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

Audit & Contrôle internes

LES FONDAMENTAUX DE L'AUDIT INTERNE

De la réflexion à la mise en place d'un plan d'audit

Dans l'actualité

Danone, Glaxo : l'émergence des risques éthiques sur le marché chinois

Idées et débats

Gestion des risques :
Un référentiel sinon rien !

Interview

Le *Chairman of the Board* de l'IIA nous en dit plus

International

La culture d'entreprise, un atout

Mémoire d'étudiant

Le contrôle interne favorise l'apprentissage de l'organisation

Fiche technique

>> La prise en compte, par l'audit interne, des risques associés à l'atteinte des objectifs stratégiques

ifaci
institut français de l'audit et du contrôle internes

N°217
Novembre-Décembre 2013

Marquez des points ...

avec la nouvelle certification professionnelle

CRMA™
CERTIFICATION IN RISK MANAGEMENT ASSURANCE

Professionnels de l'audit et du contrôle internes, cette nouvelle certification vous permettra de démontrer votre professionnalisme dans le domaine de l'évaluation de la gestion des risques, et plus particulièrement votre capacité à :

- évaluer la maîtrise des risques et la gouvernance des processus métiers de votre organisation ;
- sensibiliser la direction et le comité d'audit aux concepts liés aux risques et à la maîtrise des risques ;
- vous centrer sur les risques stratégiques de l'organisation ;
- apporter encore plus de valeur ajoutée à votre organisation.

Disponible, à la fin du premier semestre 2013, sous la forme d'un examen, le CRMA™ est accessible dès aujourd'hui via un processus de Reconnaissance de l'Expérience Professionnelle (REP). Ainsi, toute personne justifiant d'une expérience professionnelle dans les cinq domaines couverts par la certification CRMA™, et titulaire de diplômes et/ou de tout autre certificat dans le domaine de l'audit, sera en mesure de faire une demande de REP en vue d'obtenir la certification CRMA™.

Conception : ebzone communication - Photo : © PatyWingrove - Fotolia.com

ifaci
institut français de l'audit et du contrôle internes

POUR EN SAVOIR PLUS ...

Rendez-vous sur le site internet de l'IFACI (www.ifaci.com) à la rubrique « Carrière + Diplômes ».

The Institute of Internal Auditors

Audit & Contrôle internes

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

n°217 - nov./déc. 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 : décembre 2013
Photos couverture : © alphaspirit - Fotolia.com

SP EJP

Prix de vente au numéro : 25 € TTC

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

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.

Imaginer toutes les possibilités mais respecter les normes

Dans ce numéro, Paul Sobel que nous avons accueilli, en novembre dernier, à la première conférence annuelle de l'IFACI, nous en dit plus : sur son rôle – exigeant – en tant que *Chairman of the Board* de l'IIA ; sur le statut juridique de l'IIA global qui est resté un institut de membres alors que, pour les grands instituts nationaux dont l'IFACI, l'IIA ne peut être considéré à présent que comme une confédération d'instituts nationaux ce qui devrait conduire, à notre avis, à l'adoption d'une nouvelle gouvernance ; sur le défi que doivent relever les auditeurs internes face à la montée en puissance des autres acteurs de la maîtrise des risques. Et d'exhorter les auditeurs internes : soyez innovants, ayez de l'intuition, faites preuve de créativité, qu'il résume par « *imaginez toutes les possibilités* ».

A cette exhortation, répond tout d'abord l'initiative de Scott Strachan, directeur de l'audit interne d'une société de gestion d'actifs membre du FTSE anglais, de lancer et de mener à bien un audit complet de la culture et de la stratégie de son entreprise. Y répond aussi, le billet d'Antoine de Boissieu sur « *l'émergence des risques éthiques sur le marché chinois* » mais également ailleurs. Pour y faire face, il propose aux auditeurs internes de répondre à dix questions susceptibles de les alerter sur les risques de fraude, parmi lesquelles « *Y a-t-il des objectifs anormalement ambitieux ?* » ; « *La croissance est-elle cohérente avec l'évolution du marché ?* » ; « *Y a-t-il une fonction juridique, conformité, fiscale, indépendante ?* » ; « *Y a-t-il des directives explicites interdisant un certain nombre de pratiques connues, constatées ?* »…

Je vous recommande, par ailleurs, de porter une attention particulière sur le témoignage de trois responsables d'audit interne relatif à la mise en place d'un plan d'audit, l'un des trois processus majeurs de la fonction d'audit interne. Son élaboration n'est pas simple car le plan doit satisfaire aux attentes de plusieurs parties prenantes, direction générale, comité d'audit et, pour les secteurs banque et assurance, l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). Il se construit étape par étape en s'appuyant notamment sur la cartographie des risques qu'elle soit établie à l'échelle du groupe ou qu'elle soit propre au service d'audit interne, et en prenant attache avec de nombreux responsables ainsi qu'avec les commissaires aux comptes. Il doit enfin être approuvé et/ou validé par la direction générale et le comité d'audit. Tout en affichant quelques différences dont l'appréhension ne peut être qu'enrichissante pour chacun, la construction du plan d'audit présentée par ces trois responsables, parfaitement alignée sur les normes de la profession, est très instructive.

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 **Danone, Glaxo : l'émergence des risques éthiques sur le marché chinois**
Antoine de Boissieu

IDÉES ET DÉBATS

9 **Gestion des risques : Un référentiel sinon rien !**
Alexia Berroëta

INTERVIEW

13 **Le *Chairman of the Board* de l'IIA nous en dit plus**
Paul Sobel

INTERNATIONAL

30 **La culture d'entreprise, un atout**

MÉMOIRE D'ÉTUDIANT

34 **Le contrôle interne favorise l'apprentissage de l'organisation**
Marine Lacourte

DOSSIER

Les fondamentaux de l'audit interne

De la réflexion à la mise en place d'un plan d'audit p. 15 à 28

16 **Le plan d'audit : Unité des principes et diversité des pratiques**
Jacques Renard

20 **Audit bancaire : le plan d'audit, ce n'est pas seulement un calendrier…**
Christiane Legat

23 **Mise en place du plan d'audit dans un groupe d'assurances**
Bertrand Lefebvre

26 **La mise en œuvre de l'audit interne chez EDF : structure et méthodes**
Michel Uhart

LA PROFESSION EN MOUVEMENT

37 **Evénements - Lu pour vous**

FICHE TECHNIQUE N°47

>> **La prise en compte, par l'audit interne, des risques associés à l'atteinte des objectifs stratégiques**
Edwige Duterrage Baudin

Danone, Glaxo : l'émergence des risques éthiques sur le marché chinois

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

La Chine est devenue un marché prioritaire pour la plupart des grands groupes internationaux. Certains viennent cependant d'y connaître des déboires inédits. Deux sociétés parmi les leaders de leur secteur d'activité y ont ainsi eu des ennuis récemment.

Pots-de-vin et ententes

Dumex, filiale du groupe Danone spécialisé dans le lait infantile en Chine, a été mise en cause dans deux affaires distinctes. Elle a tout d'abord été accusée d'avoir payé des pots-de-vin à des médecins et des infirmières dans des hôpitaux du Nord de la Chine. En contrepartie, ces médecins et infirmières recommandaient le lait maternisé du groupe. L'enquête officielle a révélé au moins 110 cas, dans 85 hôpitaux et dispensaires. Le marché du lait infantile en Chine est estimé à 12 Mrd €, et il est prévu qu'il double dans les 4 ans à venir. A titre de comparaison, le chiffre d'affaires mondial de Danone dans cette activité était de 4,2 Mrd en 2012, le premier marché étant la Chine.

Un peu plus tôt les autorités chinoises avaient condamné plusieurs entreprises internationales, dont Dumex, à payer 80 M€ d'amendes. Ces amendes sanctionnaient des ententes sur les prix. Les différentes entreprises ont en outre dû baisser leurs prix de ventes de façon significative.

Corruption des médecins et gonflement des prix

Le laboratoire britannique GlaxoSmithkline a dû reconnaître sa culpabilité dans une affaire de pots-de-vin. Glaxo avait organisé un système de corruption de médecins pour qu'ils prescrivent ses médicaments. Le laboratoire est aussi soupçonné d'avoir corrompu des fonctionnaires afin de pouvoir gonfler le prix de vente de ses médicaments. Les résultats de l'enquête ne sont pas encore connus, mais les pots-de-vin payés se chiffreraient en centaines de millions de dollars. Glaxo, qui réalise 1,5 Mrd USD de chiffre d'affaires en Chine, a vu ses ventes chuter de 60 % au troisième trimestre à la suite de cette affaire.

Outre le fait qu'elles concernent deux grandes firmes occidentales en Chine, ces affaires présentent des points communs.

Des faits apparemment avérés

Le premier point commun est que les faits reprochés semblent être avérés. Après des dénégations initiales, Glaxo et Danone ont reconnu la véracité des accusations. Les autorités n'ont fait que sortir des cas réels, et ont obligé les sociétés incriminées à faire cesser les non-conformités.

Des mises en causes médiatisées

Les mises en cause par les autorités chinoises ont de plus été largement médiatisées ; les télés d'Etat ont sorti et largement relayé ces affaires, leur assurant un retentissement maximum. Les sociétés impliquées ont dû faire amende honorable dans les mêmes médias, reconnaissant ainsi leur culpabilité. Le management des filiales de Danone et de Glaxo a également été changé.

Un message clair des autorités

Il serait réducteur de ne voir dans cette publicité qu'une manœuvre populiste ou nationaliste du gouvernement chinois. Le fait de sortir ces affaires dans les médias traduit plutôt la volonté d'afficher que certaines pratiques ne seront plus tolérées, et que les autorités n'acceptent plus de fermer les yeux sur des infractions sous prétexte qu'elles sont généralisées et qu'elles ont été admises jusqu'ici.
Ces affaires posent plusieurs questions aux grands groupes internationaux, et pourraient pousser à une remise en cause de leur

mode de gestion en Chine et, plus généralement, dans les pays à fort taux de croissance. Pour schématiser, on peut dire que de nombreux groupes internationaux ont adopté vis-à-vis de ces pays une politique d'arbitrage entre les risques et les opportunités, que l'on peut résumer en 4 points : 1. Il faut se développer vite sur un marché en forte croissance - 2. Les autorités ont dû mal à contrôler le marché - 3. La pratique du marché est d'avoir une interprétation souple des réglementations et des règles d'éthique - 4. Le pilotage et la gestion de l'activité sur place sont largement délégués au management local.

Etudions rapidement ces 4 points :

1. Une course à la croissance

Le marché chinois est évidemment tentant, de par sa taille et son taux de croissance à deux chiffres dans beaucoup de secteurs d'activité. Les grandes sociétés ont donc la volonté de conquérir vite des parts de marché, pour disposer de positions bien établies lorsque le marché atteindra sa maturité. A court terme, il y a également une volonté d'afficher une hausse du chiffre d'affaires, les activités chinoises étant surveillées de près par les analystes financiers et généralement mieux valorisées que les activités des marchés européens matures ou en déclin.

2. Des marchés difficiles à contrôler pour les autorités

Le marché chinois est relativement récent ; l'ouverture économique et l'ouverture à la concurrence sont postérieures à 2000 dans la plupart des secteurs. Cela a pour conséquence que le marché est en évolution

rapide, et qu'il est difficile à contrôler et à réguler pour des autorités qui n'ont que très peu de recul, et peu d'expérience en la matière. Pour ne rien arranger, les autorités exerçant les pouvoirs de contrôle sont parfois corrompues, et ferment donc les yeux sur les faits qu'elles devraient réprimer.

3. La généralisation de pratiques douteuses

Sur ces marchés en évolution et en croissance, difficiles à contrôler, des pratiques illégales se sont plus ou moins généralisées suivant les secteurs : corruption, versement de pots-de-vin, montages fiscaux et douaniers que l'on qualifierait en France au mieux d'abus de droit, achat d'autorisations administratives ou de passe-droits, etc. , les sociétés locales donnant souvent le mauvais exemple. Dans certains secteurs, l'une ou l'autre de ces pratiques sont devenues la règle. C'est ainsi le cas du paiement de pots-de-vin aux médecins dans le secteur de la pharmacie.[1]

4. Une gestion locale

Ces marchés sont souvent gérés localement, par des filiales qui disposent d'une large autonomie par rapport au siège. Cette situation se justifie par l'éloignement, les différences de langue, les nombreuses spécificités locales, et enfin par la nécessité d'avoir un management capable de tisser localement les liens nécessaires. Plus cyniquement, cette gestion locale permet également au siège de redescendre la prise de risques et de responsabilités au niveau de la filiale, sans avoir à arbitrer entre le respect des règles d'éthique d'une part, et des objectifs de croissance ambitieux d'autre part.

Cette stratégie peut être remise en cause si le coût des non-conformités devait augmenter, ce que suggèrent les dernières affaires. Incidemment, on peut noter que les affaires de corruption de fonctionnaires relevées en Chine pourraient avoir des répercussions aux Etats-Unis dans le cadre du FCPA *(Foreign Corrupt Practices Act)*, ou au Royaume-Uni dans le cadre de l'*anti-bribery Act* ; dans les deux cas, le risque financier se trouve considérablement augmenté pour les sociétés incriminées.

Quel doit être le rôle de l'audit interne dans ce contexte ?

Evaluer le niveau de tolérance de la direction générale

L'audit interne doit vérifier s'il est missionné pour aller auditer ce type de risques. Autrement dit, y a-t-il un environnement de contrôle suffisamment fort sur ces questions pour que la direction accepte de prendre connaissance des faits, et de les traiter ? Dans certains cas, la direction générale se sert de l'audit interne pour identifier non pas les risques de non-conformité ou d'infraction, mais le risque d'être pris par les autorités : l'audit interne est donc utilisé comme un outil de mise en non-conformité, plus que comme un promoteur de l'éthique et des bonnes pratiques de gouvernance.

Recenser les signaux d'alerte

Si l'environnement général de contrôle est propice à l'audit de ce type de risques, l'audit interne peut essayer d'évaluer les risques. Dans beaucoup de cas, la difficulté est de mettre en évidence les faits incriminés, qui peuvent être bien dissimulés. C'était ainsi le cas des pots-de-vin payés aux médecins par différentes sociétés pharmaceutiques : ces dernières passaient par des agences de voyage pour organiser leurs congrès ; l'agence de voyage gonflait la facture en envoyant de faux justificatifs de frais, très difficiles à détecter pour les services financiers du siège, et a fortiori pour des auditeurs internes.

Le rôle de l'audit interne, comme face aux risques de fraude, doit donc d'abord être d'alerter sur les risques, sans forcément vouloir mettre en évidence les infractions. Pour cela, les auditeurs peuvent par exemple commencer par répondre à ces 10 questions :

1. Y a-t-il des objectifs anormalement ambitieux ?
2. Les taux de marge sont-ils cohérents avec ceux des autres pays ?
3. La croissance est-elle cohérente avec l'évolution du marché ?
4. Y a-t-il un manager (DAF par exemple) indépendant du management local ?
5. Y a-t-il une fonction juridique, conformité, fiscale, indépendante ? (rattachement à un DAF expatrié, rattachement fonctionnel à une fonction siège...).
6. Les CAC ont-ils connaissance de pratiques anormales dans notre secteur ?
7. Y a-t-il des directives explicites interdisant un certain nombre de pratiques connues, constatées ?
8. Les décisions clefs sont-elles validées au bon niveau ? (à l'inverse, ne sont-elles pas déléguées à un niveau trop bas, ce qui favoriserait la prise de risques).
9. Les prestations de service intellectuelles sont-elles bien indispensables et justifiées ?
10. Y a-t-il un réseau de contrôleurs internes couvrant y compris ce type de risques ?

Un nombre significatif de réponses négatives devrait pousser les auditeurs à creuser la question. ●

[1] *Ces pratiques ne sont d'ailleurs en rien spécifiques à la Chine, les grands laboratoires internationaux les ayant largement utilisées en Europe et aux Etats-Unis pendant des années. Pour les éradiquer, les autorités ont instauré des législations très restrictives et, aux E.-U., ont imposé des sanctions de plus en plus dissuasives.*

Gestion des risques : Un référentiel sinon rien !

Alexia Berroëta

Directeur Associée Enterprise Risk Management, **Cometh Consulting**

*Depuis plus de 15 ans dans le conseil, **Alexia Berroëta** intervient spécifiquement sur la gestion des risques d'entreprise, et en particulier dans le secteur assurances – mutuelles et groupes de protection sociale. Ses principales interventions portent sur la définition et la révision des dispositifs de maîtrise des risques en tant qu'outils d'aide à la décision pour les directions générales.*

Les cartographies ne sont pas une fin en soi. Certes, elles constituent un premier niveau de modélisation des risques et des processus, mais elles présentent les deux inconvénients majeurs que sont : l'absence d'une vision agrégée, indispensable au pilotage du profil de risque ; une difficulté à focaliser sur les risques « essentiels ». La solution réside sans doute dans la constitution d'un référentiel de risques unique et partagé, qu'il convient d'appliquer, non plus aux processus, mais aux entités organisationnelles.

Sous l'impulsion de la réglementation Solvabilité II, et par mimétisme aussi sans doute avec le secteur bancaire, les assureurs, mutuelles et groupes de protection sociale disposent de cartographies des risques opérationnels. Pour la réalisation de ces cartographies, bon nombre des entreprises du secteur ont eu recours à l'assistance des cabinets de conseils, dont l'approche privilégiée « *bottom up* » est fondée sur les processus. Cette approche, d'inspiration audit, a souvent eu la fâcheuse tendance à placer les risques en deuxième axe d'analyse, derrière les processus, instaurant une vision en silo des risques de l'entreprise.

Si ces cartographies constituent un premier niveau de modélisation des risques et des processus, elles présentent deux inconvénients majeurs :

- l'absence d'une vision agrégée, indispensable au pilotage du profil de risque,
- une difficulté à focaliser sur les risques « essentiels ».

En réponse à ces inconvénients structurels, des projets « risques majeurs » ou « risques importants » sont en train d'être menés, par les directions générales, afin de « faire le tri » et de mettre en exergue les vrais risques à piloter.
Si ces projets apportent un premier élément de réponse à la nécessité de focaliser sur les risques essentiels, ils ne permettent pas d'exploiter les cartographies des risques « *bottom-up* » déjà réalisées et qui ont représenté un important investissement des équipes internes.
Se posent alors les questions suivantes : comment faire cohabiter l'approche « risques majeurs » et l'approche « cartographies des risques » à des fins de pilotage global ? Comment exploiter au mieux les données pour restituer aux décideurs une vision fidèle et globale du profil de risque de l'entreprise ?

Fort de ces constats, il apparaît nécessaire de faire évoluer l'approche, de tendre vers une simplification de la démarche, quitte à accepter d'être moins perfectionniste, moins exhaustif, mais plus en phase avec la réalité opérationnelle de ce qui préoccupe les managers. Sans une revue de l'approche, les cartographies formalisées s'épuiseront et finiront par disparaître, naturellement, tant leur maintien apparaît lourd et fastidieux, pour une intégration souvent trop faible dans le quotidien opérationnel des managers, au profit des « risques majeurs ».

Nous avons la conviction forte que la solution réside dans la constitution d'un référentiel de risques unique et partagé qu'il convient d'appliquer non plus aux

processus mais aux entités organisationnelles. Tel est notre parti pris.

Selon nous, la nouvelle approche à mettre en place devra satisfaire à trois enjeux majeurs :

- proposer des axes de consolidation uniques et partagés, à des fins de *reportings* internes et réglementaires ;
- mettre en exergue les préoccupations des managers ;
- donner de la perspective à la direction générale.

Pour répondre à ces enjeux, tout en capitalisant sur l'existant, il convient de faire évoluer l'approche de la façon suivante :

1. définir un référentiel de risques unique et partagé ;
2. privilégier l'approche fondée sur le « référentiel entité » en majeur qui permet de focaliser sur les activités exercées au sein de l'entité, et non plus le « référentiel processus », qui focalise sur le détail intégrant une vision transverse entités ;
3. solliciter l'implication et la responsabilisation du *middle management* en tant que gestionnaire de risques.

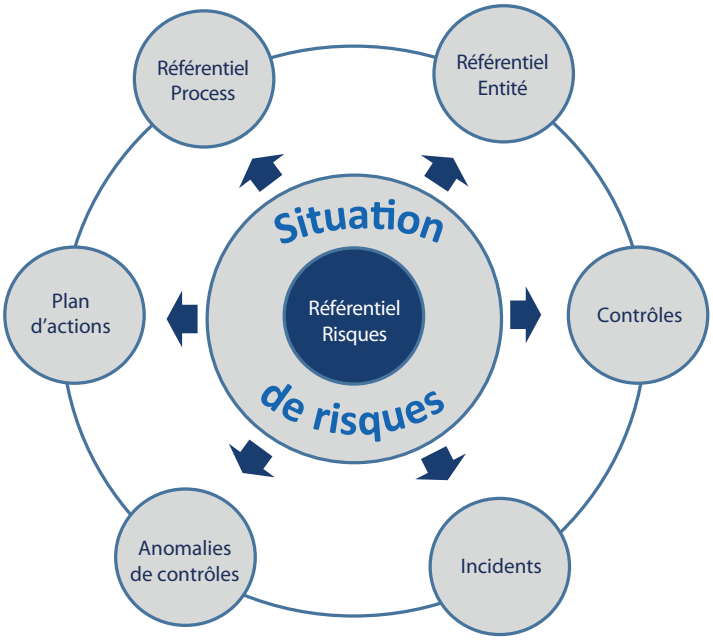
Le référentiel de risques devient le « référentiel pivot » de la gestion des risques qui offre des axes de consolidation uniques et partagés

Afin de pouvoir consolider les cartographies de risques réalisées dans les différents métiers, et d'embarquer les « risques majeurs » dans un dispositif global, il est nécessaire de définir et de rattacher chaque situation de risque à un référentiel commun de risques, partagé par toutes les entités de l'entreprise. Ce référentiel a pour objectif de :

- structurer et consolider de manière cohérente l'ensemble des situations de risque de l'entreprise (issues des cartographies réalisées par les métiers et les « risques majeurs » identifiés par la direction générale) ;
- disposer d'axes d'analyse ;
- favoriser l'unicité du langage entre les parties prenantes ;
- faciliter la comparaison entre entités.

Le référentiel de risques, qui assure le regroupement des situations de risques par catégorie, permettra la constitution de reporting globaux à destination des décideurs.

Dans la construction initiale d'un référentiel de risques, il est souvent intéressant de s'inspirer des référentiels de place ou de confrères. Il est également pertinent de consulter les référentiels d'autres secteurs, notamment à maturité différente. Les incidents sont également une bonne source d'information.
Parce que le référentiel de risques doit refléter l'entreprise, sa culture, son activité, ses préoccupations en matière de gestion des risques, chaque référentiel



est différent, quand bien même certaines catégories de risques, très générales, sont communes aux différents secteurs (ex : risque de fraude).

En effet, en fonction de la sensibilité de la direction générale à la gestion des risques et du niveau d'exposition réel de l'entreprise, les catégories de risques seront identifiées et hiérarchisées de façon distincte. Certains, par exemple, aborderont les risques issus de la directive Solvabilité II comme des risques de « non-conformité juridique », quand d'autres les aborderont comme des risques « *business* ». Certains considèreront « l'image » comme la conséquence d'un risque, quand d'autres traiteront l'image comme un risque en tant que tel.

Il n'y a pas de référentiel « idéal ». La performance d'un référentiel se mesure au travers de la simplicité et de la fiabilité avec laquelle les acteurs rattachent les situations de risques aux différentes catégories du référentiel. Si trop d'hésitations ou de questionnements se dressent, il convient de redéfinir le référentiel. En effet, la règle fondamentale est la suivante : une situation de risques ne se rattache qu'à une et une seule catégorie de risques. Une seule ambiguïté restera toujours à lever : l'arbitrage entre l'erreur d'exécution (non intentionnelle) et la fraude (intentionnelle).

Un référentiel de risques est quasi invariant, a minima sur les deux premiers niveaux de son arborescence. Le dernier niveau évolue dans le temps. A horizon 2 ou 3 ans, et sans modification majeure de l'environnement (ex : changement de localisation géographique), le référentiel de risques est quasi invariant. En revanche, le profil de risque lui, varie en fonction de la stratégie *business* / risque définie et de la performance des contrôles.

L'approche fondée sur le « référentiel entité » en majeur permet de focaliser sur les préoccupations essentielles des managers

Si l'approche fondée sur les processus a semblé être la plus naturelle voire la plus rassurante, elle présente, dans le quotidien, un certain nombre de limites :

- Ce référentiel de processus ne fait pas toujours consensus au sein de l'organisation, parfois même il ne dispose pas d'un caractère « officiel », lorsqu'il n'existe pas au sein de l'entreprise, d'entité dédiée, de type « organisation », garante du référentiel de processus.
- L'exercice d'identification des risques est mené sur le niveau le plus détaillé du référentiel de processus, ce qui favorise la surenchère dans l'identification des risques, et peine à focaliser sur les risques essentiels.
- Enfin, le déploiement de cette approche à l'ensemble des processus de l'entreprise, est lourd et fastidieux, tant le niveau de granularité est important.

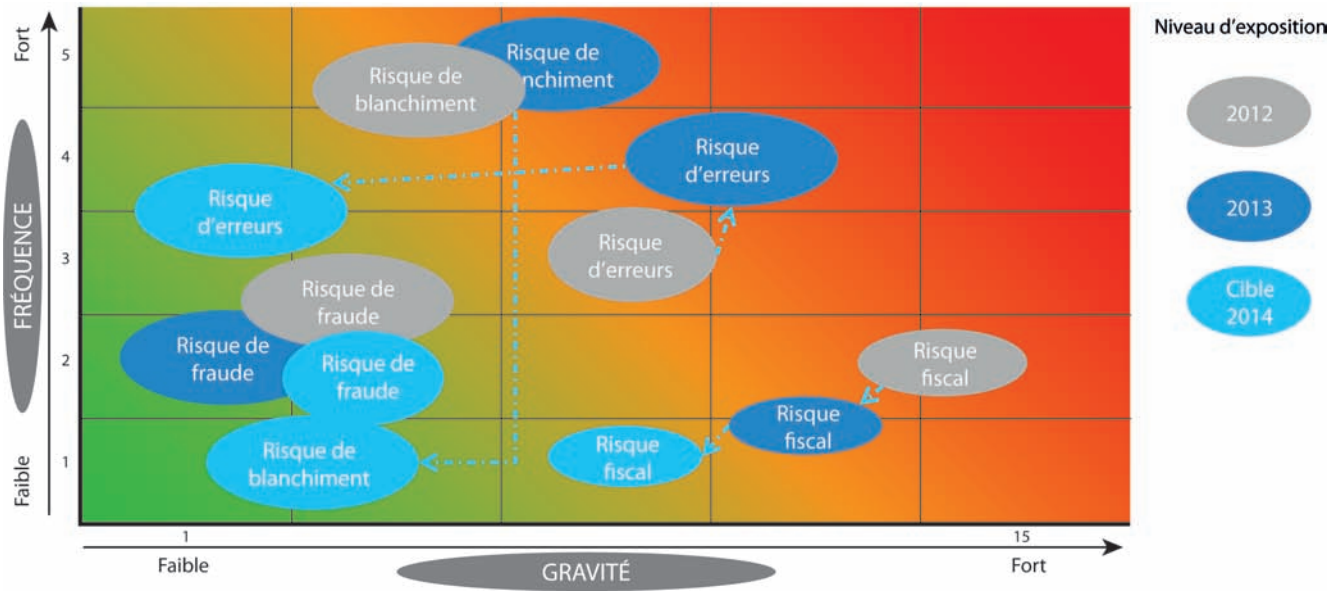
Tout d'abord, cette approche fait le choix d'un référentiel « officiel », par nature incontestable, ce qui favorise le consensus et donc l'adhésion.
Dans sa structuration même, le référentiel de processus propose souvent un découpage de l'activité qui en réalité est un mix entre processus pur et entité organisationnelle. Certains processus sont parfois même redondants dans le référentiel, puisque présents dans des entités organisationnelles distinctes. Ce mix conduit à une vision parcellaire des risques liés aux processus. Cette difficulté se présente essentiellement lorsqu'il s'agit de définir les processus transverses. Par ailleurs, il est fréquent de constater que ce référentiel n'est pas toujours actualisé.

Le deuxième bénéfice apporté par cette nouvelle approche réside dans le fait que le « référentiel entité » ou organigramme est orienté vers le « quoi » et non le « comment ».
Ce qui facilite également l'approche risque et contrôle interne en invitant les managers à se centrer non seulement sur leur périmètre exact de responsabilité mais également à un niveau de granularité plus macro à l'inverse des processus, décrits à un niveau de granularité trop détaillé, se positionnant parfois à la frontière avec le mode opératoire / la procédure opérationnelle.

Enfin, cette approche concourt, mécaniquement, à un déploiement plus rapide de la méthode d'identification et de cotation des risques.

L'implication et la responsabilisation des managers comme gage de la légitimité du dispositif vis-à-vis de la direction générale

Les cartographies des risques telles qu'elles ont été faites, n'ont pas su offrir



aux décideurs une vision globale et stratégique du profil de risques de l'organisation.

Au-delà des nécessaires évolutions à apporter à l'approche même, telles qu'évoquées supra, il convient également de repositionner les acteurs de la filière risque et contrôle au niveau des décideurs (ex : responsables de pôles, de directeurs). Ces acteurs sont eux les gestionnaires de leurs activités. Dans leurs actes de management au quotidien, ils portent la responsabilité de détecter, suivre et piloter les risques pouvant porter atteinte à la bonne réalisation de la stratégie *business*. Ce sont le plus souvent ces dysfonctionnements ou risques qui sont évoqués lors des comités de direction, c'est donc auprès de ces acteurs que la gestion des risques prend tout son sens.

La valeur ajoutée du *risk manager* vis-à-vis de la direction générale sera alors d'apporter une vision consolidée et professionnalisée des risques, quand auparavant, celle-ci était restituée unitairement et en silo.

* *
*

Le temps est venu, afin de consolider les acquis, de revisiter l'approche « processus » et la faire évoluer vers une approche résolument « *risk management* ».

Indépendamment des contraintes réglementaires en vigueur, revoir l'approche répond avant tout à la volonté d'optimiser les saines pratiques de gestion des risques et satisfaire aux enjeux de qualité et d'excellence opérationnelle.

Les trois éléments proposés permettent de faire évoluer l'approche « standard processus » vers une approche « *risk management* » à savoir la définition d'un référentiel de risques, l'application de ce référentiel de risques au « référentiel entité » en majeur puis l'implication et la responsabilisation des managers dans le dispositif.

La vision agrégée des situations de risques est l'élément fondamental pour déterminer le profil de risques de l'entreprise.

De la qualité des situations de risques identifiées dépendent la pertinence et la fiabilité du dispositif, d'où les nécessaires implication et responsabilisation des *managers* en tant que gestionnaires des risques de l'entité dont ils ont la charge.

La consolidation des situations de risques, par catégorie de risques, sera le moyen, pour le *risk manager*, en appui de la direction générale, de donner de la perspective et faciliter l'arbitrage de priorités.

Par cette nouvelle approche, le *risk manager* est en mesure de faciliter les points de rencontre entre les activités et les risques et ainsi de renforcer l'articulation de la stratégie *business* avec la stratégie risque. ●

« La mise en place de notre référentiel de risques nous permet de proposer à la direction générale une vision agrégée de nos risques, de « casser » les frontières entre nos différents métiers et de renforcer le pilotage de notre profil de risques à moyen terme. »
Yves Vanhoute, directeur finance, contrôle interne et comptabilité, groupe B2V

« Jusqu'alors, nous disposions de cartographies des risques offrant une vision détaillée et en silo des risques portés par les processus. Nous avons été séduits par la démarche qui consiste à structurer les situations de risques par la mise en place d'un référentiel de risques unique et partagé par notre groupe, en capitalisant sur les travaux déjà menés selon l'approche processus ».
Hervé Vandenbergue, responsable du département maîtrise des risques, MGEN

Le *Chairman of the Board* de l'IIA nous en dit plus

Entretien avec ...

Paul Sobel - *Chairman of the Board* de l'IIA *(The Institute of Internal Auditors)*

Louis Vaurs : *Merci Paul Sobel de vous prêter à cette interview. Ma première question porte sur les rôles respectifs de vous-même et de Richard Chambers. Comment s'organisent-ils ?*

Paul Sobel : Le rôle de Richard, en tant que président-directeur général, est de superviser et de diriger les opérations quotidiennes, mon rôle de *Chairman of the Board* étant de traiter les sujets stratégiques.
Lorsque Richard est entré en fonction, il y a quelques années, il a constaté que ses pairs étaient généralement dénommés PDG et il a donc demandé à porter le titre de président et de directeur général. Président est un lien avec le passé et directeur général est un terme plus descriptif.

L.V. : *Vous êtes membre du comité exécutif de l'IIA depuis plusieurs années et vous n'allez exercer vos responsabilités de* Chairman of the Board *que pendant un an. C'est très court !*

P. S. : C'est exact et c'est un point que nous avons abordé, en particulier dans le groupe de travail sur la gouvernance, parce que c'est un défi de faire beaucoup en un an. Vous êtes plus une figure de proue qu'autre chose. En réalité, il s'agit d'un poste bénévole qui requiert beaucoup de votre temps, notamment en termes de déplacements, et il pourrait être difficile d'occuper ce poste pendant plus d'un an. Si la plupart des entreprises sont prêtes à permettre à quelqu'un de le faire pendant un an, elles peuvent ne pas être prêtes à le faire pendant deux ou trois ans, ce qui serait probablement la durée optimale pour l'IIA.

L.V. : *Comment conciliez-vous votre travail à l'IIA et votre travail de responsable de l'audit interne de votre entreprise ?*

P. S. : Vous devez être un très bon jongleur, ce qui signifie que vous devez être en mesure de conserver plusieurs balles en l'air. Je ne peux pas laisser tomber la balle famille car j'ai certaines obligations familiales à assumer. Je ne peux pas laisser tomber la balle travail, alors, quand je suis en voyage dans le monde entier, je communique par e-mail, je prends des décisions, etc.
C'est un défi, et mon équipe de direction – les personnes qui relèvent directement de moi – doit admettre que je vais être absent un peu plus souvent. Je leur ai dit que ce serait en fait une occasion pour eux d'accélérer leur développement.

L. V. : *Voyagez-vous aux quatre coins du monde pour votre entreprise ?*

P. S. : Non. Je voyage principalement en Amérique du nord, et plus particulièrement aux Etats-Unis.
Nous avons très peu d'affaires en Europe, et quelques-unes en Amérique du sud et en Asie.

L.V. : *Qu'en est-il de votre personnel ?*

P. S. : Généralement, il voyage environ 25 % de leur temps, et presque exclusivement aux États-Unis et au Canada.

L.V. : *De combien de personnes est composée votre équipe ?*

P. S. : Mon assistante administrative et moi-même inclus, nous sommes 25.

L.V. : *Les grands instituts nationaux européens considèrent que l'IIA est plus une confédération d'instituts qu'un institut de membres et qu'il faudrait en tirer les conséquences au plan de la gouvernance. Qu'en pensez-vous ?*

P. S. : C'est un sujet controversé, qui a fait l'objet de débats. En réalité, nous sommes un modèle hybride, c'est-à-dire à la fois un institut de membres et un institut d'instituts – ou confédération d'instituts – et la raison en est double. Tout d'abord, il y a certains services de base (au premier rang desquels, les certifications et les Normes) dont nous pensons qu'ils sont mieux rendus ou mieux développés, en étant reliés à une source unique. Les membres se sentent alors faire partie d'un tout : l'IIA mondial.

Le deuxième obstacle est une question de maturité. L'IFACI et la plupart des grands instituts européens, ainsi qu'un certain nombre d'autres à travers le monde, sont assez matures et ils n'ont pas besoin de l'aide de l'IIA mondial. Cependant, de nombreux autres instituts en cours de développement, qu'ils soient en formation ou instituts à part entière, sont très immatures, et ont encore besoin d'un appui supplémentaire et de surveillance, et probablement de la discipline imposée par l'IIA mondial .

Nous devons travailler à identifier les instituts réellement matures, et ce que cela signifie dans leur relation avec l'IIA global ; et les instituts les moins matures, et ce que cela signifie.

S'il existe une organisation régionale robuste guidée par l'IIA, nous pourrions laisser cette organisation face aux instituts en question. Cependant, nous n'en sommes pas arrivés à ce stade.

Nous pouvons faire bien davantage en ce qui concerne les organisations régionales et je pense que le conseil mondial peut apporter une aide ainsi que le comité des relations avec les instituts. Il existe de nombreuses possibilités pour faire avancer ce modèle. Nous devons donc trouver un moyen par lequel nous pouvons tous travailler ensemble. Nous avons tous le même objectif et nous avons besoin de comprendre comment nous pouvons procéder de façon à ce que tous les instituts aient la possibilité de participer et d'avoir une voix dans les décisions. Il est nécessaire qu'il existe un niveau approprié de surveillance et de reddition de comptes dans les deux directions : l'IIA doit rendre des comptes aux instituts de même que les instituts doivent rendre des comptes à l'IIA.

L.V. : *Un tout autre problème concerne les autres acteurs du contrôle interne et de la gestion des risques. Nous avons publié à l'IFACI une prise de position, il y a cinq ans sur « l'Urbanisme du contrôle interne » : Comment en améliorer l'efficacité ? Quelle place pour l'audit interne ? Nous notions déjà la montée en puissance des contrôleurs internes, des* compliance officers *et des* risk managers *et insistions sur la nécessité de bien définir les responsabilités de chacun, l'audit interne parfaitement intégré dans le* business *de l'organisation devant s'assurer du bon fonctionnement de ces différents acteurs.*
Quelle est la position de l'IIA vis-à-vis de ces différents acteurs ?

P. S. : Face à eux, nous avons un grand défi à relever que l'on peut transformer en opportunité car on ne mesure pas encore à sa juste valeur l'assurance apportée par les auditeurs internes.

Par ailleurs, nous lançons une initiative issue du plan stratégique, classée haute priorité. C'est le « projet umbrella », même si je ne suis pas sûr que ce soit la bonne appellation. L'objectif ici est de considérer ce que nous devrions faire par rapport aux autres professions. Devons-nous aider les auditeurs internes à s'orienter vers les activités de la seconde ligne de maîtrise et développer plus de documentation pratique ? Faut-il fusionner avec une autre association, procéder à l'acquisition d'une association ou tout simplement les ignorer en poursuivant notre chemin ? La sagesse nous commande de dire aujourd'hui : « Nous sommes l'Institut des auditeurs internes. Ne l'oublions pas et n'essayons pas de devenir un institut pour tout le monde ».

« Nous sommes l'Institut des auditeurs internes. Ne l'oublions pas et n'essayons pas de devenir un institut pour tout le monde »

Cependant, je crois qu'il y a des possibilités pour mieux nous coordonner avec les instituts qui nous sont proches.

Je ne pense pas que nous devrions changer de nom – nous sommes encore principalement concentrés sur l'audit interne –, mais nous aurions intérêt à mieux connaître ce que font les autres acteurs car cela nous permettrait de mieux servir les auditeurs internes qui portent plusieurs casquettes.

L.V. : *En tant que* Chairman of the Board *quels sont vos objectifs prioritaires pour cette année ?*

P. S. : Je vais vous donner une double réponse. Tout d'abord, mon premier objectif est de faire en sorte que le plus grand nombre possible d'auditeurs internes dans le monde, entendent ce que je dis et répète sans cesse : « Imaginez toutes les possibilités », et assurez-vous que la profession, dans son ensemble, ne se contente pas de statu quo, mais réfléchisse à tout ce qui peut être fait à l'avenir, à la création de notre propre avenir.

D'autres initiatives plus tactiques sont ou ont été prises sans que j'en sois nécessairement l'initiateur. Certaines sont en cours, d'autres sont déjà achevées ; elles concernent des certifications, la transformation de l'examen en quatre parties du CIA à un examen en trois parties, et le déplacement de la reconnaissance de l'expérience professionnelle sur la CRMA à un examen de la CRMA. Nous avons aussi pris des initiatives avec le conseil de stabilité financière, le conseil international sur le *reporting* intégré et avec d'autres organismes de nature comparable.

Un des sujets que j'ai mis en priorité sur ma liste est la convention cadre des relations entre l'IIA et les instituts nationaux – *Master Relationship Agreement* – (MRA), et je me suis assuré que les choses avançaient.

Je reconnais toutefois que tous les projets en cours ne pourront pas être tous signés durant mon mandat de président.

L.V. : *Merci Paul de nous avoir mieux fait connaître votre rôle et de nous avoir confié, sans langue de bois, les préoccupations actuelles de l'IIA.* ●

Les fondamentaux de l'audit interne

De la réflexion à la mise en place d'un plan d'audit

16 **Le plan d'audit : Unité des principes et diversité des pratiques**
Jacques Renard

20 **Audit bancaire : le plan d'audit, ce n'est pas seulement un calendrier…**
Christiane Legat

23 **Mise en place du plan d'audit dans un groupe d'assurances**
Bertrand Lefebvre

26 **La mise en œuvre de l'audit interne chez EDF : structure et méthodes**
Michel Uhart

Le plan d'audit : Unité des principes et diversité des pratiques

Jacques Renard

Après une phase de questionnements : quelles missions d'audit faut-il conduire ? comment faire le choix ? ; une phase d'organisation et de prévisions : élaboration d'un planning annuel, est arrivée la troisième phase qui a vu le plan d'audit s'affirmer dans toutes ses dimensions, avec l'élaboration d'un plan pluriannuel.
La mise en œuvre de la norme 2010 nécessite une méthode d'évaluation des risques (cartographie) et la définition d'un univers d'audit. Reste à fixer les règles du ranking, estimer le temps de travail de chaque mission, et soumettre le plan à la DG, car c'est elle qui décide en fonction de sa politique de risque.

De tout temps les organisations, les activités se sont construites par stratifications successives, les dernières couches apportant compléments et améliorations à l'existant. L'audit interne et l'une de ses composantes essentielles, le plan d'audit, n'ont pas échappé à cette règle.
Au commencement du commencement le mot « plan d'audit » n'existait pas encore et l'on était dans la phase primaire du concept. Dans la phase secondaire, le mot est apparu qui recouvrait des réalités diverses. Puis vint une troisième période de clarification et de rationalisation qui a largement transformé le concept en outil, le réflexe en méthode de travail, la déclaration d'intentions en véritable contrat. L'existant actuel est d'autant plus solide qu'il répond à une nécessité et repose sur une obligation. Mais la démarche exige de la méthode et des compétences.

La maturation du concept et son évolution

La première question qui s'est posée dans les premiers temps de l'audit interne fut : « Quelles missions d'audit faut-il conduire ? Comment faire le choix ? » La réponse a été évidemment empirique, c'est-à-dire par essence intuitive et irrationnelle. Cela conduisit à trois attitudes possibles qui perdurent encore ça et là.

- Très souvent les intéressés choisissent en fonction de leur intuition ou de leur préoccupation. On suit l'inspiration du moment ce qui revient à se diriger dans les secteurs que l'on connaît bien. Avec des auditeurs de formation commerciale on initiera des audits dans les ventes ou le marketing et avec des auditeurs de formation financière on sera porté à investir dans des audits de comptabilité ou de contrôle de gestion. Et s'il n'y a pas d'auditeur de formation ingénieur on oubliera le domaine technique.

- Cette attitude se conjugue alors souvent avec une autre qui parfois se substitue totalement à elle. C'est celle qui fait de l'audit interne un service « à la discrétion » du président ou du directeur général. On initie alors des missions d'audit en fonction des craintes ou des préoccupations ou des difficultés de la direction générale. Et ce sont alors trop souvent les idées du moment, les hasards d'une rencontre ou d'une réflexion qui vont déclencher l'ordre de mission… sans parler des réunions du petit matin, convoquées toute affaires cessantes, pour répondre à un problème, fruit des insomnies de la nuit précédente.

- Enfin, il existe un troisième critère de choix qui est le critère événementiel. La mission est déclenchée à la faveur d'un accident, d'une erreur grave, d'une malversation… On réagit à l'événement, ce qui en soi n'est pas condamnable, mais on ne réagit **qu'à** l'événement.

Il est assez vite apparu que ces modes de fonctionnement ne pouvaient perdurer : ils privilégiaient le présent et omettaient un élément essentiel dans l'orga-

nisation du travail : la prévision. Il fallait donc avoir un plan pour savoir où l'on voulait aller.

La seconde phase est celle du plan annuel, nous dirons du *planning*. Très vite on s'est avisé qu'il fallait s'organiser et donc prévoir le travail pour mieux le réaliser. L'idée du plan s'est d'autant plus imposée que – ainsi que nous le verrons – les Normes professionnelles sont apparues et ont créé l'obligation. De surcroît il fallait bien faire coïncider les besoins avec les possibilités, les objectifs avec les moyens. On est alors parti d'un **effectif prédéterminé**, selon des critères variables et approximatifs, et parfois même sans autre critère que le fait du prince : « je peux vous donner quatre auditeurs »… et on fait avec ! Donc, compte tenu de l'effectif, on voit ce qu'on peut faire.
Ce plan annuel est déjà un progrès très sensible puisqu'il planifie les missions à réaliser et constitue un objectif précis pour l'audit interne. En cela, mais en cela seulement, il répond aux Normes de l'audit interne. Il fait l'impasse sur la notion de risque ou ne la retient que pour les missions planifiées dans l'année même si « hors plan annuel » on prend en compte les enseignements d'une cartographie des risques.
Il permet néanmoins de comparer prévisions et réalités, donc de réaliser une certaine mesure de l'efficacité de l'audit interne.

Mais c'est avec **la troisième période** que le plan d'audit s'est affirmé dans toutes ses dimensions. On a alors élaboré un plan pluriannuel (sur trois ou cinq ans). Pourquoi ?
Parce que c'était la seule façon de répondre à l'exigence de la Norme 2010 : *« Le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir les priorités cohérentes avec les objectifs de l'organisation ».* Cette troisième période n'est donc que la mise en œuvre de l'exigence normative. Le plan sur trois ou cinq ans va permettre de donner une vue d'ensemble de toutes les missions à accomplir. A partir de là on formalise la périodicité, donc la prise en compte du risque et du même coup on responsabilise les décisionnaires.

Avant de l'aborder dans le détail, observons que les situations rencontrées sont rarement pures : elles conservent souvent et tout naturellement des traces des évolutions antérieures, marquées par la culture et le milieu professionnel. Telle organisation fera encore une large place aux idées du président et telle autre fonctionnera encore avec un plan annuel mais corrigé par la prise en compte – non écrite – de la variabilité des risques sur les années à venir… ce qui est déjà une manière de plan pluriannuel. Et de fait, les applications spécifiques et partielles des grands principes ne sont pas nécessairement condamnables dès l'instant qu'elles sont prises en connaissance de cause. Le monde n'est pas géométrique et singulièrement celui de la gestion.

L'exigence normative

Dans la norme 2010 chaque mot compte :

- C'est **« le responsable de l'audit interne »** qui a la charge de la mise en œuvre du plan ; c'est lui qui doit en répondre et il ne peut s'en décharger sur personne d'autre.
- Il **« doit »** : c'est une obligation à laquelle on ne peut se soustraire. Ne

pas faire de plan d'audit c'est se placer en dehors des Normes de la profession ; c'est donc faire tout autre chose que de l'audit interne.

- On doit établir **« un plan ».** Un plan d'audit ne tient pas sur une page ; ce ne saurait être une note de synthèse ou une déclaration d'intentions ou un objectif général. Il doit y avoir a minima une liste des actions à réaliser avec des dates et des délais impartis.
- Ce plan doit être **« fondé sur les risques ».** C'est le critère qui doit être retenu pour faire les choix et il n'y en a pas d'autre. La gravité ou l'insignifiance des risques se mesure par rapport aux objectifs : le risque à prendre en compte est donc celui qui, directement ou indirectement, est susceptible de nuire à la réalisation des objectifs.
- **« Afin de définir les priorités ».** La notion de risque est prise en compte avec la définition des priorités. Ce ne sont ni le temps passé, ni la qualification des auditeurs qui sont à retenir mais uniquement le *timing* des interventions. L'activité comportant un risque grave sera auditée en priorité, donc souvent, celle représentant un risque mineur sera auditée plus rarement, d'où l'intérêt du plan pluriannuel qui fait **visuellement** ressortir la répartition des priorités.
- Et à la condition que ceci soit en cohérence **« avec les objectifs de l'organisation ».** Les secteurs ou activités à risques stratégiques sont évidemment prioritaires. D'ailleurs, afin qu'il ne soit rien omis, la norme 2010.A2 prend bien soin de préciser que *« le responsable de l'audit interne doit identifier et prendre en considération les attentes de la direction générale et du conseil ».*

Au total, cette norme essentielle exige deux préalables pour sa mise en œuvre : **l'existence d'une cartographie des risques et la définition d'un univers d'audit.**

La cartographie des risques

L'objet de cet article n'est pas de définir les règles et méthodes pour la mise en œuvre d'une cartographie. Notons simplement que la norme 2010.A1 précise sans ambiguïté *« Le plan d'audit doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois l'an ».* Peu importe qu'il y ait dans l'organisation un *risk manager* ou non. S'il existe on s'appuiera bien évidemment sur ses travaux ; s'il n'existe pas il faudra développer une méthode d'évaluation afin de satisfaire aux exigences normatives. La pratique nous offre de nombreuses méthodes, plus ou moins sophistiquées, pour y parvenir tel le système RADAR[1] qui retient trois critères d'appréciation. Le GRID Model va encore plus loin dans l'affinement en retenant des critères relevant du niveau de compétence des auditeurs[2]. Peu importe la méthode, l'important est qu'il y en ait une. Mais la MPA 2010-2/6 confirme la prééminence du risk management lorsqu'il existe *« La planification de l'audit interne* ***doit*** *s'appuyer sur le processus de management des risques de l'organisation lorsque celui-ci a été déployé ».*

L'univers d'audit

La première colonne d'un plan d'audit est constituée par la liste des missions à réaliser. Comment l'établir ? Il n'existe pas de méthode mais il y a un objectif. C'est la MPA 2010-1/1 qui nous précise la pratique à retenir : *« En élaborant le plan d'audit, la plupart des responsables de l'audit interne choisissent d'abord de développer ou d'actualiser l'univers d'audit. L'univers d'audit recense* ***tous les audits pouvant être réalisés*** *».* Il s'agit donc de la liste exhaustive de toutes les missions d'audit couvrant toutes les activités de l'organisation. C'est le grand principe : tout doit être auditable, donc audité. Et on veille à ce que les demandes de la direction générale et les attentes du management soient bien prises en compte.

C'est à partir de là que le responsable doit préparer son plan. Cet univers d'audit doit être révisé « au minimum une fois l'an » précise la MPA 2010-1. Ce qui se comprend parfaitement : nous sommes dans un domaine où tout change. Les organisations changent, les méthodes changent, les risques changent et le plan d'audit doit en tenir compte, il ne saurait être figé.

C'est d'ailleurs la raison pour laquelle le plan d'audit, fut-il pluriannuel, doit être refait chaque année. Ce n'est pas seulement un plan glissant, c'est l'ensemble qui doit être actualisé.

Cet univers d'audit va être utilisé à des fins bien précises et selon une méthode qui n'est pas uniforme. Chacun a la sienne, l'important est qu'il y en ait une. Décrivons la plus habituelle dans ses composantes essentielles.

La méthode

La cartographie des risques étant prise en compte et l'univers d'audit défini, il convient d'élaborer les méthodes appropriées afin de :

- fixer les règles du *ranking ;*
- estimer le temps de travail de chaque mission et en déduire les budgets d'effectif ;
- soumettre le plan à la direction générale.

Observons, pour ne plus avoir à y revenir, que toutes ces méthodes font largement appel à de multiples outils informatiques, statistiques… plus ou moins sophistiqués selon les objectifs et l'importance de l'organisation. Mais *in fine* il faut s'organiser pour être en mesure d'apporter une réponse à chacun des trois objectifs ci-dessus énoncés. Le plan d'audit sera alors achevé.

Le *ranking*

C'est la mise en œuvre des priorités en fonction des risques, exigée par la norme. Pour y parvenir il est indispensable que la cartographie assigne à chaque élément de l'univers d'audit (donc à chaque mission potentielle) un coefficient de risque et à partir de ce coefficient chacun définit sa règle de fréquence. Certains, partant de la connaissance qu'ils ont de l'organisation, fixent les priorités sans méthode particulière et avec le recours à la simple concertation. Pourquoi pas ? La connaissance empirique, si elle est réelle et solide, peut aussi donner de bons résultats.

On peut aussi disposer du système

basique à trois niveaux :
1. risque faible,
2. risque moyen,
3. risque fort.

On décidera alors (par exemple) :
- qu'au coefficient 1 correspond un audit tous les 4 ou 5 ans ;
- au coefficient 2, un audit tous les 3 ans ;
- et au coefficient 1, un audit tous les 1 ou 2 ans.

Le système RADAR, plus sophistiqué, utilise des coefficients allant de 1 à 27. Le *ranking* est alors déterminé par groupes de coefficients ; par exemple :
- de 1 à 8 : un audit tous les 5 ans ;
- de 9 à 15 : tous les 4 ans ;
- etc.

Les coefficients étant connus et la règle fixée, on pourra positionner la date d'intervention dans l'année adéquate en s'efforçant de réaliser en apparence un équilibre annuel de la charge de travail. Cet aspect sera peaufiné à l'étape suivante. On connaît ainsi les missions à réaliser chaque année. C'est à partir de là que l'on pourra établir le *planning* détaillé de l'année à venir.
Si l'important n'est pas la méthode choisie, il est néanmoins essentiel que celle-ci réponde à deux exigences :
- elle doit conduire à des résultats en cohérence avec la stratégie de l'entreprise ;
- elle doit être en ligne avec la culture de l'organisation.

Il convient ensuite de définir les moyens nécessaires pour atteindre les objectifs ainsi fixés. En d'autres termes : combien d'auditeurs ?

Les effectifs

On a bien compris que l'on ne part pas des effectifs pour définir un plan mais que le plan, défini en fonction des risques, va induire un certain effectif.
Cet effectif nécessaire est estimé et cette estimation n'est évidemment qu'approximative. Il s'agit de déterminer un ordre de grandeur, nous ne sommes pas dans les prévisions comptables.

Pour ce faire certains estiment le temps nécessaire en semaines / auditeurs ; d'autres, plus perfectionnistes comptent en jours / auditeurs… Peu importe, l'essentiel est d'obtenir un chiffre vraisemblable. On le définit à partir de toutes les informations disponibles. La plus parlante reste bien évidemment le nombre de semaines / auditeurs utilisés lors de la dernière mission sur le même sujet… s'il y en a eu une ! Et, même dans ce cas, il faudra ajuster le chiffre en fonction des évènements connus. L'activité s'est-elle complexifiée ou est-elle en réorganisation ? Le temps à prévoir sera alors majoré. L'équipe d'auditeurs est-elle plus expérimentée ? Plus performante ? On procédera alors à une diminution. Tous ces éléments figurent dans les commentaires IFACI de la norme 2010.
Au total et pour chaque année on va disposer d'un chiffre qui, à partir de la connaissance du nombre moyen de semaines de travail d'un auditeur dans l'année, va permettre d'arriver à un effectif nécessaire. Mais il va falloir affiner avant de passer à l'étape suivante.

Le premier ajustement va consister à ajouter une « provision » d'effectif pour évènements imprévus, donc audits imprévus. Il peut toujours y avoir une urgence, une activité nouvelle, une demande inhabituelle mais incontournable et le plan ne saurait être un obstacle à l'action. L'important est de veiller à ce que l'exception ne devienne pas la règle : on assignera donc une limite, en général + 10% maximum, et on en surveillera l'utilisation.

Le second ajustement consiste à obtenir une cohérence dans les résultats. En effet, on ne pourrait présenter un plan qui verrait les effectifs varier brutalement : 12 auditeurs en 2014 puis 21 en 2015 et 13 en 2016… Ce serait ingérable en termes de ressources humaines et de formation. On va donc, par simple glissement des missions d'une année sur l'autre (et sans modifier la périodicité), s'efforcer d'arriver à une courbe d'évolution des effectifs qui ne marque que des variations progressives, à défaut de stabilité.

On dispose alors d'un **projet de plan** ; le plus important reste à faire.

La direction générale

Car c'est elle qui décide. Et elle décide en fonction de sa politique de risque, c'est à dire des choix qui ont été faits en matière d'appétence pour le risque et de tolérance au risque. On doit donc impérativement lui présenter le projet pour approbation ou modifications. Ce n'est que l'application de la norme 2600 sur la « communication relative à l'acceptation des risques ». Et si la direction générale avance que les 12 auditeurs prévus en 2014 ne pourront être mis à disposition mais que l'on ne pourra en avoir que 10 ; alors, il lui appartient, d'indiquer sur quelle activité du plan elle accepte de prendre plus de risques que ceux qui ont été calculés. Et les ajustements seront réalisés en conformité avec ces indications.
Le plan définitif est alors achevé.

* *
*

En conclusion, le document final a bien pris la forme de ce qu'il doit être : **un contrat** passé entre l'audit interne et les organes de la direction.
Ce contrat constitue du même coup les objectifs de l'audit interne et on doit s'organiser pour être en mesure d'en suivre la réalisation et de rendre compte.
Le problème de sa communication n'est pas, non plus, résolu de façon uniforme. La règle de la transparence exigerait qu'il soit communiqué à tous les intéressés, donc à tous les audités potentiels. Mais la culture, la nature des activités, les contraintes spécifiques conduisent à retenir des procédures de communication diverses et variées.
Quoi qu'il en soit et en toute matière, le grand principe à retenir est de toujours ne mettre en œuvre que des règles simples et compréhensibles par tous.
« La simplicité est aussi une vertu intellectuelle »[3]. ●

[1] *Ressources of Audit Department Allocated by Risks.*
[2] *Pour plus de détails on consultera les ouvrages appropriés.*
[3] *A. Comte-Sponville « Petit traité des grandes vertus » PUF.*

Audit bancaire : le plan d'audit, ce n'est pas seulement un calendrier…

Christiane Legat, *Head of Internal Audit*, **General Electric Corporate Finance Bank**

La construction du plan d'audit se base avant tout sur la cartographie des risques établie par l'audit interne. La première étape consiste à traduire le niveau de risque attribué à chaque objet auditable. La deuxième étape est la prise en compte des objets auditables, dont le niveau de risque n'a pas été évalué au moyen de la cartographie. La troisième étape consiste à évaluer les moyens humains nécessaires à la réalisation des missions programmées. La dernière étape est la mise en cohérence des besoins théoriques déterminés avec les ressources et les budgets effectivement disponibles.

Le plan d'audit est un outil-clé pour l'audit interne. Il constitue une réponse à des « demandes » multiples : des normes, des recommandations, des préconisations voire une exigence réglementaire.
Sa construction nécessite la prise en compte de nombreux éléments au premier rang desquels figure la cartographie des risques établie par l'audit interne.
Enfin, la communication du plan, sa mise en œuvre et son suivi exigent du responsable de l'audit interne beaucoup de finesse.

Le plan d'audit : une réponse à des « demandes » nombreuses … des normes professionnelles

La norme 2010 « Planification » de l'IIA *(Institute of Internal Auditors)* stipule que l'audit interne doit *« établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation ».*
La norme 2010.A1 précise : *« le plan d'audit interne doit s'appuyer sur une évaluation des risques documentée et réalisée au moins une fois par an. Les points de vue de la direction générale et du conseil doivent être pris en compte dans ce processus ».*
Enfin, la norme professionnelle 2020 prévoit que *« le responsable de l'audit doit communiquer à la direction générale et au conseil son plan d'audit et ses besoins pour examen et approbation ».*

… une « nouvelle » recommandation

Dans les « Principes fondamentaux pour un contrôle bancaire efficace » publié en septembre 2012, le Comité de Bâle recommande les diligences suivantes en matière de supervision bancaire :
« L'autorité de contrôle établit que la fonction d'audit interne :

- *s'appuie sur une méthodologie permettant d'identifier les risques significatifs encourus par la banque ;*
- *prépare et réexamine régulièrement un plan d'audit reposant sur sa propre évaluation du risque et répartit ses ressources en conséquence ».*

… une attente en matière de bonne gouvernance

L'IFA (Institut Français des Administrateurs) préconise que *« le Comité d'audit soit impliqué en amont dans l'examen du plan d'audit interne afin de demander d'éventuels compléments de travaux ».*

… et surtout une exigence réglementaire

L'article 9 du règlement CRBF 97-02 mentionne deux horizons en termes de planification :

- *« Les moyens affectés au contrôle périodique […] doivent être suffisants pour mener un cycle complet d'investigations de l'ensemble des activités sur un nombre d'exercices aussi limité que possible ».* Il s'agit clairement là d'une vision pluriannuelle de la planification.
- En outre, il est précisé qu'*« un pro-*

gramme des missions de contrôle doit être établi au moins une fois par an en intégrant les objectifs annuels de l'organe exécutif et de l'organe délibérant en matière de contrôle ».

L'expression « nombre d'exercices aussi limité que possible » peut donner lieu à interprétation et peut donc poser difficulté mais on observe généralement que :

- si les pratiques diffèrent selon les pays, la durée communément admise en France n'excède pas cinq ans ;
- pour certains thèmes spécifiques, tels la lutte contre le blanchiment et le financement du terrorisme, l'homologation Bâle II, le cycle peut être d'un an ;
- les banques raisonnent et communiquent généralement en durée maximale entre deux audits en fonction du niveau de risque de leurs principales activités.

Le plan d'audit : une construction qui nécessite la prise en compte de nombreux éléments

Il est acquis, aujourd'hui, que l'élaboration du plan d'audit doit reposer avant tout sur une cartographie des risques établie par l'audit interne lui-même, en tenant compte, bien évidemment, des « cartographies » de risques élaborées par d'autres fonctions et disponibles au sein de la banque.

Outre cette cartographie des risques, d'autre « sources » peuvent ou doivent nourrir l'élaboration du plan d'audit.
Certaines missions récurrentes sont obligatoirement inscrites au plan d'audit du fait de la régularité nécessaire de ces missions : prestations de services essentielles externalisées, homologation Bâle II, lutte contre le blanchiment et le financement du terrorisme…

Dans le même ordre d'idée, l'attention croissante que porte le régulateur au suivi des recommandations peut conduire à programmer plus ou moins régulièrement des missions dédiées à ce suivi.

Par ailleurs, la stratégie de la banque peut connaitre des infléchissements, des changements (nouvelles orientations, restructuration, migration informatique, cession…) qui peuvent entrainer des demandes spécifiques de missions à intégrer dans le plan d'audit.

Enfin, l'occasion de réaliser des audits mutualisés peut amener à positionner une mission dans le plan, plus en raison de la disponibilité d'intervenants aux compétences techniques rares, par exemple, qu'en fonction d'une lecture directe et stricte de la cartographie des risques.

Il se peut aussi que des contraintes justifiées de l'entité à auditer soient à intégrer dans la construction du plan d'audit, notamment par le repositionnement de la mission à un moment plus opportun. Ce type de situation doit conserver un caractère exceptionnel.

Le plan d'audit, qu'il soit annuel ou pluriannuel, a donc vocation à présenter la totalité des missions d'audit, à l'exception de celles « hors plan » qui résultent par définition d'évènements non prévisibles au moment de l'élaboration du plan.

Peuvent être considérées comme des missions « hors plan », les missions initiées suite à la survenance d'un événement grave ou à la détection par les contrôles permanents d'un incident majeur. Elles peuvent aussi être liées à la création de nouvelles activités, à des opérations d'acquisition …
Sur cette base, le plan d'audit peut être construit en fonction de deux contraintes qui conditionnent sa faisabilité :

- les ressources humaines disponibles qui constituent une contrainte parfois très prégnante dans la planification des audits (rythme des missions, congés, compétences spécifiques disponibles, etc.) ;
- les budgets alloués à l'audit vont aussi guider la construction du plan d'audit ; après avoir calibré les besoins, ce calibrage sera confronté au budget alloué et les arbitrages entre les différentes missions du plan pourront avoir lieu.

Rappelons que le comité d'audit doit être informé de tout changement du plan et notamment des missions qui n'ont pu être réalisées faute de ressources ou suite à des arbitrages liés aux contraintes rencontrées.

Le plan d'audit : une construction en quatre étapes

La construction du plan d'audit se base avant tout sur la cartographie des risques établie par l'audit interne.

La **première étape** dans le passage de la cartographie des risques au plan d'audit consiste donc à traduire le niveau de risque attribué à chaque objet auditable par la cartographie des risques en une fréquence d'audit cohérente. Cette fréquence est le premier critère de programmation des missions dans le *planning* à élaborer par le responsable de l'audit interne.

La **deuxième étape** dans la construction du plan d'audit est la prise en compte des objets auditables dont le niveau de risque n'a pas été évalué au moyen de la cartographie.
Faute de disposer d'un niveau de risque issu de la cartographie pour la détermination de la date à laquelle positionner ces objets auditables dans le plan d'audit, la date sera alors fixée en fonction d'autres critères nécessairement plus subjectifs. A titre d'exemple, une entité récemment acquise sera souvent auditée dans l'année qui en suit la prise de contrôle, alors que pour une nouvelle activité, un délai d'un à deux ans sera parfois nécessaire avant de disposer du recul suffisant pour en effectuer une analyse pertinente.

La **troisième étape** consiste en l'évaluation des moyens humains nécessaires pour la réalisation des missions programmées dans le plan d'audit.
Ce dimensionnement, à la fois quantitatif (nombre d'auditeurs et temps alloué) et qualitatif (domaines et niveaux de compétence, durée d'expérience des auditeurs), sera fonction de critères multiples : le contexte de la mission, le degré de complexité de l'activité ou de l'organisation de l'entité auditée, la taille des équipes auditées et leur implantation, le besoin de compétences spécifiques en matière technique ou linguistique, etc.

Enfin, **la dernière étape** dans la construction du plan d'audit est la mise en cohérence des besoins théoriques déterminés avec les ressources et les budgets effectivement disponibles.

Au-delà de l'élaboration du plan d'audit, sa communication, sa gestion au quotidien et son suivi exigent de la part du responsable de l'audit interne beaucoup de finesse. On peut parler d'ajustement permanent.

Plan d'audit : information, communication et beaucoup de finesse…

La communication sur le plan d'audit est en général prévue dans la charte d'audit interne.
La communication aux organes exécutifs, délibérants ou à leur émanation (un comité d'audit par exemple) peut porter :

- d'une part, sur la cartographie des risques établie par l'audit, notamment pour clarifier les priorités et expliquer les choix effectués pour bâtir le plan d'audit ;
- d'autre part, sur le plan d'audit lui-même pour en obtenir la validation globale ce qui permet de donner un caractère officiel au dispositif. En effet, la norme professionnelle 2020 prévoit que *« le responsable d'audit doit communiquer à la direction générale et au conseil son plan d'audit et ses besoins pour examen et approbation »*.

Pour ce qui concerne la communication du plan d'audit, celle-ci pourra prendre la forme d'une présentation de la programmation des missions sur le cycle d'audit avec un focus sur le plan de l'année à venir.

La communication avec les autres fonctions en charge du contrôle interne est intégrée aux échanges réguliers définis par les règles en vigueur dans chaque banque. Certaines banques ont ainsi institué un comité de coordination du contrôle interne.

La communication avec les autres métiers de la banque est nécessairement plus restreinte compte tenu des spécificités de l'activité de l'audit interne :

- pour des questions d'indépendance liées à la fonction, la cartographie de l'audit ne fait pas l'objet d'un processus contradictoire avec les unités auditées ;
- il ne peut y avoir communication détaillée du plan d'audit aux audités afin de préserver la confidentialité des missions à venir.

En conclusion, l'élaboration et la communication du plan d'audit constituent une saine pratique de gestion. Elles permettent au responsable de l'audit interne de fournir aux instances de gouvernance de la banque une vision globale des risques et de préciser la manière dont les missions d'audit vont assurer la couverture de ces risques. ●

Christiane Legat *intègre, en 1983, le groupe Caisse d'Epargne où elle participe à la mise en place d'un nouveau système de formation.*
Elle rejoint ensuite le service inspection générale en tant que chef de mission.
Cherchant une orientation plus internationale, elle prend la responsabilité de l'audit interne de Rabobank International Paris en 1991.
En 1999, on lui propose le même type de fonction à la Bayerische Landesbank. Elle y approfondit son expertise en matière de titrisation et LBO.
Depuis 2006, elle est Head of Internal Audit de General Electric Corporate Finance Bank (GE CFB).
Titulaire d'un DESS « Banques et Finances », certifiée CFSA, elle préside le groupe professionnel « Banque » de l'IFACI.

Mise en place du plan d'audit dans un groupe d'assurances

Bertrand Lefebvre

Directeur contrôle général, **Covéa**

*Diplômé de Sup de Co Dijon, et d'un 3ème cycle de finance internationale à Londres, **Bertrand Lefebvre** a commencé sa carrière au GAN à New York de 1988 à 1990. De retour en France, il intègre la direction internationale MMA comme analyste économique et financier, avant d'être contrôleur de gestion international puis responsable de zone étrangère. Successivement chef de cabinet du directeur général MMA, puis responsable du reporting et de l'inspection générale MMA entre 1998 et 2006, il dirige depuis 2007 la direction contrôle général Covéa composée de deux directions distinctes : la direction audit interne groupe et la direction contrôle interne et conformité groupe.*

La mise en place d'un plan d'audit est un des trois processus majeurs de la fonction d'audit interne avec l'exécution des missions et le suivi des recommandations. Le plan d'audit se construit au niveau consolidé du groupe et pour chacune des principales sociétés d'assurances. L'élaboration du plan d'audit est un processus structuré et itératif qui vise la meilleure adéquation entre les besoins d'éclairage et d'assurance sur la maîtrise des risques du groupe de la part des différentes parties prenantes, et les ressources disponibles.

Un processus majeur

La mise en place du plan d'audit dans un groupe d'assurances, comme dans toute entreprise, constitue l'un des trois processus majeurs de la fonction d'audit interne. L'exécution des missions et le suivi des recommandations sont les deux autres processus qui en découlent.

Processus majeur, car il doit répondre de façon satisfaisante aux attentes de plusieurs parties prenantes, notamment la direction générale, le comité d'audit, mais aussi l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). La tutelle du secteur banque et assurances a développé récemment des exigences accrues concernant la fonction d'audit interne (cf. schéma ci-après).

L'audit interne doit pouvoir offrir une visibilité pluriannuelle sur son programme d'activité : trois ans est la norme retenue par Covéa. En complément, une mise en perspective sur cinq ans des missions au regard de l'univers d'audit permet d'effectuer une analyse de la couverture des besoins (cinq ans est le cycle d'audit adopté par le groupe). La qualité de cette couverture, et donc de facto du plan d'audit, réside dans la bonne prise en compte des principaux enjeux économiques, opérationnels, réglementaires et, bien entendu, des risques auxquels fait face l'entreprise.

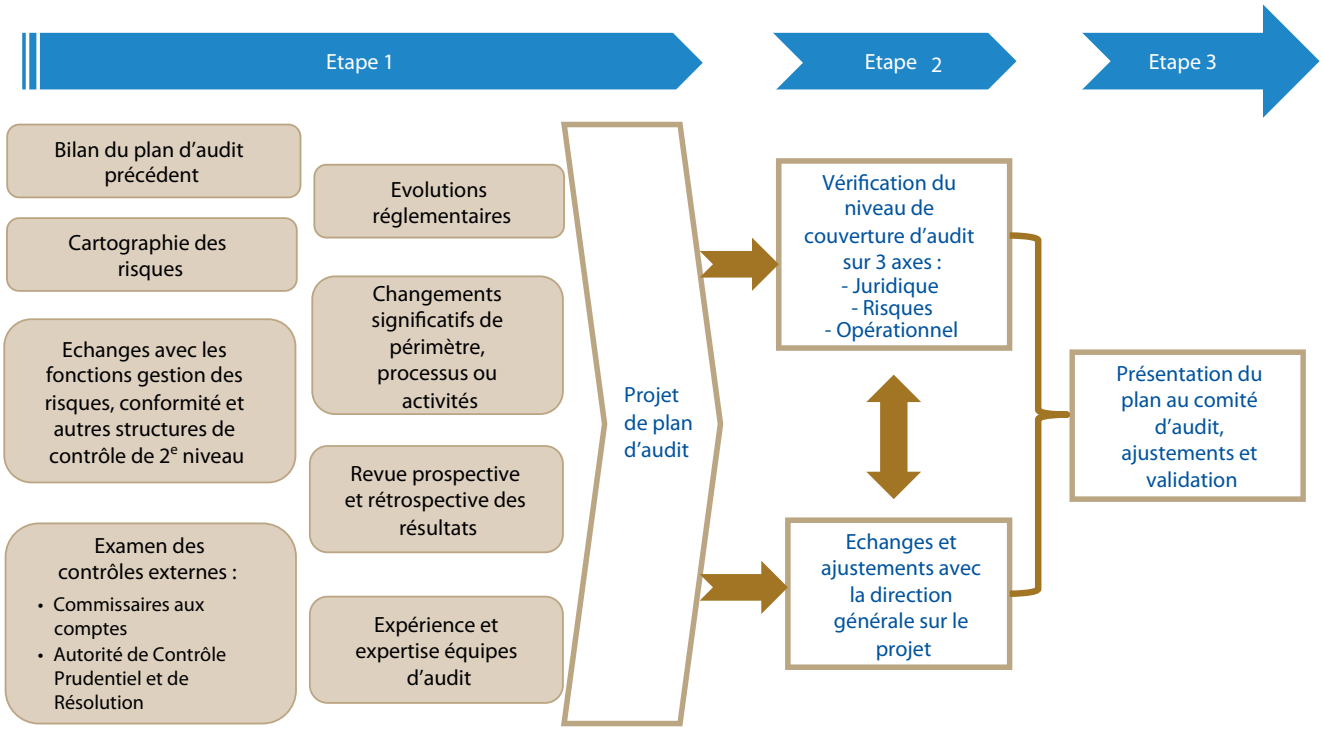
J'ajoute que le plan d'audit, tout comme la couverture des besoins, se construisent tant au niveau consolidé groupe, que pour chacune des principales sociétés d'assurances.

Enfin, gage de l'importance de ce processus, le niveau de couverture de l'univers d'audit et le respect de la déclinaison annuelle du plan figurent parmi les objectifs de notre politique d'audit interne qui sont mesurés et rapportés.

Une approche multidimensionnelle

Même si le plan fait l'objet d'actualisations récurrentes en cours d'année, son élaboration s'inscrit naturellement dans les processus généraux de planification

Schéma simplifié de construction et de validation du plan d'audit



stratégique et budgétaire du dernier trimestre. Ceci afin de bien intégrer les priorités de l'entreprise et d'anticiper du point de vue opérationnel sur les éventuels besoins en ressources externes expertes.

Première source d'alimentation du futur plan d'audit, le bilan du plan précédent : missions non réalisées faute de temps disponible, missions volontairement différées après arbitrage, enjeux non couverts ressortant de l'analyse antérieure…

Deuxième source, la cartographie des risques et les échanges avec les responsables de la gestion des risques, du contrôle interne, de la conformité et des autres structures de contrôle permanent de deuxième niveau. Y a-t-il des risques élémentaires qui s'aggravent ou des risques importants dont le dispositif de maîtrise reste insuffisant de façon notable ? Est-ce que les grandes familles de risques au niveau macro (risques financiers, assurances, opérationnels dont réglementaires, stratégiques et réputation) sont correctement couvertes ? Telles sont quelques-unes des questions que nous devons nous poser.

L'examen des revues intérimaire et définitive des commissaires aux comptes, doublé d'un échange commenté en réunion, permet d'éviter la duplication des travaux et de jouer la complémentarité (prise de connaissance de leur côté de nos missions). Les auditeurs externes se concentrent plus naturellement sur les processus concourant à l'élaboration de l'information comptable et financière.

Autre acteur de la quatrième ligne de maîtrise à prendre en compte, l'ACPR. Avoir connaissance des résultats des contrôles effectués par la tutelle ou de ceux qui sont en cours, conduit parfois à réaliser des arbitrages.

Plus généralement, il convient d'intégrer les préoccupations du régulateur, qui au-delà des législations, publie aussi désormais des recommandations et des instructions. Les thèmes relatifs à la lutte contre le blanchiment et le financement du terrorisme ou de la protection de la clientèle avec ses diverses déclinaisons (contrats d'assurances vie non réclamés, devoir de conseil en assurance vie, dispositif de résiliation des contrats Iard de particuliers dit loi Chatel, traitement des réclamations clients…) ont récemment marqué l'actualité et doivent trouver leur place dans le plan d'audit.

Une revue prospective et rétrospective des objectifs et des résultats des sociétés et des branches d'activités est menée pour faciliter le travail de priorisation. Pour mémoire, il existe, en comptant les filiales étrangères, plus d'une quarantaine de sociétés d'assurance au sein du groupe Covéa et plus d'une trentaine de branches pratiquées : automobile, habitation, assistance, loisirs, santé individuelle et collective, épargne, professions libérales, collectivités, maritime et transport, caution, aviation/spatiale… Les changements significatifs de périmètre ou de management, les évolutions d'activité ou modifications de processus clés sont également pris en considération.

Enfin, les informations collectées par les équipes d'audit de façon formelle ou informelle, l'expérience et l'expertise de

ses responsables vont venir compléter le processus de structuration du plan.
Une première version de plan est établie au niveau du groupe.

La vérification du niveau de couverture d'audit

Ce projet de plan triennal est alors comparé à l'univers d'audit qui se décline chez Covéa sur trois dimensions : l'axe juridique composé des sociétés du groupe, l'axe des risques organisé autour des grandes catégories citées plus haut, et l'axe opérationnel constitué à la fois des grandes fonctions de l'entreprise (cœur de métier, support et pilotage), des branches d'activités assurances et des différents réseaux/canaux de distribution. Les objets de l'univers, sur chacun des axes, sont classés en deux niveaux de priorité en fonction de l'enjeu.

Nous examinons à ce stade les plans d'audit développés par les fonctions d'audit locales qui concernent quelques filiales étrangères et sont supervisées par l'audit interne groupe. Nous vérifions la cohérence des propositions et intégrons ces travaux dans le plan consolidé de la fonction d'audit groupe.

Une simulation de la couverture d'audit est alors établie sur le cycle glissant de cinq ans qui est retenu (plan N+3, années N et N-1). L'analyse aboutit à un taux de couverture, notamment des enjeux prioritaires, que nous comparons à l'appétence inscrite dans la politique d'audit du groupe.
Des rectifications peuvent alors être opérées en vue d'une meilleure adéquation.

Une démarche de validation itérative

Munis de cette proposition de plan, nous rencontrons chacun des membres du comité de direction générale du groupe. Nous échangeons sur le programme que nous avons prévu sur leur périmètre et intégrons leurs remarques, besoins et priorités.

Nous menons ensuite une nouvelle consolidation qui tient compte d'arbitrages avec la direction générale (capacités à faire, priorités temporelles de planification) pour présenter une proposition au comité d'audit et des risques du groupe. Ce dernier peut l'amender en faisant part de ses attentes, avant de formellement valider le plan.
Le plan est alors progressivement mis en œuvre. Bien évidemment, il peut être ajusté en cours d'année pour intégrer des demandes exprimées par la direction générale ou prendre en compte des impératifs difficilement planifiables, comme le pilotage d'audits de *due diligence.*

Les échanges réguliers qui ont lieu toute l'année avec les directions opérationnelles et avec la direction générale sont autant d'occasions de noter des sujets qui émergent, ou au contraire, des enjeux qui deviennent moins sensibles… éléments qui vont nourrir nos réflexions pour la prochaine révision du plan.

En conclusion, l'élaboration du plan d'audit est un processus structuré et itératif qui vise la meilleure adéquation entre les besoins d'éclairage et d'assurance sur la maîtrise des risques du groupe de la part des différentes parties prenantes et les ressources disponibles. Il doit toutefois demeurer suffisamment flexible pour répondre aux urgences et divers imprévus. ●

Les futures normes réglementaires relatives à la solvabilité des organismes d'assurances européens reposent à la fois sur des critères quantitatifs (pilier 1), mais aussi sur des exigences qualitatives en matière de gouvernance (pilier 2), et sur une information des autorités de surveillance et du public (pilier 3). Parmi les exigences du pilier 2 figure l'obligation de mise en place de 4 fonctions clés au sein de l'entreprise : la fonction gestion des risques, la fonction actuarielle, la fonction conformité et la fonction d'audit interne. La directive ne détaille pas les obligations de cette dernière, hormis le respect des principes d'indépendance et d'efficacité. Cependant, l'ACPR à travers ses publications et divers échanges avec la profession, s'attend à ce que la fonction d'audit groupe dispose d'une vision globale des activités d'audit interne. La fonction d'audit interne est en charge de définir le plan d'audit qui doit couvrir suffisamment régulièrement les activités à enjeux.

Covéa est un groupe d'assurance mutualiste leader composé de trois enseignes fortes opérant sur l'ensemble des marchés d'assurances dommages, vie et santé, aussi bien pour la clientèle de particuliers que de professionnels.

Chiffres clés 2012

- 14,7 Milliards € de chiffre d'affaires consolidé *(dont 10 % à l'étranger)*
- 9,6 Milliards € de fonds propres
- 628 Millions € de résultat net
- 392 % de ratio de solvabilité *(norme S1)*
- 10,9 Millions de clients
- 26 600 collaborateurs
- 2 800 points de vente

La mise en œuvre de l'audit interne chez EDF : structure et méthodes

Michel Uhart

Directeur adjoint de la direction de l'audit, **EDF**

La cartographie des risques du groupe EDF comporte environ un millier de risques élémentaires synthétisés en une centaine de méta-risques. Le programme d'audit porte sur une période d'un an et fait l'objet d'une actualisation semestrielle, de façon à refléter au mieux l'actualité du groupe et de son environnement. Le programme fait aussi l'objet d'une concertation approfondie avec les principaux dirigeants du groupe, avant validation par le président et par le comité d'audit.

L'établissement du planning

Le programme d'audit couvre le périmètre audité par la direction de l'audit interne à ce jour, à savoir EDF SA et les filiales contrôlées, hors secteur régulé (EDF Energy, EDF Trading, etc.), ainsi que celui audité par les différentes équipes de la filière audit (Production Ingénierie, Commerce, EDF Energy, EDF Trading, EDF Energies nouvelles, EDF Luminus, Edison). Pour les filiales régulées et co-contrôlées, la DAI s'assure de l'existence d'une politique pertinente de contrôle interne et de la solidité des dispositifs de contrôle interne via les instances de gouvernance.

Le programme d'audit repose sur :

- les **audits d'entités** (filiales, grandes directions), qui comprennent notamment l'examen de la maîtrise du contrôle interne des entités considérées ; les risques de la cartographie qui concernent l'entité sont inclus dans le périmètre ; ces audits (une soixantaine) sont effectués de façon récurrente sur une période de trois à cinq ans, en fonction de la nature et du volume des entités ;
- les **audits récurrents** des processus comptables et financiers et des processus « tête de groupe », essentiellement des processus transverses financiers. les risques de la cartographie qui concernent l'entité sont inclus dans le périmètre ;
- les **audits des grands projets**, liés à l'actualité, donc non récurrents, et qui en règle générale figurent dans la cartographie des risques ;
- les **audits de couverture des risques majeurs** du groupe,qui n'auraient pas été traités par les types d'audits précédents (entité, processus, projet) ; selon une périodicité adaptée à la criticité du risque ;
- le **suivi des décisions du président-directeur général,** dont l'audit doit s'assurer de la correcte mise en œuvre ;
- les audits faisant suite à une première **mission « rouge ou orange »** (risque élevé), et dont la clôture effectuée entre douze et dix-huit mois après, était également rouge ou orange.

Le programme porte sur une période d'un an ; il a vocation à faire l'objet, si nécessaire, d'une actualisation semestrielle de manière à refléter au mieux l'actualité du groupe et de son environnement. La conception et la réalisation du programme sont coordonnées au sein de la filière audit.

Le programme fait l'objet d'une concertation approfondie avec les principaux dirigeants du groupe avant validation par le président et par le comité d'audit.

© Crédit photo : EDF MEDIATHEQUE - DIDIER MARC

La DAI coordonne ses travaux avec ceux des commissaires aux comptes. Au moment de l'élaboration des programmes, nous procédons à des échanges et à des partages d'informations. Au moins deux fois par an, nous leur communiquons les résultats de nos audits ainsi que les rapports dont ils souhaitent avoir connaissance.

Pour la présentation du projet de programme au comité d'audit, la DAI a fait l'examen de la bonne couverture des risques majeurs « rouges » et des méta-risques par les audits réalisés sur les deux derniers programmes, et prévus dans le programme à venir.
En 2013, sur la période de trois à cinq ans, près de 90% des risques « rouges » et de 90% des méta-risques sont couverts par les audits corporate.

La priorisation des risques et des missions

Le cœur du dispositif est la programmation pluriannuelle des audits récurrents d'entités et des audits de processus comptables et financiers. Ils constituent environ la moitié du programme chaque année et permettent de couvrir la quasi-totalité des risques.
L'autre moitié comprend les risques majeurs, naturellement priorisés par leur pondération selon une méthode classique : impact, probabilité, niveau de contrôle, et les projets dont le coût dépasse le seuil d'approbation par le comité des investissements du groupe.

Les audits d'entité permettent d'évaluer la fiabilité des auto-évaluations des dispositifs de contrôle interne. Notre guide d'audit d'entité prend bien sûr en compte les exigences du guide de contrôle interne. Cependant, l'appréciation de la robustesse du contrôle interne n'est pas prise en compte pour déterminer la fréquence d'audit d'une entité.

La validation du plan d'audit

Notre projet de programme, une fois bâti, est présenté pour avis, en février, aux dirigeants du groupe de niveau N-1 COMEX (ce qui représente une soixantaine d'entretiens), ainsi qu'aux membres du COMEX et au président. Une fois tous les avis recueillis et intégrés dans le projet de programme, il est soumis à l'approbation du COMEX, puis du comité d'audit de mars. Ce dernier peut encore apporter quelques modifications.

Ce programme couvre une période allant de mai à avril de l'année suivante.

Toutes les directions d'audit du groupe ont adopté ce calendrier. Je dis bien « toutes les directions d'audit », car, et c'est une particularité dans le groupe, il y a plusieurs directions d'audit. Moi-même je suis responsable de la direction d'audit *corporate* ; il y a des directions d'audit dans certaines de nos filiales les plus importantes, ainsi que dans certaines directions à l'intérieur d'EDF SA, notamment à la production et au commerce. Leur action est complémentaire de la nôtre.

L'actualisation du plan d'audit se fait annuellement au comité d'audit de mars. Certaines missions peuvent être annulées ou reportées : nous en rendons compte au comité d'audit dans notre rapport semestriel. Nous vérifions, lors de chaque rapport semestriel, que notre plan d'audit permet de couvrir, de manière satisfaisante, la cartographie des risques. C'est le cas à plus de 90% pour les risques rouges.

La cartographie des risques

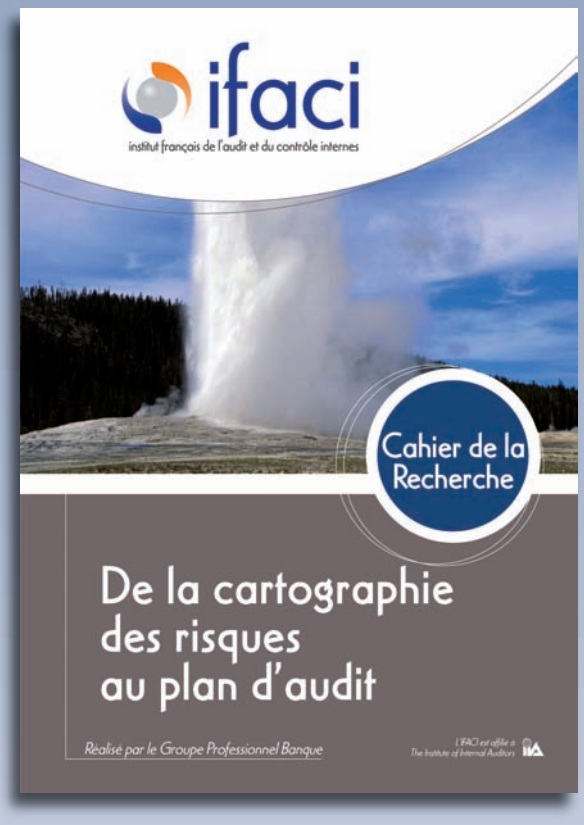
Dans le groupe EDF, il y a une direction des risques et une direction de l'audit, le patron de la direction des risques supervisant la direction de l'audit.

Les *risk managers* exercent le contrôle des risques sur les marchés financiers et sur les marchés de l'énergie ; ils jouent un rôle de deuxième ligne de défense. C'est la direction des risques qui édicte les règles en matière de risques dans le groupe et qui a en charge l'établissement de la cartographie des risques du groupe. Elle présente la cartographie en même temps que nous présentons notre programme d'audit. La cartographie nous sert de base dans le cadrage d'une mission. ●

Michel Uhart *est ingénieur de l'école centrale de Nantes. Il travaille pour EDF depuis 1982 et a exercé la majorité de sa carrière dans l'exploitation des centrales nucléaires. Il a dirigé la centrale nucléaire de Fessenheim, puis celle de Bugey, avant de prendre la fonction de directeur délégué à la maintenance au sein du comité de direction de la division production nucléaire d'EDF. Il a ensuite pris la responsabilité de la direction de l'audit d'EDF, sous l'autorité du directeur des risques et de l'audit, en mai 2010.*

Publications IFACI

Bon de commande



Le groupe professionnel « Banque » publie un cahier de la recherche sur la cartographie des risques par l'audit interne. S'il existe déjà des cartographies des risques établies par d'autres fonctions, la réalisation d'une cartographie par l'audit interne n'en présente pas moins une valeur ajoutée :

- la démarche permet d'acquérir et de formaliser une connaissance approfondie des activités et du fonctionnement de l'établissement ;
- l'analyse et l'évaluation des risques peuvent être conduites de manière indépendante vis-à-vis des métiers ;
- la granularité des cartographies existantes peut ne pas correspondre au niveau de maille des missions d'audit ;
- le champ couvert par ces cartographies est souvent partiel alors que la démarche conduite par l'audit interne permet d'avoir une vision globale de l'établissement et du périmètre auditable ;
- cette vision globale fait de la cartographie de risques réalisée par l'audit interne un outil de dialogue avec les autres prestataires d'assurance.

Le cahier de la recherche vous apportera des bonnes pratiques pour l'élaboration d'une telle cartographie, sa mise à jour et son utilisation pour la planification de l'audit interne.

AUTEUR : Groupe professionnel « Banque » IFACI - **Prix HT : 30 €** (32,10 € TTC)
Décembre 2013 - Format : 16,5 x 23 cm - ISBN : 978-2-915042-53-5

Bon de Commande

Société : .....

Nom : ..... Prénom : .....

Adresse : .....

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

Tél. : ..... Fax : ..... Mél : .....

TITRE	PRIX HT	QUANTITÉ	TOTAL
De la cartographie des risques au plan d'audit	30,00 €		
		Total HT	
		TVA 7 %	
		Net à payer TTC*	

PAIEMENT PAR :

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

DATE : ..... SIGNATURE :

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

Bon de commande à retourner à :
Marie-Thérèse Tran - IFACI
98 bis, bd Haussmann - 75008 Paris
Tél. : 01 40 08 48 16 - Fax : 01 40 08 48 20
Mel : mtran@ifaci.com - Internet : www.ifaci.com

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

La culture d'entreprise, un atout

Les services financiers sont en train d'évoluer. L'équipe d'audit interne d'Aberdeen Asset Management, société de gestion d'actifs du FTSE 100, vient de terminer son premier audit complet de la culture et de la stratégie de l'entreprise. ***Scott Strachan,*** *responsable de l'audit interne, nous explique.*

Texte de Ruth Prickett

Scott Strachan préfère les petites entreprises. Il apprécie la proximité des petites équipes, le contact direct avec les dirigeants et la façon dont les équipes de direction réduites prennent des décisions rapides. Cela peut paraître étrange, sachant qu'il est le responsable mondial de l'audit dans une société qui compte 2 000 collaborateurs dans 24 pays, qui a fait son entrée dans le FTSE 100 l'année dernière et qui gère plus de 222 milliards de livres sterling de fonds investis.

Cependant, lorsque Scott Strachan a rejoint Aberdeen en 1999, il était l'un des deux seuls auditeurs internes de l'entreprise, qui ne comptait alors que 338 collaborateurs. Depuis, la société, qui gère les placements d'investisseurs privés et institutionnels, s'est développée rapidement. Cette croissance s'est faite en partie par le biais d'acquisitions, les plus récentes portant sur les portefeuilles d'actifs et de clients d'Artio Global Investors Inc et de SVG Advisors. Bien qu'elle fasse maintenant partie du FTSE 100, la société a conservé l'essentiel de sa culture d'entreprise et une solidarité propre aux petites équipes, nous explique Scott Strachan :
« Nous avons connu une croissance rapide et nous avons intégré de nombreux actifs et collaborateurs, ce qui nous a amenés à mélanger de nombreuses cultures géographiques et cultures d'entreprise. Depuis toujours, nous sommes conscients qu'il est important de bien accomplir ce processus, mais depuis la crise financière, la culture est davantage mise en avant.
Comme toujours, le secret est de trouver un équilibre. Nous voulons conserver notre dynamisme, notre esprit d'entreprise et notre modèle opérationnel, tout en veillant à maintenir un cadre général de valeurs adéquat. »

> *« Nous faisons tout pour ne pas perdre les aspects positifs de notre culture, tout en veillant à respecter les exigences en matière de gouvernance et de structure de l'entreprise »*

C'est quelque chose auquel Scott Strachan tient. Par chance, il se trouve au bon endroit au bon moment pour contribuer à la préservation de ce bien immatériel. La culture est le maître-mot actuel dans les sociétés de services financiers – et il ne s'agit pas de devenir mécène d'un opéra à Glyndebourne.

Des paroles aux actes

Le rapport de la Commission parlementaire britannique en charge de la réglementation bancaire place la culture et le comportement au cœur des services financiers durables. Tout le monde s'accorde à dire qu'une meilleure connaissance de la culture des entreprises et du comportement des collaborateurs aurait pu contribuer à éviter la crise financière mondiale. Progressivement, le comportement des collaborateurs n'est plus vu comme un risque clé, mais comme un sujet digne d'intérêt pour l'audit interne. Il est toutefois plus compliqué de mettre ces bonnes intentions en pratique.

Ces facteurs, associés au fait que les cadres non dirigeants s'intéressaient à des problématiques liées à la culture d'entreprise, ont incité Scott Strachan à lancer le premier audit complet de la culture et de la stratégie d'Aberdeen. Bien que de nombreuses organisations en parlent, Aberdeen est selon lui l'une des premières entreprises, si ce n'est la première, à mener à bien un audit de ce genre.

Le processus intégrait de nombreux éléments qui sortaient du cadre des audits internes traditionnels (voir le complément ci-après, sur la thérapie comportementale). La longue expérience de Scott Strachan au sein d'Aberdeen et le fait qu'il ait assisté à l'évolution de la société depuis ses débuts, lorsqu'il s'agissait encore d'une toute petite organisation, se sont révélés des atouts considérables pour ce projet :
« Je ne pense pas que j'aurais pu réaliser cet audit il y a huit ans. »

S'il reconnaît qu'il existe un débat à propos de la rotation des responsables d'audit interne et de l'impact d'une telle rotation sur leur degré d'indépendance, il estime également qu'il existe des arguments forts en faveur de la création d'une relation durable entre le responsable de l'audit interne et l'entreprise : *« Vous apprenez à connaître l'équipe de direction, la sensibilité de l'entreprise, et vous développez des relations et des connaissances qui ne s'acquièrent qu'avec le temps. »*

Pour lui, même si Aberdeen affiche un bon taux de fidélisation de ses collaborateurs, la direction et lui-même reconnaissent qu'ils ne peuvent pas se reposer sur leurs lauriers ou ignorer l'importance que revêt l'intégration de nouveaux collaborateurs :
« Nous faisons tout pour ne pas perdre les aspects positifs de notre culture, tout en veillant à respecter les exigences en matière de gouvernance et de structure d'entreprise, à répondre aux attentes et à gérer les perceptions dans ce domaine.
Trouver un équilibre entre ces éléments tout en instaurant le juste niveau d'assurance représente un défi personnel. Je dois rassurer les régulateurs en leur montrant que tous les contrôles et les contrepoids sont en place lorsque nous prenons des décisions. »

« Personne n'a envie de lire un rapport d'audit de 25 pages. En revanche, si vous donnez un rapport d'une page à un dirigeant, il le lira et en comprendra le contenu »

La réputation, encore la réputation, toujours la réputation

Le défi de maintenir une culture propice à la croissance tout en respectant les exigences réglementaires et en préservant l'ethos de l'entreprise alimente le risque global qui plane sur toute société de services financiers : l'atteinte à la réputation. *« Quel que soit le projet sur lequel nous travaillons, nous devons prendre en compte le risque de réputation »*, déclare Scott Strachan. *« Sans confiance, notre modèle économique s'effondre. Et la réputation peut être entachée très rapidement. »*

Outre les principaux risques liés à la réglementation et à la réputation, l'équipe de Scott Strachan – qui compte désormais 23 collaborateurs et bénéficie de l'appui de l'un des quatre plus grands cabinets d'audit – doit également prendre en

considération d'autres risques : *« Prenez n'importe quel risque, vous pouvez être sûr que notre entreprise doit y faire face. »*

Par exemple, l'audit du risque lié aux produits implique de vérifier si les produits sont soumis à des tests de résistance, s'ils sont conformes aux principes d'investissement de l'organisation et s'ils répondent aux besoins des clients. De plus, l'équipe de Scott Strachan doit tenir compte des risques associés à la négociation : *« Tous nos systèmes ont beau fonctionner, si de mauvaises instructions sont données au sujet des transactions ou que celles-ci sont mal exécutées, l'impact peut être significatif. Pas seulement du point de vue financier, mais également vis-à-vis de la réglementation, des clients et de la réputation. »*

Scott Strachan considère que les *traders* malhonnêtes représentent un risque moindre chez Aberdeen, car l'entreprise *« n'érige personne au rang de star »*. Au contraire, l'entreprise a tendance à prendre des décisions collégiales sur la base d'un processus d'investissement bien établi, qui représente pour Scott Strachan un garde-fou essentiel : *« Encore un autre domaine qui émane de notre culture. »*

L'équipe de Scott Strachan est basée dans cinq pays et réalise près de 80 audits par an. Pour faire face aux évolutions rapides, il a développé au cours de l'année écoulée un nouveau processus de planification de ces audits. La société, qui disposait auparavant d'un plan d'audit traditionnel, fonctionne désormais avec un système « 3+9 » :

Thérapie comportementale : comment auditer les éléments incorporels de la culture

Lorsque les régulateurs se sont rendus chez Aberdeen Asset Management à la fin de l'automne dernier, ils étaient désireux de parler de culture d'entreprise, de même que les cadres non dirigeants qui s'étaient penchés sur la question. En consultation avec les dirigeants, Scott Strachan a examiné les risques et a estimé qu'il devait auditer la culture et la stratégie. Le seul écueil était qu'il n'existait que peu de modèles formels à suivre ou à partir desquels effectuer une comparaison.

Scott Strachan a donc fait venir Tim Cox, son responsable pour la zone EMEA (Europe, Moyen Orient et Afrique), et lui a demandé d'en élaborer un.

« J'ai participé à divers forums pour les responsables d'audit interne ces 12 à 15 derniers mois, et il s'agissait d'un sujet de discussion récurrent, mais je n'ai rien pu en tirer de concret », nous explique Tim Cox.

Il a commencé à planifier les travaux en février de cette année. En avril, Scott Strachan et lui ont fait leurs premières présentations aux membres du comité exécutif et à un certain nombre de cadres non dirigeants. Pour l'examen de leurs résultats, ils se sont inspirés d'anciens audits et de débats sur des thèmes bien connus et établis. Ils ont ensuite demandé à leur auditoire de discuter de ces éléments et de leur donner un retour.

Tim Cox explique qu'il s'agissait autant d'encourager la conversation et le débat sur ces thématiques que de fournir des éléments probants de tests formels.
« Ils ont fait preuve d'implication et de soutien, déclare-t-il. Le régulateur fait référence à la manière dont le comportement reflète la culture et aux méthodes d'évaluation du comportement. L'exemplarité est un élément essentiel, c'est pourquoi nous savions qu'il nous fallait convaincre l'ensemble des dirigeants de l'organisation. »

Puis, Tim Cox a rencontré les ressources humaines. C'était une étape importante puisque les éléments clés qu'il avait identifiés comme ayant une influence sur le comportement étaient les descriptions de poste, la politique de rémunération et le processus d'évaluation.

Les discussions ont conduit à améliorer les évaluations. *« Il fallait qu'il y ait un lien clair entre les évaluations et les récompenses et tout devait reposer sur le devoir de rendre compte »*, analyse Tim Cox.

En juillet, il a rencontré le comité d'audit avec Scott Strachan, et grâce au soutien du vice-président, ils ont exposé le plan d'action de l'entreprise et expliqué comment ils comptaient suivre l'avancement.
« Il ne s'agit pas d'un plan en 12 étapes qui sera terminé une fois que ces étapes auront été accomplies », précise Tim Cox. *« Il s'agit d'un processus continu qui devra être suivi sur le long terme et qui évoluera au cours des prochains mois. »*
Scott Strachan ajoute : *« La culture est désormais considérée comme une question essentielle pour l'audit interne. Ces travaux préliminaires et notre approche dynamique nous placent dans une position privilégiée. »*

En outre, la culture sera maintenant prise en compte de manière plus formelle dans d'autres audits. *« Nous allons nous intéresser à la culture de telle unité, nous demander si le comportement de tels gestionnaires de fonds dénote la culture adéquate, et voir si nous avons des dispositifs en place pour encourager cette culture »*, nous explique Tim Cox.

Bien que l'audit ait utilisé des éléments probants du comportement, le processus différait de celui d'un audit interne traditionnel : il était axé sur des présentations et des ateliers plutôt que sur des entretiens individuels, une revue de la documentation et des tests pour produire un rapport.
« Une grande partie de la culture est intangible et de nombreux sujets d'attention ne peuvent pas être audités de manière traditionnelle sur la base de faits concrets », déclare Tim Cox. *« Ce sont ces défis qui rendent ces travaux si intéressants. »*

Scott Strachan approuve : *« Ce genre d'audit fait appel à toute notre expérience et toute notre connaissance de la société, nous permet de les appliquer à des domaines moins directement quantifiables, et nous aide à développer de nouvelles méthodes de conduite de l'audit interne. »*

« Je rends compte directement au comité d'audit et, plutôt que de leur donner un plan annuel, je leur soumets à présent une liste des audits que j'estime devoir être effectués sur les trois prochains mois, ainsi qu'un historique des risques associés.
Puis, je leur expose les sujets d'audit qui sont susceptibles d'être mis en avant dans chaque division sur les neuf prochains mois. Nous n'avons pas d'engagement concernant ces audits, et nous pouvons ainsi changer rapidement notre fusil d'épaule si la situation évolue. »

Une fois les audits réalisés, l'équipe de Scott Strachan rédige des rapports d'une page environ. *« Personne n'a envie de lire un rapport d'audit de 25 pages, un tel document risque d'être ignoré. En revanche, si vous donnez une page à un dirigeant, il la lira et en comprendra le contenu. Il s'agit donc surtout de discuter des problèmes en amont, avant de rédiger le rapport. Ensuite, tout repose sur une bonne communication. Plus vous écrivez, plus vous risquez de perdre le fil et plus les gens sont susceptibles de ne pas comprendre votre message. »*

Scott Strachan rencontre également souvent les régulateurs et les clients. À ses débuts chez Aberdeen, il rencontrait rarement les clients. Aujourd'hui, cependant, ils doivent démontrer qu'ils mettent en place de bonnes procédures de gouvernement d'entreprise et ont donc besoin d'une assurance à transmettre à leurs propres investisseurs et régulateurs.

« Une grande partie de la culture est intangible et de nombreux sujets ne peuvent pas être audités sur la base de faits concrets. Ce sont ces défis qui rendent ces travaux intéressants »

Résoudre les contradictions, Scott Strachan s'y emploie constamment dans sa fonction. Il s'agit d'un auditeur interne qui aime les petites organisations mais qui a tout de même aidé son entreprise à entrer dans le FTSE 100. C'est un comptable qui a lancé l'un des premiers audits du secteur sur l'un des aspects les plus sensibles de l'entreprise – sa culture. Et c'est un responsable qui souhaite préserver les valeurs de son organisation tout en l'aidant à évoluer dans l'identification et le traitement des risques. Les sociétés de services financiers vivent une transition et Scott Strachan nous montre comment l'audit interne peut les aider à bien fonctionner à l'avenir. ●

Article traduit et reproduit avec la permission de Scott Strachan et de l'IIA UK. Cette article a été publié dans sa version originale dans le numéro d'octobre 2013 de la revue Audit & Risk publiée par l'IIA UK.

***Scott Strachan** est membre de l'Internal Audit Leaders' Forum, et président de l'IIA Écosse.*

Scott Strachan en quelques dates clés :

- ***1990 :** Étudie la comptabilité à l'Université d'Abertay. Rejoint le cabinet comptable Frame Kennedy & Forrest à Inverness.*
- ***1993 :** Diplômé de l'Institut of Chartered Accountants of Scotland.*
- ***1994 :** Rejoint Northern Audit Services, par la suite acquis par Coopers & Lybrand, qui a fusionné pour former PwC en 1999.*
- ***2000 :** Rejoint Aberdeen Asset Management en tant que responsable de l'audit interne.*

Le contrôle interne favorise l'apprentissage de l'organisation

Marine Lacourte, étudiante, **IAE de Tours**

Le Prix Olivier Lemant est destiné à récompenser le meilleur mémoire de Master(e) consacré au contrôle interne ou à l'audit interne et réalisé dans une université ou une grande école partenaire.
Les mémoires primés en 2013 sont :

- *1er prix – « Guide d'audit de la mise en conformité du middle office des dérivés de gré à gré : Nouvelle règlementation EMIR » par Loïc Kerboas (IAE Aix-en-Provence)*
- *2ème prix – « Contrôle interne et routinisation des pratiques comptables opérationnelles : un vecteur d'apprentissage ? » par Marine Lacourte (IAE Tours)*
- *3ème prix – « La maîtrise des risques liés au processus de gestion des réclamations clients » par Henri Fritsch (ESC Toulouse)*

Vous pouvez consulter ces mémoires sur le site internet de l'IFACI.

Une réalité économique … et sociale

Le contrôle interne, par son caractère régulier et permanent, génère des routines. Du fait de l'implication d'une multitude d'acteurs, l'action réelle pourra se détacher des schémas officiels et constituer une altération du dispositif. La problématique de l'implication des acteurs de l'organisation devient alors un levier majeur de son efficacité. Ayant subi la pression de divers évènements financiers, le contrôle interne, entre norme et obligation légale, devient un dispositif incontournable pour les organisations, qui doivent, de gré ou de force, le mettre en place et le faire vivre. Le groupe étudié semble adopter une approche opérationnelle empreinte d'une volonté de dynamisme favorisant l'adéquation entre la dimension officielle et les pratiques réelles de contrôle interne. Pourtant, l'intégration de ce dispositif dans les cultures des établissements pourra être freinée si on ne recourt pas à une véritable recherche du sens des actions de contrôle. Une brève revue de la littérature scientifique permet de mettre en avant le dépassement de la dimension fonctionnelle du contrôle, qui se pose aujourd'hui comme un outil de développement des connaissances de l'organisation. Le contrôle interne est critiqué pour son immobilité et l'inertie qu'il peut créer au sein d'une organisation, mais il se fonde aussi sur un retour informationnel indispensable au processus de prise de décision dans l'organisation. Il se dévoile alors comme un vecteur d'apprentissage pour l'organisation.

L'apprentissage organisationnel, pour une amélioration continue du dispositif

Le concept de l'apprentissage organisationnel, emprunté à la psychologie, trouve sa place dans l'amélioration continue du dispositif. Il ne fait pas encore l'objet d'un consensus au sein des sciences de gestion, mais on distingue deux formes majeures d'apprentissage organisationnel : par exploitation et par exploration[1]. La première forme consiste à détecter les erreurs et les corriger pour adapter les actions et les procédures en place au sein de l'organisation. Elle ne remet pas en cause la structure ou les valeurs de l'organisation, contrairement à la seconde forme d'apprentissage, qui brise les routines et favorise la créativité. L'apprentissage par exploitation des connaissances tacites et implicites contenues dans les routines est source de flexibilité et de changement[2]. Le facteur culturel semble aussi être déterminant dans la compréhension et la mise en place effective du dispositif. Les dynamiques organisationnelles sont alors prépondérantes dans la réduction de la dualité entre la dimension officielle et l'action réelle des routines de contrôle interne[3].

Voir, écouter et lire : une méthodologie tournée vers la compréhension

Cette recherche se fonde sur une étude de cas, qui permet non pas d'établir un résultat statistique mais de découvrir des éléments et de comprendre des phénomènes complexes. Elle porte sur les services comptables, garants du respect et de la bonne mise en œuvre du contrôle interne, de trois établissements situés en région parisienne. Inspirée par une démarche mise en œuvre dans des domaines comme l'ethnologie, la sociologie ou l'anthropologie, la méthodologie mise en œuvre ici vise à recueillir et comparer trois natures de données au travers de trois phases : observation des comportements, réactions et pratiques ; entretiens individuels non directifs pour recueillir les déclarations des audités ; et étude de documents officiels (communications internes, procédures écrites, documents légaux, site internet…) pour confronter les éléments précédents à la vision stratégique de l'entreprise.

Un groupe, plusieurs cultures

Suite aux premières observations, il est apparu de fortes disparités culturelles et de pratiques entre les établissements, qu'il a fallu prendre en compte en établissant un profil culturel. L'IFACI a créé, à travers un groupe de recherche, un outil permettant de classifier les organisations selon leur profil culturel[4]. A partir d'une cartographie de ces profils, il est possible de repérer les caractéristiques qui sont les plus proches du terrain. Cet outil a donc été mis en œuvre pour déterminer un profil culturel susceptible d'avoir une influence sur le contrôle interne. Sur ce point en effet, nous avons mis en avant une « confor-

mité superficielle » pour l'établissement 1, entraînée par des jeux politiques internes ; le « contrôle pour le contrôle » dans l'établissement 2, dû à une structure très hiérarchisée ; un « contrôle interne à caractère formaliste » dans l'établissement 3, où l'engagement et la responsabilisation des collaborateurs sont peu marqués.

De la sécurité à l'efficience …

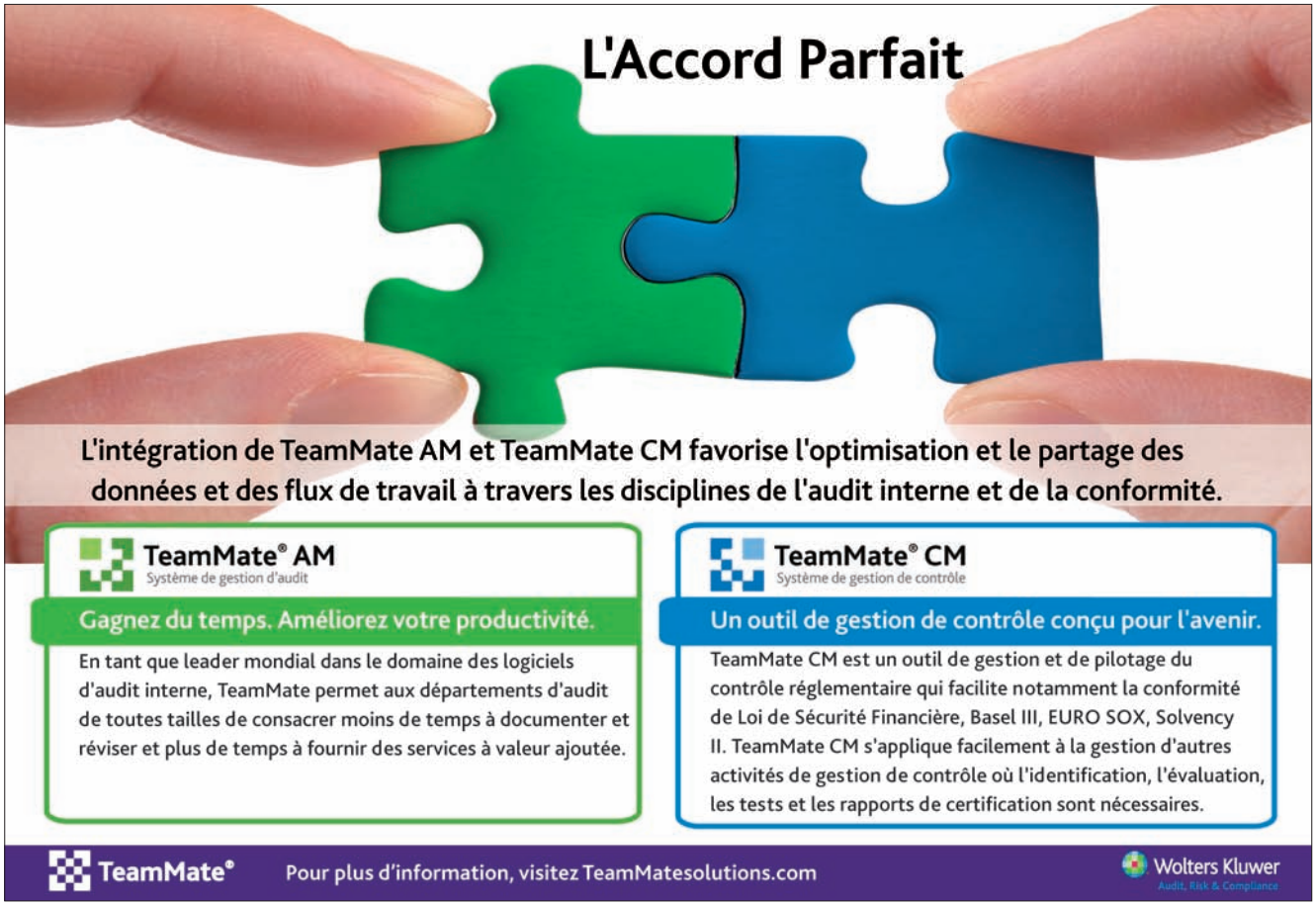
Si les perceptions du contrôle interne sont souvent négatives, insistant sur les contraintes qui y sont liées, les entretiens ont permis de mettre en avant cinq dynamiques organisationnelles favorisant la mise en place du dispositif, tout en soutenant une forme d'apprentissage par exploitation : sécurisation des opérations et des actifs de l'entreprise grâce à un dispositif de prévention et détection des fraudes, protection des salariés et de leur statut contre les éventuelles conséquences d'une mauvaise réalisation de leurs tâches, régulation des activités par l'apport de supports de travail servant de référentiels, compréhension profonde des enjeux liés au dispositif de contrôle interne par la recherche de sens, et une forme d'apprentissage par détection et correction des erreurs et quête de l'efficience.

… l'accompagnement des équipes demeure un levier majeur

Les dynamiques relationnelles complexes, source de responsabilisation et de compréhension vis-à-vis du dispositif, entretiennent et développent son amélioration continuelle et montrent l'importance du soutien et de l'accompagnement des équipes comptables dans la mise en place de ce dispositif. A ce titre, le partage des connaissances entre les employés d'une même fonction dans différents établissements peut permettre de créer ce lien relationnel nécessaire à la compréhension et à l'implication, tout en atténuant, parfois, les relations hiérarchiques.
Le contrôle interne, malgré la perception négative qu'il engendre, est aussi considéré comme un moyen de construire des connaissances et d'utiliser les acquis de l'expérience au sein de l'organisation. Selon les tendances culturelles des organisations et l'appui managérial qui y réside, la bonne mise en œuvre du dispositif de contrôle interne pourra être portée par différentes dynamiques qu'il s'agit d'identifier et de comprendre pour maîtriser leurs portées et les utiliser dans l'amélioration continue du dispositif. ●

[1] *Argyris et Schön, 1978 ; Fiol et Lyles, 1985 ; Senge, 1990 ; Nonaka, 1994*
[2] *Feldman et Pentland, 2003*
[3] *Rerup et Feldmand, 2011*
[4] *Voir Cahier de Recherche « Les variables culturelles du contrôle interne », décembre 2011.*

*Lauréate en 2012 du 2ème prix Olivier Lemant récompensant les travaux de recherche de fin de cycle Master, **Marine Lacourte** est diplômée en Hôtellerie-Restauration et en Management, une double compétence qu'elle a pu mettre à profit en occupant des postes en gestion des ressources humaines, contrôle de gestion et contrôle interne, notamment au sein d'un groupe hôtelier international.*



Publications IFACI

Bon de commande

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

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

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

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

AUTEUR : The Research Foundation (The IIA) / IFACI - **Prix HT : 61,61 €** (65,92 € TTC)
Septembre 2011 - Format : 17 x 24 cm - ISBN : 978-2-915042-33-7

Bon de Commande

Société : .....

Nom : ..... Prénom : .....

Adresse : .....

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

Tél. : ..... Fax : ..... Mél : .....

TITRE	PRIX HT	QUANTITÉ	TOTAL
Manuel d'audit interne	61,61 €		
		Total HT	
		TVA 7 %	
		Net à payer TTC*	

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

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

PAIEMENT PAR :

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

DATE : ..... SIGNATURE :

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

Evénements

Evolution de la réglementation Informatique et Libertés, labellisation et audit interne

Réunion mensuelle du 20 novembre 2013

Les risques liés aux données à caractère personnel

Les données à caractère personnel doivent être traitées avec une attention particulière. En effet leur traitement peut faire courir des risques d'atteinte à la vie privée des personnes concernées. Le dommage réputationnel en cas de violation de la loi est critique. De plus le traitement, encadré par la loi Informatique et Libertés, s'assortit de sanctions pénales et administratives, la CNIL faisant un usage de plus en plus systématique de son pouvoir de sanction et de contrôle.

En application de la loi Informatique et Libertés, les entreprises doivent en particulier : définir la finalité du traitement ainsi qu'une période au-delà de laquelle les données à caractère personnel seront supprimées ; mettre en œuvre les mesures de sécurité nécessaires et suffisantes pour préserver la sécurité des données ; après identification des risques, prendre des mesures pour les réduire, etc. Les différents domaines de la loi Informatique et Libertés vont servir de grille de lecture aux diligences d'audit. Le projet de règlement européen prévoit la désignation d'un délégué à la protection des données, un label européen de protection des données et une obligation de conduire des audits pour démontrer la conformité réglementaire. Ces audits doivent être diligentés par des auditeurs internes ou externes indépendants. Les différentes thématiques à aborder au cours des audits Informatique et Libertés nécessitent l'intégration d'équipes pluridisciplinaires complémentaires : juristes spécialisés sur les questions Informatique et Libertés ; auditeurs des risques et de la sécurité des systèmes d'information, pour évaluer l'adéquation des processus mis en place, tester le déploiement opérationnel des procédures de pilotage de la conformité, et mesurer les niveaux de sécurité du SI pour protéger les données personnelles.

La CNIL et la labellisation

En 2004, la modification de la loi a introduit la possibilité pour la CNIL de délivrer des labels « à des produits ou à des procédures ». Depuis juin 2012, elle délivre ses labels.

L'objectif de la labellisation est d'attester de la qualité des produits et procédures. Elle ne doit pas pour autant aboutir à une standardisation des produits et procédures proposés sur le marché.

L'intérêt du label, pour les organismes, est la possibilité de se distinguer en garantissant un haut niveau de protection des données. Pour les clients, c'est un indicateur de confiance leur permettant d'identifier et de privilégier ceux qui garantissent un haut niveau de protection de leurs données personnelles. Pour la CNIL, c'est un moyen d'encourager les organismes à adopter des pratiques respectueuses de la protection des données.

La durée de validité du label est de trois ans. Le renouvellement doit se faire au moins six mois avant expiration. On trouve la liste des produits et des procédures labellisées sur le site de la CNIL. En cas de non respect des conditions d'utilisation du label, il peut être retiré. ●

Lu pour vous

Finance et Contrôle au quotidien

Sous la direction de : Laurent Cappelletti et Christian Hoarau
Editeur : Dunod

Deux parties : finance d'entreprise et contrôle de gestion. Vingt dossiers – dix dans chaque partie – parmi lesquels : analyse financière ; gouvernance, audit et risque ; gestion du cash-flow et de la trésorerie ; fusions acquisitions ; nouvelles démarches budgétaires ; contrôle, qualité et maîtrise des risques ; réduction des coûts et création de valeur… Dans chaque dossier cinq fiches : problématiques et enjeux ; contexte, normes, acteurs ; outils clés ; démarches et méthodes ; perspectives et prospectives. Soit au total cent fiches, synthétiques et directement applicables.

Cet ouvrage ambitieux, à vocation pratique, fournit à tout directeur, responsable financier ou contrôleur de gestion, les solutions opérationnelles à des problèmes concrets.

n° 206

n° 207

n° 208

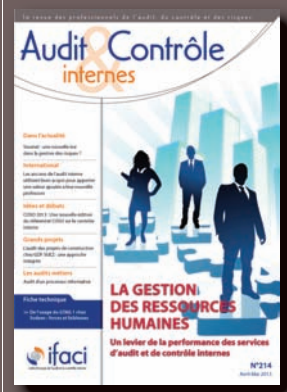
n° 209

n° 210

n° 211

n° 212

n° 213



n° 214

n° 215

n° 216

Audit & Contrôle internes

Retrouvez la liste des articles parus dans la revue « Audit & Contrôle internes » sur le site Internet de l'IFACI www.ifaci.com

☐ **OUI**, je désire recevoir le(s) numéro(s) :

☐ 206
☐ 207
☐ 208
☐ 209
☐ 210
☐ 211
☐ 212
☐ 213
☐ 214
☐ 215
☐ 216

au prix unitaire de 25 € TTC

☐ **OUI**, je souhaite m'abonner à la revue « Audit & Contrôle internes » pour les 5 prochains numéros au prix de :

☐ adhérents IFACI : *inclus dans l'adhésion*

☐ non adhérents IFACI : 105 € TTC

Nom . . . . . Prénom . . . . . N° adhérent IFACI . . . . . .
Organisation . . . . . .
Adresse . . . . . .
. . . . . .
Code Postal . . . . . Ville . . . . . Pays . . . . . .
Date Signature

Paiement par :

☐ chèque bancaire ou postal (à l'ordre de l'IFACI)

☐ virement au HSBC Paris Champs-Elysées - Compte IFACI n° 30056-00148-01485415521-72

☐ carte de crédit - n° . . . . . Date d'expiration . . . . . .

Signature autorisée

ifaci
institut français de l'audit et du contrôle internes

Commande à retourner à :

I F A C I - 98 bis, boulevard Haussmann - 75008 Paris - Tél. : 01 40 08 48 00 - Fax : 01 40 08 48 20 - Mel : institut@ifaci.com

Vous pouvez également commander ou vous abonner à la revue « Audit & Contrôle internes » sur le site Internet www.ifaci.com

ifaci
institut français de l'audit et du contrôle internes

Calendrier 2014

- 20% pour un participant inscrit simultanément à 4 formations

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

IDEA
Data Analysis Software

VERSION NEUF

Passez à la vitesse supérieure avec IDEA V9

Découvrez le plus convivial et le plus performant des outils d'analyse de données, disponible sur le marché

www.caseware-idea.fr

FICHE TECHNIQUE

Audit & Contrôle internes

La prise en compte, par l'audit interne, des risques associés à l'atteinte des objectifs stratégiques

Edwige Duterrage Baudin

Directeur du Pôle Processus Commerciaux, Inspection Générale, **La Banque Postale**

STRATÉGIQUE ! Voilà un terme qui se décline sur tous les tons, dans tous les domaines et relayé avec force grandiloquence par les média. Face à un tel engouement terminologique, il semble raisonnable de revenir aux fondamentaux et de s'interroger sur la notion même de « stratégie », sa définition, son périmètre. En effet, s'il est commun de rencontrer le mot, rares sont les textes qui en explicitent le sens. Un petit exercice de définition montre d'ailleurs que là où le mot « stratégie » est employé, il s'agit davantage de « tactique » qui renvoie à l'emploi de moyens habiles pour atteindre les résultats voulus.

Ceci étant, si le concept même de stratégie a envahi différentes strates de la vie économique et politique, le sujet qui nous occupe ici est celui de l'univers de l'entreprise vu plus spécifiquement par le prisme de l'audit interne.

Objectifs stratégiques : quelle définition ?

Mais d'abord de quoi parlons-nous ? Avec une racine grecque (« stratos » armée et « agein » conduire), le terme de « stratégie » est au sens premier du terme défini comme *« l'art de coordonner l'action de forces militaires, politiques, économiques et morales impliquées dans la conduite d'une guerre ou la préparation de la défense d'une nation ou d'une coalition »*[1]. Le concept premier de stratégie vient de l'univers militaire et nous entraîne à la suite de Carl Philip Von Clausewitz, théo-

Les thèses défendues ici n'engagent que leur auteur et en aucun cas l'organisation à laquelle il appartient.

ricien militaire prussien, dont les théories constituent encore aujourd'hui une quasi référence universelle. Le lecteur pourra penser ici qu'on souhaite l'égarer au hasard de quelque champ de bataille très éloigné des préoccupations de l'audit. Nous sollicitons donc sa patience et son indulgence car les théories de Clausewitz font un découpage de la logique stratégique qui est d'une transposition aisée dans le domaine qui nous occupe. Ainsi, selon lui, la stratégie requiert au préalable un « objectif politique » qui doit être élaboré et fixé au plus haut niveau de l'Etat – on dirait aujourd'hui par l'instance de gouvernance. Ensuite, en fonction de cet objectif, le *modus operandi* se décline selon que l'on vise l'anéantissement immédiat de l'adversaire ou bien son essoufflement sur une plus longue période (stratégie dite de l'usure). On voit donc bien ici que la stratégie sert l'objectif et doit se décliner jusqu'au niveau opérationnel le plus fin de l'organisation.

En s'appuyant, pour les élargir, sur les théories militaires, il est alors aisé de définir la stratégie comme l'art de diriger et coordonner les actions nécessaires à l'atteinte d'un objectif prédéterminé. Cet objectif prédéterminé est donc « l'objectif stratégique » qui va ensuite être décliné au sein de l'entreprise par le biais de différents plans, pour finir par se cristalliser – dans les sociétés commerciales – en objectifs commerciaux.

Il est de la responsabilité de l'audit interne d'évaluer la déclinaison des objectifs stratégiques à tous les niveaux opérationnels

La déclinaison des objectifs stratégiques au sein de l'entreprise

Pour toute société commerciale, l'orientation stratégique évidente est la réalisation de bénéfices : il s'agit pour l'entreprise d'engranger les fonds propres nécessaires au financement de sa politique et donc à la fin des fins à sa propre pérennité. Dans ce contexte, l'entreprise va observer des arbitrages et des positionnements à moyen et long terme en fonction de l'appréciation qu'elle a de son environnement et du potentiel économique qu'il représente pour elle : ce sont ses objectifs stratégiques.

Une fois définis, les objectifs stratégiques doivent être déclinés à tous les niveaux de l'entreprise pour lui permettre de se mettre en ordre de marche et d'assurer le succès de son « *business plan* ». Cette déclinaison peut passer par les phases suivantes :

1- **les valeurs :** identification des grands principes qui doivent impérativement guider l'entreprise dans la mise en œuvre de sa stratégie (éthique, développement durable, etc.) ;

2- **les acteurs :** identification des directions / départements responsables de la déclinaison des objectifs stratégiques ;

3- **les indicateurs :** fixation des grands indicateurs de suivi des objectifs stratégiques qui vont permettre de mesurer le degré de réalisation ;

4- **la planification :** définition de la trajectoire et des jalons qui seront des temps de bilan intermédiaire ;

5- **les risques :** analyse des éléments endogènes et exogènes qui peuvent constituer autant d'obstacles à la bonne réalisation des objectifs stratégiques et mise en place des dispositifs de maîtrise des risques. Les modalités pratiques d'application nous indiquent ici qu'il incombe à la direction générale d'identifier et de gérer ces risques.

Une fois ce contexte de déclinaison des « objectifs stratégiques » établi, il faut s'interroger sur le rôle que tient l'audit interne dans ses missions de contrôle et surtout à quel niveau il intervient, étant entendu que l'on attend légitimement de lui qu'il aide l'entreprise à atteindre ses objectifs « *en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise, en faisant des propositions pour renforcer leur efficacité* »[2].

L'évaluation par l'audit des risques liés à l'atteinte des objectifs stratégiques : le contrôle de l'exécution de la stratégie

On vient de voir que les objectifs stratégiques en eux-mêmes ne sont rien d'autre que des arbitrages et des postures assumées de l'entreprise au regard de son environnement économique. Ces choix sont de l'évident ressort des Présidents et de leurs comités exécutifs, ils sont arrêtés au plus haut niveau de

l'organisation : on parle ici de vision et de projet d'entreprise. Il ne revient pas à l'audit interne d'évaluer l'opportunité des décisions et postures des dirigeants d'entreprise et ce d'autant plus qu'il existe un certain nombre de contrepoids liés à la structure même des organisations qui permettent de challenger les choix des dirigeants (assemblée des actionnaires, conseil d'administration, de surveillance, etc.).

S'il semble ainsi difficile pour l'audit interne de prévoir ce type de missions de contrôle d'opportunité, il est en revanche pleinement de son rôle d'évaluer la déclinaison des objectifs stratégiques à tous les niveaux opérationnels. Ainsi, la norme de référence 2120.A1 rappelle-t-elle que l'audit interne évalue les risques afférents au gouvernement d'entreprise, aux opérations et aux systèmes d'information de l'organisation au regard notamment de l'atteinte des objectifs stratégiques de l'organisation.

L'audit est tout à fait fondé à vérifier la transposition des objectifs stratégiques en véritables plans opérationnels et indicateurs (plan marketing, objectifs commerciaux). Il s'agit ainsi de s'assurer qu'au bon niveau de l'organisation les managers « clés » sont parfaitement informés et ont bien appréhendé les « quoi », « pourquoi », « comment », « quand », « qui » de la politique stratégique et qu'ils ont décliné cette politique dans leur périmètre. En clair, il s'agit de vérifier que les objectifs stratégiques ont bien été convertis en actions opérationnelles et mesurables à tous les niveaux de l'entreprise.

L'appréhension par l'audit des objectifs stratégiques

Les MPA 2120-3 indiquent que « *l'audit devrait avoir connaissance de la stratégie de l'organisation, de la manière dont elle est mise en œuvre, des risques qui lui sont associés et de la manière dont ils sont gérés* ».

L'audit doit évidemment être informé des objectifs stratégiques de l'entreprise. Le plus couramment cette stratégie prend la forme de plans pluriannuels que la présidence élabore et diffuse à tous les niveaux de l'entreprise. L'audit bénéficie ainsi à l'instar des autres départements d'une communication du « plan stratégique », des « ambitions » ou de la « trajectoire » de l'organisation. La stratégie de l'entreprise pour mener au succès doit emporter l'adhésion de tous les collaborateurs, elle doit être « embarquée » – comme on le dit aujourd'hui – dans toute activité quotidienne pour

La planification est un élément essentiel pour la gestion et l'efficience de l'audit interne. Ainsi, la Norme 2010 de l'IIA précise que « *le responsable de l'audit interne doit établir un plan d'audit fondé sur les risques afin de définir des priorités cohérentes avec les objectifs de l'organisation.* » Afin de définir les priorités en cohérence avec les objectifs, le responsable de l'audit interne recueille les points de vue de la direction générale et du conseil (Norme 2010.A1).
Pour établir un plan d'audit fondé sur les risques, le responsable de l'audit interne prend en compte les risques, mais également les menaces. Il peut s'appuyer aussi sur l'univers d'audit et les contributions de la direction générale et du conseil (MPA 2010-1). Le management des risques permet au responsable de l'audit interne d'ajuster et de réviser son plan d'audit interne (MPA 2010-2). La MPA 2120-3, publiée cet été, vient compléter la liste non exhaustive des éléments à prendre en compte dans la planification, à savoir les risques spécifiques à l'atteinte des objectifs stratégiques. Les systèmes d'information devenant de plus en plus prégnant dans les organisations, le responsable de l'audit interne peut définir la part des audits des SI dans le plan d'audit (GTAG 4 – Management de l'audit des SI) ou alors choisir d'élaborer un plan d'audit spécifique aux SI (GTAG 11 – Elaborer un plan d'audit des SI).
L'IFACI traduit et met à jour régulièrement le Cadre de Référence International des Pratiques Professionnelles de l'audit interne. Pour retrouver l'intégralité du CRIPP et notamment les Normes, MPA et GTAG liés à la planification, rendez-vous dans la bibliothèque en ligne du site Internet de l'IFACI.

devenir une force mobilisatrice des équipes. On peut ainsi légitimement s'interroger sur les chances de succès d'une stratégie confidentielle. Toutefois, dans l'hypothèse où une organisation ne choisirait pas de communiquer sur sa stratégie, le directeur de l'audit interne doit a minima bénéficier d'une information spécifique qui lui permettra d'orienter ses missions. Dans le cas contraire, le risque est grand d'avoir un audit cantonné dans sa Tour de Babel, au mieux réduit à une analyse des risques mineurs de l'entreprise, au pire susceptible de réaliser des analyses en contradiction avec ses orientations stratégiques.

La stratégie : clé impérative de lecture de l'univers d'audit

Si l'on part du principe que l'audit interne bénéficie d'une parfaite connaissance des objectifs stratégiques, ceux-ci doivent dès lors devenir une clé de lecture de l'univers d'audit. En effet, l'ensemble des missions de contrôle va être conduit avec en toile de fond les objectifs stratégiques. En procédant à une investigation au sein d'une unité opérationnelle – une ligne « métier » par exemple – via un processus ou plus spécifiquement sur une thématique, l'audit va nécessairement utiliser, entre autres, le prisme des objectifs stratégiques pour faire son analyse de risque. Ceci étant, le directeur de l'audit peut également estimer que la déclinaison des objectifs stratégiques doit faire l'objet d'une mission dédiée pour précisément faire un état des lieux global de la mise en œuvre de la stratégie en s'assurant que tous les risques ont bien été identifiés et font l'objet d'un dispositif de maîtrise. Dans cette hypothèse, une telle mission sera inscrite au plan d'audit.

Par conséquent, on voit bien que pour construire son plan de contrôle, l'audit va nécessairement prendre en compte les objectifs stratégiques : ils seront un élément de construction de la cartographie des risques de l'audit. Cette cartographie des risques constitue *« une démarche dynamique d'identification et d'évaluation des risques qui permet d'en donner une représentation synthétique et visuelle. Elle constitue ainsi un outil de mise en évidence des risques à couvrir en priorité »*[3], au sein duquel évidemment les risques stratégiques ont toute leur place.

Par conséquent, on le voit bien ici, les objectifs stratégiques doivent être nécessairement pris en compte par l'audit interne. Toutefois, l'audit doit veiller à ne pas se laisser happer par le tourbillon stratégique. En effet, le contexte économique d'hyper-compétitivité organise le cercle vicieux de l'hyper-compétition où les organisations sont en permanente mutation, transformation. La remise en cause des équilibres naturels devient l'écosystème habituel de l'entreprise et l'ensemble des collaborateurs est prisonnier de la « roue du hamster » : c'est la course permanente à la créativité marketing et commerciale. L'audit interne doit alors être un facteur de stabilité capable de remettre l'accent sur des risques dits « classiques » mais qui, relégués en arrière plan, peuvent devenir majeurs. Le cœur de métier de l'audit reste la maîtrise des risques financiers, opérationnels et d'entreprise ; la stratégie apporte un éclairage tel une ligne d'horizon vers laquelle il faut tendre, qui permet alors à l'audit de s'inscrire dans une dimension d'analyse de risques prospective. ●

---

[1] *Définition de l'encyclopédie Larousse.*
[2] *International Professional Practices Framework.*
[3] *Définition donnée par le Cahier de la Recherche « De la cartographie des risques au plan d'audit - Groupe Professionnel Banque » publié par l'IFACI.*

Edwige Duterrage Baudin *est actuellement directeur du pôle processus commerciaux de l'inspection générale de La Banque Postale. Diplômée d'un DEA de droit communautaire, elle a commencé sa carrière au secrétariat général de la Commission Européenne. En 2002, elle intègre la direction des affaires juridiques et fiscales de HSBC France. Elle rejoint ensuite La Banque Postale en 2007 où elle a exercé différentes fonctions à la direction de la conformité et à la direction des opérations avant d'être nommée à l'inspection générale.*