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

Audit & Contrôle internes

NUMÉRO SPÉCIAL

LES OUTILS INFORMATIQUES AU SERVICE DES AUDITEURS ET DES CONTRÔLEURS INTERNES

Leurs fonctionnalités et leurs atouts

ifaci
institut français de l'audit et du contrôle internes

N°212
Novembre - Décembre 2012

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™.

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°212 - novembre-décembre 2012

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 2012
Crédit photos : © Sergey Nivens - Fotolia.com

Prix de vente au numéro : 22 € TTC

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

ifaci
institut français de l'audit et du contrôle internes

Les articles sont présentés sous la responsabilité de leurs auteurs.

Les outils informatiques au service des auditeurs et contrôleurs internes

Tout le monde s'accorde à dire que le professionnalisme des auditeurs internes est essentiel pour la crédibilité et la légitimité de leur fonction. Une formation continue et adaptée aux besoins de chacun, couronnée ou non par une certification individuelle (CPAI ou CIA) s'avère de ce point de vue indispensable.

Tout aussi nécessaire apparaît aujourd'hui l'utilisation, par les services d'audit et de contrôle internes, d'outils informatiques appropriés. Afin de vous permettre de faire le bon choix, nous présentons, dans le dossier de ce numéro, un tableau des principaux outils que l'on trouve actuellement sur le marché, accompagné des témoignages précieux d'utilisateurs de certains d'entre eux. Pour un complément d'information, je vous invite à vous reporter sur notre nouveau cahier de la recherche « *Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet* » qui sera sur le site internet de l'IFACI dès ce mois-ci.

Dans la rubrique « Dans l'actualité », en partant de nombreux exemples de dirigeants forcés de démissionner pour comportements condamnables, il est mis en avant que le « *tone at the top* » n'est pas qu'une notion théorique mais une composante importante de l'environnement de contrôle, qui doit être auditée et évaluée par l'audit interne. Parmi ces comportements condamnables, il y a la question des conflits d'intérêts dont on lira avec le plus grand intérêt l'article qui lui est consacré.

J'attire également votre attention sur les principales évolutions, en 2013, des Normes de l'IIA ainsi que sur la présentation du nouvel ouvrage de Jacques Renard « *Comprendre et mettre en œuvre le Contrôle Interne* », vaste sujet toujours d'actualité.

A vous tous, lecteurs de la revue « Audit & Contrôle internes », je souhaite ainsi qu'à ceux qui vous sont chers de très bonnes fêtes de fin d'année. ●

Louis Vaurs - Rédacteur en chef

ifaci
Certification

Progressez sur des bases solides

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

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

DOSSIER

Les outils informatiques au service des auditeurs et contrôleurs internes

Leurs fonctionnalités et leurs atouts p. 11 à 36

Exemplarité du management : contre-exemples récents

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

L'actualité récente a fourni une longue liste de cas de dirigeants forcés de démissionner de manière brutale, dans des secteurs et des pays très différents. Les derniers exemples en date, presque simultanés, datent du mois de novembre : le directeur de la CIA, le général Petraeus, a ainsi dû quitter son poste après la révélation d'une liaison extra-conjugale. Au même moment, Christopher Kubasik, le futur DG de Lockheed-Martin, quittait la société, là encore pour des relations « inappropriées » avec l'une de ses collègues. Auparavant, toujours début novembre, l'on avait appris le départ du ministre russe de la Défense, Anatoli Serdioukov, officiellement pour corruption lors de l'attribution de marchés. Officieusement, d'autres explications ont circulé sur les motifs de ce départ[1]. Ces trois départs font écho à ceux de ministres chinois et indiens survenus ces derniers mois, les plus marquants étant ceux du ministre des transports chinois pour « conduite inappropriée » (c'est à dire corruption), et du ministre des télécommunications indiens, là aussi pour corruption. Les deux sont actuellement en prison.

Des points communs malgré des différences

Ces différents cas, s'ils sont très différents, ont tous un point commun : dans tous les cas, les dirigeants se sont vus reprocher leur manque d'exemplarité, en étant pris en défaut sur des points où ils auraient dû être exemplaires. Analysons les rapidement.

Si la liaison extra-conjugale du général Petraeus a été prise si au sérieux, ce n'est pas par pudibonderie ou excès de morale : c'est parce qu'il est demandé aux agents de la CIA de ne pas avoir de liaison extra-conjugale pour ne pas risquer d'être victimes de pressions ou de chantage. Le général Petraeus, en tant que directeur de la CIA, l'exigeait de ses collaborateurs. Il lui a donc été reproché d'être le premier à ne pas respecter les règles contraignantes qu'il imposait à ses agents.

La situation est similaire pour l'ex-futur DG de Lockheed-Martin. Lockheed-Martin est l'une des premières industries de défense au monde. Ce secteur a connu ces dernières années de nombreuses affaires de corruption et d'espionnage industriel et commercial. En tant que DG d'une des deux premières entreprises du secteur, C. Kubasik se devait donc d'être exemplaire, en prouvant qu'il ne tolérait pas de comportements contraires à la charte d'éthique et au code de bonne conduite de la société. Le fait d'enfreindre le code de conduite avant même d'être nommé directeur général l'a déconsidéré.

Le cas d'A. Serdioukov peut s'analyser de la même façon. En tant que ministre de la défense, A. Serdioukov a en effet beaucoup lutté contre la corruption qui régnait au sein du ministère ; il donnait l'image de vouloir améliorer le quotidien des soldats russes en mettant un terme au pillage en règle des ressources et matériels de l'armée. Or, il lui est officiellement reproché d'avoir détourné 80 millions d'euros, et d'avoir fait traîner des travaux de construction de logement pour le personnel du ministère : ce sont précisément les deux points sur lesquels il se devait d'être exemplaire.

La chute du ministre des transports chinois résulte du même mécanisme. Les réseaux de transport, notamment ferroviaires, sont en effet vus comme une vitrine de la réussite du modèle économique chinois, tant en interne que vis-à-vis de l'étranger. La corruption dont est accusé Liu Zhijun (qui semble avérée) est aggravée par les circonstances dans lesquelles elle est intervenue. Liu Zhijun

est en effet accusé d'avoir bénéficié de pots-de-vin d'entreprises attributaires de marchés publics. L'une des contreparties de ces pots-de-vin aurait été un assouplissement des contrôles qualité, permettant aux sociétés attributaires des marchés de livrer des matériels (notamment ferroviaires) qui ne respectaient pas les exigences fixées par les cahiers des charges. L'une des conséquences de cette corruption aurait été un nombre élevé d'accidents sur le réseau ferré, le plus emblématique étant celui du TGV survenu en 2011. Ce qui est reproché au ministre n'est donc pas tant le fait d'avoir touché des pots-de-vin, que d'avoir consenti à une baisse du niveau de sécurité et de qualité du réseau de transport, et d'avoir ainsi mis en péril la sécurité des passagers et l'image de marque du régime.

On retrouve la même logique dans l'affaire de l'attribution des licences de téléphonie mobile en Inde. Le gouvernement indien a attribué en 2010 des licences de téléphonie mobile à des opérateurs, essentiellement étrangers. Le ministre des télécommunications de l'époque est accusé d'avoir grossièrement sous-évalué la valeur de ces licences, en percevant au passage quelques dizaines de millions de dollars. Or, cette mise aux enchères des licences de téléphonie était un projet emblématique du gouvernement indien, contrôlé par le parti populiste BJP : elle était censée montrer que l'Etat cédait au prix fort certaines ressources de la nation, afin de financer des projets de développement en faveur du plus grand nombre. Le vrai reproche fait au ministre n'était donc pas d'avoir empoché au passage quelques dizaines de millions de dollars, mais de l'avoir fait en faisant perdre au budget de l'Etat plusieurs dizaines de milliards de dollars, au profit de sociétés étrangères ou de magnats locaux. Pour un gouvernement populiste, se voulant au service des masses et faisant de la justice sociale et du développement économique ses priorités, il s'agit là d'un crime impardonnable.

Quels enseignements en tirer pour l'audit et le contrôle internes ?

Ces affaires rappellent tout d'abord que l'exemplarité du management, le *« tone at the top »*, n'est pas qu'une notion théorique. Il s'agit au contraire d'une composante essentielle de l'environnement général de contrôle, qui doit donc être auditée et évaluée par les auditeurs internes. Cette évaluation est parfois délicate, notamment lorsque l'audit interne ne dispose pas de l'indépendance nécessaire. Certains points peuvent cependant être systématiquement audités par les auditeurs internes pour apprécier l'exemplarité du management : la politique de rémunération, le contrôle des frais professionnels, le respect des procédures d'achats, l'existence de parties liées… Même s'ils sont parfois vus comme des contrôles de conformité, tous ces domaines ont une importance particulière dans la mesure où ils peuvent révéler une faille dans l'environnement général de contrôle.

Le deuxième enseignement est que l'exemplarité du management est une notion qui peut varier selon les contextes, les mêmes faits pouvant être considérés comme acceptables ou bénins dans un contexte donné, et graves dans un autre. L'auditeur doit donc analyser avant sa mission les points sur lesquels on attend du management qu'il soit exemplaire, et les auditer.

Enfin, le troisième enseignement de ces affaires est que la meilleure garantie de l'exemplarité du management est sans doute le fait de le soumettre à des contrôles indépendants réguliers. Ainsi, à la demande de leur Conseil d'administration, certaines sociétés (souvent américaines) décident de faire auditer tous les ans la rémunération et les frais professionnels de leurs dirigeants ; ces audits sont réalisés soit par l'audit interne, mandaté par le Conseil ou le Comité d'audit, soit par des auditeurs extérieurs. De même, certains groupes internationaux font auditer tous les ans les achats du siège social : les enjeux sont limités en termes financiers, mais ces audits visent à garantir que les achats réalisés à haut niveau, par la direction du groupe, sont bien exemplaires. Des audits similaires peuvent être organisés sur la politique de recrutement, de promotion et d'évaluation des cadres.

De façon plus générale, ces affaires viennent valider les orientations données par les législations récentes, qu'il s'agisse de la 8ème directive européenne, de la loi américaine Sarbanes-Oxley ou de ses déclinaisons locales au Japon, en Corée, en Suisse... : toutes ces législations insistent en effet sur l'importance pour le Comité d'audit d'orienter et de suivre l'activité de l'audit interne, qui doit pouvoir être un outil donnant au Conseil d'administration l'assurance de l'exemplarité de la direction générale qu'il a nommée. ●

[1] *M. Serdioukov est le gendre de M. Zoubkov, ancien premier ministre et proche très influent de V. Poutine. La presse spécialisée a suggéré que les vraies raisons de son départ seraient d'ordre purement privé.*

Gouvernance et éthique

Comment prévenir les conflits d'intérêts dans la vie publique ?

Sylvie Le Damany

Avocat et associée, **cabinet JeantetAssociés** *(Contentieux, Gouvernance, Risques et Conformité)*

Les entreprises de dimension internationale connaissent bien le sujet des conflits d'intérêts, notamment dans le cadre de la lutte contre la corruption. Des programmes de sensibilisation sont mis en place sur une grande échelle (diffusion de chartes éthiques, codes de conduite, référentiels de déontologie…). On peut regretter que dans la sphère de la vie publique, en France, les mesures préventives préconisées tardent à voir le jour. Des projets de loi devraient être soumis au Parlement en 2013, particulièrement en matière de prévention des conflits d'intérêts dans la vie publique.

La question des conflits d'intérêts tant dans le secteur privé que public est une préoccupation majeure dans le monde entier

Les entreprises de dimension internationale connaissent bien le sujet des conflits d'intérêts notamment dans le cadre de la lutte contre la corruption. En la matière, des programmes de sensibilisation sont mis en place au moyen de la diffusion de chartes éthiques, codes de conduite, référentiels de déontologie, voire de vastes compliance programmes destinés aux collaborateurs et parties prenantes des entreprises sur ces questions sensibles qui sont loin d'être théoriques. Le rappel des textes réglementaires applicables aux activités (Foreign Corrupt Practices Act, UK Bribery Act...), des règles et procédures internes est le minimum requis pour alerter et informer les personnes les plus exposées dans leurs activités professionnelles. Les procédures d'alerte et les programmes de formation elearning deviennent pratiques courantes au sein des entreprises, tous secteurs confondus, alors que ces sujets continuent d'alimenter l'actualité.

Conflit d'intérêts et corruption

Le lien entre le conflit d'intérêts et la corruption est un sujet en soi. Il peut exister un conflit d'intérêts sans pour autant que le délit de corruption soit commis. Cela étant, si les conflits entre les intérêts privés et les missions publiques des agents publics ne sont pas convenablement gérés, il peut y avoir corruption[1].

Si l'on constate que la prévention des situations de conflits d'intérêts fait bien partie intégrante des politiques anti-corruption des entreprises internationales, il faut regretter que dans la sphère de la vie publique, les mesures préventives préconisées tardent à voir le jour en France.

Qu'est-ce qu'un conflit d'intérêts ?

Nous pouvons nous référer à la définition suivante :

« Un conflit d'intérêts naît d'une situation dans laquelle un agent public a un intérêt personnel de nature à influer ou paraître influer sur l'exercice impartial et objectif de

ses fonctions officielles. L'intérêt personnel de l'agent public englobe tout avantage pour lui-même ou elle-même ou en faveur de sa famille, de parents, d'amis ou de personnes proches, ou de personnes ou organisations avec lesquelles il ou elle a ou a eu des relations d'affaires ou politiques. Il englobe également toute obligation financière ou civile à laquelle l'agent public est assujetti »[2].

Toutefois, cette notion de conflit d'intérêts ne doit pas être limitée au secteur public. Le Service central de prévention de la corruption (SCPC), placé auprès du ministre de la Justice, donne une définition qui peut s'étendre au secteur privé :

« Un conflit d'intérêts naît d'une situation dans laquelle une personne employée par un organisme public ou privé possède, à titre privé, des intérêts qui pourraient influer ou paraître influer sur la manière dont elle s'acquitte de ses fonctions et des responsabilités qui lui ont été confiées par cet organisme ».

L'intérêt personnel est compris de façon très large. Il peut être direct ou indirect, concerner la personne et elle seule (intérêt propre) ou ses proches. L'intérêt peut être de nature économique, financière, politique, professionnelle, confessionnelle ou sexuelle.

Le SCPC identifie :

- **Le conflit potentiel :** il n'existe pas encore de conflit proprement dit, dans la mesure où il n'existe pas à ce moment de lien direct entre les intérêts de la personne et sa fonction. Néanmoins, un changement dans sa situation (prise de fonctions, promotion, mutation) pourrait créer ce conflit.
- **Le conflit apparent :** les faits en cause ne sont pas certains : aucun intérêt particulier suspect n'a pu être prouvé, il n'est que « possible ». Une analyse de la situation devra être menée pour écarter tout doute sur la probité de la personne suspectée.
- **Le conflit réel :** lorsqu'il est « avéré » qu'un intérêt personnel peut venir « influencer » le comportement de la personne exerçant ses fonctions professionnelles.

En France, les commissions, les rapports et les recommandations se succèdent…

Il est intéressant de relever que le SCPC a développé des actions de formation et de sensibilisation destinées aux secteurs public et privé[3]. Cela ne suffit pas néanmoins.

Transparency International France (TI France), présidé par Daniel Lebègue, a émis des recommandations destinées à prévenir les conflits d'intérêts dans la vie publique française[4]. A l'issue de l'année 2010, les recommandations ont été présentées au groupe de travail de l'Assemblée nationale alors en charge du sujet, puis début 2011 à la Commission des lois du Sénat. Le rapport plaide pour une déontologie renforcée avec l'instauration de sanctions pénales qui s'appliqueraient en cas de violation des règles édictées.

« Il peut exister un conflit d'intérêts sans pour autant que le délit de corruption soit commis. »

Le point principal est l'adoption d'une loi qui définit la notion de conflit d'intérêts dans la vie publique et impose des obligations aux élus, membres du gouvernement et fonctionnaires d'autorité :

- **obligation d'établir une déclaration préalable d'intérêts,** mise à jour annuellement et rendue publique, qui indiquerait l'ensemble des fonctions et mandats, rémunérés ou non, occupés actuellement ou au cours des cinq années écoulées, les revenus et avantages en nature tirés de ces activités ainsi que les activités des conjoints ;
- **obligation de déclarer tout risque de conflit d'intérêts** avant toute délibération ou décision sur un sujet pour lequel l'intéressé a – ou semble avoir – des intérêts personnels ;
- **obligation de s'abstenir de participer à la délibération et à la décision.**

TI France a proposé la création d'un code de déontologie et une fonction de déontologue pour chaque catégorie d'acteurs publics (membres du gouvernement, parlementaires, élus locaux, fonctionnaires) qui serait un sage indépendant (par exemple, un ancien magistrat) pouvant être saisi par les intéressés, donner des conseils et avis sur la mise en œuvre des règles.

Certaines propositions émises par TI France ont été reprises dans le très remarqué rapport Sauvé rendu public le 26 janvier 2011 qui ne fut malheureusement pas suivi d'actions immédiates[5].

Le conflit d'intérêts dans la vie publique est un sujet qui fait couler beaucoup d'encre.

La Commission de rénovation et de déontologie de la vie publique a rendu son rapport le 9 novembre 2012

L'Assemblée nationale et le Sénat ont créé fin 2010 des groupes de travail sur la prévention des conflits d'intérêts. Des rapports ont été émis en 2011 suivi de recommandations.

Aucune loi n'a été adoptée pour mettre en œuvre toutes ces propositions mais le rapport Sauvé sert néanmoins de fondement aux travaux en cours.

Le Président de la République a créé en juillet 2012 un nouveau groupe de travail : « la Commission de rénovation et de déontologie de la vie publique » (dite Commission Jospin) et a demandé à cette commission de *« faire des propositions relatives à la prévention des conflits d'intérêts, tant à l'égard des parlementaires et des membres du Gouvernement que des titulaires de certains emplois supérieurs de l'Etat, de manière à garantir, par la définition de règles déontologiques, la transparence de la vie publique ».*[6]

Le 9 novembre 2012, la Commission a présenté au Président de la République son rapport contenant 35 propositions[7]. L'un des chapitres de ce rapport est consacré à la mise en œuvre d'une « stratégie globale de prévention des conflits d'intérêts ». Suite à ces propositions, plusieurs projets de loi devraient être soumis au Parlement au début de l'année 2013 notamment en matière de cumul des mandats, de prévention des conflits d'intérêts dans la vie publique et de contrôle citoyen.

En matière de prévention des conflits d'intérêts, la Commission Jospin rejoint, pour l'essentiel les recommandations de TI France ainsi que celles formulées par la Commission du Président Jean-Marc Sauvé en janvier 2011. Les parlementaires ainsi que les titulaires de certains emplois publics supérieurs de l'Etat et les membres et principaux responsables d'autorités administratives indépendantes sont également concernés par les mesures proposées : adoption d'une loi sur la prévention des conflits d'intérêts, et nécessité de promouvoir le développement des bonnes pratiques, en d'autres termes, nouvelles obligations, nouvelles sanctions et mise en place de règles déontologiques.

« Le conflit d'intérêts dans la vie publique est un sujet qui fait couler beaucoup d'encre. »

« Les différentes approches adoptées par les pays membres [de l'OCDE] pour gérer les situations de conflits d'intérêts sont le reflet de leurs traditions historiques, juridiques et administratives. Des mesures institutionnelles telles que les audits et vérifications externes à caractère constructif ou les autres méthodes de contrôle interne ont tout à fait leur place dans la gestion des situations de conflits ».[8]

Il convient de souligner que le rapport de la Commission de rénovation et de déontologie de la vie publique propose de mettre en place un dispositif ouvert d'alerte éthique tel qu'il existe dans plusieurs pays de l'OCDE. Ce dispositif serait ouvert à tout citoyen témoin d'actes illicites ou qui identifierait un risque avéré ou potentiel de conflit d'intérêts. Il ne s'agirait pas d'une procédure à connotation pénale telle que celle prévue à l'article 40 du code de procédure pénale. La Commission estime qu'un tel dispositif d'alerte pourrait contribuer utilement à la rénovation de la vie publique.

Rapport à suivre … ●

[1] *Cf. Recommandation du Conseil OCDE du 28 mai 2003 – n° C(2003)107 sur les lignes directrices pour la gestion des conflits d'intérêts dans le service public Annexe § 4.*

[2] *Recommandation du 11 mai 2000 n° R (2000)10 du Comité des ministres du Conseil de l'Europe sur les codes de conduite pour les agents publics.*

[3] *Cf. Rapport du SCPC 2004 et son Rapport 2010 notamment sur le conflit d'intérêts ou l'émergence progressive d'une nouvelle norme juridique (Chapitre V).*

[4] *Rapport 2010 TI France Prévenir les conflits d'intérêts dans la vie publique.*

[5] *Rapport au Président de la République de la Commission de réflexion pour la prévention des conflits d'intérêts dans la vie publique présidée par Monsieur Jean-Marc Sauvé vice-président du Conseil d'Etat.*

[6] *Extrait de lettre du Président de la République.*

[7] *Cf. : www.vie-publique.fr*

[8] *Cf. Recommandation du Conseil OCDE du 28 mai 2003 – n° C(2003)107 sur les lignes directrices pour la gestion des conflits d'intérêts dans le service public Annexe § 6.*

Les outils informatiques au service des auditeurs et des contrôleurs internes

Leurs fonctionnalités et leurs atouts

Les outils informatiques au service des auditeurs et contrôleurs internes

Yohann Vermeren - Directeur, **KPMG Advisory** - Membre de l'Unité de Recherche Informatique de l'IFACI

Lorsqu'on se pose la question « quels sont les outils informatiques mis au service des directions d'audit et du contrôle internes ? », on s'imagine que ces directions utilisent l'ensemble des outils mis à disposition de l'ensemble de la société, c'est-à-dire, la messagerie, les applications bureautiques et éventuellement les solutions intranet et portails collaboratifs, ce qui est effectivement le cas en tout premier lieu. Néanmoins, bon nombre de sociétés ont déjà mis en place tout ou partie de solutions plus poussées et dédiées à l'amélioration de l'efficacité, de la qualité et de la communication des métiers d'auditeurs, de contrôleurs et de gestionnaires des risques.

Les outils supports des processus « métier »

On observe durant l'ère Sarbanes Oxley (2003 - 2004) puis LSF (Loi de Sécurité Financière) une vague importante de déploiement d'outils permettant de documenter les processus de « contrôle interne », d'évaluer les contrôles et les tests, et d'en faire un suivi régulier. De la même manière, quelques directions d'audit ont déployé des outils spécialisés dans la fonction « audit interne ». Il en est de même pour la fonction « gestion des risques ».

Depuis maintenant plusieurs années, on constate une tendance forte vers la convergence des processus de gouvernance, risques, contrôle et conformité[1]. « *GRC (Governance, Risk and Compliance)* » est une approche orientée processus permettant d'identifier les risques au sein d'un processus, d'évaluer les contrôles en place pour s'assurer de la mise sous contrôle de ces risques. Les éditeurs des différents domaines (risques, contrôle interne, audit, processus) ont fait évoluer leurs solutions pour couvrir tout ou partie du spectre complet de la « GRC » (Bwise, Enablon, eFront, RVR, etc.). On note aussi l'arrivée des éditeurs d'ERP sur une partie des fonctionnalités couvertes par la « GRC » (Oracle ou SAP). Les fonctionnalités couvertes par de tels outils sont la conformité (évaluation du contrôle interne), la gestion des risques, la gestion de l'audit et la gestion des politiques et procédures.

Il n'en reste pas moins que de nombreuses entreprises, n'étant pas convaincues par l'apport d'une solution intégrée, choisissent une approche modulaire en fonction de leur besoin précis, c'est-à-dire en déployant seulement les fonctionnalités d'audit interne ou de contrôle interne d'un outil par exemple.

Les analyses considèrent que les solutions proposées sur le marché ont atteint une maturité en termes de couverture fonctionnelle ; la différenciation se joue désormais sur les fonctionnalités de gestion de risques et de la prise en compte des impacts de ces risques sur la performance de l'entreprise. La tendance du marché va aussi clairement vers une plus forte intégration avec les outils de type CACM (présentés ci-dessous), de *Business Intelligence*, pour améliorer le pilotage global de l'entreprise, voire même avec les ERP pour une intégration encore plus complète.

Les outils de contrôle et audit continus

L'audit continu (CA pour *Continuous Auditing*) et le contrôle continu (CM pour *Continuous Monitoring*) ont pour objectif d'offrir une meilleure transparence des opérations et d'assurer la régularité de la production du *reporting*, et ce au plus près du temps des activités opérationnelles, grâce à des outils de détection et de pilotage.
Le contrôle continu est un mécanisme automatisé permettant au management de s'assurer que les systèmes et les contrôles fonctionnent conformément aux dispositions établies lors de leur conception, et que le traitement des opérations est régulier. L'audit continu consiste à assurer la collecte automatisée, régulière ou continue, de preuves d'audit et d'indicateurs.

Les bénéfices attendus de telles solutions sont les suivants :

- accroître les capacités de surveillance des risques et des contrôles à l'aide d'outils de pilotage et d'identification anticipée des risques (notamment liés à la fraude) ;
- optimiser la réalisation de tests d'efficacité des contrôles et des opérations grâce à l'automatisation ;
- communiquer des indicateurs d'activité pertinents au Comité de direction.

On retrouve sur ce type de solutions des acteurs différents :

- les éditeurs d'ERP (Oracle, SAP) qui ont accès facilement aux données de leurs propres solutions ;
- les éditeurs d'outils d'analyse de données (ACL) qui facilitent le traitement et la restitution des données pour les contrôleurs et auditeurs ;
- les éditeurs de GRC (Bwise) proposent des fonctionnalités permettant d'intégrer le CACM au sein de leur plateforme.

Les outils d'analyse de données

Ce dossier présente un dernier type d'outil utilisé par les directions d'audit et du contrôle internes que sont les outils d'analyse de données. Ces outils sont très largement répandus au sein des directions (notamment ACL ou IDEA), sans être utilisés de manière systématique et sans tirer profit de l'ensemble des fonctionnalités qui sont proposées.
Selon le GTAG 16[3], l'utilisation des technologies d'analyse de données est de nos jours un atout majeur qui permet aux auditeurs d'accroître la couverture de leurs audits, d'être plus efficaces et d'avoir un degré d'assurance plus important.
Ces solutions permettent de réaliser une analyse approfondie du contrôle interne afin :

- de définir et de sélectionner des échantillons de tests ;
- d'évaluer l'efficacité d'une chaîne de contrôles ;
- d'analyser des transactions spécifiques et/ou significatives au sein d'un système d'information ;
- de revoir le paramétrage d'un système d'information ;
- de quantifier l'impact d'un contrôle défectueux.

On ne peut plus parler d'outils d'analyse de données sans parler de contrôle et d'audit continus (CACM), l'analyse de données systématique et industrialisée étant la première brique à la mise en place d'un contrôle permanent récurrent. Ces outils permettent effectivement l'automatisation des requêtes de contrôles, des tableaux de bord d'alertes.

* *
*

Il existe de nombreux autres outils spécialisés, pouvant éventuellement faciliter la réalisation de missions d'audit ou l'évaluation du contrôle interne, qui ne sont volontairement pas mentionnés ici. La liste en serait trop longue et comporterait des outils trop spécifiques (détection du risque de blanchiment, assurance, intrusions réseaux informatique, etc.). ●

[1] *Etude KPMG international « The convergence challenge » 2010, 64 % des répondants considèrent la mise en place d'une organisation GRC intégrée comme une priorité.*

[2] *Global technology audit guide 16: data analysis technologies / Altus J. Lambrechts, et al. – IIA, 2011.*

Liste des outils informatiques à disposition des auditeurs et contrôleurs internes

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
ACL	**ACL AuditExchange**	Plateforme d'audit et de contrôle continu centralisant l'ensemble des contrôles metiers et leurs diffusion via des interfaces web.	3 à plus de 100 utilisateurs	de 13 à 30 k€	Mode Client/Serveur avec des mécanismes de diffusion via intranet.
	AX Dashboard	Solution Tableaux de bord pour ACL AuditExchange 3.0	de 3 à plus de 100	1 100 € par utilisateur	Web et Client/Serveur avec le module AX™Exception.
	AX Exception	Solution de gestion des alertes et workflow pour leur suivi.	de 3 à plus de 100	1 300 € à 500 € par utilisateur	Architecture Web avec la plateforme ACL AuditExchange 3.0
	ACL Workpapers	Référentiel d'audit pour la gestion des missions d'audit.	Illimités	Locatif à partir de 90 € par mois	Cloud technology avec rapatriement de vos données.
	ACL Desktop	Solution d'analyse et de création de contrôles autonomes.	de 1 à plus de 100	2 200 € par utilisateur	Client installé sur un PC portable ou local.
	ACL Importer	Solution Add-on basé sur Monarch pour extraire les données complexes.	Utilisateur Desktop	895 €	Client installé sur un PC portable ou local avec ACL Desktop.
	ACL Acerno	Solution add-on d'excel pour analyser des données avec des fonctions d'audit.	de 1 à plus de 100	250 € par utilisateur	Add-on excel.
	ACL Direct Link	Solution pour sélectionner et extraire des données SAP et les charger au format ACL soit pour le contrôle périodique ou continu.		9 000 € par paysage SAP	Connecteur pour le client ACL™ Desktop ou la solution serveur AX™Core.
Actimize	**Actimize**	Prévention de la fraude, gestion du risque (secteur financier). Actimize est une plateforme de gestion des risques financiers. Les 4 piliers de la solution sont les suivants : détection de la fraude ; lutte anti-blanchiment ; compliance ; enterprise risk management. La solution est utilisée par plus de 250 banques, organismes financiers et autorités de régulation dans le monde.	NC	NC	NC
BPS Resolver	**GRC Cloud**	GRC Cloud est un référentiel et une application de rapports de la performance des gestion de risques, de la conformité, de l'audit et de la performance de l'entreprise. Liste des fonctions d'audit et de contrôle internes : planification basée sur les risques ; Issue and Action Tracking ; Workflow configurable ; Scoping ; rapports flexibles ; tableaux de bord ; planification automatisée ; écrans simplifiés pour les utilisateurs ; Library Management ; plusieurs niveaux d'approbation.	NC	NC	GRC Cloud est une application basée sur le Web. Nos applications peuvent être déployées à travers l'i-cloud ou sur l'infrastructure propre client. L'interface est basée sur un navigateur et ne nécessite donc pas d'être installé sur l'ordinateur de l'utilisateur. Pour les utilisateurs ayant un accès limité à internet, des options en mode hors connexion sont déployées.
BWise (Nasdaq OMX)	**BWise 4.1 SP3.5**	BWise offre des solutions pour : l'audit interne, le contrôle interne, la gestion de risques, la gestion de la conformité, et les sujets de développement durable et de responsabilité sociale. Chacune de ces solutions, basée sur un savoir-faire métier, fait partie de la plate-forme de GRC standard et intégrée. BWise permet une description structurée de votre organisation et de vos cadres d'architecture (processus, risques, contrôles) ainsi qu'une mise en mouvement de cette description via la gestion des évaluations ou des programmes de travail, et des actions de remédiations. Un reporting complet permet le suivi et l'analyse de l'activité.	de quelques dizaines à plusieurs dizaines de milliers	la tarification des licences est basée sur les rôles utilisateurs (auditeur, contrôleur interne, risk manager…)	BWise est proposé en mode acquisition, hébergement ou SaaS. Application n-tiers entièrement web accessible par les navigateurs internet du marché. Compatibilité Oracle ou SQL Server.

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
		X		X	X					www.acl.com/solutions/products/acl-auditexchange/	**ACL Europe Ltd** Atlantic House Imperial Way Reading, Berkshire RG2 0TD United Kingdom Contact : Pascal Gadea Tél: +33(1) 61381503 ou 33 6 62 40 32 93 pascal_gadea@acl.com
		X							X	www.acl.com/solutions/products/acl-auditexchange/	
		X							X	www.acl.com/solutions/products/acl-auditexchange/	
X	X						X			www.acl.com/solutions/products/acl-workpapers/	
				X	X					www.acl.com/solutions/products/acl-desktop/	
				X						www.acl.com/solutions/products/acl-desktop/	
				X						www.acl.com/solutions/products/acl-acerno/	
				X						www.acl.com/solutions/hot-topics/sap-erp/	
							X		X	www.niceactimize.com	**EMEA** 176 Avenue Charles de Gaulle 92200 Neuilly-sur-Seine Tél. : + 33 (0) 01 4138 5000
X	X		X			X	X	X	X	www.bpsresolver.com	**BPS Resolver** 703 Evans Avenue, Suite 107 Toronto, ON, Canada M9C 5E9 Contact : Peter Trinz Tél. : +1 416 622 2299 (Ext 229) peter.trinz@bpsresolver.com
X	X	X	X	X	X	X	X	X		www.bwise-grc.fr	**BWise France** 19 Boulevard Malesherbes 75008 Paris Contact : Stéphane Dorchin Tél. : 01 55 27 37 28 stephane.dorchin@bwise.com

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
CaseWare-IDEA	**IDEA Version 8.5** *(prochainement V. 9)*	IDEA est reconnu pour sa simplicité d'utilisation. Les principales fonctions sont : • le croisement de différentes tables ; • la recherche de transactions suspectes ; • la vérification des calculs ; • la vérification du respect des seuils d'autorisation ; • les doublons, les ruptures de séquences ; • les analyses de saisonnalité et tendance ; • les échantillonnages.	plus de 250 000	2 500 €/HT (Version Monoposte)	Monoposte, Réseau, Client-Serveur.
Cura Software solutions	**Cura Enterprise GRC platform**	La suite Cura GRC permet de gérer : • les risques de l'entreprise : gestion des risques financiers, opérationnels, de l'information et risques liés à des projets clés ; • la modélisation des risques quantitatifs ; • la gestion des incidents ; • la conformité aux normes, lois et réglements ; • l'audit interne : élaboration du plan d'audit, gestion des ressources, suivi de la mission et des recommandations ; • les plans de continuité d'activité.	NC	NC	NC
Cogis Software	**Cogis Software**	Cogis Software (Groupe Alpha Centauri) propose une solution GRC axée autour de 3 piliers : • le contrôle interne : pilotage de campagnes de contrôle interne, suivi de la mise en place de plans d'actions, etc. ; • l'audit interne : planification, réalisation et suivi des missions d'audit, suivi des recommandations, etc. ; • la gestion des risques : élaboration de fiches de risque, de cartographie des risques, etc.	NC	NC	NC
Datawatch	**Monarch Report Analytics**	Monarch est un outil d'extraction de données. La solution est capable d'extraire des données depuis des factures papiers, des fichiers textes ou PDF et de les exporter sous Excel, Access, etc.	NC	NC	NC
Devoteam	**RVR Risque, Contrôle, Audit**	La solution RVR est une plateforme GRC intégrée, innovante, spécialisée sur la gestion des risques, le contrôle interne et l'audit. RVR permet en particulier de gérer : • le processus d'audit : plan d'audit, planification et réalisation des missions, papiers de travail, rapport d'audit, suivi des recommandations ; • le contrôle interne : gestion des référentiels, campagnes d'évaluation, testing, suivi de plans d'actions. RVR offre des capacités multiples d'analyse et de reporting à chaque niveau de l'organisation.	de quelques dizaines à plusieurs milliers d'utilisateurs	nous consulter	La solution RVR est une application full-web développée sur une plateforme technique Java/J2EE, fonctionnant sur les grands standards du marché de : bases de données (Oracle, SQL Server) ; serveurs d'application (Websphere, Tomcat) ; systèmes d'exploitation (Windows Server, Linux, AIX). L'application apporte un haut niveau de sécurité et d'interopérabilité. Sa configurabilité permet de concilier flexibilité d'adaptation à la méthodologie du client, rapidité d'intégration et évolutivité. Devoteam offre ses solutions en mode licence classique ou en mode SaaS.
eFront	**Front GRC**	eFront est spécialisé dans les métiers de Gouvernance, de gestion des risques et de la conformité. FrontGRC présente une large couverture fonctionnelle : risques, contrôle interne, contrôle permanent, conformité, audit interne, plans de continuité d'activité, Corporate Governance, Continuous Control Monitoring avec ACL. eFront propose une offre sectorielle s'appuyant sur ces solutions métier tout en intégrant les spécificités en terme de contenu et de processus des secteurs d'activités qu'il s'adresse. eFront est le seul acteur spécialisé de la GRC à avoir développé (Intégration native) une solution d'analyse et de reporting multidimensionnelle.	Contrôleur = 200 Utilisateurs = 5 000 Audit = 40 Total (incluant les audités) = 500	Small deal = 50 K€ Large Deal = 500 K€ Average = 150 K€	eFront s'appuie sur une plateforme technique (WebEdge 5 .NET), une technologie Microsoft qui garantit : interopérabilité ; reporting & analyse multidimensionnelle (FrontAnalytics) ; support de Multi-device ; performance ; sécurité, traçabilité, Workflow, GED, administration, multilinguisme / Devise ; "Google-like" search engine ; gestion des droits multidimensionnelle. WebEdge 5 .NET supporte : plusieurs navigateurs ; IE10 support ; HTML5. Authentification and SSO

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
X		X	X							www.caseware-idea.fr	**Caseware IDEA** 12 Place St Hubert 59000 Lille Contact : François Lienart Tél : 03 59 56 06 80 francois.lienart@caseware.com
X	X		X		X	X	X	X		www.curasoftware.com	**Cura Europe** Suite 125, Berkeley Square House Berkeley Square, London, W1J 6BD United Kingdom Tél. : +44 (0) 20 7887 1584
X			X			X	X			www.cogis-software.com	**COGIS SOFTWARE FRANCE** 1-3 Bd Charles de Gaulle 92700 Colombes Contact : Philippe Donguy Tél. : + 33 1 47 82 40 59
				X	X					www.datawatch.com	**Datawatch Corporation** Quorum Office Park 271 Mill Road Chelmsford, MA 01824 USA
X	X		X		X	X	X	X		www.devoteam.com	**Devoteam** 73 rue Anatole France 92300 Levallois Perret Contact : Paul Chegaray Tél. : 06 71 05 28 44 paul.chegaray@devoteam.com Contact : Agnès Poyard Tél. : 06 59 91 35 10 agnes.poyard@devoteam.com
X	X	X	X	X	X	X	X	X	X	www.efront.com	**EFRONT** 2-4, rue Louis David 75116 Paris Contact : Birame Fall Tél. : +33 1 49 96 94 31 Mobile : +33 7 78 69 52 21 bfall@efront.com

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
EMC (Archer)	**RSA Archer eGRC**	La solution RSA eGRC Archer comprend différents modules nativement interconnectés permettant de gérer les processus liés aux audits, aux contrôles internes et à la gestion des risques. Le module "Audit Management" permet d'avoir une vue consolidée de votre programme d'audit. Le module "Risk Management" permet de gérer les risques et de piloter les différents plans de traitements mis en œuvre. Le module "Policy Management" permet de gérer les différentes politiques, standard, procédures ou régulations liées à votre activité. Le module "Compliance" permet d'automatiser les contrôles et de gérer les écarts de conformité constatés.	NC	NC	La solution RSA eGRC Archer est une application Web dont l'architecture est scindée en un bloc "Applicatif" et un bloc "Base de données". Le bloc "Applicatif" est installé sur un serveur Windows sur lequel sont installés Microsoft IIS et le Framework .NET. La base de données (qui stocke les données de configuration et les datas) est une base de données MS SQL. Chacun des composants peut être installé sur un serveur physique ou un serveur virtualisé. En fonction des spécificités de nos clients des architectures "Single-Host" (un seul serveur) ou "Multi-Host" (plusieurs serveurs) sont proposées.
Enablon	**Suite Enablon ERM**	Enablon propose une offre complète et intégrée de solutions logicielles couvrant l'ensemble des problématiques de gestion des risques, contrôle et audit Interne. Les solutions Enablon permettent aux entreprises d'identifier et gérer leurs risques, améliorer leurs dispositifs de contrôle, faciliter leurs audits de performance et assurer la continuité de leurs activités. Les solutions Enablon sont utilisées par plus de 1 000 grandes entreprises, 300 000 utilisateurs et des dizaines de milliers de PME dans tous les secteurs d'activité.	10 à 40 000 utilisateurs selon les solutions et les projets	NC	Les solutions Enablon sont conçues sur l'infrastructure Technologique full Web Enablon Operations permettant une utilisation des solutions partout et à tout moment sans installation sur le poste client. Cette technologie supporte aisément des déploiements auprès de plusieurs milliers d'utilisateurs. Souple et flexible, elle possède un environnement de paramétrage intégré pour une personnalisation précise et rapide et une gestion facilitée des profils et droits d'accès. L'infrastructure technologique Enablon comprend le serveur applicatif, l'environnement de développement Application Builder, les Modules Administration, les Connecteurs et l'API.
Greenlight technologies	**Audit Analytics**	Audit Analytics est un outil de contrôle continu de transactions et d'activités d'utilisateurs en lien avec des processus clés (paye,notes de frais, clôture, etc.). La solution permet d'améliorer l'efficacité des processus de l'entreprise à travers le suivi d'indicateurs clés de performance, la remontée d'incidents et les propositions d'améliorations formulées par l'outil.	NC	NC	NC
IBM	**OpenPages GRC**	IBM OpenPages GRC Platform est une plateforme intégrée de gestion de la gouvernance, du risque et de la conformité. La plateforme de base permet de suivre les thématiques suivantes : gestion des risques financiers et opérationnels ; gouvernance informatique ; audit interne ; compliance. Une plateforme étendue permet également de gérer le risque vendeur et fournisseur, le plan de continuité d'activité, etc.	NC	NC	NC
	Cognos	IBM Cognos est une solution de business intelligence et de pilotage de la performance. Elle propose des outils de reporting, de tableaux de bord, d'analyse, de planification budgétaire et d'intelligence collaborative pour faciliter la prise de décision. Ces outils sont également accessibles depuis un terminal mobile.	NC	NC	NC
Lawson	**Approva Corporation**	Approva propose une solution d'audit et de contrôle continu. Plusieurs modules sont disponibles : audit continu ; prévention de la fraude ; compliance ; rationalisation des contrôles ; gestion des accès ; environnement de contrôle de l'entreprise.	NC	NC	NC

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
X	X	X	X			X	X	X		www.emc.com	**EMC Corporation** 80 Quai Voltaire CS 21002 95876 Bezons Cedex
X	X		X	X	X	X	X	X		www.enablon.fr	**Enablon** Tél.: 01 47 33 64 65 info@enablon.net
		X								www.greenlightcorp.net	**Green light Corp.** Europe Operations - Headquarters London UK Knyvett House Watermans Business Park The Causeway - Staines Middlesex - TW18 3BA
X	X		X		X	X	X	X		www.ibm.com	Tél. : 01 58 75 39 92 Code prioritaire : 101KR29W
				X							
		X			X	X	X	X		www.approva.net	**Consider Solutions, Ltd.** 16-20 Ely Place London EC1N 6SN United Kingdom Tél. : +44 (0) 870 163 0850

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
MethodWare (Jade software)	**ERA Kairos 8.1**	Kairos est une solution GRC tournée vers le secteur financier, présente surtout dans les pays anglo-saxons. Son offre est axée autour de : • la gestion des risques : risques financiers et opérationnels, risque fournisseur/client, gestion des incidents, plan de continuité d'activité, etc. ; • la compliance avec les lois et réglements internationaux : SOX, Bâle II et III, Solvency II, etc. • l'audit interne : planification et suivi des missions, gestion électronique des documents, suivi des recommandations, etc.	NC	NC	NC
Magique Galileo	**Risk and Audit Management Software**	Magique est une solution présente surtout dans les pays anglo-saxons. En plus d'une offre de base centrée sur la gestion des risques (cartographie, risk scoring, etc.), l'outil propose en option une offre dans les domaines suivants : un système de suivi et d'évaluation des incidents ; problématiques de contrôle interne : questionnaires d'auto-évaluation, gestion de campagnes de contrôle interne ; compliance. Galileo est un outil associé qui permet de gérer entièrement le plan, les ressources et les missions d'audit interne.	NC	NC	NC
MEGA	**MEGA GRC (version 4)**	MEGA GRC se compose de trois modules : gestion des risques, contrôle interne et audit interne. Le module d'audit interne couvre l'ensemble du processus d'audit : • créer un plan d'audit orienté risque, qui assure la couverture régulière des entités et processus, et qui intègre des missions de suivi ; • planifier et staffer les missions en fonction de la disponibilité et des compétences des auditeurs ; • préparer chaque mission et automatiser la génération du programme de travail ; • réaliser les tests, superviser l'équipe et générer le rapport final ; • suivre les recommandations par workflow ; • automatiser les rapports de synthèse pour la direction.	de 2 à + 200 utilisateurs	NC	MEGA GRC peut être installée localement ou accédée via le Cloud. Elle repose sur une architecture 3 tiers : Base de données, Server Web et application.
MetricStream	**Audit Management Solution and GRC Platform 6.0**	La solution GRC permet de gérer : l'audit interne (gestion du plan, des ressources et des missions d'audit, archivage des documents) ; les risques financiers, opérationnels, informatiques et environnementaux ; la compliance ; le contrôle interne. La plateforme GRC peut s'interfacer avec d'autres solutions de MetricStream couvrant la gestion électronique des documents, la gestion du changement, des formations, etc.	NC	NC	NC
Mkinsight	**Audit & risk management solutions**	Mkinsight a des clients principalement dans le secteur financier et dans les pays anglo-saxons. La solution permet de piloter l'audit interne (planification, déroulement des missions, suivi des recommandations, etc.) et la gestion des risques de l'entreprise.	NC	NC	NC
Oracle	**Oracle Enterprise Governance, Risks, and Compliance - Version 8.4.3.300**	Oracle GRC est une solution modulaire et intégrée servant à gérer la gouvernance, la mise en conformité, les risques, et la mise en place de contrôles continus. EGRCM permet de gérer la stratégie d'une entreprise, ses risques, et ses exigences réglementaires/corporate. Vous définissez les risques de l'entreprise, les contrôles destinés à les diminuer, et d'autres objets (organisations, projets, etc.) où les risques interviennent et les contrôles doivent être appliqués. EGRCC permet d'automatiser les contrôles (transactionnels, séparation des tâches, configuration des applications et préventifs). GRCI apporte une couche BI à l'ensemble.	de moins de 10 utilisateurs pour les PME, à plusieurs milliers. La moyenne des utilisateurs se situe vers 80.	Le prix moyen d'une vente peut aller quelques dizaines de milliers d'euros à quelques centaines de milliers d'euros.	Oracle GRC est une application Internet (pas de composants sur la station de travail) et utilise : • Base de données : Oracle 11.2x • Développement et maintenance : Oracle JDK 1.6 • Serveurs & Middleware : Apache Tomcat 6.0.24 ou Weblogic Server 10.3.5 • Autre Middleware : Oracle BI EE 11.1.1.5 et Oracle Identity Directory 11.1.1.6 • OS Serveur d'application : Linux x86-64, Oracle Linux 5.6, Red Hat Enterprise Linux 6.0 Notre solution peut aussi fonctionner en environnement virtualisé avec Oracle VM Server : 2.2.1

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
X			X			X	X	X		www.methodware.com	**EMEA** 4th Floor 4-6 Throgmorton Avenue London EC2N 2DL United Kingdom Tél. : +44 (0) 20 7151 5050 london@methodware.com
X	X		X			X	X			www.magiquegalileo.com	**Magique Galileo Software Ltd** 60 Cannon Street London EC4N 6NP United Kingdom Tél. : +44 (0) 20 7002-1370 info@magiquegalileo.com
X	X	X	X			X	X	X		www.mega.com/fr	**MEGA International** 9 avenue René Coty 75014 Paris Contact : Christophe Gontier Tél. : 01 42 75 40 00 mega.fr@mega.com
X	X		X			X	X	X		www.metricstream.com	**MetricStream, Inc.** Immeuble LE SIRIUS 124, rue de Verdun 92800 Puteaux Tél. : +33-(0)180048557 info@metricstream.com
X	X		X				X			www.mkinsight.com	**Morgan Kai Group Limited** West One Wellington Street Leeds - LS1 1BA United Kingdom Tél. : +44 (0)113 245 5558
X	X	X	X	X	X	X	X	X		www.oracle.com/fr/solutions/corporate-governance/index.html	**Oracle** Portes de la Défense 15, boulevard Charles de Gaulle 92715 Colombes Contact : Christian Meyer Tél. : +33 1 57 60 23 86 Mobile : +33 6 08 41 84 32 christian.meyer@oracle.com

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
Oxial	**Risk Management Solution**	La solution BlueSuite d'Oxial s'articule autour de 3 axes : • BlueRisk, gestion des risques : élaboration et gestion de la cartographie des risques, remontée et suivi des incidents, etc. ; • BlueControl, contrôle interne : gestion des référentiels et des campagnes de contrôle interne ; • BlueAudit : gestion du plan, des ressources et des missions d'audit interne. BlueSuite propose également des modules de développement durable, gouvernance IT et gestion des réclamations clients.	NC	NC	NC
Pentana	**PAWS Audit & Risk Management Software**	Pentana est un éditeur anglo saxon qui développe la solution PAWS (Pentana Audit Work Solutions), articulée autour de 3 axes : audit interne, contrôle interne, gestion des risques.	NC	NC	NC
Protiviti	**Portail de GRC et Audit Interne : PGP**	Audit interne : plan d'audit, réalisation de missions, rapports d'audit, suivi des recommandations. Gestion des auditeurs, des plannings et des notes de frais. Mode "offline" pour travailler déconnecté. Gestion des risques et contrôle interne : gestion du référentiel processus et SI, risques et contrôles. Cartographie des risques, campagnes d'auto-évaluation, gestion des plans d'action. Autres fonctionnalités : gestion des incidents, workflow et emails, reporting, attachement de documentation, export-import de données, base multillangues... Intégration de référentiels (COSO, AMF) et méthodologie d'audit conforme aux normes IIA.	20 à 1 000 +	Variable en fonction du nombre d'utilisateurs	Plateforme technologique intégrée, sans nécessité de synchronisation entre les différents modules. PGP est accessible en mode SaaS. L'authentification unique SSO et la connexion au LDAP sont disponibles, permettant une intégration de l'application dans des contextes intranet ou extranet. Cette solution couvre l'ensemble des besoins fonctionnels et est aisément paramétrable, sans besoin de développement spécifique. Un mode offline est disponible pour le module Audit Interne.
Qlikview	**Qlickview**	Qlikview est une solution de business intelligence destinée à partager l'information et à faciliter la prise de décision, facilement utilisable par une équipe d'audit interne. QlikView permet d'appréhender l'activité en consolidant des données pertinentes issues de : • différentes sources dans une seule et même application ; • explorant les associations entre les données ; • visualisant les données à l'aide de graphiques soignés et performants ; • utilisant des applications, des tableaux de bord et des analyses dynamiques.	NC	NC	NC
ROK	**ROK solution**	ROK est une startup francaise très dynamique qui a bâti une plateforme visant à intégrer les différents progiciels utilisés par l'entreprise (comptabilité, business process management, risques, etc.) au sien d'une seule interface pour simplifier le pilotage de l'entreprise.	NC	NC	NC
RunBook	**Internal Control**	La plateforme RunbookOne permet de relier les outils de GRC de l'entreprise avec l'ERP afin d'automatiser les contrôles et de développer le continuous monitoring.	NC	NC	NC
SAP	**SAP GRC 10.0**	La suite SAP GRC 10.0 est une suite unifiée et intégrée d'applications : • SAP Access Control pour la gestion des risques liées aux autorisations et aux accès aux systèmes SAP et non-SAP et permettant ainsi de garantir la séparation de tâches ; • SAP Risk Management pour la gestion des risques d'entreprise de tous types (stratégiques, financiers, opérationnels, IT ...) ; • SAP Process Control pour évaluer le contrôle interne, garantir la conformité des contrôles par rapports aux politiques internes et aux réglementations et optimiser les processus ; • SAP Audit Management pour l'audit interne dont les plans d'audit peuvent être basés sur les risques.	NC	NC	La Suite SAP GRC 10.0 repose sur une architecture n-tiers centralisée avec une base unique, s'appuyant sur la plate-forme technique SAP Netweaver. La solution GRC 10.0 s'appuyant sur SAP Netweaver tire parti des fonctionnalités de ce socle. En particulier, SAP Netweaver fournit le mécanisme de transport qui permet d'échanger données et éléments de paramétrages entre environnement. SAP NetWeaver mise sur des standards Internet tels que HTTP, XML et Web services. Il sert en outre de base à une architecture orientée services (SOA). Le déploiement de la solution GRC 10.0 s'effectue par un client Web. Il suffit d'un navigateur supporté par Netweaver : IE, Firefox, Safari.

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
X			X			X	X			www.oxial.com	**Oxial - France** 15 rue Taitbout 75009 Paris Tél. : +33 (0)1 73 02 15 71 contact@oxial.com
X	X		X				X	X		www.pentana.com	**Pentana Ltd.** Gate House, Fretherne Road Welwyn Garden City Hertfordshire - AL8 6RD United Kingdom Tél. : +44 (0) 1707 373335 info@pentana.com
X	X	X	X			X	X	X		www.protiviti.com/grc-software	**Protiviti** 21, Boulevard Haussmann 75009 Paris Contact : Vincent Clostre Tél. : 01.42.96.22.77 vincent.clostre@protiviti.fr
				X						www.qlikview.com	**Qlik Technologies** 93, avenue Charles de Gaulle 92200 Neuilly sur Seine Tél. : +33 (0)1 55 62 06 90 infofr@qliktech.com
X							X			www.rok-solution.com	**ROK** 94, rue Saint Lazare 75009 PARIS Tél. : 01 42 81 51 98
		X	X			X	X	X		www.runbook.com	**Runbook Company Inc.** 163 Madison Ave. Suite 220-026 Morristown, NJ 07960 - USA Tél. : +1 973 867 7020 info@runbook.com
X	X	X	X	X	X	X	X	X	X	www.sap.com	**SAP BusinessObjects France** Immeuble Capital 8 32 rue de Monceau 75008 Paris Cedex Tél. : 01 44 45 20 00

Editeurs	Progiciel	Fonctionnalités / spécificités	Nombre moyen d'utilisa-teurs	Coût moyen des licences	Architecture
Software AG	**Aris R&C Manager 4.0**	La plateforme Aris Risk & Compliance Manager est une plateforme intégrée permettant de piloter : • la gestion des risques : cartographie des risques, gestion des incidents ; • le contrôle interne : gestion des référentiels et des campagnes de contrôle interne ; • l'audit interne : gestion du planning, des ressources et des missions d'audit interne ; • la gestion des procédures et des processus.	NC	NC	NC
Sword Achiever	**Sword Achiever 5**	Sword Achiever est une plateforme intégrée de gestion des risques orientée autour de 4 axes : • enterprise risk management : gestion des risques, contrôle interne et audit interne ; • gestion de la performance : suivi de KPI et KRI, outils de reporting, tableaux de bords ; • compliance avec les lois et réglementations ; • plan de continuité d'activité.	NC	NC	NC
Symbiant	**Symbiant Risk Suite and Symbiant Tracker**	La suite Symbiant Risk s'articule autour de la gestion des risques et du contrôle interne. Symbiant Tracker est un outil complémentaire permettant de piloter le suivi et la gestion des incidents ainsi que le suivi des recommandations issues des missions d'audit interne.	NC	NC	NC
Tableau	**Tableau desktop**	Tableau Desktop est une solution de business intelligence issue d'une technologie de l'université de Stanford, qui permet d'utiliser les données provenant de différents sytèmes pour les restituer dans une interface unique et personnalisable afin de faciliter l'analyse et la décision.	NC	NC	NC
Thomson Reuters	**Thomson Reuters GRC (GRC -Formally Paisley)**	Promotion de l'efficience et de l'efficacité : • Favorise la cohérence – Met à profit une vaste bibliothèque de modèles, de listes de contrôles et de cadres standards qui favorisent le respect des procédures et des pratiques professionnelles approuvées par la direction. • Collaboration. • Une seule source de référence. Visibilité en temps réel des audits : • Visibilité – Une base de données sécurisée. • Rapports – La génération de rapport automatisée offre des informations en temps réel aux principaux intervenants.	5 - 1 000	$2,000	• Licence perpétuelle sur site – Mise en oeuvre des logiciels dans votre environnement ; gestion des mises à niveau d'infrastructure et de logiciel. • Sur demande – Accès au logiciel via un navigateur Web. Thomson Reuters gère l'infrastructure GRC et les mises à niveau de logiciels. • Licence perpétuelle hébergée – Accès au logiciel via un navigateur Web, gestion de vos propres mises à jour.
Wizsoft	**Data Mining Tools for Internal Audits**	Wizsoft est un outil de data mining et d'analyse de données applicable à des activités d'audit interne.	NC	NC	NC
Wolters Kluwer	**TeamMate suite, Audit Management System (AM)**	TeamMate a été conçu comme un outil capable d'augmenter l'efficacité et la productivité de l'ensemble du processus d'audit, permettant aux utilisateurs de consacrer plus de temps aux tâches et services à forte valeur ajoutée. TeamMate est utilisé dans tous les secteurs d'activités et dans les services d'audit de toute taille. TeamMate permet de gérer l'intégralité du cycle de vie de la mission d'audit avec notamment : évaluation des risques, programmation des missions, préparation et documentation des missions, suivi des durées et dépenses, création de rapports d'audit, suivi des recommandations et reporting.	nombre moyen de 40 utilisateurs par organisation	Tarifs applicables par tranche d'utilisateurs et disponibles à la demande.	Un serveur de base de données est nécessaire pour les applications Web de TeamMate et recommandé pour les applications de bureau. Les spécifications du serveur de base de données varient selon les besoins et le nombre d'utilisateurs dans une organisation. Les bases de données prises en charge sont Microsoft SQL Server 2005 SP1/ SP2/SP3, Microsoft SQL Server 2008 SP1/SP2, Microsoft SQL Server 2008 R2, ainsi que MS SQL Express 2005 et 2008. L'option cloud hosting est disponible.
	TeamMate suite, Control Management (CM)	TeamMate CM a été conçu pour SOX et autres (AS-123,...) pour aider à gérer facilement les activités de gestion de conformité où l'identification, l'évaluation, la vérification et les rapports de certifications sont nécessaires. TeamMate CM fournit une relation souple entre les entités, processus, comptes des états financiers et structures hiérarchiques. TeamMate CM permet de basculer entre les vues afin de visualiser les risques et contrôles de différentes hiérarchies. L'outil permet de mettre à jour les informations de contrôle et d'appliquer les modifications aux instances actives de ce contrôle dans les évaluations.	NC	NC	Interface web. Version tablette disponible. Disponible Q1 2013

Champs d'application										Site internet	Contact et coordonnées
Gestion de l'audit	Automatisation des papiers de travail	Audit et contrôle continus	Auto-évaluation des contrôles	Extraction et analyse des données	Détection / prévention de la fraude	Evaluation du contrôle interne	Gestion et analyse des risques	Conformité (Sarbanes Oxley)	Solutions spécifiques		
X	X		X			X	X	X		www.softwareag.com	**Software AG** Uhlandstr. 12 D-64297 Darmstadt Germany Tél. : +49 6151 92-0 webinfo@softwareag.com
X	X		X			X	X	X		www.sword-achiever.com	**Sword Achiever** Tél. : +44 208 232 2555 info@sword-achiever.com
X	X				X		X			www.symbiant.co.uk	**Symbiant** Westgate House 100 Wellington Street Leeds. LS1 4LT United Kingdom Tél. : +44 113 237 3954
				X						www.tableausoftware.com	**Tableau Software** Tél. : 33 (0) 970 444 196
X	X		X	X	X	X	X	X		www.accelus.thomsonreuters.com/solutions/internal-audit	**Thomson Reuters** 6 boulevard Haussmann 75009 Paris Contact : Alexandre Lyons Tél. : 00 33 01 495190 alex.lyons@thomsonreuters.com
		X		X	X					www.wizsoft.com	NC
X	X	X	X			X*	X	X*		www.teammatesolutions.com	**Wolters Kluwer Audit** Risk and Compliance 1 rue Eugène et Armand Peugeot 92500 Rueil Malmaison Contact : Farid Boukhlifa Tél. : +33 (0)1 76 73 33 87 Mobile : +33 (0)6 14 80 28 34 fboukhlifa@wolters-kluwer.fr

** Disponible Q1 2013*

Siemens mène ses audits plus rapidement et à moindre coût

ACL

Sandeep Bhatkhande - Directeur du Service d'analyse des données, **Siemens**

« *En automatisant les processus d'audit avec ACL, notre entreprise a bénéficié d'améliorations dans plusieurs domaines. Nous avons pu notamment réduire de 70 % la durée et le coût de nos analyses.* »

Basé à Berlin et à Munich, Siemens exerce des activités très diversifiées dans le monde entier. Le groupe devait donc impérativement disposer d'une technologie d'analyse de données économique, standardisée et automatisée. Son département financier a créé un service d'analyse des données, avec pour objectif l'automatisation des tests et de l'analyse des données d'environ 60 sociétés Siemens réparties dans 20 pays de la zone Asie-Pacifique.

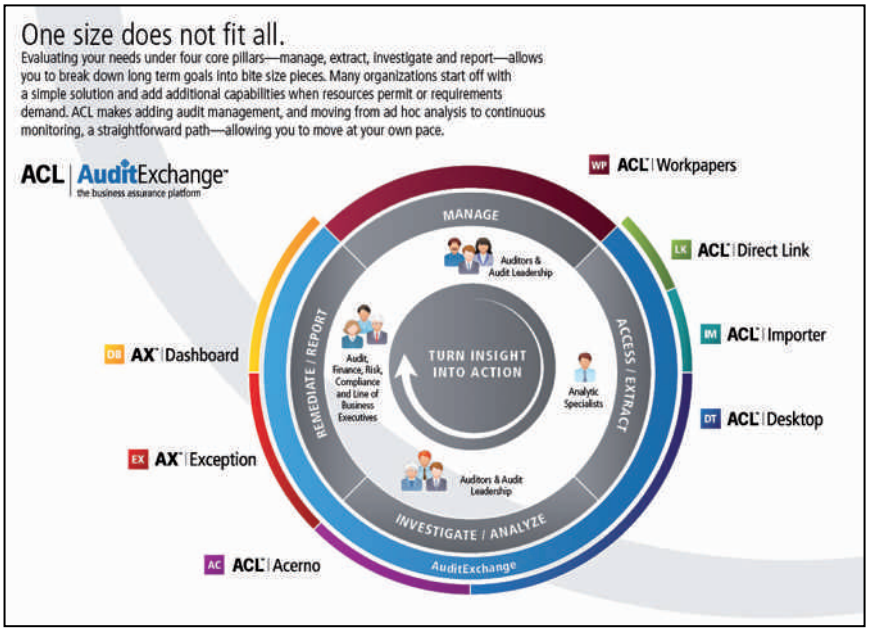
Avec ACL, ces opérations sont à présent centralisées et traitées depuis un serveur commun. En automatisant ses activités d'analyse de données, l'équipe d'audit a réalisé 70 % d'économie en temps et en coût et elle bénéficie d'une visibilité totale sur ses transactions de paiement. La technologie ACL a permis à Siemens de détecter les transactions anormales, d'améliorer la planification de ses audits et d'atteindre ses objectifs d'excellence en matière de contrôle des processus de gestion, tout en réduisant ses coûts.

Disposer impérativement des fonctionnalités étendues d'analyse de données

Le département Finances et Audit financier du groupe devait disposer impérativement d'une solution performante, capable de standardiser les analyses de données et le *reporting* des exceptions, tout en limitant l'échantillonnage afin de minimiser les failles dans les contrôles, les risques, les fraudes et les pertes de revenu.
Il souhaitait également automatiser les processus manuels et améliorer la rentabilité des projets d'analyse de données sans que cela fasse l'objet d'un apprentissage dissuasif ni qu'il faille recourir à des technologies complexes impliquant un support informatique conséquent.

Plateforme standardisée d'analyse de données

Le siège social international de Siemens a porté son choix sur les solutions ACL, dans le but de standardiser et d'automatiser un ensemble de tâches variées, et a institué un service d'analyse des données chargé de piloter cette mission. ●



ACL Europe Ltd
Atlantic House - Imperial Way - Reading, Berkshire - RG2 0TD
United Kingdom
Contact : Pascal Gadea - Tél: +33(1) 61381503 ou 33 6 62 40 32 93 - pascal_gadea@acl.com
www.acl.com

Un outil au service de la gestion des risques et de l'audit interne chez AG2R La Mondiale

BWise

Patrick Saint-Maxent - Responsable du département Pilotage des risques opérationnels et de la qualité, **AG2R LA MONDIALE**

AG2R La Mondiale est le 1er groupe de protection sociale en France. Il allie performance économique et engagement social au travers des valeurs portées par le paritarisme et le mutualisme. En 2011, il a géré 15,5 Md€ de collecte pour 8 millions d'assurés.
AG2R La Mondiale dispose de toutes les expertises en assurance de personnes. Le Groupe couvre l'ensemble des besoins de protection sociale et patrimoniale tout au long de la vie de ses assurés. Il apporte des réponses individuelles et collectives, aussi bien en prévoyance qu'en santé, en épargne comme en retraite complémentaire et supplémentaire, quels que soient l'âge, le statut social et le secteur professionnel.

La problématique

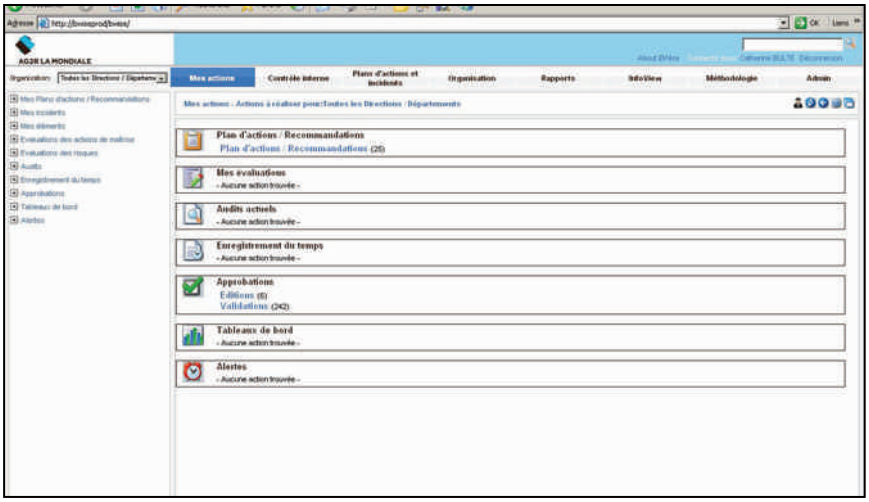
La sélection d'un outil a été initialement motivée par trois objectifs principaux. Compte tenu des enjeux croissants pour les sociétés d'assurance en matière de gestion des risques et face à une réglementation de plus en plus contraignante, il était important de diffuser une culture « risques » et une culture de vigilance à l'égard de ces risques au sein du Groupe. Le deuxième enjeu était de centraliser et structurer l'ensemble des données relatives aux risques pour pouvoir disposer d'informations immédiatement accessibles et homogènes. Enfin, nous souhaitions pouvoir effectuer un *reporting* fiable et pertinent de la gestion des risques. Nous avons complété récemment ces objectifs pour répondre à un nouveau défi : l'accompagnement du travail de l'équipe d'audit interne, en particulier dans le cadre du suivi des recommandations et du processus de certification IFACI en cours.

Ce que l'outil m'a apporté

BWise nous a accompagnés dans le déploiement opérationnel de notre démarche de contrôle interne et de gestion des risques au sein du groupe. La solution et les experts BWise nous ont permis d'industrialiser le processus de suivi des risques et d'assurer le cycle complet de gestion des risques : cartographies des risques, actions de maîtrise, plans de contrôles, suivi des plans d'actions. Grâce à BWise, nous avons à notre disposition une base des incidents majeurs du Groupe. De plus, nous sommes en mesure de communiquer sur les risques à travers du *reporting* et de partager l'information en temps réel. BWise nous permet également de préparer sereinement notre conformité à la norme Solvabilité II. Récemment, nous avons étendu l'usage de BWise à l'audit interne. En effet, nous nous sommes engagés dans le processus de certification de notre direction d'audit interne par l'IFACI, démarche facilitée par la mise en place du suivi des recommandations et plans d'actions associés au sein de BWise.

Les avantages et les limites de l'outil

L'ergonomie de la plate-forme logicielle a été un élément déterminant dans la sélection de BWise, ce qui a contribué à la bonne acceptation de l'outil par les utilisateurs. Sa grande adaptabilité a également été un élément-clé car nous voulions un logiciel capable d'accompagner la méthodologie que nous avions développée. BWise est un outil très complet et évolutif qui est donc capable de répondre aussi bien à nos besoins actuels qu'à nos défis futurs. La disponibilité et l'expertise des consultants BWise sont des atouts supplémentaires qui nous permettent de réfléchir ensemble à notre développement. ●



Une assurance élevée et appréciée

IDEA

Jean-Luc Meurisse - Directeur de l'audit interne, **Sonepar**

Sonepar est un distributeur de solutions techniques aux professionnels de l'électricité, avec un chiffre d'affaires 2011 de 14,7 milliards d'€ réalisé dans 35 pays avec 160 filiales et 33 000 collaborateurs. Nous avons une équipe d'une vingtaine d'auditeurs internes basés au siège du groupe à Paris, ou à l'étranger, notamment en Amérique du Nord.

La problématique

Dans notre métier, la distribution professionnelle, le volume des flux et le nombre de transactions sont très élevés. Les fichiers sont souvent de grande taille et de formats divers ; leur analyse nécessite un outil à la fois plus rigoureux et plus puissant qu'un tableur, et tout aussi accessible. L'objectif de Sonepar en acquérant IDEA était de faciliter les tests d'audit et de les systématiser, pour élever le niveau d'assurance obtenu.

Ce que l'outil nous apporte

Nous utilisons IDEA depuis deux ans et demi, d'abord au siège, puis aux Etats-Unis, et depuis un an au Mexique. Les principales applications chez Sonepar, avant et pendant une mission, sont l'échantillonnage statistique, notamment pour mesurer la fiabilité des stocks, l'analyse des données d'un processus ou d'un type de transaction, le rapprochement par « jointure » de fichiers d'origines différentes et la recherche d'exceptions, non conformités ou fraudes.
Outre sa puissance, sa capacité volumétrique et sa facilité d'utilisation après deux jours de formation, l'outil nous apporte:

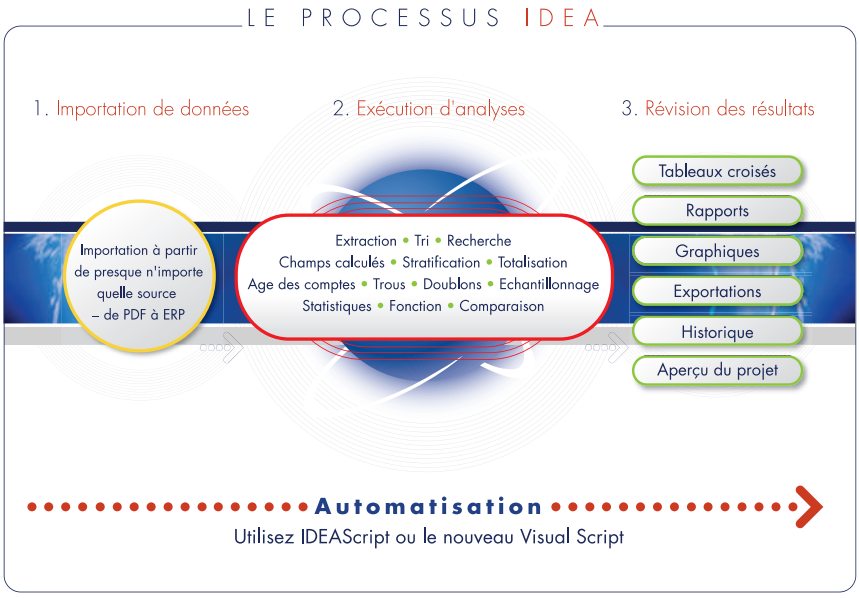
- productivité : nombreuses fonctions intégrées, traçabilité et reproduction des tests (modélisation et scripts) ;
- universalité et exhaustivité : importation des principaux formats de fichiers, 100% des données sont analysées.

Ainsi, nous nous sommes plusieurs fois assurés de l'absence de doubles paiements ou du respect complet d'une règle de gestion, et ce sur des périodes supérieures à un an. Cette assurance est très appréciée des auditeurs et du management.

Que faire pour réussir la mise en place et l'utilisation ?

- utiliser et faire utiliser fréquemment l'outil, si possible à chaque audit ;
- décrire clairement chaque test : quel est l'objectif recherché ?
- définir précisément les données : qu'est-ce que je demande, sous quelle forme ?
- qualifier les données obtenues, par exemple à partir d'états financiers ou statistiques de la période ;
- gérer le savoir dans les équipes et d'une mission à l'autre.

Nous documentons nos tests standards et leurs demandes de données associées, avec l'aide ponctuelle d'un utilisateur chevronné, auditeur « expert » de l'équipe locale ou consultant, toujours sur un cas réel, en mission. ●



L'évaluation du contrôle interne dans le groupe Bouygues

Solution RVR de Devoteam

Renaud Vorms - Directeur du contrôle interne, **Bouygues**

Bouygues est un groupe industriel diversifié, dont les métiers s'organisent autour de deux pôles : la construction avec Bouygues Construction, Bouygues Immobilier et Colas, et les télécoms-médias avec TF1 et Bouygues Telecom.
Présent dans 80 pays, le groupe a réalisé un chiffre d'affaires de plus de 32 milliards d'euros en 2011 avec plus de 130 000 collaborateurs.

Les objectifs du projet

Le groupe Bouygues a construit un référentiel de contrôle interne Groupe, applicable à tous ses métiers, et a défini une méthode d'auto-évaluation des principes de contrôle interne.

Le Groupe a souhaité se doter d'un outil informatique afin de faciliter le déploiement de l'évaluation des principes de contrôle interne, et en particulier de :

- rendre plus fluide, plus fiable et plus rapide le déploiement des campagnes d'évaluation dans chacun des métiers, et suivre leur avancement ;
- automatiser les remontées des évaluations ;
- faciliter la production d'états de restitution des résultats de l'évaluation ;
- stocker de manière fiable et centralisée les données historiques.

La solution RVR a été choisie par Bouygues après la consultation de cinq éditeurs.
Le projet s'est déroulé en 2011 ; les premières campagnes d'évaluation ont été lancées en juillet 2011.

La mise en commun des besoins

La solution déployée sur les cinq métiers du Groupe et sur la *holding*, compte plus de 2 000 utilisateurs qui participent aux évaluations tout au long de l'année.

Afin de répondre, dans un même outil, aux besoins fonctionnels des cinq métiers, il a fallu tenir compte des spécificités de chacun (en particulier en termes de principes métiers, d'organisation et de *workflow*) en les intégrant à un cadre structuré et commun. Nous avons affiné ensemble l'ergonomie de l'application et les états de restitution.

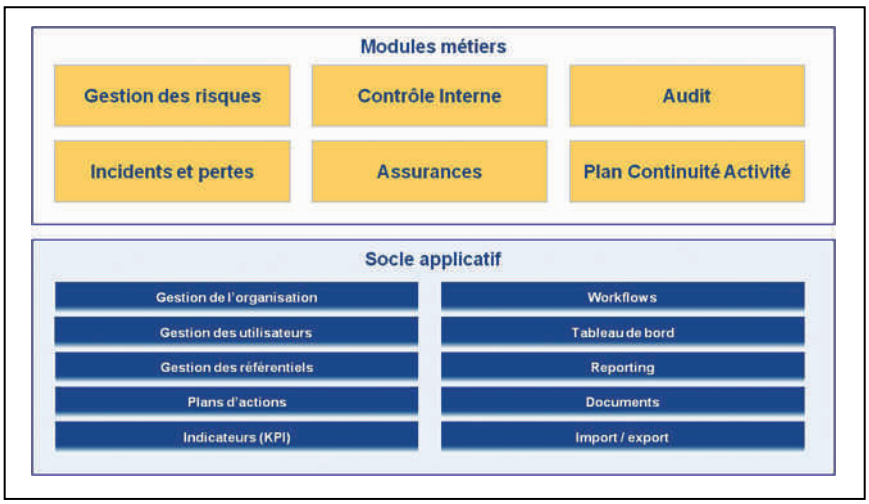
Chaque métier du Groupe étant organisé de manière autonome, nous avons choisi de décentraliser la gestion des campagnes et l'administration fonctionnelle. Notre méthode d'évaluation repose sur une affectation nominative des principes aux répondants et validants de chaque entité, et sur un *workflow* précis de validation.

Les apports de l'outil

Un effort important a été réalisé pour proposer un bon niveau d'ergonomie afin de minimiser les efforts de formation et faciliter la prise en main de l'outil par l'ensemble des utilisateurs.

La solution donne la possibilité pour les utilisateurs d'éditer des états de restitution et d'analyse prédéfinis et propose également des fonctionnalités d'analyse croisée des données.

L'outil permet aussi un suivi simple de l'avancement des plans d'actions définis dans le cadre des campagnes d'évaluation. ●



La gestion des risques et de l'audit interne de la MAIF

FrontGRC Risk, FrontGRC Control et FrontGRC Audit

Vianney Dumont - Directeur de l'audit interne, **MAIF**
Armand Forgerit - Responsable de projet maîtrise des risques contrôle interne, **MAIF**

6ème assureur dommages des particuliers et 1er assureur du secteur associatif, la MAIF couvre l'ensemble des besoins de ses 2,7 millions de sociétaires (assurances de biens, prévoyance, santé, assistance, épargne, crédit…). En 2011, le groupe MAIF a réalisé un chiffre d'affaires de plus de 3 milliards d'euros.

La problématique

Le département de gestion des risques a été créé en 2007. Jusqu'alors, Excel était l'outil utilisé et a rapidement montré ses limites. La MAIF avait donc besoin d'un outil spécifique pour gérer les risques et le contrôle permanent ; eFront correspondait parfaitement aux besoins de la MAIF, notamment grâce à l'évolutivité de ses paramétrages.

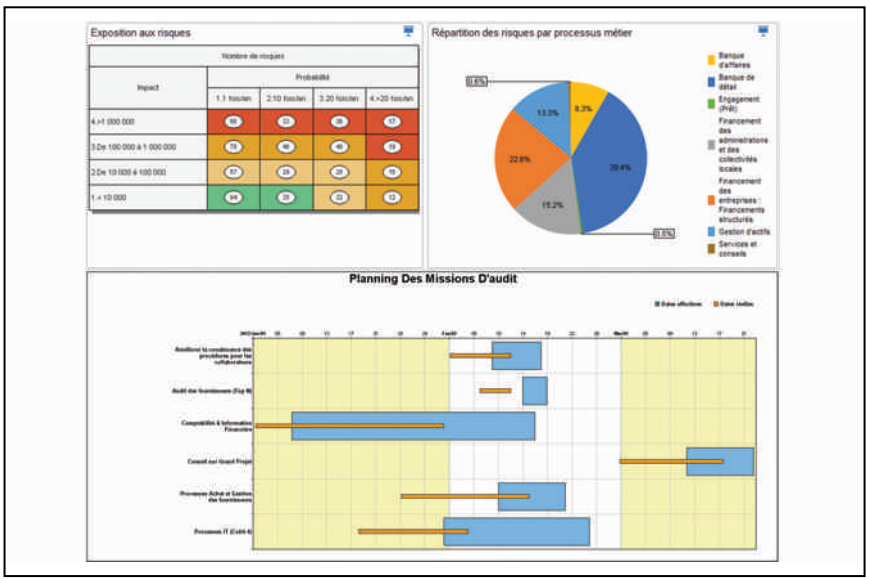
Ce que l'outil m'a apporté

« Cinq ans après, nous ne regrettons pas d'avoir fait ce choix », explique Armand Forgerit, responsable de projet maîtrise des risques contrôle interne à la MAIF. *« Une fois la solution eFront sélectionnée, la mise en production s'est faite en moins de 7 mois. Entre-temps, 8 séquences de travail ont été mises en place entre les deux entités afin de définir le paramétrage de l'outil. »* Armand Forgerit poursuit : *« Ces ateliers ont été menés de main de maître avec un cadencement bien défini sur l'atelier paramétrage d'administration de l'outil ainsi que sur les paramétrages d'écrans spécifiques. »*

Les avantages et les limites de l'outil

M. Forgerit confirme : *« La solution eFront nous permet de créer et d'automatiser l'ensemble des reportings afin de répondre aux besoins du législateur et des métiers, notamment du contrôle permanent. Nous avons en outre développé un outil spécifique d'auto-contrôle adapté aux responsables des entités commerciales et des centres de gestion des sinistres. »*

La MAIF étant satisfaite de l'outil eFront retenu pour sa cartographie des risques et l'animation de son contrôle permanent, il était logique que l'audit interne s'intéresse en priorité à FrontAudit au moment de choisir un outil pour faciliter la réalisation de ses missions. Vianney Dumont, directeur de l'audit interne, précise : *« Aujourd'hui, nous l'utilisons pour nos audits d'entités commerciales et de gestion de sinistres pour lesquels nous avons conçu un référentiel d'une centaine de contrôles par entité que nous avons implémentés dans le progiciel eFront. Cela nous permet de mener chaque mission en 15 à 20 j/h, de l'analyse des données initiales jusqu'à la production du rapport, en passant par le séjour sur site. Nous pensons qu'il nous reste encore une marge d'optimisation en perfectionnant les paramétrages. Notre enjeu va être maintenant de transposer dans l'outil notre méthodologie de missions longues d'audit de processus puis la gestion du plan d'audit lui-même. L'outil est fiable, son adaptabilité est grande avec pour corollaire le besoin d'une charge significative de paramétrage. »* ●



Disposer d'une vue agrégée du risque d'entreprise

RSA Archer

Marshall Toburen - Vice President and Operations Risk Manager, **UMB Financial Corp.**

La problématique

UMB Financial est l'une des plus grandes banques indépendantes aux États-Unis et fournit une large gamme de produits et de services à ses clients. De ce fait, UMB se doit de protéger les données de ses clients et de se conformer de manière précise aux exigences du *reporting* financier.
La direction des Opérations et la direction des Risques se sont échinées pendant des années avec un outil ERM *(Enterprise Risk Management)* non intégré et inefficace, reposant principalement sur des feuilles de calcul et des emails provenant des managers afin de disposer d'un état du niveau de risque encouru par la société. Il leur manquait une vue agrégée, prenant en compte les informations provenant des différents silos de données de l'entreprise, ainsi qu'un système accessible via l'intranet, supportant les *workflows*, et qu'elles pourraient complètement adapter à leurs processus métier.

Ce que l'outil nous a apporté

Quand la direction des Opérations et la direction des Risques ont appris que la solution RSA Archer était implémentée par la DSI d'UMB afin de gérer ses besoins de pilotage de la sécurité, la flexibilité et l'ouverture de RSA Archer les ont décidées à construire le système ERM dont elles avaient besoin.

UMB a donc choisi RSA Archer afin de gérer l'agrégation de données provenant des différents silos et nécessaires à la gestion du risque, le contrôle de processus et le *reporting* multi-niveaux, en plus du suivi des incidents, de la gestion des biens, l'audit et la conformité auprès des organismes de régulation.
La solution RSA Archer est utilisée par près de 500 employés au sein d'UMB, dont les membres du Conseil d'administration, la direction, les responsables métier et l'équipe IT. Un tableau de bord des risques de l'entreprise fournit aux managers et aux régulateurs la bonne information en temps et heure.

Les avantages et les limites de l'outil

RSA Archer permet à UMB de minimiser le risque d'entreprise et d'améliorer l'efficacité au sein de l'entreprise tout en renforçant la confiance dans les efforts entrepris pour garantir la conformité.

Un des principaux avantages que nous avons vu depuis la mise en œuvre de RSA Archer est une plus grande transparence de l'information. Nous pouvons organiser les résultats des enquêtes et le contenu de notre base de données de contrôle des risques au sein de différents tableaux de bord.

En outre, la plate-forme RSA Archer permet à UMB de modéliser ses propres processus métier sans faire appel à des développements de services tiers. Nous pouvons apporter des modifications « à la volée » afin d'adapter le système à nos besoins. ●

Comment Provimi a mis en œuvre sa stratégie GRC en optimisant ses processus métier et IT

SAP GRC Process Control & SAP Access Control 10.0

Basée aux Pays-Bas, Provimi Holding est l'une des trois plus importantes sociétés d'aliments pour animaux en Europe occidentale. Provimi a mis en œuvre la suite SAP GRC pour augmenter la valeur de l'entreprise en déployant un dispositif de maîtrise des risques et de contrôle interne.

La problématique

Avant le projet, Provimi avait toutes les caractéristiques d'une organisation décentralisée, avec une *holding* très réduite (25 employés), un modèle organisationnel basé sur des centres de profit, une culture du risque peu développée, un nombre important de systèmes ERP hétérogènes (7 fournisseurs différents). La décision a été prise de transformer Provimi en une *holding* (75 personnes) avec une organisation déclinée en cluster s'appuyant sur un nouveau modèle de gouvernance et de maîtrise des risques, une direction informatique centralisée s'appuyant sur un ERP SAP unique et une plate-forme GRC associée. Les objectifs du projet GRC consistent à ancrer une culture d'entreprise en alignant l'organisation sur les directives du *top management*, à déployer un code de conduite, des normes et des procédures partagées par tous, une procédure d'alertes *(whistle blowing)*.

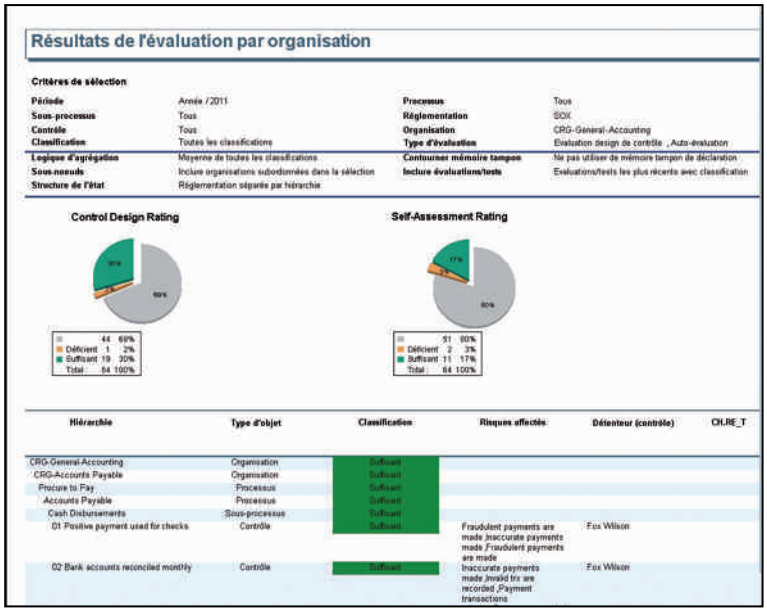
Ce que l'outil m'a apporté

La mise en place de SAP GRC a permis la mise en œuvre d'un cadre de contrôle global et de surveillance continue avec une attention accrue pour la GRC par la direction et les actionnaires, une meilleure transparence et efficience des contrôles et la conformité par rapport aux réglementations en vigueur (UK Bribery Act, US Foreign Corrupt Practices Act - FCPA).
SAP Access Control a permis de réduire les risques d'accès et de séparation de tâches liés aux autorisations affectées aux utilisateurs.
SAP Process Control a permis de surveiller de manière continue les contrôles dans les processus opérationnels, d'attester la réalité des contrôles, de réduire les temps passés par les parties prenantes (contrôleurs, auditeurs internes et externes) en remplaçant les contrôles manuels par des contrôles automatisés.

Les avantages et les limites de l'outil

Access Control permet la gestion préventive des risques d'accès pour éviter la propagation de nouveaux conflits lors de la création d'une nouvelle demande d'accès et lors de la maintenance des rôles. SAP Process Control permet de définir des cadres de contrôle multiples, à tous les niveaux (groupe, division, filiale, entité).
SAP Access Control et SAP Process Control peuvent être associés à SAP Audit Management pour la gestion des audits internes et externes et à SAP Risk Management pour le pilotage des risques.

« Les Solutions SAP GRC nous ont permis de faire la preuve que nous contrôlons nos risques de manière effective. Être en mesure de le démontrer a valorisé considérablement notre entreprise ». **Louis van Vliet**, *Group Internal Audit Manager,* Provimi Holding B.V. ●



Un outil d'amélioration de l'efficacité des missions d'audit de Zodiac Aérospace

TeamMate Audit Management System (AM)

Arnaud Dubant - Responsable de l'audit interne Groupe, **ZODIAC AÉROSPACE**

Lors de mon arrivée chez Zodiac Aérospace en tant que directeur de l'audit et du contrôle internes Groupe en 2009, j'ai mené une réflexion pour améliorer l'efficacité des missions d'audit.

Problématique

Jusqu'à mi 2011, les missions d'audits internes locales étaient gérées via un outil interne permettant un suivi de la couverture du plan d'audit pluriannuel ainsi qu'un état d'avancement des recommandations. Cet outil bien qu'efficace nécessitait néanmoins beaucoup de temps de mise à jour et de nombreuses opérations manuelles. Un projet Groupe a été initié afin de sélectionner un outil reconnu sur le marché permettant la réduction du temps de gestion administrative des missions, l'automatisation de la production des rapports d'audits, l'échange avec les audités et le suivi des plans d'action.

Ce que l'outil m'a apporté

Le logiciel TeamMate a parfaitement répondu à nos attentes. Après un déploiement rapide, il est aujourd'hui utilisé par tous les auditeurs ainsi que par toutes les *Business Units* du Groupe via un portail web (TeamCentral).
Les auditeurs utilisent l'outil en mode déconnecté lors des missions terrains, synchronisent avec la base de données régulièrement, permettant ainsi au responsable de mission de suivre l'avancement de la mission. Ils génèrent automatiquement le rapport d'audit interne à partir de l'outil ce qui permet un premier débriefing structuré avec les audités sur les écarts majeurs avant la fin de la mission.
Enfin, les audités utilisent le rapport généré par l'outil pour nous faire part de leurs remarques, ces dernières étant automatiquement réintégrées dans l'outil pour la version finale. Une fois la mission finalisée, via la solution web, les audités mettent à jour le suivi des plans d'actions.

Les avantages et les limites de l'outil

Outre la réduction du temps administratif des missions d'audit, l'outil nous a permis d'améliorer notre processus de gestion des risques (le module TeamRisk est utilisé depuis début 2012 pour réaliser des campagnes d'auto-évaluations de toutes les BU du Groupe).
Le fait d'avoir chargé notre programme d'audit standard dans la bibliothèque TeamStore nous a également aidé à uniformiser la démarche de chaque auditeur, à mieux documenter chaque point de contrôle et à lier des procédures ainsi que des outils Groupe.
Concernant les limites de l'outil, nous ne disposons pas aujourd'hui de fonctionnalité de questionnaire de contrôle interne sur le site web partagé avec les *Business Units* du Groupe (fonctionnalité livrée sur la dernière version) et nous aimerions voir apparaître quelques évolutions par rapport aux fonctionnalités du rapport automatique de l'outil. ●

Pour une sélection judicieuse et une utilisation optimale d'un logiciel

Unité de Recherche Informatique

L'Unité de Recherche Informatique de l'IFACI vient de finaliser une publication concernant la sélection d'outils pour les services d'audit ou de contrôle internes. Elle préconise une expression claire des besoins et donne les clés permettant d'apprécier les « coûts » du déploiement en termes financiers, de temps, ou d'insertion dans les processus existants. La démarche de gestion de projet proposée permet de gérer ces risques et de tirer vraiment partie des fonctionnalités retenues.

La professionnalisation croissante des services d'audit et de contrôle internes, leur insertion dans des environnements de plus en plus complexes justifient l'usage croissant des outils informatiques.

Le contexte

Les avantages les plus couramment attendus de solution informatique visent à :

- l'amélioration des performances (productivité, *knowledge management*, etc.) ;
- la maîtrise des activités (planification supervision, communication, suivi) ;
- la qualité (adoption des bonnes pratiques, amélioration continue).

Les avantages sont indéniables, mais il n'est pas rare de voir des services d'audit et de contrôle internes ne pas pouvoir profiter de toutes les opportunités que permet une solution logicielle, faute de ne s'être pas posé les bonnes questions. Les travaux de l'URI (Unité de Recherche Informatique de l'IFACI) cherchent à lever cet écueil en :

- proposant une démarche de gestion d'un tel projet ;
- rappelant les risques principaux à chaque étape de ce processus (à savoir les questions à se poser pour les évaluer et les dispositifs de maîtrise adéquats) ;
- illustrant la démarche par des bonnes pratiques et des retours d'expériences de professionnels de l'audit et du contrôle internes qui ont été confrontés à cette problématique de sélection et de déploiement d'outils.

Le leitmotiv de l'Unité de Recherche est qu'il faut continuellement apprécier les « coûts » en termes financier, de temps, de pertinence des analyses ou encore de production d'indicateurs à la mesure des bénéfices attendus. En effet, toute utilisation de logiciel présente des risques et peut donc poser plus de problèmes qu'il n'en résout.

La démarche proposée

L'URI propose un système de gestion des risques à chaque étape du choix et de la mise en œuvre d'un outil.
Mettre en place un outil passe par les étapes suivantes :

- tenir compte de l'environnement ;
- exprimer les besoins et les prioriser ;
- étudier les options (acquisition d'un logiciel, développement, réorganisation, évolution, etc.) ;
- concevoir une stratégie de test cohérente avec les besoins ;
- évaluer les logiciels et les faire fonctionner *(proof of concept)* ;
- choisir le logiciel à déployer ;
- maquetter, développer ;
- tester ;
- mettre en place (reprise de l'existant, formation des utilisateurs…) ;
- administrer et maintenir.

Les rôles et responsabilités doivent être clairement définis avant le lancement du projet. Il est préconisé de formaliser les affectations de chaque personne impliquée, la charge estimée de travail sur le projet, la fréquence des réunions de travail et d'avancement, ainsi que les contributions attendues.

La structure de projet est à ajuster en fonction de l'ampleur de votre équipe. Elle comporte généralement :

- un sponsor ayant la responsabilité d'arbitrer les décisions clés,

- un comité de pilotage,
- un comité de projet.

La désignation du chef de projet est un point critique pour le succès de la démarche. Il convient de s'assurer que l'ensemble des directions impactées par le déploiement de l'outil informatique soit partie prenante du comité de pilotage. Il faut également inclure les bons acteurs. De même, le prestataire informatique interne doit être associé en amont du projet (pour une meilleure performance et plus de sécurité, etc.) même lors d'une acquisition d'un progiciel du marché.

Partir des besoins pour orienter les choix

S'il est tentant pour les responsables de service de croire que l'achat d'un logiciel résoudra leurs problèmes, en pratique le bilan peut être plus mitigé lorsque l'outil choisi ne convient ni aux objectifs, ni au périmètre, ni à l'organisation du système d'audit et de contrôle internes.

L'URI préconise une analyse du besoin selon la règle des « 3 pourquoi ». Ces besoins peuvent être d'ordre fonctionnel. L'outil vient alors supporter le pilotage du service (gestion des ressources), sa communication (ex. : production d'indicateurs de performance et tableaux de bord), ou des activités (ex. : feuilles de travail, analyse de données). Mais les besoins peuvent également répondre à des exigences non fonctionnelles, sur le modèle de l'ISO 9126-1:2001 Génie du logiciel – Qualité des produits.
Par exemple, on pourra préciser ses exigences en termes de lisibilité de la documentation utilisateur, d'ergonomie du logiciel, de facilité d'apprentissage ou encore de facilité de maintenance.
Le responsable du service doit s'assurer de la classification de ces besoins.

Choisir une solution

Un outil logiciel n'est pas, dans notre contexte, un objectif, mais un moyen, une solution possible (Cf. Schéma).
Il convient donc d'analyser des options au regard des besoins identifiés.

Lorsque l'option retenue est « acquérir un logiciel », l'étape suivante consiste à analyser les différentes solutions. Pour ce faire, un cahier des charges définissant les critères de consultation et de sélection devrait être établi. Ces critères vont au-delà de l'aspect fonctionnel et permettent notamment de :

- préciser le périmètre de la consultation. Inclut-il, par exemple, les plateformes techniques (serveurs, base de données et applications) ? Tient-il compte des synergies avec d'autres services potentiellement utilisateurs (AI / CI / Risques, notamment) ?
- définir les modalités de consultation au regard des contraintes de planning du service et des procédures d'achat.

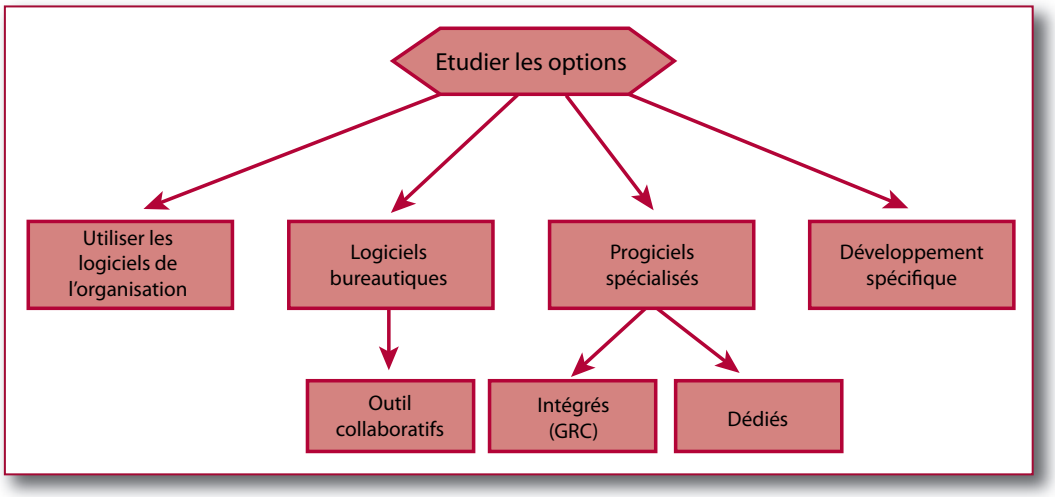
Enfin, l'éditeur à même de déployer la solution souhaitée est sélectionné, au regard des critères préalablement définis. Un nombre restreint d'éditeurs sont invités à préciser leur offre lors d'entretiens oraux, voire de tests.

Mener le projet

La notion de jalon est rappelée comme un élément essentiel de maîtrise de la dérive du projet. Il n'y a pas de « petit projet » qui justifierait de s'affranchir de ces étapes clés, où l'on s'interroge toujours et encore sur la pertinence des options choisies. La conduite de projet est de savoir déterminer son état d'avancement. Comme les Romains l'avaient compris, il n'y a qu'un bon moyen de savoir où on en est, c'est de placer des jalons le long de sa route.

Maquetter / développer / paramétrer

Compte tenu des besoins spécifiques à chaque organisation, tout progiciel nécessite une personnalisation qui peut aller du plus simple (quelques informations tapées sur l'écran) au plus compliqué (développement de fonctionnalités spécifiques par exemple). Cette phase peut, bien souvent, engendrer des surprises tant sur les délais que sur les coûts. Plus l'expression des besoins aura été claire, plus des ajustements pourront être effectués en amont et gérés en connaissance de cause.



Développer les stratégies de tests et de déploiement

La conception des tests devrait être une étape de l'expression des besoins, surtout si l'analyse des risques a permis une sensibilité importante du service voire de l'entreprise, à la bonne mise en œuvre du projet. Il est nécessaire de bien dérouler et suivre les plans de tests afin de n'oublier aucun point important au moment de la recette de la solution.

Par ailleurs, il peut être intéressant de définir un certain nombre d'indicateurs de performance qui permettront de suivre et mesurer en temps réel la résolution par l'éditeur ou par l'intégrateur des écarts constatés :

- nombre de défaillances résolues entre deux phases de tests,
- temps de traitement / résolution des problèmes constatés.

La phase pilote va permettre de s'assurer que les fonctionnalités de l'outil « s'emboîtent » correctement et que l'outil gère les cas particuliers.
Il est important que le périmètre fonctionnel et organisationnel de la phase pilote soit suffisamment large pour couvrir les principales fonctionnalités. De même, dans le cadre d'un questionnaire d'auto-évaluation du contrôle interne, inclure une filiale à l'étranger peut aider à anticiper d'éventuels problèmes techniques (type connexion à distance) avant le lancement de la campagne « classique ». La phase pilote doit faire l'objet d'un retour d'expérience et, éventuellement, d'un questionnaire de satisfaction de la part des utilisateurs pilotes.

Gérer le changement et administrer l'outil

Le changement se gère de l'expression des besoins jusqu'à la mise en œuvre, en mettant les utilisateurs au cœur de la démarche :

- l'évolution répond-t-elle à une demande des utilisateurs ?
- l'évolution facilite-t-elle le travail des utilisateurs ?
- l'évolution enrichit-elle le travail des utilisateurs ?
- les utilisateurs sont-ils acteurs de toutes les étapes du projet ?

Par ailleurs, plusieurs axes d'administration peuvent être dégagés :

- l'administration des données (ex. gestion des accès),
- le contrôle de conformité aux procédures (utilisation des bons formulaires),
- le contrôle de la fiabilité des données,
- le support aux utilisateurs, trop souvent négligé et mal dimensionné dans ce type de projet,
- la formation des nouveaux arrivants dans le service,
- la gestion des modifications du progiciel (ex. planification du changement de version).

Il ne faut pas sous-estimer le poids en temps passé consacré aux tâches d'administration qu'implique le recours à des logiciels « intégrés », notamment lorsque l'équipe d'audit interne est d'un effectif inférieur ou égal à 10 personnes.
Il convient d'identifier la ou les personne(s) en charge de l'administration et de la ou les former en conséquence.
Un outil ne permet pas de s'exonérer du travail préalable de compréhension des données à traiter : que signifient-elles (quel est leur sens), couvrent-elles nos besoins d'audit, sont-elles fiables et utilisables ?

* *
*

Le cahier de la recherche « Sélectionner un outil informatique pour les services d'audit et de contrôle internes : un véritable projet » sera mis à disposition sur le site internet de l'IFACI à partir de décembre 2012. Il sera maintenu à jour par l'URI grâce à une veille sur les besoins et les offres.
Vous pourrez y trouver différents éléments pour guider votre démarche :

- références bibliographiques,
- bonnes pratiques,
- points de vigilance,
- exemples,
- témoignages.

En vous y référant ne cherchez pas à trouver LA solution toute faite. C'est, en effet, au futur utilisateur d'identifier le logiciel qui convient à ses besoins propres et c'est l'ambition de ce cahier de la recherche de lui fournir les éléments suffisants pour faire les choix les mieux adaptés. D'ailleurs, même si le cahier propose une caractérisation des outils du marché et peut citer des outils à titre d'exemple, nous nous sommes interdits toute préconisation sur ce sujet.

Enfin, au-delà des opportunités offertes, l'URI rappelle que l'outil ne règle pas tout. Il est donc nécessaire de clarifier ses objectifs et de s'être d'abord posé la question de l'organisation, de la qualité des procédures, de la formation, avant de se lancer sur un chantier d'informatisation. L'outil ne crée pas la compétence, en d'autres termes, l'organe (le logiciel) ne crée pas la fonction.

Enfin, attention aux biais induits par l'outil. La généralisation de listes de contrôle, bien utiles lors de missions récurrentes ou de conformité, peut générer une démobilisation de l'intelligence au profit d'une routine tenant lieu de méthode. ●

Evénements

Rôles et responsabilités des directions fonctionnelles au sein d'un dispositif de contrôle interne

Réunion mensuelle du 17 octobre 2012

Le bon fonctionnement d'un dispositif de contrôle interne est fonction de l'implication de l'ensemble du personnel de l'organisation.

EDF

Principes clés de la politique de contrôle interne. Pour les activités qui lui sont déléguées, chacun des managers du groupe est responsable de : maîtriser les risques ; vérifier cette maîtrise pour chacun des domaines subdélégués ; adosser et proportionner ses dispositifs et activités de contrôle aux risques identifiés ; auto-évaluer les dispositifs de contrôle ainsi mis en œuvre, et en rendre compte de façon formelle et régulière à son autorité de rattachement.
Soixante entités environ, opérationnelles et fonctionnelles, élaborent un rapport d'auto-évaluation annuel transmis à la direction de l'audit interne. Chaque manager de ces entités nomme et mandate un animateur de contrôle interne pour piloter la mise en œuvre du dispositif de contrôle interne au sein de son entité.
Un dispositif d'audit unique, rapportant au PDG du groupe, permet de vérifier périodiquement la pertinence des dispositifs et la sincérité des auto-évaluations, et d'apporter aux dirigeants une assurance raisonnable sur la couverture des principaux risques.

Les acteurs clés dans le contrôle interne groupe. Les animateurs de contrôle interne, nommés et mandatés par les managers, sont chargés de piloter la mise en œuvre du dispositif de contrôle interne au sein de l'entité.

Responsabilité des entités. Chaque entité est responsable de sa comptabilité. Elle met en œuvre un plan de contrôle interne dans lequel figure un volet comptable et financier. Le directeur d'entité signe une lettre d'engagement.

SNCF

Quelques principes de base. Les branches, domaines et directions fonctionnelles sont responsables de leur contrôle interne, sur le périmètre du groupe. La direction de l'audit et des risques assure le pilotage et l'animation, en lien avec la direction financière du groupe. Pour chaque branche, domaine et direction fonctionnelle, une feuille de route précise les périmètres et processus d'intervention ; des guides de contrôle interne mettent à disposition des entités opérationnelles, pour chaque point de contrôle clé, les bonnes pratiques et modes opératoires de contrôle associés.

Les directions fonctionnelles sont en responsabilité directe sur leurs opérations et donc sur leur contrôle interne ; elles sont en responsabilité indirecte sur la partie des processus assurée par d'autres acteurs qui ne leur sont pas rattachés hiérarchiquement, et interviennent alors en tant que propriétaires de processus.

Comment impliquer les directions fonctionnelles en tant que propriétaires de processus ? En les associant à tous les travaux de contrôle interne concernant le processus (ateliers, séminaires, auto-évaluations...) ; en ne les sollicitant que sur les points de contrôle correspondant au périmètre sur lequel ils sont en responsabilité directe ; en ne recherchant pas formellement leur responsabilité indirecte.

Orange Business Services

La direction du contrôle interne groupe pilote le dispositif de contrôle interne du groupe. Dans ce cadre, elle doit notamment s'assurer de la mise en œuvre et du suivi, par les fonctions opérationnelles, des plans d'action jugés nécessaires.

Les directions de contrôle interne local ont pour mission d'assister les managers opérationnels, afin de les aider à structurer et maintenir un dispositif de contrôle interne efficace. Elles sont en charge de l'application de la méthodologie, de la formation et du soutien aux opérationnels.

SOX est le vecteur principal du contrôle interne. Les activités de contrôle du dispositif SOX sont implantées au plus près des métiers et des processus, et les responsables de ces activités de contrôle sont choisis au sein des directions fonctionnelles : contrôleurs de gestion, comptables, qualiticiens, responsables des SI… Il y a de fortes interactions entre le contrôle interne, SOX et les directions fonctionnelles.

Mobilité, « *Bring your own device* » et cybercriminalité : faire évoluer ses pratiques face à la réalité des menaces dans le cyberespace

Réunion mensuelle du 21 novembre 2012

Le *BYOD* est une stratégie d'entreprise : des employés apportent sur leur lieu de travail leurs propres équipements qu'ils utilisent pour accéder aux ressources de l'entreprise, comme le courrier électronique, les serveurs de fichiers…

Pourquoi le *BYOD* ?

Pour le *iWorker*, le matériel utilisé est plus ergonomique, plus ludique. Il bénéficie, en outre, d'une

meilleure connectivité. Pour la DSI, il permet de répondre à la pression des utilisateurs, et assure un déploiement plus rapide des nouvelles technologies. Pour l'entreprise, il garantit un meilleur engagement des employés, ainsi qu'une productivité et une motivation améliorées. 65% des *iWorkers* français s'estiment plus productifs avec leurs propres outils qu'avec ceux de leurs employeurs ; 46% des *iWorkers* en France résolvent des problèmes qu'ils ne peuvent pas résoudre avec les outils mis à disposition par la DSI.

Quels sont les risques ?

Les risques techniques : fuite de données ; accès à des informations confidentielles ; usurpation d'identité ; destruction du SI. La criticité de ces risques est toujours importante et parfois majeure.
Les risques organisationnels : d'un point de vue réglementaire, comment sont assurées la gestion des licences, la supervision réglementaire des communications, la traçabilité des opérations ? Du point de vue des RH, à quelles populations l'accessibilité est-elle réservée ? Comment le contrôle du temps de travail pour les collaborateurs non autonomes est-il organisé ? Concernant les coûts, comment se fait la répartition collaborateur/entreprise ? Sous quelle forme (avantages en nature) ? Quel impact en cas de dépassement ?

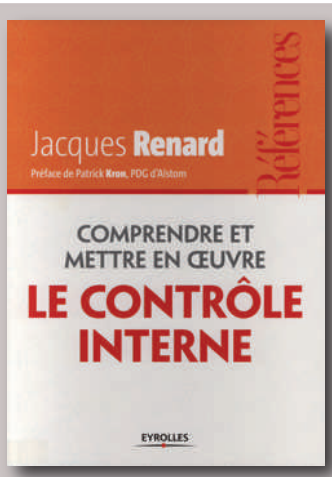
Comment limiter les risques ?

En plaçant l'identité au cœur des préoccupations : qui doit accéder aux systèmes d'information ? En sécurisant les données confidentielles plutôt que les accès ou applications. En se focalisant sur les usages plutôt que sur les droits (habilitations).

Les menaces

Il existe des menaces logicielles relatives à la mobilité et au *BYOD*. Des logiciels permettent de transformer un simple téléphone portable en téléphone « espion ». Un exemple : la manipulation peut être réalisée sur n'importe quel téléphone de dernière génération IPhone, Symbian, Black Berry. L'installation du logiciel sur le téléphone demande trois minutes. Il est alors possible, par l'intermédiaire d'un simple navigateur Web, de connaître le contenu du répertoire, des SMS, des emails, de géolocaliser le téléphone, d'émettre des appels, d'envoyer des SMS, de lire les fichiers, etc., sans que l'utilisateur ne détecte quoi que ce soit. ●

Lu pour vous



Comprendre et mettre en œuvre le contrôle interne

Auteur : Jacques Renard
Editeur : Editions Eyrolles

On a beaucoup dit, beaucoup écrit et beaucoup glosé sur le contrôle interne. Et l'IFACI a largement pris sa part dans ce débat d'idées par les travaux et publications de la Direction Recherche, les colloques, les réunions mensuelles… Il n'est donc pas inutile qu'un auteur se saisisse du sujet pour tenter d'en faire le tour et la synthèse dès l'instant que significativement tous convergent dans une même direction et que les contradictions et les divergences de fond restent exceptionnelles.

C'est ce travail qu'a voulu réaliser Jacques Renard dans son nouvel ouvrage : **« Comprendre et mettre en œuvre le contrôle interne ».** Ouvrage essentiellement didactique et pédagogique et qui rendra à n'en pas douter de nombreux services à ceux qui veulent aller à l'essentiel et bien assimiler les notions fondamentales.

L'ouvrage se découpe en quatre parties. Dans la première partie, Jacques Renard, conformément à son habitude, s'attache au sens des mots, au langage et à la compréhension des concepts, préalables indispensables pour une bonne appréhension du sujet. La seconde partie est une présentation raisonnée des référentiels, textes législatifs et réglementaires qui ont jalonné ces dernières années. Et l'auteur s'attache à en montrer le fil directeur, tous procédant d'un mouvement général vers une plus grande clarification et une plus grande universalité. La troisième partie, très pédagogique, décline de façon pratique le concept de dispositif de contrôle interne. Quant à la dernière partie, elle est consacrée à une méthodologie de mise en œuvre du contrôle interne dans une organisation.

L'ensemble de l'ouvrage est balisé par des « illustrations » qui sont autant d'exemples tirés de l'expérience de l'auteur.

Soulignons que la préface est signée Patrick Kron, PDG d'Alstom, et on se souviendra qu'Alstom a reçu en 2010 le Grand Prix du jury du Trophée du Contrôle interne de l'IFACI : ceci peut expliquer cela.

Vous pouvez consulter cet ouvrage à la bibliothèque de l'IFACI.

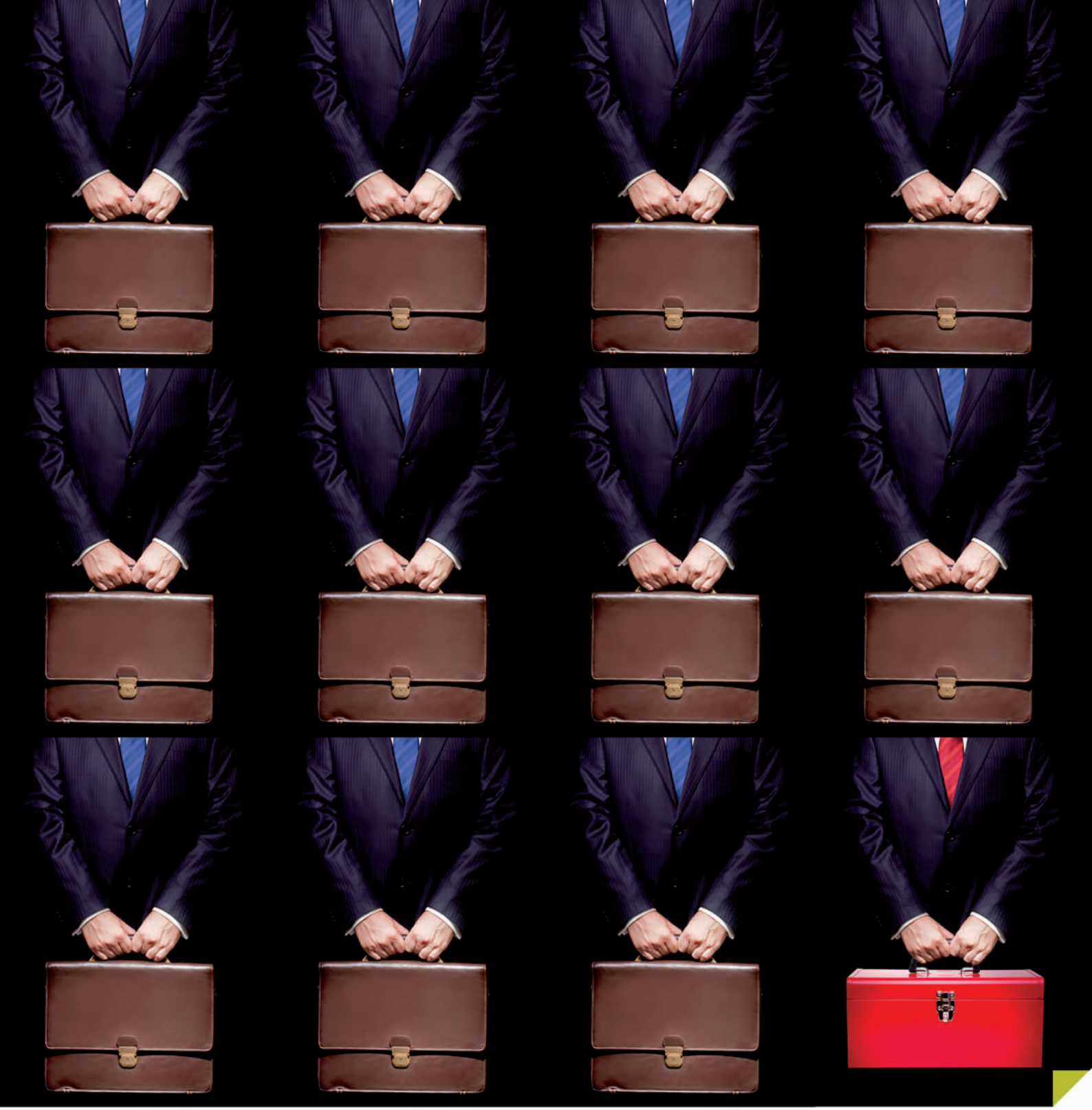
ifaci
institut français de l'audit et du contrôle internes

Calendrier 2013

- 20% pour un participant inscrit simultanément à 4 formations

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

IFACI Formation - Tél. : 01 40 08 48 08 - Mel : formation@ifaci.com - Retrouvez également le programme complet sur le site internet www.ifaci.com



VOUS AVEZ LE **SAVOIR**, NOUS AVONS LES **OUTILS**

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

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

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

IDEA
Logiciel d'analyse de données

CaseWare
IDEA

FICHE TECHNIQUE

Audit & Contrôle internes

Nouvelles Normes : une évolution sous le double sceau de la clarification des responsabilités et de la prise en compte de nouvelles pratiques professionnelles

Béatrice Ki-Zerbo - Directeur de la Recherche, **IFACI**

Conformément aux dispositions prises avec l'adoption du CRIPP (Cadre de référence international des pratiques professionnelles de l'audit interne - IPPF) en 2009, l'IIA s'est engagé à assurer un suivi continu des Normes qui doivent être entièrement revues au moins tous les trois ans. Ce suivi, assuré par le *Standards Board*, peut aboutir à des mises à jour, comme cela a été le cas en janvier 2009 et en 2011. Cet article concerne les mises à jour applicables au 1er janvier 2013. Il fait le lien avec les précédentes évolutions et avec les principes qui sous-tendent l'évolution du CRIPP.

Quelles sont les principales évolutions des Normes 2013 ?

Les récentes modifications des Normes peuvent être schématiquement reliées à deux types d'objectifs :

La **clarification des responsabilités** de l'auditeur interne, du responsable de l'audit interne (RAI), du Conseil	• Responsabilité individuelle / collective (Introduction) • Définition et rôle du Conseil (Glossaire, Normes 1110, 2210.A3) • Rôle du RAI dans la communication des résultats et des niveaux de risques inacceptables (2440, 2600)
La prise en compte de **nouvelles pratiques professionnelles**	• Evaluations externes (1312) • Plan d'audit agile (2010) • Prise en compte des objectifs stratégiques (2120.A1 et 2130.A1) et des processus de gouvernement d'entreprise (2201) • Processus de contrôle • Opinions au niveau d'une mission • Opinion globale

Ces évolutions s'intègrent dans la stratégie de maintenance du CRIPP qui s'articule autour de 3 axes :

1. Clarification :
Des interprétations ont été ajoutées ou précisées. Rappelons qu'elles ont la même valeur obligatoire que l'énoncé principal de la Norme. Le glossaire a également été révisé.

2. Transparence du processus :
Les Normes 2013 ont été élaborées selon un processus accessible sur le site internet de l'IIA pour toutes les parties intéressées. Elles ont en particulier fait l'objet d'une consultation publique. Le suivi de la conformité du processus étant assuré par un *Oversight Council* constitué de parties prenantes externes indépendantes du *Standard Board*.

3. Evolutivité :
C'est l'objet même de cet article. Chaque norme doit être revue au moins tous les 3 ans. En réalité le *Standard Board* est constitué de groupes de travail qui assurent une surveillance régulière de chaque série de normes. Ce suivi permet d'intégrer l'évolution des pratiques professionnelles voire de les anticiper. Il prend également en considération l'évolution des autres composantes du CRIPP.

Des modifications qui s'inscrivent dans la continuité de celles de 2009 et 2011

Il n'y a pas de nouvelles Normes en 2013. Toutes les modifications apportées concernent des normes préexistantes. Les éléments ci-après s'inspirent des travaux menés dans le cadre de l'unité de recherche de l'IFACI qui assure la traduction et l'adaptation du CRIPP.

➲ **Responsabilité individuelle / collective (Introduction)**
L'introduction des Normes a été complétée par un paragraphe spécifiant les responsabilités en ce qui concerne la conformité aux Normes. Il était effectivement nécessaire d'insister sur les exigences professionnelles individuelles et le respect du code de déontologie qui s'impose à chaque auditeur interne. Notons néanmoins que la conformité aux Normes ne dépend pas uniquement de la volonté et du professionnalisme de chaque auditeur interne. Des éléments, tels que la maturité de l'organisation, l'implication des organes dirigeants (notamment en ce qui concerne les Normes de qualification), les ressources effectivement allouées à l'audit interne (notamment en termes d'accès à l'information) entrent également en ligne de compte. C'est pourquoi les responsables de l'audit interne doivent s'assurer que les conditions de cette conformité sont réunies et en rendre compte. Bien entendu leur action sera facilitée par les différentes initiatives au niveau de l'IIA et des instituts locaux pour sensibiliser les parties prenantes de l'audit interne sur l'importance des Normes et la nécessité de donner aux auditeurs internes les moyens de leur professionnalisme.

➲ **Définition et rôle du Conseil (Glossaire, Normes 1110 et 2210.A3)**
Une nouvelle définition du Conseil est proposée dans le glossaire. Elle prend en compte les bonnes pratiques de gouvernance (notamment la notion d'administrateur indépendant) et explicite le fait que le rôle assigné au Conseil dans les Normes peut être assumé par un Comité d'audit « auquel l'organe de gouvernance a délégué certaines fonctions ». L'interprétation de la Norme 1110 a été complétée pour préciser la relation fonctionnelle de l'audit interne avec le Conseil. Ainsi, le budget prévisionnel de l'audit interne et la rémunération du responsable de l'audit interne pourront faire l'objet d'une discussion avec le Conseil. Ils viennent compléter d'au-

tres éléments permettant au Conseil de conforter l'indépendance de l'audit interne. Dans une prise de position commune avec l'IFA, l'IFACI avait également donné des pistes pour entretenir des relations étroites avec le Conseil. Au niveau européen, une prise de position commune ECODA (association européenne des administrateurs) ECIIA (réseau d'instituts d'audit interne) est en cours d'élaboration.

Dans les commentaires des modifications apportées à la Norme 1110, le groupe de travail de l'IFACI a souhaité attirer l'attention sur le fait que :

- l'approbation du budget doit s'appuyer sur l'analyse des critères objectifs, notamment au regard du plan d'audit à réaliser ;
- la discussion sur la rémunération doit être reliée à une évaluation de la performance du responsable de l'audit interne, notamment sur la base de la qualité des informations adressées au Conseil.

En outre, les échanges avec le Conseil pourront porter sur des points significatifs de désaccord avec le management conformément au processus décrit dans la Norme 2600.

Enfin, la Norme 2210.A3 concernant les objectifs de la mission précise désormais le rôle du Conseil dans la définition de critères adéquats servant à apprécier si les objectifs et les buts ont été atteints. Dans la pratique, le Conseil délègue à la direction générale la responsabilité de définir ces critères et d'en rendre compte. Dans l'esprit de la Norme 2600, lorsque les critères d'évaluation sont inadéquats, il y a un risque de non maîtrise des processus qu'il convient de discuter avec les managers concernés puis avec la direction générale et enfin avec le Conseil, lequel intervient en dernier ressort pour les écarts significatifs.

➲ Rôle du RAI dans la communication des résultats et des niveaux de risques inacceptables (2440, 2600)

Le rôle du RAI en matière de revue, d'approbation et de diffusion des résultats est réaffirmé (2440) : « *Lorsque le responsable de l'audit interne délègue ces fonctions, il/elle en garde l'entière responsabilité* ». C'est pourquoi l'unité de recherche recommande que le RAI définisse, a priori, des règles homogènes de diffusion et les modalités d'accès aux rapports d'audit. Ces règles préétablies pourront tenir compte de la complexité et de la sensibilité de la mission. Pour chaque catégorie de mission, des destinataires habituels pourront être identifiés de même que les modalités de gestion des diffusions ou des demandes d'accès exceptionnelles.

La Norme 2600 a été revue pour clarifier le rôle du RAI lorsque le niveau de risque constaté est jugé inacceptable. Dans la pratique, le RAI devra se forger une opinion en fonction de l'appétence au risque et des seuils de tolérance définis par l'organisation, ou de sa perception de la qualité des dispositifs de traitement des risques en place.

➲ Evaluations externes (1312)

Une nouvelle interprétation a été ajoutée à la Norme 1312 pour préciser les modalités d'évaluation externe et de l'implication du Conseil.

Par ailleurs, l'unité de recherche de l'IFACI considère que la direction générale devrait être préalablement informée des modalités d'implication du Conseil et plus particulièrement des éléments qui lui seront communiqués.

La discussion que le RAI doit avoir avec le Conseil sur la fréquence de l'évaluation externe devra tenir compte de l'évolution de l'environnement, du profil de risque de l'organisation, de la sensibilité des parties prenantes, de la nature des travaux de l'audit interne et de son organisation.

➲ Plan d'audit agile (2010)

L'interprétation de la Norme 2010 a été complétée pour inciter les responsables d'audit interne à réviser, dès qu'ils le jugent nécessaire, le plan d'audit (et pas uniquement à l'échéance annuelle habituelle). Néanmoins l'unité de recherche insiste sur la qualité de la préparation du plan initial qui est un « contrat » passé avec les organes dirigeants. Il convient de limiter leur sollicitation. Ce serait donner un mauvais signal quant au professionnalisme de l'audit interne si ces modifications étaient prévisibles.

➲ Prise en compte des objectifs stratégiques (2120.A1 et 2130.A1) et des processus de gouvernement d'entreprise (2201, 2210.A3)

Désormais l'évaluation des processus de contrôle et de management des risques doivent prendre en compte les objectifs stratégiques en plus des quatre objectifs classiques que sont :

- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

Les critères d'évaluation à prendre en considération lors de la définition des objectifs de la mission ne concernent plus uniquement les processus de contrôle ; la Norme 2210.A3 intègre désormais les processus de management des risques et de gouvernement d'entreprise. Ce dernier a également été rajouté dans la Norme 2201 « considérations relatives à la planification ».

➲ Processus de contrôle

La définition du processus de contrôle est précisée pour prendre en compte les contrôles automatisés et la notion d'appétit pour le risque de l'organisation.

➲ Opinions au niveau d'une mission et opinion globale

Les opinions d'audit introduites dans la version de 2011 sont expliquées dans le glossaire. Notons qu'un guide pratique a été publié sur ces modalités de communication des résultats de l'audit interne.

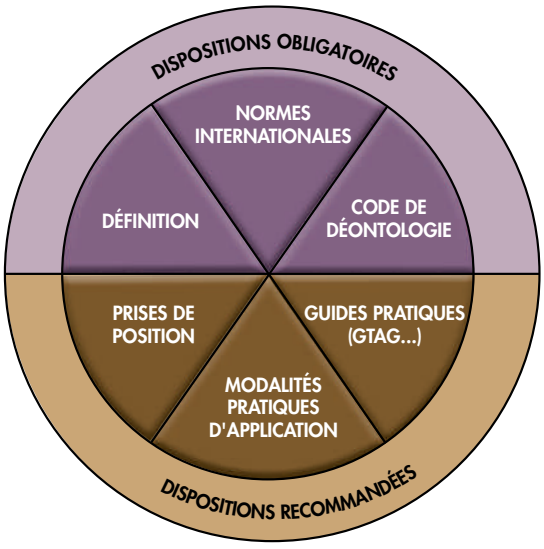
Toutes ces modifications s'inscrivent dans la continuité par rapport aux précédentes évolutions. Ainsi, en 2009 six nouvelles normes avaient été ajoutées selon 3 axes :

- Une réaffirmation du **professionnalisme** de l'audit interne en rappelant les dispositions obligatoires dans la charte et l'utilisation de la **mention de conformité aux Normes.** Cette orientation se retrouve dans l'évolution de l'introduction des Normes 2013.
- L'importance de l'**objectivité et de l'indépendance** qui passe par la **relation avec le Conseil** ou la vigilance sur **l'implication des audits internes dans les processus de management des risques.** Les relations fonctionnelles avec le Conseil (dont la nouvelle définition évite la confusion avec d'autres types d'instances), gage de l'indépendance de l'audit interne sont précisées dans l'interprétation de la Norme 1110. L'implication de l'audit interne dans la gestion des risques est de nouveau abordée à travers la Norme 2600.
- De **nouvelles thématiques** prenant en compte l'évolution des **pratiques des auditeurs internes** et du **niveau de maturité** des organisations (audit de la **gouvernance des SI, risque de fraude**). En 2013, l'accent est mis sur la flexibilité du plan d'audit annuel ainsi que sur la prise en compte des objectifs stratégiques.

En 2011, deux nouvelles normes prenaient en compte l'évolution des pratiques des auditeurs internes à travers les opinions de l'audit interne. La formulation de ces normes est d'ailleurs assez intéressante puisqu'elle n'oblige pas l'audit interne à émettre de telles opinions mais plutôt à s'interroger sur les attentes des organes dirigeants en la matière et le cas échéant le format de telles opinions. Le glossaire 2013 précise la distinction entre « opinion au niveau d'une mission » et « opinion globale ». De même, le cru 2011 avait permis de développer des thématiques liées à l'indépendance de l'audit interne et l'évaluation du processus de management des risques.

Au-delà des Normes, une maintenance en continu de chaque composante du CRIPP

L'évolution des Normes est d'autant plus importante que ce sont des composantes clés du CRIPP. En effet, au cœur des dispositions obligatoires, les Normes prescrivent des principes qui sont directement liés à l'énoncé de la Définition et du Code de déontologie. En outre, chaque disposition fortement recommandée peut être reliée à une norme.



Les dispositions recommandées évoluent à leur propre rythme. Ainsi, début novembre, un inventaire des parutions 2012 des guides pratiques permettait de dénombrer 11 nouvelles publications. Pour mémoire, il s'agit de :

- Assessing Organizational Governance in the Private Sector
- Developing the Internal Audit Strategic Plan
- GTAG - Auditing IT governance
- GTAG - Information technology outsourcing (2nd edition)
- GTAG - Change and patch management controls (2nd edition)
- GTAG - Information technology risk and controls (2nd edition)
- Auditing Privacy Risks, 2nd Edition (remplace le GTAG 5)
- Integrated Auditing
- Evaluating Ethics-related Programs and Activities
- Quality assurance and improvement program
- Coordinating Risk Management and Assurance

Au-delà des Normes, il est donc important de se tenir régulièrement informé de la parution de ces documents.

En outre, un processus de révision de la Définition adoptée en 1999 est en cours. Nous aurons plus d'informations début 2013 sur l'option retenue par l'IIA : soit un maintien de la définition actuelle, soit une nouvelle définition. Au-delà des résultats de ces différentes évolutions qui aboutissent à des lignes directrices et à des propositions pratiques lesquelles ont une incidence directe sur la pratique de l'audit interne, il est intéressant de noter à quel point l'IIA tient à s'appliquer le principe de l'amélioration continue. En effet, toutes les composantes sont régulièrement révisées et un processus d'élaboration et de validation a été formalisé. En d'autres termes le CRIPP a son dispositif de contrôle interne. ●