internes sont notamment des métiers :

- en voie de professionnalisation,
- dynamiques, qui recrutent,
- attractifs, une prépondérance donnée à d'autres facteurs de motivation que la rémunération.

Les ressources humaines du contrôle interne

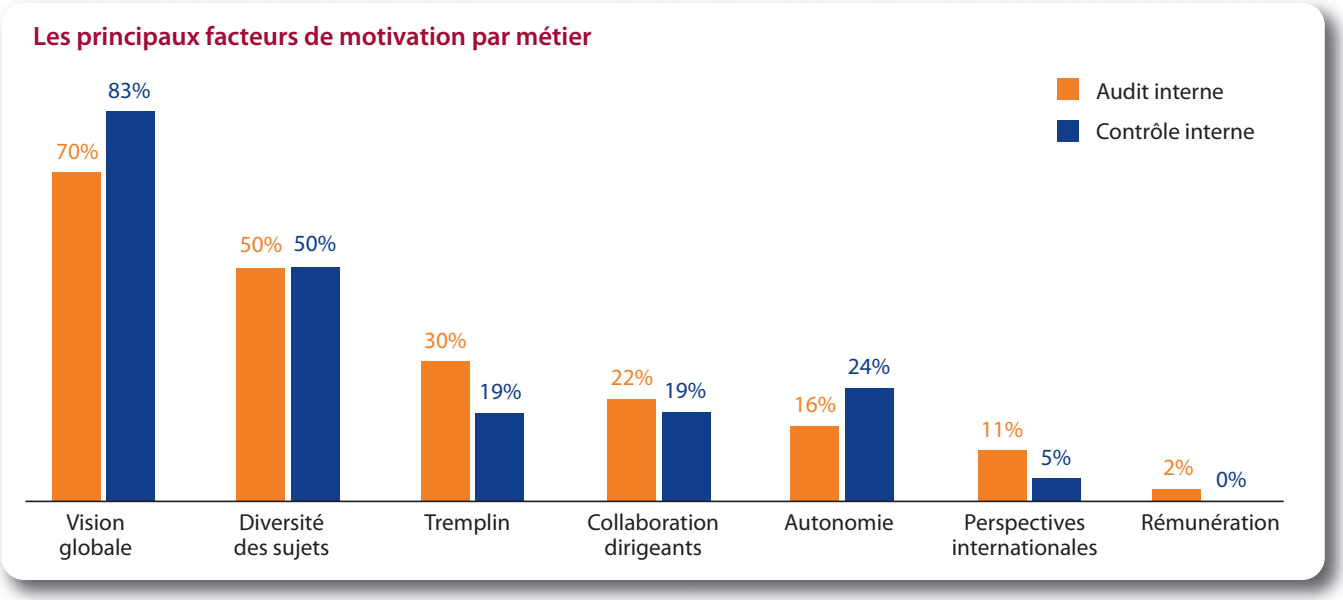
Qui est-il ?

La fonction de contrôle interne a pour objectif de développer le dispositif de contrôle interne, le promouvoir et piloter sa mise en œuvre dans l'ensemble de l'organisation. Afin de remplir ses missions, le contrôleur interne doit avoir certaines compétences.

Ses premières compétences, le contrôleur interne les acquiert au cours de ses études. Selon l'enquête IFACI / Robert Half réalisée en 2012[1], près de 90 % des répondants du contrôle interne ont un niveau d'étude BAC+5, notamment dans la filière économie, finance, gestion (63%). En ce sens, le contrôleur interne possède des connaissances[2] qui lui permettent de modéliser des processus, d'analyser et d'évaluer des risques, de maîtriser les outils d'analyse de données et de gérer les projets. Ces connaissances s'appuieront sur des savoir-faire tels que savoir définir et fixer des objectifs, définir des indicateurs de pilotage, animer un réseau, être pédagogue ou encore évaluer l'efficacité des contrôles. Le contrôleur interne acquiert également ses savoir-faire grâce à son expérience. Ainsi, selon l'enquête IFACI / Robert Half, les répondants ont exercé principalement des fonctions au sein de directions opérationnelles (39%) ou au sein de directions financières (32%).

Quelles sont ses motivations ?

Les motivations du contrôleur interne ont évolué. En 2008, la collaboration avec les dirigeants (61%) et l'autonomie (53%) étaient les principaux facteurs de motivations cités par les contrôleurs internes. En 2012, ces facteurs ont été moins cités (respectivement 19% et 24%), puisque les contrôleurs internes sont fortement motivés par la vision globale qu'ils ont de leur entreprise et la diversité des sujets abordés.



Résultats de l'enquête 2012 – IFACI / Robert Half – Les métiers de l'audit et du contrôle internes

Par la suite, le contrôleur interne peut faire reconnaître son expérience grâce à la certification professionnelle. Cependant, les certifications actuelles reconnaissent principalement les connaissances et l'expérience en audit interne. C'est pourquoi, l'enquête IFACI / Robert Half a montré qu'un contrôleur interne sur deux envisage d'obtenir la certification professionnelle CIA, spécifique au métier de l'audit interne.

Toutefois, depuis janvier 2012, l'IIA a développé une nouvelle certification dans le domaine de l'évaluation de la gestion des risques (CRMA – *Certification in Risk Management Assurance*). Cette certification permet de reconnaître les principes élémentaires du management des risques, la théorie et les pratiques de contrôle, les objectifs opérationnels et la performance organisationnelle. C'est ainsi que 28% des contrôleurs internes envisagent de préparer cette certification et donc de se professionnaliser. Cette tendance se confirme avec le souhait d'évolution au sein de son métier (23% des répondants souhaitent rester dans le contrôle interne).

Comment gérer son départ ?

En 2012, 70% ont indiqué leur souhait d'évoluer à moyen terme. Lorsque le contrôleur interne évolue à l'extérieur de son organisation, il reste dans son métier (39%) ou il se tourne vers le management des risques (18%). Et, lorsqu'il évolue au sein de la même organisation, évoluer dans son métier reste le premier choix (23%) même si les possibilités d'évolution au sein de son organisation sont variées. Ainsi, de par ses liens réguliers avec l'ensemble de l'organisation, le contrôleur interne peut se diriger vers des fonctions dans les directions opérationnelles (21%), le management des risques (21%), les directions support (16%) ou la direction comptable et financière (16%).

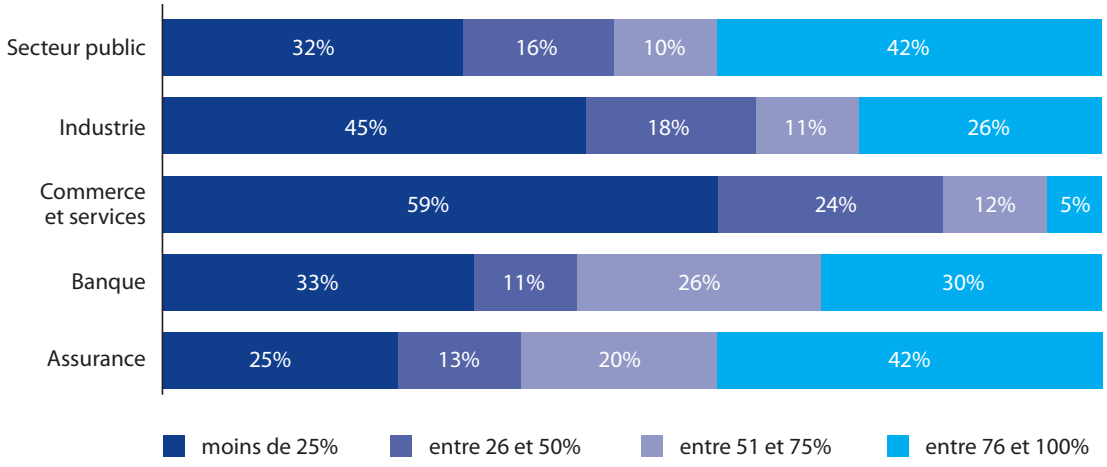
Si les contrôleurs internes ont la possibilité d'évoluer dans d'autres directions de l'organisation, c'est inversement le cas pour les recrutements. En effet, les responsables du contrôle interne recrutent principalement en interne (54% recrutent plus de la moitié de leurs effectifs en interne). Les responsables du contrôle interne interrogés dans cette enquête évoquent des difficultés de recrutement compte tenu de la rareté du profil recherché (58%).

Les ressources humaines de l'audit interne *(enquête Robert Half 2012, CBOK 2011)*

Qui est-il ?

Les auditeurs internes ont une formation initiale Bac + 5, majoritairement (62%) en Finance, Economie, Gestion. Au-delà de ces acquis, l'auditeur interne doit être indépendant, objectif, avoir un esprit d'équipe, savoir communiquer et posséder un jugement professionnel. Au-delà de ces compétences comportementales[3], la connaissance des systèmes d'information est une compétence technique et un savoir-faire recherchés. De plus, les connaissances techniques telles que savoir extraire et analyser des données (90% des répondants) ou l'échantillonnage statistique (85%) sont les principaux outils des auditeurs internes pour émettre des recommandations pertinentes, ce qui valorise l'apport de l'audit interne auprès des audités.
L'auditeur interne a une expérience professionnelle antérieure (99% des répondants de l'enquête IFACI / Robert Half).

Population de l'audit interne issue de la mobilité interne selon le secteur d'activité



Résultats de l'enquête 2012 – IFACI / Robert Half – Les métiers de l'audit et du contrôle internes

Cette expérience professionnelle s'est forgée au sein d'une direction opérationnelle (36%), d'une direction financière (25%). 23% des auditeurs internes ont précisé avoir une expérience en audit externe.

Quelles sont ses motivations ?

En 2008, l'auditeur interne considérait son métier principalement comme un tremplin (69%) vers d'autres fonctions. Un an après[4], les responsables de l'audit interne définissaient la valeur ajoutée de leur activité par une bonne gestion de la crise, la pertinence des recommandations émises ainsi que la capacité à anticiper les risques. De ce fait, les motivations de l'auditeur interne aujourd'hui sont d'avoir une vision globale de l'organisation (70%) et d'avoir une diversité des sujets (50%) dans leur activité. L'audit interne étant considéré comme un accélérateur de carrière, un auditeur interne sur 3 voit également son métier comme un tremplin. Ce tremplin peut être en interne, car 36% des répondants évoluent dans une direction opérationnelle de son organisation.

Toutefois, l'audit interne peut être également un tremplin pour évoluer dans son métier en interne (20%) mais surtout dans une autre organisation (44%). Afin de faire reconnaître son expertise professionnelle, l'auditeur interne pourra obtenir une certification professionnelle en audit interne : près d'un auditeur sur deux possède le CIA (76% envisagent de le passer) et un auditeur sur quatre possède le DPAI (25% envisagent de passer la certification de l'IFACI).

Comment gérer son départ ?

Plus d'un tiers des responsables de l'audit interne ont des difficultés pour recruter, car pour 57% d'entre eux le profil recherché est rare sur le marché.
Le responsable de l'audit interne utilise les cabinets de recrutement spécialisés (30%), et, dans une moindre mesure, recrute en interne (58% recrutent moins de la moitié de leurs effectifs en interne). Cependant, ces pratiques de recrutement diffèrent selon le secteur d'activités de l'organisation. Les secteurs public, d'assurance et de banque recrutent à l'inverse davantage en interne.

* *
*

Les professionnels de l'audit et du contrôle internes ont des profils identiques dans leur formation initiale et souhaitent se professionnaliser dans leur métier respectif. Les fonctions antérieures exercées et les motivations pour leur métier montrent un fort dynamisme des auditeurs et contrôleurs internes. Les responsables de service ont ainsi le choix de recruter des profils ayant une expérience dans des fonctions opérationnelles et des profils ayant une expertise dans les métiers de l'audit et du contrôle internes. Grâce à cette mixité, de plus en plus d'équipes d'audit interne ou de contrôle interne ont les compétences adéquates pour remplir leur mission et ainsi apporter de la valeur à leur organisation. ●

[1] *Enquête Les métiers de l'audit et du contrôle internes, IFACI / Robert Half, 2012*
[2] *Fiches métiers « Responsable du contrôle interne » et « contrôleur interne métiers », IFACI, 2013*
[3] *Enquête Common Body Of Knowledge – IIA/IFACI, 2011*
[4] *Enquête – Les pratiques de l'audit et du contrôle internes en France en 2009 – IFACI, 2010*

Le professionnalisme des auditeurs conditionne étroitement l'essor de l'audit interne au sein des ministères

Hervé Toro

Inspecteur général de l'administration du développement durable, Chef de la mission ministérielle d'audit interne pour le ministère de l'écologie, du développement durable et de l'énergie (MEDDE), et le ministère de l'égalité des territoires et du logement (METL)

Le comité de modernisation des politiques publiques a prévu la mise en place de structures formelles d'audit interne au sein des départements ministériels et le développement de l'audit et du contrôle interne au sein de l'administration. Depuis 2006, la montée en puissance de l'audit interne a été facilitée par les exigences de la LOLF. L'objectif primordial est de disposer d'auditeurs qualifiés, au sens des exigences professionnelles, pour la totalité des agents ayant à réaliser des missions d'audit.

L'audit interne et l'inspection ont-ils des points communs pour les agents en charge de ces missions ?

L'inspection et l'audit sont des activités de contrôle exercées par des agents de haut niveau qui n'exercent pas de fonction opérationnelle. C'est la raison pour laquelle les inspections et conseils généraux sont prédisposés à l'exercice des fonctions d'auditeur interne.

Les règles de déontologie, en particulier l'indépendance et l'objectivité des auditeurs constituent en outre une exigence commune, quel que soit le type de mission.

Les constats, les recommandations, ne doivent pas être entachés d'un quelconque défaut d'indépendance ou d'objectivité susceptible de mettre en cause la crédibilité des auditeurs ou inspecteurs, et par conséquent des productions.

Cet enjeu réel, commun à toutes les missions du Conseil général de l'environnement et du développement durable (CGEDD), l'a conduit il y a quelques semaines, outre la charte de l'audit interne qui régit les rapports entre audités et auditeurs, spécifique à l'audit interne, à mettre en œuvre une charte de déontologie commune à toutes les missions, y compris les inspections. Cette charte de déontologie va plus loin que les exigences posées par les normes d'audit, par exemple en formalisant une déclaration individuelle d'intérêt.

Quelles sont les singularités de l'audit pour les agents missionnés par rapport aux autres missions remplies par le Conseil général ?

Le CGEDD exerce trois types de missions principales :

- des missions de contrôle qui regroupent l'inspection, l'audit, et des enquêtes administratives,
- des missions d'expertise et de conseil,
- des missions d'évaluation.

L'audit est une activité normée

Les particularités résultent du fait qu'il s'agit d'une activité qui est normée au plan mondial, contrairement aux autres missions qui ne le sont pas. Les exigences posées par ces normes relèvent selon le cas d'obligations ou de simples recommandations.

Professionnalisme, méthodologie et évaluation externe

Les principales exigences concernent de manière très synthétique :

- le professionnalisme des auditeurs qui doivent avoir suivi une ou plusieurs formations appropriées,
- l'utilisation d'une méthodologie ad hoc qui ne s'improvise pas,
- et l'évaluation externe périodique de l'audit interne, quant au respect effectif des exigences édictées par les normes.

Après de multiples expériences y compris techniques, dans l'armée de l'air, à la délégation générale pour l'armement, à la Cour des comptes, et à la direction générale de l'aviation civile, en particulier en matière de contrôle de gestion, d'audit, et de finances, ***Hervé Toro*** *a été nommé inspecteur général de l'administration du développement durable en août 2011 et responsable ministériel de l'audit interne en février 2012. Il est diplômé entre autres d'un DESS de droit des entreprises commerciales, d'un executive MBA et de l'école supérieure d'administration de l'armement.*

Quel est l'état des lieux en matière d'audit interne ?

Le comité de modernisation des politiques publiques du 30 juin 2010 a prévu la mise en place de structures formelles d'audit interne au sein des départements ministériels, et de développer l'audit et le contrôle internes au sein de l'administration.

Cette décision a donné lieu à un décret en date du 28 juin 2011 précisé par circulaire du premier ministre du 30 juin 2011. Chacun des ministères a dû structurer sa politique d'audit interne autour de deux nouvelles instances : **un comité ministériel d'audit interne** présidé par le ministre et **une mission ministérielle d'audit interne** rattachée au Conseil général du développement durable. Pour le MEDDE et le METL, ces deux instances ont été créées le 6 janvier 2012 par arrêté de la ministre de l'écologie, du développement durable, des transports et du logement. Le comité ministériel est présidé par les deux ministres. Le champ des missions est très large puisqu'il concerne : l'écologie, le développement durable, l'énergie, l'égalité des territoires, le logement, mais aussi les transports, la mer, et la ville.

La part prépondérante de l'audit dans la programmation 2013

La part relative de l'audit au sein de l'activité CGEDD progresse de manière très importante depuis 5 à 6 ans. Elle représentait moins de 10% du programme annuel en 2006 alors que pour la programmation 2013 elle représentera **une part prépondérante de 35%** (30% pour les conseils et expertises, 20% pour l'inspection et 15% pour l'évaluation).

Les raisons de cette évolution

Cette évolution résulte de trois facteurs principaux :

- Depuis 2006, la montée en puissance de l'audit interne a été facilitée par les exigences posées par la loi organique relative aux lois de finances (LOLF), par l'implication du collège gestion administrative, financière, régularité, en particulier de son coordonnateur Jean-Claude Diquet, et par le rôle dévolu à la Cour des comptes en tant que certificateur des comptes de l'Etat. **Le champ des audits internes au sens strict était alors limité au seul périmètre des risques financiers et comptables.** Cependant la matérialisation d'une cartographie des risques comptables et financiers par le secrétariat général, d'une part, et la signature d'un protocole en 2010 entre la Cour des comptes et le CGEDD, d'autre part, ont permis d'accélérer cette évolution.

- Parallèlement au guide spécialisé du CGEDD relatif aux audits comptables, ont été progressivement rédigés et mis en œuvre des guides spécialisés spécifiques à certains risques « métiers ». Il s'agit :
  - de l'audit de programme ;
  - de l'audit des organismes sous la tutelle ou le contrôle du ministère ;
  - de l'audit de la mise en œuvre de la politique de prévention des risques naturels et hydrauliques ;
  - de l'audit de la mise en œuvre des politiques de l'eau et de la biodiversité ;
  - de l'audit des parcs nationaux.

- Enfin une action de formation spécifique à l'audit a été initiée depuis plus de deux ans à l'attention des cadres du CGEDD pratiquant des audits « métiers », afin de se rapprocher autant que faire se peut des exigences édictées par les normes, y compris par

Tour PASCAL

l'animation de séminaires internes de sensibilisation.

Quelles sont les évolutions attendues en matière de professionnalisation à court et moyen terme ?

Les évolutions attendues portent principalement sur la méthodologie, le professionnalisme des auditeurs et l'évaluation externe de l'audit interne. Cette évaluation externe sera dans un premier temps limitée au périmètre des audits comptables et financiers.

Par ailleurs, un programme de travail mené en liaison avec le secrétariat général vise à déterminer un état des lieux exhaustif des risques potentiels, de toute nature, pour la fin de cette année.

La méthodologie

Les guides d'audit du CGEDD ont été rédigés par des auditeurs qualifiés pratiquant l'audit depuis plus de cinq ans sur les audits financiers. Ils sont en cours d'actualisation depuis trois mois pour :

- d'une part, les mettre en adéquation avec le guide méthodologique relatif au dispositif qualité de mai 2012 s'appliquant à toutes les missions du Conseil ;
- d'autre part, les améliorer au regard des risques spécifiques, de préparation, de la conduite, et de l'exécution des missions, de la communication, du suivi des recommandations et du plan d'action éventuel. Des annexes intégrant des modèles faciliteront le travail des auditeurs. Ces mises à jour seront terminées pour le mois de juin 2013. Un nouveau guide relatif à l'audit de la mise en œuvre de la politique de prévention des risques naturels et anthropiques sera enfin élaboré pour le mois de juin 2013.

Le professionnalisme des auditeurs est le principal vecteur d'amélioration des pratiques

La pratique de l'audit interne exige des auditeurs qualifiés, c'est-à-dire ayant suivi des formations spécifiques à l'audit et aux missions à conduire.

La totalité des auditeurs du CGEDD pratiquant des audits financiers et comptables (20 environ) ont suivi des formations à l'audit, dont 9 personnes diplômées (ou en formation) du *Certified Internal Auditor* (CIA) ou du master Cour des comptes – Université Paris X Auditeur en organisations publiques. Les autres ont suivi des modules de formation spécifiques animés par l'IFACI ou la mission nationale d'audit de la DGFiP.

Ce professionnalisme des auditeurs s'étend depuis deux ans progressivement aux auditeurs (environ 80) réalisant des audits métiers. Des actions de formation de sensibilisation à l'audit sont animées par la 6ème section du

Conseil général à l'attention des missions d'inspection générale territoriale et des autres sections du CGEDD. Des formations externes, y compris diplômantes, au profit des agents appelés à pratiquer ce type de mission sont également réalisées.

En outre le recrutement d'agents en début et milieu de carrière permet depuis deux ans de réellement favoriser la pratique de l'audit. Cette orientation nouvelle aura en outre un effet de levier sur l'amélioration du contrôle interne des directions et services opérationnels et une meilleure maîtrise des risques, puisque ces auditeurs, après une formation et une pratique de 3 à 5 années de l'audit, iront exercer des activités opérationnelles.

L'objectif à long terme est bien de disposer d'auditeurs qualifiés au sens des exigences professionnelles, pour la totalité des agents ayant à réaliser des missions d'audit. L'effort de formation, coordonné avec la 7ème section du Conseil général sera donc poursuivi afin d'atteindre cet objectif. Il est également hautement probable que l'impact des travaux du Comité d'harmonisation de l'audit interne (CHAI) présidé par la ministre chargée de la réforme de l'Etat, sera très bénéfique en particulier quant à l'amélioration de la pratique des audits métiers.

L'évaluation externe de l'audit interne

L'audit interne doit faire l'objet périodiquement d'une évaluation externe.
L'IFACI a réalisé un audit à blanc de certification des audits internes comptables du Conseil général fin 2012 ; l'audit réel est prévu pour 2013.

Le rapport mentionne de nombreux points forts concernant notre professionnalisme et nos pratiques, en particulier :

- la structuration progressive de la démarche ;
- la motivation et l'engagement du management général et des équipes chargées de l'animation des activités d'audit interne ;
- la coordination d'audit (Cour des comptes, Mission nationale d'audit (MNA/ DGFiP), Service des affaires financière (SAF/SG) ;
- la mise en place de référentiels ;
- l'effort de formation.

Seules trois non conformités importantes sont à corriger avant de pouvoir obtenir la certification externe visée fin 2013 :

- le comité d'audit doit disposer des éléments qui lui permettraient de se positionner par rapport à la notion d'acceptation de risque ;
- la gouvernance de l'audit interne doit être améliorée ;
- la programmation doit être fondée sur une analyse des risques.

Le Conseil général met tout en œuvre pour réduire ces trois écarts d'ici la fin de l'année 2013. ●

Manuel d'audit interne

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 a été adoptée par de nombreux pays de par le monde. 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.

Pour commander le manuel, rendez-vous sur le site Internet de l'IFACI : www.ifaci.com

Evolution et transformation d'une équipe d'audit

Jean-Denis Malpelet

Responsable de l'audit, **Allianz France**

***Jean-Denis Malpelet** est responsable de l'audit d'Allianz France depuis septembre 2010. Ingénieur des Mines, actuaire, il travaille depuis plus de 20 ans chez Allianz. Son parcours varié a commencé à la gestion du personnel commercial et au contrôle de gestion. Ensuite, la direction des ressources humaines du réseau commercial puis la responsabilité commerciale d'une région ont précédé son retour à la direction marketing d'Allianz au moment du changement de marque d'AGF vers Allianz.*

A l'audit d'Allianz France, le recrutement des collaborateurs est une étape clé. Nous privilégions les recrutements internes et, en cas de besoin de compétences très pointues, nous faisons appel à des spécialistes. Nous investissons beaucoup dans la formation ; nous évaluons nos collaborateurs très régulièrement, selon un système qui permet de construire individuellement les évolutions et donc collectivement l'évolution de l'audit.

Revue « Audit & Contrôle internes » : *La gestion des ressources humaines commence par le recrutement, comment gérez-vous cette étape clef pour recruter des collaborateurs compétents ?*

Jean-Denis Malpelet : Le recrutement est effectivement un moment des plus importants. Et même essentiel pour construire l'évolution et la transformation d'une équipe d'audit. A l'audit d'Allianz France, nous privilégions aujourd'hui les recrutements internes. C'est un choix structurant qui oblige à anticiper à travers plusieurs actions. Un point clef est de construire puis de gérer un vivier de collaborateurs qui ont, un jour, marqué leur intérêt pour l'audit. En plus des compétences et du comportemental qui forment le socle minimum pour exercer le métier d'auditeur, on va aussi rechercher, au moment du recrutement, des compétences métiers qu'il est nécessaire de développer au sein de la direction. Par exemple, l'audit interne d'Allianz France ne peut pas se permettre de manquer au global de compétences actuarielles – c'est un point clef pour les professionnels de l'assurance que nous sommes – je dois donc être attentif à la présence de cette compétence chez certains des auditeurs… et au sein de notre vivier.

Pour faciliter l'alimentation du vivier, l'image de l'audit, école naturelle d'excellence, est à travailler sur un mode très marketing. Vu la qualité des outils, des méthodes et des effectifs en place, ce n'est pas le plus difficile mais cela implique une communication régulière sur nos activités.

Le reste de ce qui fait un recrutement réussi reste très important mais rejoint les bases communes et n'est pas propre à l'audit : collaboration étroite avec les ressources humaines, processus d'entretiens construit et transparent, clarté des échanges…

A&CI : *Un recrutement seulement interne ne vous pose-t-il pas des problèmes pour certains profils ?*

J.-D. M. : Je ne vous cache pas que c'est un point sur lequel j'avais quelques réserves à mon arrivée, il y a presque 3

ans. Dans les faits, la richesse des ressources internes d'Allianz France a toujours permis jusqu'ici, de trouver le profil recherché. De toute manière, lorsque l'on recherche des compétences très pointues, comme par exemple les risques opérationnels liés aux données informatiques ou les risques liés à la solvabilité, il est préférable de faire appel à des spécialistes. Chez Allianz, ces spécialistes peuvent, le plus souvent, se trouver en interne. L'appartenance à un grand groupe international permet de trouver facilement des spécialistes en provenance d'autres filiales en France ou dans d'autres pays. Nous pouvons aussi ponctuellement faire appel à une prestation d'audit externe.

Le CIA comme motivation à moyen terme

A&CI : *Une fois le recrutement effectué, que développez-vous pour l'intégration ?*

J.-D. M. : Même si nous avons chez Allianz une discipline de coût stricte, la formation, et plus particulièrement, la formation initiale, est un point sur lequel nous n'hésitons pas à investir. Nous nous appuyons sur un ensemble complet d'outils et de méthodes tant en interne, avec l'appui des auditeurs seniors, des responsables de mission, qu'en externe avec la formation IFACI. La qualité de cette intégration, gage d'une base solide, nous permet d'être ambitieux sur l'évolution de notre audit. Le plus important, au-delà du contenu du parcours initial de formation, est, à court et à moyen terme, de créer et d'entretenir la motivation à apprendre. A court terme, c'est la participation immédiate et opérationnelle à des missions d'audit. A moyen terme, c'est la volonté de décrocher la certification CIA ou CISA. Tous les recrutements se font avec cet engagement d'aller vers l'excellence reconnue pour cette fonction.
Notre mode de fonctionnement favorise une intégration rapide. Nos missions d'audit durent environ deux à trois mois. Au terme de chaque mission, l'auditeur récent va pouvoir bénéficier de l'expertise d'un responsable de mission différent. C'est à la fois exigeant, motivant et très favorable à une bonne intégration.

Une évaluation très régulière

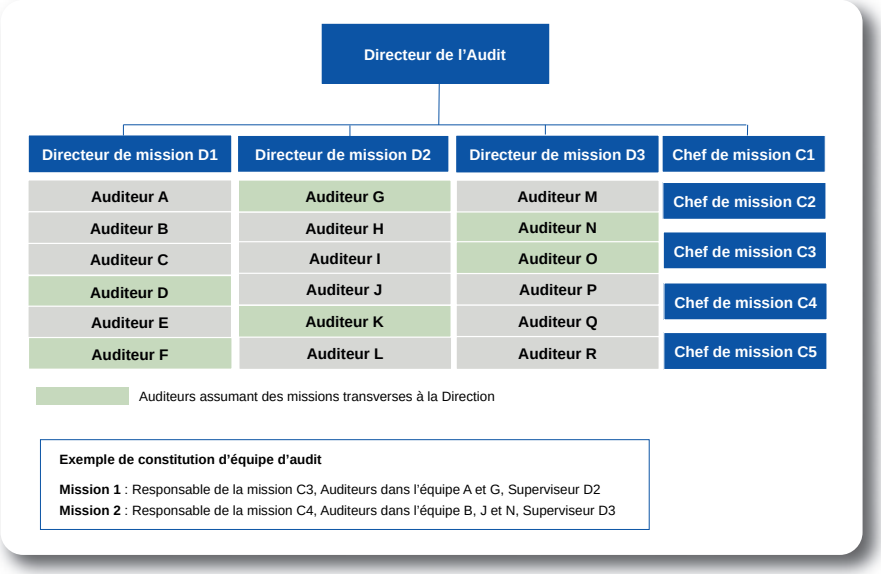
A&CI : *Comment les évaluer ?*

J.-D. M. : Comment ? Je dirai, pour répondre par une boutade… souvent. Chez Allianz, nous pratiquons un rotationnel fort dans les affectations de missions. Cela se traduit pour les auditeurs, d'une part par des participations à des missions variées, mais aussi, d'autre part, par des rattachements à plusieurs responsables de missions. Notre organisation simplifiée (Cf. schéma ci-dessous) permet bien cela.

Chaque directeur de missions a la responsabilité hiérarchique d'un ensemble d'auditeurs. Chacun de ses auditeurs est affecté, à chaque cycle d'audit, à une mission d'audit conduite par un responsable de mission qui peut être un directeur de mission ou un chef de mission (en bleu sur le schéma). Au terme de chaque mission, une évaluation formelle et partagée avec l'auditeur est réalisée. C'est naturel et cela permet de donner un *feed-back* construit et bienveillant sur le travail d'audit. Une évaluation similaire, sur des critères différents bien sûr, se fait par le superviseur pour le chef de mission. Nous avons également mis en place une démarche assez originale de *feed-back* anonyme de l'auditeur vers le responsable de la mission. Presque un 360° en continu pour les responsables de mission en quelque sorte. L'ensemble de ces processus d'évaluations servent à améliorer nos procédures sans se substituer pour autant aux moments d'évaluations récurrents qui sont des repères pour tous chez Allianz. C'est une évaluation forte et claire qui permet de construire individuellement les évolutions et donc collectivement l'évolution de l'audit.

A&CI : *Comment faire évoluer les auditeurs ?*

J.-D. M. : Une fois terminée la formation initiale, nous devons prendre en compte, de manière très attentive, les différents profils d'auditeurs. L'évolution va d'abord se traduire par une maîtrise des techniques d'audit, la capacité à les mettre en œuvre de manière autonome, à contribuer à des phases plus en amont de la mission comme la construction de



Partenaire et assureur officiel du Comité National Olympique et Sportif Français (CNOSF), Allianz a souhaité partager avec les athlètes et le grand public, l'émotion et la passion pour les Jeux Olympiques 2012

parties du programme de travail ou bien la responsabilité du suivi de mise en œuvre de recommandations.

Ensuite, selon les profils, des responsabilités peuvent être assumées sur des fonctions transverses à la direction. Par exemple, certains contribuent à la maintenance régulière de notre univers d'audit.

Une autre piste existe aussi, rendue possible par notre appartenance au grand groupe international qu'est Allianz. Certains auditeurs peuvent être amenés à conduire des missions à l'étranger. La maîtrise de la langue, principalement anglaise, doit alors être suffisante pour permettre une collaboration en milieu international. La limite de l'exercice est, bien sûr, le coût induit par les transports et l'hébergement, mais cela reste extrêmement profitable. Le fait que nous opérons comme une seule et même fonction au sein du groupe Allianz, avec plus de 600 auditeurs, ouvre naturellement ce type de possibilité.

Une autre piste d'évolution que nous avons ouverte récemment est de confier à des auditeurs seniors des missions de A à Z. Cela permet à la fois de leur donner des moments de pleine autonomie avec seulement une supervision, mais aussi de couvrir le plus parfaitement possible notre univers d'audit : certains objets d'audit seraient sans cela couverts de manière trop anecdotique par des missions plus globales.

Et, bien évidemment, nous sommes également très attentifs à réaliser des promotions internes. C'est une voie naturelle mais qui n'est pas la seule.

A&CI : *Quel mode de rémunérations adoptez-vous ?*

J.-D. M. : En ce qui concerne les auditeurs, nous n'avons pas de rémunération sur objectifs, mais les mécanismes d'augmentations individuelles viennent s'appuyer de manière cohérente sur les évaluations que nous avons évoquées précédemment.

En ce qui concerne les responsables de missions, une part de la rémunération se fait sur objectifs. La qualité du travail d'audit, son efficacité aussi, sont des critères qui sont directement intégrés à la rémunération. Une partie de leurs objectifs prend aussi en compte la dynamique de changement, importante au sein de l'audit à travers les composantes du plan d'amélioration de la qualité. Même si les pratiques professionnelles encouragent de telles démarches de changement, il n'est pas inutile de les conforter par un intéressement pour ceux qui les mettent en œuvre.

A&CI : *Comment gérez-vous les départs ?*

J.-D. M. : Comme les arrivées : en anticipant le plus possible. Cela, encore une fois, nécessite un travail de coopération avec la DRH. C'est aussi la relation de confiance au sein de la direction qui permet d'anticiper ces événements. L'idée est de favoriser de bons départs qui répondent au mieux à une évolution qui fait sens pour l'auditeur. En cela, l'image de l'audit comme fonction tremplin ou boost dans la carrière est presque contre productive car elle amène l'auditeur à être très sélectif dans son évolution au sortir de l'audit. La valeur d'un passage à l'audit se révèle en partie immédiatement et en partie dans le temps. Un peu de modestie ne nuit jamais quand on retrouve des contextes très opérationnels.

Le principe d'avoir environ une grosse moitié de la direction de l'audit en rotationnel conduit de toute façon à un taux de *turn over* qui rend l'événement assez courant. C'est à la fois une menace car il ne faut pas banaliser, mais aussi une double opportunité : bénéficier de promoteurs précieux dans différentes directions et s'assurer de comportements « œil neuf » qui n'hésitent pas à questionner les modes de fonctionnement de la direction d'accueil. C'est très dynamisant !

A&CI : *Une dernière remarque plus générale ?*

J.-D. M. : Une réflexion sur les normes internationales. Ce cadre de référence est souvent, et à juste titre, la base pour tout ce qui concerne le cœur de l'activité opérationnelle de l'audit. Il est également très efficace pour développer une gestion des ressources humaines optimum pour l'audit. ●

Auditeur, une étape positive pour construire son plan de carrière

Florence Vincent

Directeur de l'audit, **Michelin**

La gestion des carrières dans le groupe Michelin s'appuie sur un triangle dans lequel trois acteurs ont un rôle important à jouer : la personne, son manager et le gestionnaire de carrière. Les personnes qui sont le plus rapidement évolutives font l'objet d'un suivi particulier de la part des gestionnaires de carrière. Ce que deviendra l'auditeur après son passage à l'audit est important, afin que l'audit soit considéré comme une étape positive dans la construction d'une carrière professionnelle.

Revue « Audit & Contrôle internes » : *Pourriez-vous nous présenter en quelques mots l'organisation de l'audit chez Michelin ?*

Florence Vincent : Les auditeurs appartiennent à la direction groupe de l'audit et des risques (DGAR) qui a pour mission d'aider l'entreprise à mieux maîtriser ses risques. Cette direction est directement rattachée à la présidence du groupe afin d'assurer son autorité et son indépendance.

Nous bénéficions d'une gouvernance au plus haut niveau de l'entreprise avec un propriétaire pour chaque risque. En plus de l'équipe d'auditeurs internes, nous nous appuyons sur un réseau d'une quarantaine de correspondants « *Risk management* » dans chacune des entités du groupe Michelin.

Les auditeurs internes de risque vérifient l'efficacité de l'ensemble du dispositif :

- Ils mesurent la qualité de la maîtrise des risques par des audits.
- Ils aident les entités concernées à définir et mettre en œuvre les plans d'actions nécessaires.
- Ils s'assurent que les plans d'actions avancent comme prévu et alertent le Groupe en cas de dérive.

L'équipe mondiale d'auditeurs est répartie sur deux sites. A Clermont-Ferrand, où se situe le siège du groupe ; et à Greenville, en Caroline du Sud, où est installé le siège de notre activité nord-américaine. Tout auditeur, quelles que soient sa base géographique et sa nationalité, a vocation à agir au niveau mondial puisque nos activités sont par définition mondiales.

A&CI : *Quelles compétences attendez-vous d'un auditeur ?*

F.V. : Notre profil cible se conjugue en trois dimensions : le profil métier, l'expérience et le comportement professionnel attendu.

A&CI : *Pouvez-vous tout d'abord préciser quel est le profil métier ?*

F.V. : Notre métier consiste à évaluer la qualité de la maîtrise des risques par le groupe Michelin. Notre périmètre englobe 13 familles de risques (Cf. schéma 1). Nos 13 familles requièrent donc chacune des compétences pointues.
Par exemple, évaluer la maîtrise des risques de rupture d'approvisionnement suppose d'avoir des auditeurs qui connaissent les produits achetés.

Auditer la maîtrise des risques environnementaux suppose de son côté d'avoir des auditeurs qui connaissent ces risques, qui les ont vécus sur le terrain et qui connaissent les prescriptions du

Schéma 1 : Les 13 familles de risques chez Michelin

groupe et l'organisation de la réglementation internationale.
Auditer les risques sécuritaires liés au produit suppose d'avoir dans notre équipe des personnes qui ont conçu et développé des pneus et des équipes qui ont fait partie du dispositif de garantie qualité, par exemple des directeurs qualité de leur entité.
Au travers de ces quelques exemples, vous comprenez déjà que nous avons besoin d'une équipe multidisciplinaire capable de couvrir nos treize familles.

A&CI : *Qu'en est-il de l'expérience professionnelle ?*

F.V. : Tout d'abord, la clarté sur le profil attendu dans le poste s'impose. Il faut parfaitement définir ce profil qui n'est d'ailleurs pas uniforme puisque notre panoplie d'audits est extrêmement large : elle touche aussi bien les aspects comptables que l'informatique, la *supply chain* ou l'outil industriel.
Evaluer la maîtrise d'un risque suppose d'avoir une robuste expérience dans le métier en question. Car tout n'est pas normé et il faut donc pouvoir faire un audit sans cadre référent. Cela requiert une hauteur de vue suffisante pour apprécier la qualité des analyses de risques et des choix politiques effectués et pour identifier si les dispositifs de prévention, de protection et de contrôle sont suffisants (Cf. schéma 2).
Il faut également être capable de présenter les conclusions aux dirigeants du groupe et de faire des recommandations pertinentes pour les équipes propriétaires des risques. Ces dernières sont en règle générale expertes dans leur domaine.
Cette expérience suppose une « tête bien faite » et au moins 15 ans dans un métier donné.
Notre seule exception concerne les domaines des risques comptables, de la finance et de la fraude pour lesquelles nous demandons 5 ans d'expérience préalable en audit externe.

A&CI : *Quels comportements professionnels attendez-vous d'un auditeur ?*

F.V. : Les premières qualités auxquelles je pense sont la rigueur intellectuelle, la capacité d'analyse, la faculté de synthétiser et de communiquer clairement, tant à l'oral qu'à l'écrit – dans les deux langues officielles du groupe que sont le français et l'anglais. L'auditeur doit également avoir un grand sens de l'éthique car c'est non seulement l'une des valeurs du groupe Michelin mais aussi une exigence particulière du métier.
Nous avons d'ailleurs défini les compétences générales nécessaires à la pratique du métier d'auditeur. Elles figurent dans un manuel de compétences :

- connaissance de ce qu'est le contrôle interne ;
- maîtrise des principaux concepts de la gestion des risques ;
- expertise en évaluation de la maîtrise des risques ;
- maîtrise des techniques de l'audit ;
- maîtrise des techniques de communication à l'oral et à l'écrit ;
- efficience opérationnelle dans l'utilisation des outils de bureautique ;
- bagage interculturel ;
- capacité à bien travailler en équipe ;
- maîtrise du français et de l'anglais.

Le groupe Michelin a en outre prescrit les cinq comportements attendus de l'ensemble de ses collaborateurs. Ces comportements sont particulièrement adaptés à l'audit :

- la pratique des valeurs ;
- l'anticipation ;
- l'agilité dans l'exécution ;
- la coopération ;
- le progrès constant.

***Florence Vincent**, diplômée de HEC, a d'abord exercé plusieurs postes de responsabilité à la Société Générale et chez Accenture. Elle est entrée dans le groupe Michelin en 1992. D'abord en charge de missions d'audit financier, elle a ensuite fait partie de l'équipe chargée du stage d'intégration des nouveaux embauchés, un système propre à Michelin. Elle a ensuite été en charge de la rémunération pour le groupe de cadres dirigeants. Après avoir occupé un poste de stratégie industrielle aux États-Unis, elle a été nommée en 2005 responsable de l'audit interne. Ce poste de responsabilité s'est par la suite étendu à la gestion des risques.*

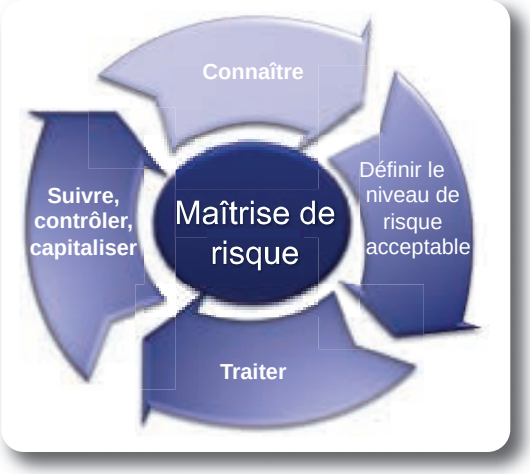


Schéma 2 : La roue des risques

A&CI : *Comment repérez-vous vos futurs auditeurs ?*

F. V. : La clé du succès de notre démarche réside dans un dialogue permanent avec la direction du personnel[1]. Ce dialogue passe par l'existence au sein de cette direction d'un interlocuteur dédié à nos activités : le gestionnaire de carrière. Je rencontre chaque mois cette personne qui constitue notre liaison avec la direction du personnel et je discute avec elle de nos besoins présents et à venir ainsi que des candidats potentiels.

Lors de ces rencontres avec le gestionnaire de carrière nous nous efforçons d'anticiper les besoins, de rechercher des candidats et de prévoir les sorties en identifiant à l'avance des propositions de postes futurs pour ces personnes.

A&CI : *Plus concrètement, comment attirez-vous les candidats potentiels ?*

F.V. : Au sein du groupe nous avons tout d'abord l'opportunité de présenter tous les trimestres notre activité dans le cadre du stage d'intégration de tous les nouveaux entrants. Dans le cadre de cette session qui réunit une centaine de managers et ingénieurs de toutes nationalités, je présente durant environ une heure notre activité de façon interactive. L'objectif est de sensibiliser l'auditoire à la gestion des risques et de lui présenter notre direction. De plus, des auditeurs viennent présenter leurs activités aux « stagiaires » au cours d'un forum de deux heures et répondent aux questions posées par les nouveaux entrants.

Nous disposons d'un deuxième vecteur de communication interne avec notre site intranet. Nous y présentons les enjeux de la gestion des risques et expliquons comment notre direction audit & risques contribue à l'amélioration de la maîtrise des risques. Nous en profitons pour attirer de nouveaux talents avec une rubrique spécifique « nous rejoindre ».

Dans cette rubrique figure également le témoignage des anciens auditeurs qui illustre la facilité du « rebond » après un passage chez nous. C'est d'ailleurs une particularité de la direction de l'audit & risques : nous maintenons des liens actifs avec nos anciens qui peuvent être amenés à nous servir de relais dans leurs nouvelles entités. Nos anciens sont en quelque sorte nos « ambassadeurs ». Ils assurent dans leurs nouvelles fonctions la promotion de nos activités et témoignent de l'apport d'un passage par l'audit dans la construction d'une carrière.

Enfin, nous mettons en avant sur notre site intranet le témoignage de membres du Comité exécutif du groupe Michelin sur la qualité et l'utilité des audits. Nous bénéficions donc de la part de notre direction générale d'un satisfecit qui valorise le métier.

A&CI : *Et comment s'opère le recrutement ?*

F.V. : Il faut distinguer les candidatures internes des candidatures externes.

Pour une embauche interne, nous analysons le parcours de la personne. Nous y décelons les qualités attendues pour le poste d'auditeur. Ensuite, nous organisons plusieurs entretiens avec des membres de notre propre équipe de direction.

Enfin, nous demandons au candidat de rencontrer individuellement trois ou quatre auditeurs qui seront ses futurs collègues, en faisant en sorte que ce soient des auditeurs aux profils différents. Ces rencontres permettent au candidat de se faire une idée assez précise de la nature des missions d'audit et d'évaluer les avantages à devenir auditeur tout en prenant conscience des difficultés éventuelles.

Les candidats viennent donc chez nous en pleine connaissance de cause !

A&CI : *Et comment s'opère le recrutement d'un candidat venant de l'extérieur ?*

F.V. : Depuis toujours, le groupe qui privilégie largement la promotion interne, recrute chaque nouveau salarié dans la perspective d'un parcours dans la durée, au-delà d'un poste particulier. Ceci est notamment rendu possible par l'organisation spécifique à Michelin des gestionnaires de carrière qui accompagnent les personnes dès l'embauche et tout au long de leur parcours dans l'entreprise.

Il faut donc préciser que nos embauches externes ne représentent qu'environ dix pour cent de nos recrutements car les seules embauches externes que nous réalisons concernent les domaines du risque financier et le manquement à l'éthique.

Nous cherchons dans ce cas un candidat venant d'un cabinet d'audit externe, en général de l'un des quatre grands cabinets connus dans le métier, et ayant 3 à 5 ans d'expérience. Cette personne va passer par le processus classique de recrutement chez Michelin. Après analyse positive de son CV, cette personne bénéficiera d'un premier entretien avec la direction du personnel.

Le candidat passera alors une journée entière d'entretiens à Clermont-Ferrand. Au cours de cette journée, il rencontrera deux personnes de la direction de l'audit & risques, un gestionnaire de carrière et un manager issu d'une autre direction. La décision de faire une offre – ou pas – au candidat est donc prise de façon collégiale.

A&CI : *Quel est le mode d'intégration des nouveaux auditeurs à votre direction ?*

F.V. : Il existe deux dates d'entrée idéales pour nous rejoindre. Soit en septembre car cela coïncide avec notre formation annuelle de deux semaines (à laquelle toute l'équipe participe) qui permet au candidat de s'intégrer très vite chez nous et d'acquérir les premiers rudiments du métier. Soit en janvier car nous organisons à ce moment-là notre réunion mondiale de la direction audit & risques. Nous y dressons le bilan de l'année écoulée, établissons le plan de l'année à venir et travaillons pendant trois jours en ateliers sur nos chantiers d'amélioration.
Tout nouvel entrant bénéficie en outre d'un programme de formation individuel qu'il prépare, dès les premières semaines, à partir d'un plan de formation type.
Nous avons par ailleurs mis en place un « *coaching* » du nouvel arrivant par un autre auditeur plus expérimenté qui devient en quelque sorte son référent pour toutes les questions, petites ou grandes, qu'il se pose.
L'auditeur réalise ses premiers audits dans une équipe pilotée par des auditeurs « seniors », ce qui lui permet de bénéficier de l'expérience des autres. Il est en outre membre d'équipes de projets d'actions de progrès.
Nous veillons également à développer l'esprit collectif. L'intégration se fait plus rapidement et plus facilement car les auditeurs travaillent dans des bureaux paysagers. Nous avons un moment collectif tous les matins à 10h pour un café qui permet de réunir tous ceux qui sont sur Clermont-Ferrand ce jour-là pendant quelques minutes. Et, le vendredi, ce café de dix heures se transforme en « *breakfast management* » à l'occasion duquel un auditeur explique à ses collègues l'une de ses missions.

A&CI : *Quelles sont les formations prodiguées pour rendre les auditeurs rapidement opérationnels ?*

F.V. : Nous avons un plan de formation qui se déroule sur quatre ans et qui totalise plus de 40 jours de formations. Le cœur de ce plan réside dans une session annuelle de deux semaines qui rassemble toute l'équipe. Comme tout le monde n'est pas au même niveau d'expérience, nous avons en parallèle quatre programmes de formation différents : un pour les nouveaux arrivants, un autre pour ceux qui sont là depuis un an, etc. Chaque programme comporte un tiers de méthodes sur l'audit et les risques, un tiers de méthodes et d'outils de résolution de problèmes et un tiers de formation consacrée à la communication.
Cette session s'effectue à l'extérieur de nos sites pour que l'équipe se déconnecte de son travail quotidien. Elle s'effectue au retour des vacances d'été, lorsque les « affaires » n'ont pas encore repris et à un moment où chacun est reposé et ouvert. Nous faisons appel à quelques invités externes à notre direction de l'audit & risques. Au total, ce sont quarante modules de formation qui sont déployés, dont une moitié est animée par le management de la direction de l'audit et des risques et l'autre moitié par des prestataires externes. Il y a en gros 10 % de théorie, l'essentiel étant consacré à des ateliers et donc à des travaux en commun.

A&CI : *Comment évaluez-vous les auditeurs ?*

F. V. : Nous évaluons les auditeurs de façon permanente. Lors de chaque mission d'audit, le manager procède à une évaluation détaillée tenue à jour tout au long de la mission. Il s'y ajoute une auto-évaluation des auditeurs ainsi qu'une réunion d'échange entre les auditeurs et le manager au cours de laquelle est dressé le bilan de la mission.

Equipe DGAR

Pour les missions comportant une équipe composée de plusieurs auditeurs, nous confions à l'un d'entre eux le fait d'être « responsable » de la coordination de la mission et nous évaluons alors sa capacité à manager son équipe. Nous procédons de même pour chaque suivi de plans d'actions.

Pour les objectifs annuels des auditeurs nous retenons cinq indicateurs :

- La réalisation du plan d'activité (communiqué en début d'année) dans le délai prévu. Ce plan comporte des audits mais également d'autres activités (réalisation de guides d'audits, de synthèses, etc.).
- La réalisation du plan de progrès (communiqué lui aussi en début d'année). Les chantiers de progrès sont en effet menés par des équipes d'auditeurs à l'image de ce qui se passe pour les audits.
- La réalisation du plan de suivi de plans d'action.
- Le degré de conformité aux tests de contrôle interne de nos propres audits.
- L'évolution de la maîtrise des risques du groupe sur un cycle de 4 ans.

A&CI : *Plus concrètement, comment se passe l'évaluation ?*

F.V. : Nous utilisons en fin d'année le système d'appréciation du groupe Michelin qui prend en compte l'atteinte d'objectifs annuels, les résultats et la mise en œuvre des compétences métier, des comportements professionnels et éventuellement des compétences managériales.
En fin d'année, l'équipe de direction de DGAR (direction groupe de l'audit et des risques) se réunit durant une journée pour procéder aux appréciations de l'ensemble des auditeurs. Celle-ci se fait donc de manière collégiale. Ensuite, un autre collège, commun à plusieurs directions (celles de la qualité, du personnel et de l'organisation dans notre cas) s'assure de la cohérence de cette évaluation avec les autres fonctions.

A&CI : *Quel est le mode de rémunération des auditeurs ?*

F.V. : Nous sommes bien entendu rattachés au système de rémunération du groupe Michelin. La rémunération globale se compose d'un salaire fixe et une part variable. Il existe une échelle unique pour tous les métiers du groupe. Nous avons défini deux niveaux de responsabilité pour les auditeurs – confirmé et senior – et un troisième pour les managers.
Le système est conçu pour permettre de gérer les personnes dans la durée, avec des passerelles entre les métiers ou avec des passages à l'étranger le cas échéant. Il est basé sur les références du marché national de l'emploi.

A&CI : *Comment gérez-vous la carrière de vos collaborateurs ?*

F. V. : Les auditeurs bénéficient d'une mise en visibilité à l'intérieur du groupe puisqu'ils ont l'opportunité de rencontrer des personnes de tous horizons et jusqu'au plus haut niveau.
Pour le reste, nous suivons le processus classique de gestion de carrière du groupe Michelin.
Les auditeurs restent généralement quatre à cinq ans chez nous. Si, le plus souvent, ils viennent d'un métier vers lequel ils reviendront ensuite, le passage à l'audit peut aussi être pour eux l'opportunité de changer de métier. D'ailleurs, nous profitons souvent de leur présence à l'audit pour leur faire découvrir d'autres métiers et élargir leurs compétences.
Chez Michelin, chacun est réputé avoir un potentiel et nous nous attachons à permettre à chaque personne de réaliser le sien, avec l'appui du manager et du gestionnaire. La gestion des carrières dans le groupe s'appuie en effet sur un triangle dans lequel trois acteurs ont un rôle important à jouer : la personne, son manager et le gestionnaire de carrière. La personne est invitée à exprimer ses souhaits d'évolution et les managers ont pour mission de favoriser le développement de leurs équipiers. Certaines personnes, en particulier les expatriés, savent, lorsqu'elles arrivent chez nous, quel est le prochain poste qu'elles occuperont ensuite.
Nous identifions en outre ceux qui sont le plus rapidement ou le plus fortement évolutifs. Ils font l'objet d'un suivi particulier au niveau des gestionnaires de carrière.
Nous prévoyons les départs environ 12 mois à l'avance. Lors de notre entretien mensuel avec le gestionnaire de carrière, nous discutons des départs et des entrées.
Nous tenons à jour un plan de succession. La carrière d'un auditeur chez Michelin étant en moyenne de quatre années, il faut en permanence accueillir dans et accompagner hors de notre entité un certain nombre de personnes en veillant à conserver la richesse de l'équipe faite de l'addition des diversités de compétences de chacun. Nous avons donc défini un profil d'équipe cible qui nous permet d'avoir les compétences répondant à notre plan d'audit.
Ce que deviendra l'auditeur après son passage chez nous est également important afin que l'audit soit considéré comme une étape positive dans la construction d'une carrière professionnelle. Nous nous sommes fixé l'objectif que le niveau de compétence professionnelle des auditeurs, tel que suivi par la direction du personnel, soit en moyenne supérieur d'un niveau à leur sortie de l'audit qu'à leur entrée.

Au final, ce dont je suis la plus fière, c'est de voir des personnes se développer personnellement et professionnellement à l'audit avant de repartir plus riches de cette expérience vers une nouvelle étape de leur carrière. ●

[1] *Michelin reste attaché au terme de « service du personnel » et à l'idée ainsi transmise d'une activité au service des personnes.*

Constituer et gérer une équipe d'audit et de contrôle internes dans une collectivité territoriale

Yannis Wendling

Directeur de l'audit et du contrôle internes et de la gestion des risques,
Conseil général de Seine-Saint-Denis

Après avoir travaillé au sein du cabinet d'audit Arthur Andersen et au sein de deux cabinets de conseil en management / RH /organisation et de conseil dans la mise en œuvre de stratégies publiques, ***Yannis Wendling*** *a rejoint le conseil général de la Seine-Saint-Denis pour mettre en place la direction de l'audit interne. Depuis, il est en charge de l'audit interne, du contrôle interne et de la gestion des risques (ERM). Il assure également la présidence du groupe professionnel collectivités territoriales au sein de l'IFACI.*

Dans les organisations où les fonctions d'audit et de contrôle internes ne sont pas assujetties à des normes, à l'instar des collectivités territoriales, attirer, recruter au sein d'un service d'audit interne ou de contrôle interne peut être une gageure. Savoir constituer une équipe, valoriser la fonction, accompagner et fidéliser ses collaborateurs, leur ouvrir des perspectives, sont autant de défis permanents à relever.

Comme d'autres professionnels au sein de nos organisations, qu'elles soient publiques ou privées, les auditeurs internes et les contrôleurs internes font très souvent l'objet de représentations. Ils seraient tantôt des experts travaillant seuls, forts de leurs expériences et responsabilités passées, et tantôt de jeunes aux hauts potentiels, disposant de compétences méthodologiques et de capacités d'analyse éprouvées.

Bien entendu, ces deux manières de nous décrire possèdent une part de vérité. Pour autant, il convient de se méfier de cette approche qui pourrait conduire à considérer que ces professionnels n'auraient besoin d'aucune approche managériale ou de ressources humaines particulières. La fonction d'audit interne en particulier aurait vocation à accueillir temporairement des cadres à potentiel qui construiraient leur carrière seuls ou à être l'aboutissement d'un parcours professionnel réussi. Au quotidien, force est de constater que la réalité est plus nuancée et complexe et que la gestion des collaborateurs d'un service d'audit interne comporte bien des écueils à contourner et bien des défis à relever au quotidien.

Dans les organisations où les fonctions d'audit et de contrôle internes ne sont pas assujetties à des normes, à l'instar des collectivités territoriales, attirer, recruter au sein d'un service d'audit interne ou de contrôle interne peut être une gageure. Retenir nos collaborateurs et leur offrir des perspectives tout en les formant sur nos approches spécifiques est aussi une préoccupation de chaque instant. De là à dire que tout responsable d'un service d'audit et de contrôle interne est avant tout un responsable RH serait sans doute excessif mais force est de constater que c'est une dimension essentielle de la fonction et a fortiori dans les collectivités territoriales.

Savoir constituer et préserver son équipe

Il existe certaines entreprises ou administrations, où les fonctions d'inspection générale ou d'audit interne constituent des viviers traditionnels où sont formés les cadres de demain. Dans le secteur public, les membres de certains corps de contrôle sont recrutés directement à la sortie de l'Ecole Nationale d'Administration et sont amenés à exercer les plus hautes responsabilités dans le secteur public voire en dehors. Aujourd'hui, les décrets et les circulaires de 2011 qui imposent à chaque ministère de se doter d'une fonction d'audit interne ont conduit certains de ces corps de contrôle à constituer en leur sein des équipes d'auditeurs internes qui sont de fait de nouveaux débouchés pour ces hauts potentiels.

« Dans une collectivité territoriale, constituer ou conserver son équipe d'auditeurs internes est un véritable défi à relever »

Au sein des villes, départements, régions et de leurs établissements publics, la situation est très différente, la présence de ces inspections générales n'étant ni une obligation ni une situation fréquemment rencontrée. Les cadres supérieurs recherchent avant tout, après leur titularisation au sein de la fonction publique territoriale, des postes de management ou de chargés de mission auprès des directions générales. Ainsi, constituer ou conserver son équipe d'auditeurs internes est un véritable défi à relever.

Il convient à la fois d'attirer des collaborateurs qui disposent d'une appétence pour la fonction mais aussi des collaborateurs solides techniquement qui seront reconnus comme légitimes au sein de la structure. Tout cela, s'effectue alors que le répertoire des métiers de la fonction publique territoriale n'identifie pas à ce jour cette fonction qui est émergente.

Les leviers dont disposent les responsables des directions de l'audit interne sont malgré tout nombreux. L'accueil de stagiaires et d'apprentis est un outil précieux pour repérer de futures recrues. Ainsi au Conseil général de Seine-Saint-Denis, nous accueillons chaque année des stagiaires de l'Université Paris XIII et des apprentis de l'IAE d'Aix-en-Provence afin d'une part de soutenir les filières de formation existantes, de former des personnes susceptibles de postuler dans les collectivités territoriales, mais aussi de détecter d'éventuels futurs candidats à un emploi dans notre collectivité.

Bien entendu, cette démarche est exigeante car elle suppose de disposer du temps pour encadrer ces personnes et des missions adaptées. Par ailleurs, l'accès à l'emploi public obéit à des prescriptions bien précises pour des personnes non titulaires de la fonction publique.

Un autre levier consiste à accueillir aussi des cadres expérimentés disposant d'une légitimité au sein de l'organisation et intéressés par un nouveau parcours professionnel. L'absence d'encadrement hiérarchique et la possibilité de valoriser sa connaissance des métiers de la collectivité sont deux composantes de notre profession qui peuvent attirer des cadres de haut niveau. Ces mêmes cadres seront ensuite des relais précieux pour valoriser la fonction et faciliter des recrutements à venir. L'équipe de contrôle interne du Conseil général est, ainsi, composée de trois agents et d'un auditeur interne ayant ce profil.

Enfin, il appartient à chaque responsable de service de communiquer et de valoriser ces métiers au sein de son organisation et à l'extérieur. Avec d'autres responsables, nous intervenons ainsi auprès du Centre National de la Fonction Publique Territoriale pour faire reconnaître la fonction d'auditeur interne et développer des filières de formation. Le temps passé en dehors concourt à valoriser ce métier et à faciliter le recrutement et doit donc être considéré comme un investissement.

Accompagner et fidéliser ses collaborateurs

Une fois le recrutement effectué, le défi consiste à fidéliser ses collaborateurs, non pas pour un bail indéterminé, mais sur une période suffisante qui permette d'acquérir et de consolider les expériences. Loin d'être simple, cette entreprise se heurte à l'envie des collaborateurs d'évoluer soit vers une collectivité ou une entreprise plus attractive, soit vers une fonction d'encadrement et/ou vers une fonction dite opérationnelle. Malheureusement, bien souvent force est d'admettre que les collaborateurs les plus performants sont ceux qui sont le plus tentés par d'autres responsabilités.

En tant que responsable, il est vain et improductif de retenir ses collaborateurs. Nombreuses sont les inspections générales qui proposent des parcours à ses membres et qui confortent ainsi leur attractivité au sein de l'Etat. Pour autant, afin de capitaliser les expériences et de maîtriser la rotation des équipes, différentes actions peuvent être menées.

La visibilité et la lisibilité du parcours d'apprentissage sur le poste est primordiale. Pour ce faire, la construction de parcours de formation est essentielle. Elle permet d'apporter des compétences à des personnes en conciliant à la fois leurs projets et aspirations personnels (évolution vers des postes comptables et

financiers, vers des fonctions logistiques …), en développant l'esprit de curiosité, mais aussi en répondant aux besoins de la direction dont le plan d'audit annuel nécessite l'acquisition de savoirs spécifiques. L'offre de formation de l'IFACI est ainsi très précieuse car elle propose des formations destinées à la fois à des débutants, à des auditeurs aguerris, et des formations spécifiques ainsi que des itinéraires.

L'organisation d'échanges de pratiques de retours d'expérience, ou de transmissions de compétences en interne suite aux colloques et formations suivis permet aussi de valoriser les compétences de chacun. Ce faisant, on travaille aussi sur le collectif et les liens entre les auditeurs.

Au-delà de la conduite des audits ou de la réalisation de missions de contrôle interne, il faut veiller à ce que le service dispose de son propre projet auquel chacun contribue. Dans le cas contraire, les collaborateurs sont renvoyés à leurs propres projets ou missions ce qui ne contribue pas à leur fidélisation. Outre les aspects traditionnels de gestion du personnel, la dimension managériale est une vertu cardinale du responsable d'audit interne.
La cohabitation d'auditeurs d'âges et de parcours différents peut également être un atout dans la mesure où elle permet de faire du service un lieu d'échanges et d'ouverture, sans se limiter aux audits et contrôles menés, propice au développement de projets professionnels.

Enfin, les démarches de certification du service ou des auditeurs (CIA, DPAI), peuvent être encouragées pour d'une part valoriser les individus et d'autre part reconnaître la performance collective.
S'agissant du contrôle interne, les approches sont les mêmes. Au Conseil général de la Seine-Saint-Denis, les trois directrices déléguées en charge de ce projet sont toutes des anciens cadres expérimentés qui à travers leur nouvelle fonction peuvent accompagner les autres cadres et ainsi valoriser leur expérience. Pour elles, le contrôle interne est une opportunité pour valoriser leur ancienneté dans la structure.

Donner des perspectives

Malgré toutes ces démarches, la question des perspectives professionnelles des auditeurs se pose. L'audit interne voire le contrôle interne est un métier de passage, de transition, de tremplin. Pour respecter le principe d'indépendance et conserver le regard critique, il est souhaitable que les personnes ne fassent pas carrière au sein du service. L'employeur mais aussi le responsable de l'audit doit créer les passerelles et les conditions qui faciliteront cette transition. S'il n'est pas possible de contractualiser cela, il est utile de faire figurer dans les projets du service les actions engagées en ce sens.
Durant le séjour de la personne à l'audit interne, les audits confiés ou le rôle assuré sur les missions d'audit (travaux de vérification, encadrement d'auditeurs juniors ou de stagiaires …) sont à adapter en fonction du stade de développement professionnel des personnes et de leurs projets.
Certains auditeurs peuvent aussi prendre en charge des activités de formation ou l'animation de démarches d'échanges de pratiques au sein du service. Au sein de la direction de l'audit interne, l'ensemble des auditeurs ont également un rôle de représentation de la direction au sein d'instances internes au Conseil général sur certains projets mais aussi pour une auditrice un rôle d'initiation à l'audit interne des cadres de la collectivité dans le cadre du cycle d'appui aux managers portés par le service de la formation.
La participation à des groupes de travail au sein de l'IFACI ou d'associations participe également au développement personnel des auditeurs. Cela leur permet d'enrichir leurs parcours et leur procure une visibilité.

Le risque serait de ne pas réunir les conditions qui permettront aux auditeurs de pouvoir valoriser leur métier comme un atout pour leur projet personnel.
Le responsable d'audit interne doit ainsi après avoir recruté ses proches collaborateurs, les avoir accompagnés et leur avoir permis de développer leurs compétences créer les conditions de leurs futurs projets. En ce sens, il lui appartient de valoriser et de promouvoir ses collaborateurs sans pour autant se substituer à la direction des ressources humaines qui a en charge les programmes de gestion de la mobilité. Dans une collectivité territoriale où la fonction est nouvelle et où les passerelles sont à construire, de nombreuses étapes sont encore à franchir pour y parvenir.

Au final, il apparaît bien que le responsable d'audit interne ne peut s'abstenir de bâtir son projet RH. Ceci ne peut intervenir au sein des collectivités territoriales qu'en s'appuyant sur les démarches collectives pour faire reconnaître ce métier en émergence. L'appui de l'IFACI et la constitution du groupe professionnel collectivités territoriales en son sein avec le concours de la conférence des inspecteurs et auditeurs territoriaux sont, en ce sens, essentiels. ●

Audit d'un processus informatisé

Dominique van Egroo

Consultant

La quasi-totalité des processus des organisations est aujourd'hui supportée par une ou plusieurs applications informatiques. Peu d'organisations pourraient par ailleurs pouvoir se passer de l'outil informatique. C'est pourquoi l'audit d'un processus informatisé devrait être maîtrisé par tout auditeur quels que soient la taille ou le secteur d'activité de l'organisation à auquel il appartient.

*Disposant d'une double formation en informatique et droit, **Dominique van Egroo** a exercé au sein de grandes entreprises et cabinets d'audit et conseil internationaux. Il a également été directeur des systèmes d'information et avocat. Il est expert en informatique près la cour d'appel de Paris.*

Le terme « processus informatisé » peut rebuter voire faire craindre à bon nombre d'auditeurs que l'audit d'un processus informatisé est un audit technique nécessitant une bonne maîtrise des systèmes d'information. Certes, l'audit d'un processus informatisé nécessite quelques connaissances de base en matière de systèmes d'information. En revanche, l'audit d'un processus informatisé est à la portée de tout auditeur et impose davantage une bonne compréhension, sous un angle fonctionnel, du processus audité.

Qu'est-ce qu'un processus informatisé ?

La plupart, sinon la totalité des organisations utilisent aujourd'hui l'outil informatique. Cet outil informatique est devenu au fil des années un outil incontournable pour les organisations. Celles qui ont pris conscience de sa nécessité et de son importance peuvent en tirer un avantage concurrentiel indéniable.

Lorsque l'on regarde les processus de son organisation, il est rare de trouver un processus qui n'utilise pas, à un moment donné, une application informatique. Ainsi, tout processus, qui utilise à un instant donné une application informatique, pourrait être qualifié de processus informatisé.

Il est donc rare pour un auditeur d'auditer un processus qui ne soit pas un processus informatisé

Obtenir la cartographie applicative

Lorsque l'on se penche sur un processus, on constate bien souvent, au-delà d'une simple application informatique, l'existence d'une multitude d'applications qui communiquent les unes avec les autres. Pour faciliter cette compréhension, on ne peut que recommander à l'auditeur qui ne la possède pas encore, de récupérer la cartographie applicative auprès de la direction informatique.

Ce schéma, qu'il soit sous format informatisé ou non, permet à l'auditeur d'avoir une vision globale des applications du système d'information et des liens entre les applications. Grâce à elle, l'auditeur pourra ainsi avoir une compréhension synthétique des principales applications supportant le processus audité. Selon les organisations, elle permettra également à l'auditeur d'identifier bon nombre d'interlocuteurs à rencontrer.
Les cartographies applicatives peuvent également mentionner les interfaces. Celles-ci permettent aux applications informatiques de communiquer entre elles et d'échanger des données. Elles sont donc, par là même, source de risques car des données peuvent être perdues ou altérées au sein des interfaces.

Une étape préalable indispensable

Une bonne compréhension du processus audité est indispensable. Pour ce faire, il est recommandé de formaliser le processus audité sous forme de diagramme de flux, encore appelé *flowchart* ou logigramme.
Pour bien réaliser un *flowchart*, il est indispensable de bien identifier l'ensemble des acteurs participants au processus. Le processus sera formalisé à l'aide des différents symboles définis par la norme ISO 5807 selon les étapes suivantes :

- le nom des différents acteurs sera indiqué horizontalement sur un schéma ;
- un trait vertical sera alors tiré entre le nom de chaque acteur ;
- enfin, dans la colonne associée à chaque acteur, seront formalisées les différentes actions réalisées par celui-ci.

Le schéma ci-contre représente les principaux symboles utilisés. Sur le diagramme de flux, il sera indiqué dans chaque symbole à quoi il correspond. Ainsi, s'il s'agit par exemple d'un document, il sera précisé quel type de document : facture, dossier, etc.

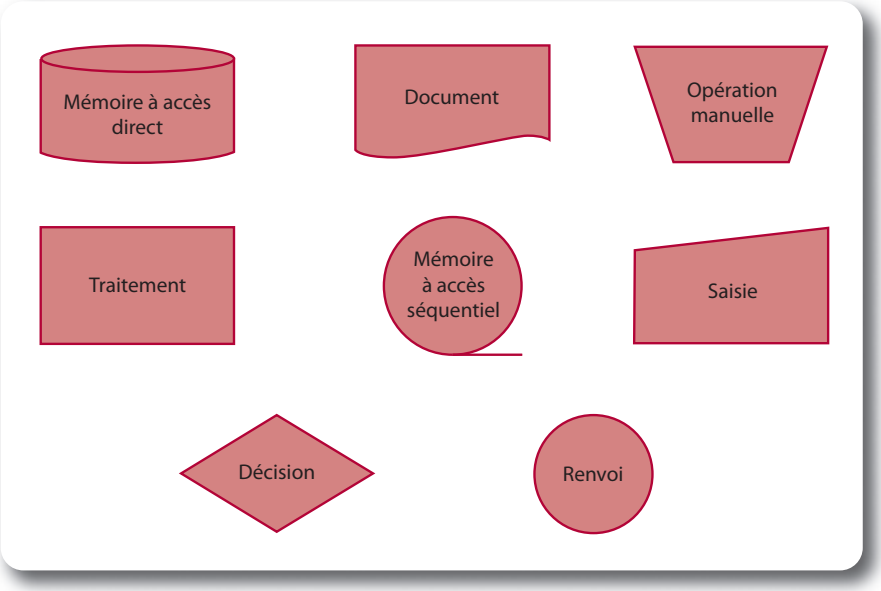
Les différents symboles seront reliés par des traits, de préférence verticaux ou horizontaux pour indiquer l'enchaînement des actions et opérations.
Précisons l'utilité de certains des principaux symboles de la norme :

- La mémoire à accès direct correspond typiquement à un disque dur ou une clé USB c'est-à-dire à une mémoire dans laquelle on accède directement aux informations.
- La mémoire à accès séquentiel correspond typiquement à des cassettes c'est-à-dire à une mémoire dont l'accès aux informations est séquentiel.
- Le losange correspond à une opération de décision. Une décision est généralement la suite d'une opération, d'un traitement ou d'une saisie. Le résultat de la décision sera dans bon nombre de cas « oui » ou « non ».
- Le symbole renvoi correspond à une zone ou le *flowchart* s'arrête pour reprendre à un autre endroit (cas d'un bas de page par exemple).

Les principaux risques couverts

Lors de l'audit d'un processus informatisé les principaux risques à couvrir sont :

- la prise en compte d'informations non autorisées pouvant conduire par exemple à des fraudes ou à la réalisation d'opérations non autorisées ;
- la prise en compte non exhaustive des informations pouvant par exemple conduire à des pertes financières, des erreurs, des pertes de temps ;
- la prise en compte d'informations inexactes pouvant par exemple conduire également à des erreurs ou pertes de temps ;
- la mise à jour incomplète ou inexacte des données pouvant conduire par exemple à des erreurs de calcul ;
- l'altération de l'intégrité, de l'exhaustivité et de l'exactitude des données stockées pouvant conduire également par exemple à des fraudes, erreurs ou pertes financières ;
- l'accès non autorisé aux données pouvant conduire notamment à la divulgation, l'altération ou la destruction des données.



Que doit-on évaluer ?

Chaque processus informatisé est différent. Cependant, pour couvrir les risques précédemment énoncés et audités, l'auditeur devra évaluer l'existence et l'efficacité des contrôles au niveau des :

- pièces justificatives,
- saisies dans les applications,
- traitements, y compris les traitements *batch*,
- sorties des applications,
- interfaces.

Ces contrôles sont communément appelés des « contrôles applicatifs » car intégrés aux applications des processus métiers. Ils sont spécifiques à chaque application. Ils concernent l'exhaustivité, l'exactitude, la validité, l'autorisation des données ainsi que la séparation des tâches.

Une bonne connaissance et compréhension du processus audité ainsi que de ses objectifs sont donc nécessaires. Précisons que la responsabilité des contrôles applicatifs relève des propriétaires des processus métiers. C'est donc à ces derniers de définir les exigences de contrôle à inclure dans tous les processus métiers.

Des dysfonctionnements ou faiblesses dans les contrôles des applications peuvent engendrer les risques précédemment énoncés et avoir des impacts importants sur la capacité des métiers à traiter les transactions au travers des différentes applications.

Parmi les différents types de contrôles existants, on peut par exemple citer :

- les contrôles d'autorisation, de validité,
- les contrôles de format, d'existence,
- les contrôles de valeur limite,
- les contrôles d'intégrité, les totaux de contrôle,
- les contrôles d'accès.

De nombreux autres types de contrôles peuvent également exister. Même si certains contrôles applicatifs peuvent paraître très simples, ils n'en sont pas moins très importants. Ainsi, l'absence de contrôles de format et longueur sur une entrée (la saisie d'une adresse email pour l'inscription à une *newsletter* sur un site internet par exemple) pourrait permettre, dans certains cas, à une personne mal intentionnée de voler ou altérer la base de données de l'application, voire de récupérer les identifiants et mots de passe des utilisateurs. L'inexistence ou l'inefficacité d'un contrôle simple peut donc engendrer, dans certaines situations, un risque significatif.
Lors de l'audit d'un processus informatisé, une attention particulière doit également être portée sur l'identification, l'enregistrement et le traitement des erreurs. En effet, si les erreurs ne sont pas identifiées et traitées, cela peut notamment avoir pour conséquence des pertes de données ou de disposer de données non fiables et de mauvaise qualité.

Et ensuite ?

En matière de systèmes d'information, on distingue deux catégories de contrôles : les contrôles applicatifs vus précédemment et les contrôles généraux informatiques. Les contrôles généraux informatiques portent sur l'environnement des applications. Ils concernent ainsi par exemple : les développements, la sécurité logique, la sécurité physique, les sauvegardes, la gestion des incidents, la gestion de l'exploitation.

Lors de l'audit d'un processus informatisé, l'auditeur évalue l'existence et l'efficacité des contrôles applicatifs. Cependant, on ne peut que recommander de procéder également à l'évaluation des contrôles généraux informatiques. Ceci, de manière à pouvoir apprécier plus globalement les risques auxquels l'organisation est exposée et plus particulièrement les risques portant sur l'environnement des applications.

A minima, il est recommandé de procéder à une évaluation de la sécurité logique d'accès aux bases de données des applications supportant le processus informatisé audité. En effet, un niveau insuffisant de sécurité logique d'accès aux bases de données des applications pourrait remettre en cause un niveau satisfaisant de sécurité logique d'accès à l'application ainsi qu'une séparation des tâches satisfaisante. ●

ifaci
institut français de l'audit et du contrôle internes

Calendrier 2013

- 20% pour un participant inscrit simultanément à 4 formations

SESSIONS	Durée	Tarifs adhérents	Tarifs non adhérents	janv.	févr.	mars	avril	mai	juin	juil.	sept.	oct.	nov.	déc.
SE FORMER AU CONTRÔLE INTERNE														
S'initier à la maîtrise des activités et au contrôle interne	2 j	950 €	1 125 €	10-11	11-12	14-15	8-9	13-14	10-11	3-4	9-10	3-4	14-15	2-3
Réaliser une cartographie des risques	3 j	1 675 €	1 875 €	14-16	13-15	18-20	10-12	15-17	12-14		11-13	7-9		4-6
Elaborer un référentiel de contrôle interne	2 j	1 200 €	1 350 €	21-22	19-20	21-22		21-22	17-18	8-9	16-17	10-11	18-19	
Piloter un dispositif de maîtrise des activités et de contrôle interne	2 j	1 200 €	1 350 €	23-24	21-22	25-26		23-24	20-21		19-20		20-21	10-11
Le contrôle interne des systèmes d'information	2 j	1 200 €	1 350 €	29-30		27-28			24-25			14-15		
Maîtrise des activités, contrôle interne et communication Nouveau	2 j	1 200 €	1 350 €		25-26			27-28			23-24			12-13
SE FORMER À L'AUDIT INTERNE														
Les fondamentaux de l'audit interne														
S'initier à l'audit interne	2 j	950 €	1 125 €	10-11	5-6	14-15	4-5	16-17	6-7	1-2	5-6	3-4	7-8	2-3
Conduire une mission d'audit interne : la méthodologie	4 j	1 950 €	2 150 €	14-17	11-14	18-21	8-11	21-24	10-13	1-4	9-12	7-10	12-15	9-12
Maîtriser les outils et les techniques de l'audit	3 j	1 625 €	1 775 €	21-23	18-20	25-27	15-17	27-29	17-19	8-10	16-18	14-16	18-20	16-18
Maîtriser les situations de communication orale de l'auditeur	2 j	1 050 €	1 150 €	24-25	21-22	28-29	18-19	30-31	20-21	11-12	19-20	17-18	21-22	19-20
Réussir les écrits de la mission d'audit	2 j	1 050 €	1 150 €	28-29	25-26	25-26	22-23	30-31	24-25	11-12	23-24	21-22	25-26	19-20
Exploiter les états financiers pour préparer une mission d'audit	3 j	1 525 €	1 675 €	30-01/02		20-22		15-17			25-27			4-6
Désacraliser les systèmes d'information	3 j	1 525 €	1 675 €			27-29			3-5		25-27			16-18
Détecter et prévenir les fraudes	2 j	1 050 €	1 150 €		27-28		24-25		26-27		23-24	23-24		2-3
Le management														
Piloter un service d'audit interne	2 j	1 300 €	1 450 €	16-17				23-24				15-16		
Manager une équipe d'auditeurs au cours d'une mission	1 j	685 €	770 €			25				4			29	
L'audit interne dans les petites structures	1 j	685 €	770 €			18			28			1		
Balanced Scorecard du service d'audit interne	1 j	685 €	770 €		22				19				15	
Le suivi des recommandations	1 j	685 €	770 €	18			11		14		30		18	
Préparer l'évaluation externe du service d'audit interne	2 j	1 300 €	1 450 €		20-21			13-14					25-26	
L'audit interne, acteur de la gouvernance	1 j	685 €	770 €				12					14		
Audit interne, contrôle interne et qualité : les synergies	1 j	685 €	770 €		19			17				7		
Les audits spécifiques														
Audit du Plan de Continuité d'Activités - PCA	2 j	1 300 €	1 450 €			26-27			25-26				19-20	
Audit de la fonction Comptable	2 j	1 300 €	1 450 €				15-16					17-18		
Audit de performance de la gestion des Ressources Humaines	3 j	1 525 €	1 675 €				23-25						27-29	
Audit de la fonction Achats	2 j	1 300 €	1 450 €		12-13				13-14			23-24		
Audit des Contrats	1 j	685 €	770 €			1				3			14	
Audit de la fonction Contrôle de Gestion	2 j	1 300 €	1 450 €			28-29							25-26	
Audit de la Sécurité des Systèmes d'Information	2 j	1 300 €	1 450 €			20-21					26-27			
Audit des Processus Informatisés	2 j	1 300 €	1 450 €				17-18							11-12
Audit de la Conformité à la Législation Sociale	2 j	1 300 €	1 450 €		25-26							21-22		
Audit du Développement Durable	2 j	1 300 €	1 450 €					29-30				3-4		
Audit des Projets et Investissements Nouveau	2 j	1 300 €	1 450 €				9-10						27-28	
SE FORMER DANS LE SECTEUR PUBLIC														
Le contrôle interne dans le secteur public	2 j	1 300 €	1 450 €		14-15			15-16			9-10		14-15	
Pratiquer l'audit interne dans le secteur public	4 j	1 950 €	2 150 €			26-29			17-20			8-11		10-13
SE FORMER DANS LE SECTEUR BANCAIRE ET FINANCIER														
Le contrôle permanent et la conformité dans le secteur bancaire et financier	3 j	1 525 €	1 675 €						5-7		18-20			11-13
Pratiquer l'audit interne dans une banque ou un établissement financier	4 j	1 950 €	2 150 €						10-13		23-26			16-19
SE FORMER DANS LE SECTEUR DES ASSURANCES														
Le contrôle interne dans le secteur des assurances	2 j	1 300 €	1 450 €		7-8			21-22			5-6		21-22	
Pratiquer l'audit interne dans le secteur des assurances	4 j	1 950 €	2 150 €			19-22			24-27			15-18		3-6
SE FORMER DANS LES SECTEURS INDUSTRIE ET COMMERCE														
Audit de la gestion des stocks et de la logistique Nouveau	2 j	1 300 €	1 450 €	30-31						1-2				
Audit du processus de ventes Nouveau	2 j	1 300 €	1 450 €				3-4					24-25		
ACQUÉRIR UNE CERTIFICATION	*Voir notre site internet : www.ifaci.com*													

VOUS AVEZ LE SAVOIR, NOUS AVONS LES OUTILS

Depuis 1987, **IDEA** est l'outil d'extraction et d'analyse de données par excellence utilisé par de nombreux professionnels de l'audit, de la comptabilité et de la finance à travers le monde.

IDEA vous permet d'améliorer le rendement et l'efficacité de vos contrôles, de détecter des indices de fraudes et d'être un meilleur auditeur sans connaissances techniques poussées.

IDEA possède plusieurs fonctionnalités et caractéristiques introuvables dans les autres logiciels d'audit.
Découvrez-les en commandant votre version de démonstration sur
www.caseware-idea.fr

IDEA
Logiciel d'analyse de données

CASEWARE
IDEA

Audit & Contrôle internes

De l'usage du GTAG 1 chez Sodexo : forces et faiblesses

Entretien avec ...

Alain Rogulski - Directeur de l'audit des systèmes d'information, **Sodexo**

Revue « Audit & Contrôle internes » : *Comment l'audit interne IT se situe-t-il dans l'organigramme de Sodexo ? Comment est-il organisé ? Quelles sont les relations avec les auditeurs internes généralistes ?*

Alain Rogulski : L'audit interne groupe, chez Sodexo, est une équipe *corporate* centrale, de 28 auditeurs répartis sur 3 lieux géographiques : Paris, Londres et Washington. Dans cette organisation géographique, il y a un certain nombre de centres de compétences sur des sujets spécifiques liés soit à des connaissances techniques, soit à des connaissances métiers. L'audit des systèmes d'information est un pôle de compétences, composé d'une équipe de 5 auditeurs, totalement intégrée dans le département d'audit interne, et répartis géographiquement sur les sites de Paris, Londres et Washington.

Cette équipe, dont j'ai la responsabilité, rapporte directement au directeur de l'audit interne groupe, sans aucun lien hiérarchique ou fonctionnel avec la DSI. Le DAI est lui-même rattaché directement au président du Conseil d'administration avec un *reporting* vers le Comité d'audit.

Les missions réalisées par l'équipe audit des systèmes d'information se répartissent globalement de la façon suivante : 1/3 d'entre elles sont spécifiquement informatiques, avec une implication exclusive des auditeurs systèmes d'information ; 2/3 représentent des missions dans lesquelles nous sommes intégrés à une équipe pluri-disciplinaire, et qui comportent une composante informatique forte.

Typiquement, la revue d'une filière à l'étranger comporte quasi systématiquement un volet informatique qui sera, selon la complexité de l'entité, couvert soit par un auditeur généraliste, quand on se situe dans un contexte assez simple, soit par un auditeur système d'information confirmé, si l'environnement est plus complexe ou si les enjeux le nécessitent.
Par exemple, une activité majeure de Sodexo dans le

*Après 7 ans en cabinets d'audit, chez Ernst & Young et PricewaterhouseCoopers, à Paris et à New York, **Alain Rogulski** rentre chez Alcatel-Lucent en 2001 en tant que manager puis directeur de l'audit des systèmes d'information. En 2011, il rejoint le groupe Sodexo pour diriger l'équipe d'audit des systèmes d'information, couvrant toutes les activités et les pays du groupe.*

monde, qui s'appelle « services avantages et récompenses », concerne la mise en place, la production et la gestion de systèmes de cartes et chèques de services (chèques restaurant, CESU en France). Cette activité de production et de gestion de moyens de paiement est totalement dépendante de ses systèmes d'information, comme une production bancaire, et notre équipe de « spécialistes informatiques » intervient donc beaucoup lors des missions portant sur cette activité.

A&CI : *Quelles sont, selon vous, les principales modifications apportées – ajouts, suppressions – dans la deuxième édition du GTAG 1 ? L'ajout essentiel n'est-il pas la typologie des contrôles proposés, mais est-il vraiment utile sur le terrain ?*

A. R. : Le changement de titre illustre bien le changement majeur entre les deux éditions. De « Contrôles des systèmes d'information », on est passé à « Contrôle et risques des systèmes d'information ». Effectivement, cette deuxième édition recentre le propos sur les risques informatiques ou induits par l'informatique, ce qui permet ensuite de mieux appréhender les différentes notions de contrôles expliquées et développées par la suite dans le guide.

Une autre modification majeure concerne la dizaine d'annexes qui figuraient dans l'édition 1, et qui se voulaient un catalogue de méthodologies et de référentiels, des points d'entrée vers des cadres de contrôle comme CobiT ou COSO. Elles ont disparu ou ont été mieux intégrées au sein même du document.

La typologie des contrôles, décrite dans la première édition, a été remaniée pour être beaucoup plus claire, notamment quant à la distinction entre les contrôles généraux et les contrôles applicatifs. Une meilleure explication de la typologie est importante, peut-être moins sur le terrain, mais plus lors de la préparation et la planification des audits, pour être mieux à même de définir le périmètre d'intervention des auditeurs internes.

Lorsqu'une mission d'audit va porter sur un processus fortement supporté par des applications, il sera nécessaire de revoir les contrôles applicatifs. Dans ce cas-là, une double compétence est indispensable : la connaissance ou compréhension du processus (processus achat, financier, opérationnel) doit être couplée à celle de l'application et de sa technologie (par exemple SAP ou Microsoft Dynamics). Par contre, si le périmètre de l'audit se limite à ce qui est communément appelé contrôles généraux informatiques, on est beaucoup plus sur des processus informatiques et peu sur les processus métiers. Seule la compétence d'audit informatique peut alors s'avérer nécessaire.

Au final, le GTAG est maintenant plus didactique et permet à un non expert en systèmes d'information de mieux comprendre les enjeux pour l'audit interne, donc les risques et les contrôles.

A&CI : *Concernant les compétences, qu'en est-il de la nécessaire complémentarité entre les auditeurs généralistes et les auditeurs experts ?*

A. R. : Ce point est malheureusement très peu abordé dans le GTAG, comme il l'est d'ailleurs dans les autres GTAG. Une page fait référence à l'*Integrated Competency Framework* de l'IIA, mais ne répond pas vraiment à la question des compétences et, à travers quelques exemples, initie tout juste le propos.

Si l'on veut vraiment parler des compétences nécessaires en audit informatique, il faut d'abord se poser les questions de base : Que demande-t-on à l'audit interne ? Comment veut-il lui-même se positionner ou comment un Comité d'audit ou un Comité exécutif veut-il positionner l'audit interne sur la partie systèmes d'information ?

Une petite équipe comme la nôtre ne peut pas posséder toutes les expertises informatiques. A l'audit interne de Sodexo, nous avons décidé d'être pertinents sur un certain nombre de sujets, et donc de nous doter, en interne, de compétences spécifiques dans les domaines clés suivants : la gouvernance des systèmes d'information, la gestion de projets informatiques, la technologie SAP, et la sécurité des systèmes d'information. Nous voulons impérativement couvrir à un niveau assez fin ces quatre domaines, avec une vraie valeur, et être en mesure de challenger ce que nous voyons sur le terrain, qui nous est expliqué par les DSI et les directions métiers, ainsi que les plans d'action définis par le management suite aux audits.

Nous avons fait ce choix, mais les compétences que l'on veut mettre sur la partie système d'information dépendront du niveau de valeur que l'on veut ajouter, que l'on veut donner au management, dans l'organisation.

A&CI : *Le GTAG 1 a l'ambition de donner des clés pour une communication des enjeux SI aux organes dirigeants. A votre avis, quelle est l'appétence des organes de gouvernance, en particulier du Comité d'audit, par rapport à des sujets très techniques ? Quelles bonnes pratiques, sur le contenu et le rythme de reporting ? Comment les mobiliser sur leurs responsabilités, notamment sur la question de l'appétence pour les risques ?*

A. R. : C'est une question complexe. Les bonnes pratiques vont dépendre de l'activité de l'entreprise, et donc de l'importance qu'auront les systèmes d'information.
Aujourd'hui, dans presque toutes les entreprises, la composante systèmes d'information est forte, et le degré d'implication devrait donc dépendre du niveau des risques liés aux systèmes d'information.

L'appétence sur ces sujets est en général fonction de la culture de l'entreprise et de ses organes, des différentes personnalités qui composent un Comité d'audit, de leur parcours et de leur sensibilisation à ce sujet. C'est le rôle de l'audit interne – s'il n'y en a pas ou pas assez – de créer cette sensibilisation. Indépendant de la DSI, il doit donc être là pour pointer du doigt les risques et être capable de les expliquer à un Comité d'audit qui n'a pas forcément une vision technique des choses.

Ces sujets ne doivent donc pas être abordés sous un angle technique. Il faut faire le lien entre le risque technique qui a été identifié, et l'impact, les conséquences qu'il peut avoir sur l'activité. Les faiblesses trouvées dans les systèmes d'information (ou les processus de gestion de ces systèmes) doivent être traduites en risques de continuité, d'efficacité du service qui est proposé par l'entreprise, de son activité

© Sodexo

même, en termes de fraude potentielle, de retard de déploiement de solutions qui vont impacter la mise en place d'un service sur un marché. Il ne faut surtout pas parler des risques purement informatiques, mais des risques *business* sous-jacents.

Pour prendre un exemple, nous avons mené un audit sur la gestion des données personnelles. Ici, le danger serait d'aborder le sujet sous un angle informatique ou juridique. Il faut tout de suite parler du risque *business* : si on ne gère pas correctement des données personnelles, il y a un risque de ne pas pouvoir répondre à certains appels d'offres, puisque les clients, de plus en plus, nous demandent de nous engager sur un certain niveau de protection de données. Le risque d'image ou le risque concurrentiel sont les risques *business* que nous devons mettre en avant devant un Comité d'audit. Il faut donc rester simple dans le vocabulaire et aborder directement l'impact métier.

Les Comités exécutifs sont généralement sensibles aux risques stratégiques. Les questions qu'ils se posent, sur la partie informatique, sont beaucoup plus liées à la conduite du changement : Comment stan-

dardiser des processus à travers la mise en place de nouvelles solutions informatiques ? Quels sont les risques de résistance, de retard de déploiement et l'impact sur les ROI ? Ils s'intéressent à la gouvernance et aux projets informatiques.

Le Comité d'audit, chez nous, est très intéressé par les problématiques de sécurité informatique, de fraude, de piratage, de continuité de service, leurs incidences sur nos activités. Dans le cadre de la 8ème Directive Européenne, il avait demandé, il y a quelques années, à la DSI de lui expliquer les différents risques liés aux systèmes d'information, et les mesures en place. L'an dernier, il a demandé lors d'une présentation spécifique, la vision de l'audit interne, du contrôle interne et de la DSI sur les risques informatiques principaux dans le groupe.

Le rythme ou la fréquence de ce *reporting*, encore une fois, est directement lié au métier. Mais on peut, je pense, considérer que dans le cadre de la présentation du plan d'audit annuel et du bilan du plan précédent, le risque informatique devrait être inclus, comme les autres. Il est évident que dans des métiers spécifiques – je pense aux établissements financiers – la fréquence est nécessairement plus grande.

A&CI : *A propos des projets informatiques, lorsqu'il est développé ou mis en place un nouveau système, êtes-vous consulté au titre de conseil ?*

A. R. : Cela dépend. Depuis deux ans que je suis chez Sodexo, à plusieurs reprises, des chefs de projets – notamment au siège – nous ont interrogés sur les *best practices* de gestion du risque dans les projets, et demandé conseil sur les méthodologies à appliquer. En général, nous organisons alors une réunion avec eux et exposons les principes, les méthodologies qui peuvent être appliquées, et je leur fournis un exemplaire du GTAG 12, excellent.

Quoi qu'il en soit, s'il s'agit d'un projet clé, son audit sera inclus dans le plan annuel et fera l'objet d'une mission spécifique, en pré-implémentation, post-implémentation, voire les deux. C'est arrivé très récemment sur une application opérationnelle majeure. La DSI nous a demandé d'auditer le processus de fourniture de la solution, et nous auditerons le déploiement et sa gouvernance prochainement.

A&CI : *Les auditeurs internes sont de plus en plus rompus aux techniques d'évaluation des risques. Quelles sont les spécificités, en ce qui concerne l'évaluation des risques SI ? Comment estimer les fréquences d'occurrence ? Quid de l'impact ? Comment gérer des échelles d'impact aussi éclatées ?*

A. R. : Chiffrer un impact est un des gros problèmes de l'audit informatique. On est capable de le faire sur certaines composantes comme la disponibilité du système d'information, en valorisant l'impact d'une perte de continuité d'activité pendant x jours, ou l'impact du retard d'un projet sur son ROI. Mais il en est de toute façon impossible de chiffrer la fréquence d'occurrence. Donc, plutôt que d'essayer de calculer des montants et des fréquences qui de toute façon seront facilement questionnables, je suis davantage adepte de l'utilisation systématique d'échelle qualitative (de 1 à 4 par exemple). Elle est bien sûr subjective et sujette à discussion avec les audités, mais elle est *in fine* une opinion d'audit et a l'avantage de fixer les priorités. Par exemple, même s'il est impossible de calculer un impact ou une fréquence d'un risque sur l'image de l'entreprise lié au piratage du site web institutionnel, on doit fournir au management les éléments qui l'aideront à appréhender le risque. On se bat souvent avec les audités sur la notion de risque, d'impact et de fréquence. Souvent, dans nos rapports d'audit, le risque que nous percevons, est différent du risque perçu par les audités. Néanmoins, l'exercice doit être fait : essayons de le mener de la façon la plus raisonnable et pragmatique possible.

« Le GTAG est maintenant plus didactique et permet à un non expert en systèmes d'information de mieux comprendre les enjeux pour l'audit interne, donc les risques et les contrôles »

Le GTAG reste très général sur le sujet, ce qui me convient bien parce que je n'ai pas connaissance de pratique efficace dans ce domaine. Les théories existantes, très élaborées, s'appliquent mal au risque informatique, malheureusement.

A&CI : *La question de la gouvernance des SI est le point central du guide. Comment l'audit interne peut-il concrètement aborder un si vaste sujet ?*

A. R. : La gouvernance du système d'information était un point très peu abordé dans la première édition. Ici, elle est vraiment replacée dans le cœur du document, comme vous l'avez dit.

D'expérience, la gouvernance du système d'information est souvent la cause principale des dysfonctionnements informatiques que l'on peut constater. En matière de sécurité par exemple, les faiblesses techniques que nous sommes amenées à relever proviennent généralement d'un manque de moyens affectés, parce que la gouvernance n'a pas correctement évalué les risques et a donné d'autres priorités en acceptant le risque à un niveau insuffisant de management. Il en est de même pour les déploiements de solutions, la gestion des priorités de projets, etc.

La nouvelle édition du GTAG permet de mieux comprendre les enjeux de cette gouvernance des systèmes d'information par les différents acteurs.

L'audit interne doit couvrir ce sujet, et nous essayons systématiquement dans nos audits de toucher du doigt la problématique de la gouvernance. Mais elle est complexe, car notre rôle d'auditeurs n'est pas de juger de la stratégie du *business*, mais d'essayer de voir si les mécanismes en place au sein de l'organisation permettent de s'assurer que les DSI travaillent effectivement dans la direction que lui donne le *business*, tout en prenant en compte ses propres contraintes.

Ensuite, selon la taille et la complexité des organisations, il est possible soit de découper le sujet et de « l'embarquer » dans les audits informatiques réalisés (audit de fonction informatique de filiale, de projet, de sécurité), soit de le traiter globalement sur les filiales et les projets significatifs. Dans les deux cas, l'audit interne peut s'appuyer sur le guide de la gouvernance des systèmes d'information. Ce guide, rédigé conjointement par l'IFACI, le CIGREF et l'AFAI, en 2011, explique de façon très concrète les risques, les bonnes pratiques et les critères d'évaluation de chacune des composantes de la gouvernance. En approfondissant les notions introduites dans le GTAG 1, il permet d'établir son plan de travail sur un très bon référentiel, qu'il reste à adapter à la taille, aux pratiques et aux risques de son organisation.

A&CI : *Le GTAG 1 est un guide introductif ; quels autres guides de la collection recommanderiez-vous ?*

A. R. : Le point d'entrée est le GTAG 1, qui liste l'ensemble des concepts : risque, contrôle, organisation d'un système d'information.

Ensuite, il y a 2 catégories de GTAG : les GTAG généraux qui aident à mettre en place un audit informatique. Le GTAG 4 est le *Management of IT Auditing*. Le GTAG 11 sur *Developing the IT Audit Plan* : il aide à structurer l'activité d'audit.

Enfin, les GTAG thématiques approfondissent les sujets particuliers qui peuvent soit être intégrés dans des missions globales, soit faire l'objet d'audits eux-mêmes. Je citerai particulièrement le GTAG 9, sur *Identity and Access Management*, très utile, ainsi que le 15, sur *Information Security Governance*, pour des audits axés sur la sécurité. Il y en a deux autres, que j'utilise régulièrement : le 12, *Auditing IT Projects*, qui donne un bon cadre très exhaustif, et le GTAG 7, *IT Outsourcing*, qui permet de comprendre les risques particuliers liés à l'externalisation des services informatique.

Ces GTAG, très instructifs, permettent d'aborder rapidement et concrètement des sujets parfois complexes, mais ne sont pas toujours abordables par des auditeurs non familiarisés avec l'informatique. ●