revue internationale des auditeurs et des contrôleurs internes

audit & risques & contrôle

« ON NE PEUT OPPOSER INNOVATION ET PROTECTION DES DONNÉES PERSONNELLES »

Isabelle Falque-Pierrotin
Présidente de la CNIL

DOSSIER

Cybersécurité et protection des données

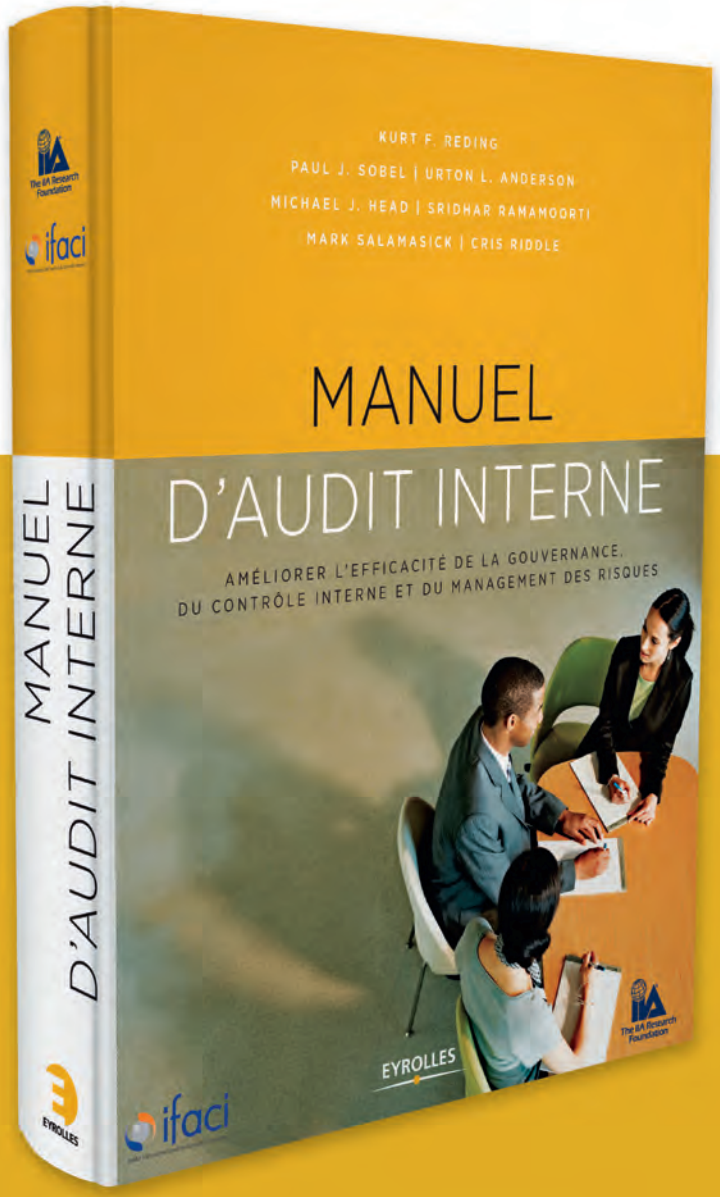
Quel rôle pour l'audit interne ?

N°003
3e trimestre 2015

ifaci
institut français de l'audit et du contrôle internes

The Institute of Internal Auditors

LA NOUVELLE ÉDITION DU MANUEL D'AUDIT INTERNE



DÉJÀ PARU :
LE COSO ET LES OUTILS DE L'AUDIT INTERNE

ifaci — EYROLLES — The IIA Research Foundation

audit, risques & contrôle

SOMMAIRE

05 EDITO

Cybersécurité et protection des données
Quel rôle pour l'audit interne ?

06 CHRONIQUE

Attaques informatiques
3 déclinaisons pour un risque en forte hausse

08 VOIX DE LA FRANCOPHONIE

La force du réseau de l'UFAI
ses conférences et colloques

10 RENCONTRE AVEC ...

Isabelle Falque-Pierrotin, Présidente de la CNIL

15 DOSSIER

16 Cybersécurité : un domaine incontournable et à valeur ajoutée pour l'audit interne

19 Tendances significatives de l'enquête Global State of Information Security 2014 de PwC

22 Cybersécurité et protection des données personnelles : le point de vue du Cigref

24 La conformité à la loi informatique et libertés a été un levier d'action

25 Une action conjointe des deuxième et troisième lignes de maîtrise

26 L'audit interne face aux risques de cybersécurité

30 LIBRES PROPOS

Pour une nouvelle approche intégrée
Objectifs, processus, risques, contrôles et gouvernance

35 BONNES PRATIQUES

La fraude interne dans les collectivité territoriales : Un risque zéro ?

37 PRIX OLIVIER LEMANT

Trois réflexions sur les outils développés sur Excel

39 LU POUR VOUS

39 Le business de l'anti-corruption

41 Guide d'audit des achats et des ventes

42 ACTUALITÉ

15 DOSSIER
Cybersécurité et protection des données : Quel rôle pour l'audit interne ?

Cadre de référence pour un audit interne efficace

Le nouveau CRIPP

CRIPP

Cadre de Référence International des Pratiques Professionnelles de l'audit interne

Des évolutions dans l'environnement économique et des risques associés en perpétuelle accélération

L'exercice de l'audit interne engage des responsabilités. D'où la nécessité d'un cadre de référence avec des principes clairement énoncés, des normes reflétant des pratiques exemplaires et, des lignes directrices publiées en temps opportun qui ne se contentent pas de prendre en compte les changements mais les anticipent.

Afin que l'audit interne puisse garder le cap dans un environnement en constante évolution, le Cadre de Référence International des Pratiques Professionnelles (CRIPP) doit également évoluer pour accompagner efficacement la profession et répondre aux futurs défis (instabilité du profil de risque, modification des attentes des parties prenantes, exigences légales et réglementaires concernant l'amélioration de la gouvernance, de la gestion des risques et du contrôle interne).

En savoir plus sur le nouveau CRIPP, la mission de l'audit interne, les principes fondamentaux pour la pratique professionnelle de l'audit interne ainsi que les améliorations à venir.

www.theiia.org/goto/IPPF

The Institute of Internal Auditors

audit, risques & contrôle
La revue internationale des auditeurs et des contrôleurs internes
n°003 - 3e trimestre 2015

EDITEUR
Union Francophone de l'Audit Interne (UFAI)
Association Loi 1901
98 bis, boulevard Haussmann - 75008 Paris (France)
Tél. : 01 40 08 48 00 - Mel : institut@ifaci.com
Internet : www.ufai.org

DIRECTEUR DE PUBLICATION
Mireille Harnois

RESPONSABLE DE LA RÉDACTION
Philippe Mocquard

RÉDACTEUR EN CHEF
Louis Vaurs

COMITÉ RÉDACTIONNEL
Louis Vaurs - Mireille Harnois - Eric Blanc - Antoine de Boissieu - Jean-Loup Rouff

SECRÉTARIAT GÉNÉRAL
Eric Blanc - Tél. : 06 15 04 56 32 - Mel : eblanc@ifaci.com

CORRESPONDANTS
Amérique : Farid Al Mahsani
Maghreb : Nourdine Khatal
Afrique subsaharienne : Fassery Doumbia

RÉALISATION
EBZONE Communication
22, rue Rambuteau - 75003 Paris
Tél. : 01 40 09 24 32 - Mel : ebzone@ebzone.fr

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

ABONNEMENT
Michèle Azulay - Tél. : 01 40 08 48 15
Mel : mazulay@ifaci.com

Revue trimestrielle (4 numéros par an)
ISSN : 2427-3260
Dépôt légal : octobre 2015
Crédit photos couverture : © CNIL

Prix de vente au numéro : 25 € TTC

Les articles sont présentés sous la responsabilité de leurs auteurs.

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

IMPRIM'VERT
Cette revue est imprimée avec des encres végétales.

PEFC
Certifié PEFC
pefc-france.org

Cybersécurité et protection des données

Quel rôle pour l'audit interne ?

Selon l'enquête de PwC de 2014 dédiée à la cybercriminalité, les cyber-attaques sont en augmentation, et l'Europe et les grandes entreprises sont particulièrement menacées. Dans le dernier baromètre des risques publié par Allianz, le risque « cyber » figure à présent dans le top 5 des menaces identifiées par les entreprises.

La cybersécurité autour des données personnelles est un enjeu important pour toutes les organisations, et les auditeurs internes doivent y prendre toute leur part. Le « Dossier » de ce numéro ainsi que la chronique d'Antoine de Boissieu lui sont consacrés.

Lorsqu'on parle de données personnelles et de leur nécessaire protection, on pense immédiatement à la CNIL (Commission Nationale de l'Informatique et des Libertés). Je vous recommande la lecture de l'entretien qu'a bien voulu nous accorder Isabelle Falque-Pierrotin, sa présidente. Au fil des ans, nous dit-elle, la CNIL s'est métamorphosée ; elle est devenue « un régulateur des données personnelles, ce qui va bien au-delà de la seule protection de l'individu ». La CNIL s'est notamment dotée d'un département Innovation et Prospective, et Isabelle Falque-Pierrotin « s'inscrit en faux avec l'idée qu'il faut opposer innovation et protection des données personnelles ». Un texte européen est en discussion finale et devrait aboutir dans le courant de cette année, avec application directe en 2017. « Ce règlement, précise-t-elle, devrait être un coup de tonnerre : il allège fortement le contrôle amont et renforce considérablement le contrôle aval ce qui devrait mobiliser grandement les auditeurs internes ».

Enfin, la président de la CNIL nous fait part de l'existence d'un réseau francophone des Autorités de protection des données regroupant 16 pays, le secrétariat étant assuré par l'Autorité française. Son objectif qui est de « mutualiser le plus possible les ressources, les transferts de compétence entre le nord et le sud » est évidemment en phase avec celui que poursuit l'UFAI comme Mireille Harnois, sa présidente, en fait la démonstration dans la rubrique la Voix de la Francophonie.

L'article de Tommaso Capurso « Pour une nouvelle approche intégrée : processus, risques, contrôle et gouvernance » mérite toute votre attention. Il y développe notamment l'approche cindynique de la gouvernance intégrée en précisant qu'une « gouvernance efficace doit viser à assurer la transparence, la confiance et éviter idéalement toute asymétrie de l'information »

Vous pourrez lire également un article fort intéressant du groupe professionnel « Collectivités locales » sur la fraude interne dans les collectivités territoriales avant la parution, d'ici à la fin de l'année, d'un document plus complet sur ce thème.

Le prix Olivier Lemant a été attribué cette année à un mémoire étudiant consacré à « l'audit de la gestion et de l'architecture des UDA développés sur Excel ». Vous pourrez en lire une synthèse dans ce numéro.

Etonnant et passionnant l'article sur « Le *business* de l'anticorruption » tiré de The Economist, qu'il ne faut pas oublier de lire.

Dans son « Guide d'audit des achats et des ventes », Pierre Schick se fait le chantre de l'auto-diagnostic. Il nous en donne les raisons dans ce numéro.

Bonne lecture. ■

Louis Vaurs - *Rédacteur en chef*

Après avoir été pendant 15 ans un acteur clé de la revue de l'IFACI, Jean-Loup Rouff a souhaité, pour des raisons personnelles, arrêter sa contribution active à la revue internationale AR&C. Au nom comité de rédaction, je tiens à le remercier chaleureusement pour tout ce qu'il a apporté à la revue, sa compétence, ses connaissances, sa disponibilité et… un sens inné de l'écrit « en bon français ». Merci infiniment Jean-Loup.

Attaques informatiques

3 déclinaisons pour un risque en forte hausse

Le piratage du site de rencontres extra-conjugales Ashley Madison a fait les gros titres des journaux cet été. Il a remplacé dans l'actualité le piratage des données personnelles de 25 millions de fonctionnaires américains, révélé en juin dernier. Il ne se passe désormais plus de mois sans qu'une attaque informatique majeure n'aboutisse.

On peut distinguer 3 risques différents dans ces attaques qui visent les données des entreprises et des administrations.

1- L'espionnage industriel

Le premier type d'attaques concerne l'espionnage industriel et commercial. Le phénomène n'est pas nouveau, et il est logique que le cyber-espionnage se développe en complément des techniques classiques d'espionnage industriel. Les cas de cyber-espionnage sont généralement peu médiatisés : les attaquants (« cyber-pirates ») ont en effet tout intérêt à dissimuler leurs attaques, tandis que les cibles soit n'ont pas conscience d'avoir été attaquées, soit n'ont pas d'intérêt à le révéler sur la place publique. Le fait qu'il ne fasse que rarement la une des journaux ne signifie pas que le cyber-espionnage soit un phénomène marginal, encore moins qu'il soit en déclin.

Une hausse de 50 % en 2014

Dans une étude de juillet 2015, le FBI estime ainsi que le nombre de cas a augmenté de 50 % en un an aux Etats-Unis. Le 31 août, le Washington Post annonçait que le gouvernement américain étudiait des mesures de rétorsion à l'encontre de la Chine, l'accusant d'avoir porté le cyber-espionnage à un niveau insupportable.

De façon générale, les secteurs d'activité les plus exposés sont les secteurs traditionnels de l'espionnage industriel : l'aéronautique et la défense, la pharmacie, l'automobile, l'ingénierie, les sociétés technologiques (dans l'énergie, les télécoms, l'industrie du logiciel...). L'espionnage commercial proprement dit touche également, outre les secteurs précédents, le BTP, les fournisseurs de biens d'équipement, le secteur des matières premières.

Des attaques tentantes car peu risquées

Mais potentiellement, avec le développement des ERP, de la messagerie, du *cloud*, de l'externalisation, tous les secteurs d'activité deviennent des cibles abordables pour le cyber-espionnage. Les attaques deviennent de plus en plus tentantes parce qu'elles peuvent être menées de l'étranger, de façon discrète et difficile à tracer, avec de faibles moyens. Comme le démontrent de nombreux tests d'intrusion positifs, la principale difficulté pour les *hackers* n'est pas d'accéder aux données de l'entreprise ciblée, mais d'exploiter la masse de données récupérées. Des *hackers* bien dirigés, par exemple par une équipe d'un concurrent, peuvent cependant trouver rapidement ce qu'ils cherchent.

Une position américaine ambigüe

Dans ce contexte, l'indignation américaine vis à vis de la Chine ne manque pas d'ironie, compte tenu des capacités d'accès aux données d'entreprises dont disposent les Etats-Unis, que ce soit via leurs programmes de surveillance (autorisés ou non), leurs officines spécialisées (d'ex de la NSA ou de la CIA), ou leurs programmes de *« monitoring »* imposés aux sociétés (généralement européennes) ayant conclu des accords à l'amiable avec la justice.

2- Le vol des données individuelles

Le deuxième type d'attaques informatiques consiste à voler les données d'une administration ou d'une entreprise pour les revendre. Les données visées sont les données individuelles des clients, usagers, employés, adhérents... Des dizaines de cas, portant parfois sur des millions de personnes, sont révélés chaque année. On pourrait se demander comment les pirates peuvent exploiter les bases de données individuelles récupérées, et à qui ils peuvent les revendre. Plusieurs solutions sont possibles (voir encadré).

Des attaques massives et systématiques dans certains secteurs

Nous reviendrons dans un prochain article sur ces différents cas, en analysant certains exemples récents. Ce qu'il faut retenir de ce phénomène est qu'il a littéralement explosé depuis 2008, pour devenir systématique dans tous les secteurs qui gèrent des données personnelles : santé, assurance, banque, hôtellerie, opérateurs téléphoniques, vendeurs en ligne, grande distribution, sociétés internet B to C, administrations publiques... Les cibles potentielles subissent généralement des milliers (parfois beaucoup plus) de tentatives d'attaques chaque année, certaines atteignant des niveaux de sophistication très élevés.

Un report des attaques vers des cibles plus petites, moins défendues

En réaction, les secteurs exposés ont mis en place des défenses de plus en plus élaborées. Les pirates commencent donc à s'attaquer à des cibles plus petites, moins intéressantes, mais beaucoup moins défendues. Autrement dit, le risque est en train de se déplacer vers les secteurs jusqu'ici relativement épargnés, mais qui pour cette raison n'ont pas encore mis

© DreamA - Fotolia.com

en œuvre les mesures de défense adéquates. Les données RH d'une moyenne entreprise, la liste des clients fidèles d'une boutique de luxe, ou la liste des clients d'un cabinet d'avocats fiscalistes deviennent désormais des cibles valables pour des cyber-pirates.

3- Le sabotage en ligne

Le troisième type d'attaques informatiques est le sabotage en ligne, ou « cyber-sabotage ». C'est sans aucun doute le moins courant, mais c'est celui qui peut avoir les impacts les plus forts, beaucoup plus qu'une perte de secret industriel ou que la divulgation de données clients.
Dans le sabotage en ligne, le but n'est plus de consulter les données de la cible, ou de les voler pour les revendre : il s'agit de modifier les données dans les systèmes de la cible, à son insu.

Données ciblées	Exploitation
Coordonnées bancaires, numéros de cartes de crédit	Réalisation d'achats en ligne (les systèmes de paiement en ligne sont moins sécurisés en Amérique et en Asie qu'en Europe)
Numéros de police d'assurance-santé	Usurpation d'identité pour bénéficier d'une prise en charge hospitalière ou médicale (aux Etats-Unis notamment ou le système d'assurance-santé est privé)
Déclarations de revenus, adresses, données familiales	Ciblage de campagnes publicitaires
Base de données des programmes de fidélisation	Usurpation d'identité pour bénéficier des avantages réservés aux clients membres (aérien, hôtellerie, transports...)
Données d'état civil, déclarations de revenus	Chantage à la divulgation (sites de rencontres, administrations publiques...)
Liste des clients avec le montant des avoirs	Chantage à la divulgation (banque d'affaires, gestionnaires de patrimoine)

On pourrait se demander quel est l'intérêt pour l'attaquant. Pour un attaquant réellement mal intentionné, le cyber-sabotage ouvre plusieurs perspectives très intéressantes.

Perturber le fonctionnement

La première utilisation consiste à perturber les processus de la cible, par exemple le processus de production. C'est ce qu'ont fait les « mystérieux »[1] auteurs du virus *Stuxnet* pour saboter les centrifugeuses iraniennes. Les déclinaisons possibles de cette idée sont illimitées : on peut par exemple modifier les données cliniques recueillies par une entreprise pharmaceutique pour retarder son programme de R&D, modifier les systèmes de mesure sur une chaîne de production, modifier le réglage de robots afin d'augmenter le nombre d'incidents de production ou de produits non conformes, modifier les bases clients pour perturber la facturation...

Interrompre l'activité

La deuxième utilisation du cyber-sabotage peut être d'arrêter purement et simplement les opérations de la cible, en mettant ses systèmes de production hors service. C'est par exemple ce qu'ont fait les équipes de guerre électronique nord-coréenne lorsqu'elles ont attaqué des banques et des médias sud-coréens en 2013. Des tentatives du même type contre des centrales électriques ont aussi été détectées avant qu'elles aboutissent. Là encore, compte tenu de l'automatisation croissante des processus de production, qu'il s'agisse de biens ou de services, la liste des cibles possibles est illimitée.

Détruire les actifs

La troisième utilisation possible est la plus inquiétante : il s'agit de prendre le contrôle du système de la cible non pas pour l'empêcher de fonctionner, mais pour détruire les actifs de production (voire plus, selon les intentions de l'attaquant).
C'est par exemple ce qu'ont réussi des cyber-pirates en attaquant une entreprise sidérurgique allemande en 2014. L'attaque a été détectée et stoppée, mais le haut-fourneau visé avait été endommagé. Il a dû être arrêté pendant plusieurs mois avant d'être remis en service. Les impacts se chiffreraient en millions, voire en dizaines de millions, d'euros. Dans ce cas, la motivation des pirates était financière (il s'agissait de chantage), mais elles auraient pu être différentes.
Potentiellement, des cyber-pirates pourraient prendre le contrôle de nombreux systèmes connectés. Des chercheurs américains ont ainsi réussi cet été à prendre le contrôle par internet d'une Jeep Cherokee, sans intention maligne, mais obligeant tout de même Fiat Chrysler (le constructeur) à rappeler 1,4 millions de véhicules pour installer une mise à jour du système. L'opération a sans doute dû coûter pas loin de 50 M$.

Vivre avec le risque

Des risques qui ne peuvent qu'augmenter

Trois tendances lourdes font que ces attaques ne vont pas diminuer, mais vont au contraire se multiplier et se complexifier :

1- Le nombre d'objets connectés explose : par exemple, selon une étude d'IHS, le nombre de voitures connectées à internet passera de 35 millions en 2015 à plus de 150 millions en 2020. Cela multiplie donc les cibles potentielles.
2- Les entreprises et administrations perdent le contrôle physique de leurs données : elles utilisent de plus en plus des infrastructures et des réseaux publics, connectés entre eux (donc accessibles de l'extérieur). Cela multiplie les possibilités d'accéder aux données.
3- Les entreprises et administrations perdent le contrôle des systèmes utilisés : les programmes sont développés par des fournisseurs, la maintenance applicative et l'exploitation sont de plus en plus externalisées, les serveurs sont de plus en plus gérés par des tiers (hébergeurs, solutions *cloud*). Tout cela multiplie le nombre de personnes, et de tiers, pouvant avoir accès aux systèmes.

Intégrer les cyber-risques à la prise de décision

Les risques de cyber-attaque doivent désormais être considérés comme des risques inhérents à toute activité. Les décideurs doivent en particulier s'interroger sur la façon dont ils veulent gérer ces risques, en répondant notamment aux questions suivantes :

- à quels risques d'attaques veut-on s'exposer ?
- faut-il transférer la gestion de ces risques à des partenaires mieux outillés ?
- faut-il mettre tous ses œufs dans le même panier, ou prévoir différentes solutions (par exemple en répartissant les données sensibles entre plusieurs bases de données gérées par des systèmes différents) ?

Le défi pour certaines organisations, publiques ou privées, va être de faire évoluer le management au même rythme que les technologies. Les risques de cyber-sécurité pouvaient en effet jusqu'à il y a peu être considérés comme secondaires, non stratégiques et purement techniques. Leur évolution brutale oblige maintenant les décideurs, au plus haut niveau, à les intégrer dans leur processus de décision. ■

Antoine de Boissieu

[1] *Tout désigne les gouvernements américain et israélien, qui n'ont d'ailleurs jamais démenti.*

© vege - Fotolia.com

La force du réseau de l'UFAI : ses conférences et colloques

« L'Union fait la Force ». Ce proverbe qui remonte au 18ème siècle, s'applique parfaitement aux communautés francophones qui font la force du réseau de l'Union Francophone de l'Audit Interne (UFAI).

En juin dernier nous rappelions que le pourcentage de francophones au sein de l'IIA ne représentait que 5 % des adhérents de l'IIA, d'où la nécessité de mutualiser les énergies et de développer nos capacités de renforcement.

IIA Côte d'Ivoire a depuis bien longtemps senti ce besoin et a régulièrement provoqué des rencontres et organisé des colloques permettant de réunir la communauté d'auditeurs francophones afin d'échanger, d'apprendre et de renforcer les liens. L'UFAI était en Côte d'Ivoire déjà en 2010, en 2013 et, tout récemment, pour le 2ème colloque régional de l'**Union des Instituts d'Audit Interne de l'Afrique de l'Ouest (UIAI-AO)**.

En 2011, nous avions vécu la naissance du 1er colloque régional de l'UIAI-AO tenu à Ouagadougou (Burkina Faso) et c'est avec un succès renouvelé que s'est tenue cette deuxième édition, les 18 et 19 juin, en cette « terre éternelle d'accueil ».

Sous le thème « Audit interne, acteur majeur de la mise en œuvre de la directive financière de l'UEMOA et de la gouvernance des entreprises publiques et privées de l'espace UEMOA », cette rencontre internationale s'est avérée un lieu privilégié pour regrouper les instituts régionaux, les autorités, les acteurs clés, et permettre d'échanger entre professionnels de l'audit interne et décideurs.

L'Union Économique et Monétaire Ouest Africaine (UEMOA), créée en 1994, couvre une superficie de 3 509 600 km² et compte plus de 103 millions d'habitants. Huit États côtiers et sahéliens, liés par l'usage d'une monnaie commune, soit le franc CFA, et bénéficiant de traditions culturelles communes composent l'UEMOA : le Bénin, le Burkina Faso, la Côte d'Ivoire, la Guinée-Bissau, le Mali, le Niger, le Sénégal et le Togo.

L'objectif essentiel de l'UEMOA est l'édification, en Afrique de l'Ouest, d'un espace économique harmonisé et intégré, au sein duquel est assurée une totale liberté de circulation des personnes, des capitaux, des biens, des services et des facteurs de production.

UFAI, UIAI-AO et UEMOA, trois unions réunies !

Cette rencontre à Yamoussoukro restera marquée dans les esprits puisqu'elle a donné lieu à des mises à jour importantes, des échanges précieux et essentiels sur l'état des lieux permettant de partager les préoccupations mais aussi d'apporter des recommandations et des pistes de solutions

POUR ALLER PLUS LOIN ...

http://www.lepatriote.net/actualite_det.php?id=3317

http://carnetdadresses.info/gouvernance-des-entreprises-les-premiers-rapports-bientot-disponibles/

à différents niveaux, du contrôle interne, à la gouvernance.
Nous avons entendu et bien retenu les propos de Monsieur Abdourahmane Cissé, ministre auprès du 1er ministre chargé du budget : transposition de la directive « Transparence » de l'UEMOA ; feuilles de route pour les dirigeants des entreprises publiques en matière de bonne gouvernance ; création de comité d'audit dans toutes les structures bénéficiant de fonds de l'Etat.
Nous avons également pris bonne note de l'intervention de madame Viviane Zunon-Kipre, présidente de l'Institut National des Administrateurs de la Côte d'Ivoire (INAD CI), qui considère l'audit interne comme un acteur important de la bonne gouvernance et qui s'efforce de sensibiliser les conseils d'administration sur la nécessité de disposer dans toute organisation d'un contrôle interne efficient.

Il y a encore de grandes choses à bâtir et c'est la mutualisation des énergies entre les organisations, les autorités, et les Instituts qui permettront d'avancer à grand pas.

À l'IIA on vit le progrès par le partage. Dans sa mission, l'UFAI apporte son soutien et ses contributions par le biais de gens passionnés de l'audit interne qui se réjouissent de faire avancer la profession.

La mission et les objectifs principaux de l'UFAI vivent à travers ces rencontres qui permettent d'échanger mais aussi de développer des pistes d'accompagnement et de collaborations avec les différentes organisations.
De ces colloques naissent des idées et des initiatives pour faire progresser et évoluer nos sociétés et nos communautés.

Conférence du 30ème anniversaire de l'IIA-Maroc

Dans ce même état d'esprit, en y ajoutant un volet célébrations, l'IIA Maroc (AMACI) a organisé en mai dernier sa Conférence du 30ème anniversaire de l'IIA Maroc avec pour thème « L'audit interne, face aux nouveaux défis ». Les sujets traitaient des changements environnementaux, technologiques, réglementaires ou professionnels et ont suscité de riches débats. Bien entendu, la gouvernance était au rendez-vous, un incontournable, les compétences maintenant recherchées, les nouvelles approches méthodologiques et les nouvelles synergies entre audit interne et audit externe.

L'audit interne fait face à de nouveaux défis

Le rôle et la perception de l'audit interne ont subi une transformation majeure depuis 20 ans mais plus particulièrement au cours de la dernière décennie. La complexité des opérations, l'émergence des technologies nouvelles, les exigences croissantes des dirigeants et des régulateurs, la lutte contre la fraude et la corruption ont entraîné un profond changement dans le monde de l'entreprise et des organisations. À cela s'ajoutent l'obligation de résultats ainsi que la quête de transparence. En conséquence, l'audit interne a ainsi vu ses responsabilités augmentées. Les attentes des parties prenantes se sont accrues et l'audit interne se voit de plus en plus sollicité.
Il importe que les auditeurs internes prennent conscience de l'importance de leur rôle et de leur apport évident à la bonne gouvernance des organisations.

Ce colloque en terre marocaine venait bien à propos pour traiter de tous ces sujets et provoquer des discussions animées.

Nous avons tous encore grandi par le biais de ces rencontres du réseau francophone, qui permettent d'approfondir nos connaissances et solidifier notre profession au service des organisations. ■

Mireille Harnois, Présidente de l'Union Francophone de l'Audit Interne

Colloque international et rencontre de l'UFAI, l'UIAI-AO et l'UEMOA (Yamoussoukro, Côte d'Ivoire)
Première rangée au centre : Madame Alimata Soumahoro, présidente UIAI-AO ; Madame Mireille Harnois, présidente UFAI ; Monsieur Abdourahmane Cissé, ministre auprès du 1er ministre chargé du budget

L'Union des Instituts d'Audit Interne de l'Afrique de l'Ouest (UIAI-AO) a tenu à Yamoussoukro, son Assemblée. L'UFAI tient à féliciter et réitérer sa collaboration aux nouveaux membres du Bureau directeur dont la présidence sera assumée par Madame Alimata Soumahoro (Côte d'Ivoire). Les membres du Bureau sont : Kadiatou Konate (Mali), Amadou Djibo (Niger) et Maxime Soffonou (Bénin).

Bon succès à la nouvelle équipe.

On ne peut opposer innovation et protection des données personnelles

Isabelle Falque-Pierrotin, Présidente de la CNIL

Louis Vaurs : Créée en 1978, la Commission Nationale de l'Informatique et des Libertés (CNIL) est une autorité administrative indépendante dont l'objectif principal était au départ de protéger l'individu par rapport à l'informatisation de l'Etat. Qu'en est-il aujourd'hui ? Ses responsabilités ont elles évoluées ?

Isabelle Falque-Pierrotin : Nous avons plus qu'évolué. La CNIL s'est métamorphosée. En 1978, son objectif principal était de protéger l'individu contre les grands fichiers publics et quelques traitements privés. Il lui appartenait de prévoir des règles précises pour garantir les droits de l'individu par rapport à cette informatisation de l'administration. Et vous vous souvenez, il y avait ce fameux projet Safari, avec l'idée d'avoir un identifiant unique, et donc que l'individu puisse être vraiment tracé dans tous ses contacts avec l'administration.

C'est bien sûr encore le métier de la CNIL. Mais sa responsabilité principale, actuellement, c'est surtout d'être un régulateur des données personnelles, ce qui va bien au-delà de la seule protection de l'individu compte tenu de la place que ces données ont pris, et de leur importance économique qu'elles n'avaient pas dans les années 80. Il y a donc tout un champ nouveau de la régulation des données pour qu'elles puissent être utilisées par les entreprises, à des finalités parfaitement légitimes, mais tout en préservant le droit des personnes.

L'autre champ ouvert concerne les individus eux-mêmes, qui ne souhaitent pas seulement que les données sur leur vie privée soient protégées, mais qu'ils puissent les

utiliser pour avoir aussi une vie publique, une identité numérique, une expérience de vie en ligne. Nous nous retrouvons donc face à des aspirations des individus mais aussi des acteurs économiques, qui sont beaucoup plus complexes que celles qui existaient auparavant.

Il y a 20 ans, on demandait simplement au régulateur d'assurer la protection. Aujourd'hui, il doit assurer la conciliation entre un objectif de protection des droits des personnes et les nouvelles demandes vis-à-vis des données, exprimées tant par les individus que par les entreprises. Tout cela a un impact sur les métiers de la CNIL. En particulier, Il faut être conscient de tout ce que les innovations technologiques permettent, de tout ce qu'elles peuvent apporter au *business*, de tout ce qu'elles peuvent offrir comme nouveaux services. C'est pourquoi il était devenu impératif de développer l'activité Prospective / Innovation de la CNIL.

Confrontée à cette abondance des données, il n'était pas possible de réagir de façon statique. Les technologies évoluent énormément et le régulateur doit être capable d'anticiper ces nouvelles demandes sociales. Il a donc été créé, au sein de la CNIL, un département Innovation et Prospective, extrêmement important, avec un laboratoire qui nous permet de tester des produits ou des services. Dans le même esprit, la CNIL s'est ouverte considérablement aux autres acteurs, car il est évident que la CNIL Régulateur ne peut pas être une CNIL enfermée dans une tour d'ivoire. Nous sommes donc conduits à travailler avec d'autres, beaucoup plus que par le passé. Nous avons toute une activité à destination des centres de recherche, des *start-ups*, pour nous imprégner des écosystèmes très compliqués qui se développent autour des données.

L. V. : Ce département Innovation dispose-t-il d'un effectif nombreux ? Quel est le profil de ses membres ?

I. F.-P. : Ce sont des ingénieurs, des prospectivistes, des économistes.

Ils sont cinq. Mais en réalité, ils sont adossés au département de l'expertise technique de la CNIL qui, lui, s'est considérablement renforcé dans les années récentes.

C'est toute une direction qui regroupe l'expertise technique et les ressources de prospective de la CNIL, soit une trentaine de personnes pour un effectif global d'un peu moins de deux cents.

C'est une direction un peu moins développée que les autres directions traditionnelles de la CNIL, mais en termes de direction support, elle est absolument essentielle.

L. V. : Vous vous appuyez beaucoup sur elle, je présume.

I. F.-P. : Oui car c'est aussi la construction de l'avenir.

Compte tenu de ce « nouveau rôle » de régulateur de la CNIL, il nous a fallu modifier notre organisation interne, déterminée jusqu'ici selon une logique administrative : les autorisations, les déclarations, etc., et nous réorganiser en fonction de nos publics, je dirais même de nos clients.

Ce que nous avons voulu mettre en place, c'est une direction de la conformité ayant pour objectif, secteur par secteur (secteur public, secteur social, secteur économique, secteur RH, etc.), avec des responsables de secteur, de mobiliser, au profit du secteur, l'ensemble des outils de conformité présents et futurs que le régulateur est capable de proposer.

L. V. : Avez-vous des relations privilégiées avec les *start-ups* ?

I. F.-P. : Oui, mais plutôt par le biais du département Prospective.

La direction de la conformité traite, elle, avec des acteurs qui sont plus établis et qui sont en demande d'outils de mise en conformité. Les *start-ups*, en fait, on les traite différemment, parce qu'on ne veut justement pas leur plaquer une démarche de conformité trop exigeante tout de suite…

L. V. : La CNIL est donc passée d'une activité « fichier » à une activité « donnée ».

I. F.-P. : Oui, mais en réalité, l'activité fichier existe toujours.

Mais ce que je veux vous faire toucher du doigt, c'est que lorsque l'on passe des fichiers aux données, on passe à une régulation nécessairement complètement différente ; les fichiers, c'est un univers stable, statique même, et qui est très hiérarchisé, avec des acteurs bien identifiés, etc.

Ce monde-là a quasiment disparu, et l'on est dans un monde de fluidité de la donnée : celle-ci est collectée au départ par quelqu'un mais utilisable potentiellement par d'autres. Elle

circule. Du point de vue du régulateur, on ne peut pas du tout traiter le problème de la même manière.
C'est toute cette métamorphose que l'on a souhaité prendre en compte et accompagner dans les cinq dernières années.
Et c'est un très gros changement.

L. V. : Lorsqu'on a un traitement qui relève de la CNIL que faut-il faire ?

I. F.-P. : Nous avons depuis quelque temps lancé un vaste programme de simplification de nos formalités. On dispose d'un système de déclarations online extrêmement simples, un système d'autorisations unique et l'on s'est efforcé de rendre les choses aussi fluides que possible. Dans un certain nombre de cas, cependant, il faut un avis spécifique, une autorisation spéciale du régulateur. Le dossier est alors instruit par les équipes de la CNIL et une réponse est donnée à l'entreprise ou à l'organisation.

L. V. : Et vous avez des inspecteurs qui font des contrôles.

I. F.-P. : Nous avons en effet développé la dimension répressive, c'est-à-dire que l'on organise annuellement, tout un programme de contrôles et d'inspections. 400 contrôles annuels nous permettent d'aller sur le terrain. Ces contrôles peuvent également être réalisés on line, ce qui économise nos ressources. Et il y a la phase de sanction proprement dite. Par an, nous prononçons une vingtaine de sanctions, ce qui n'est pas beaucoup. Nous recevons 6 000 plaintes par an. Chaque plainte est instruite. Chaque plainte donne lieu soit à une information, soit à des échanges de lettres avec le responsable de traitement. Et, dans la plupart des cas, à la mise en conformité de l'entreprise. Quelques plaintes, pour des motifs de non-conformité, conduisent à des mises en demeure ; j'en prononce à peu près 80 par an. Si la mise en demeure n'est pas suivie d'effet, il existe une possibilité de sanction qui peut aller jusqu'à 150 000 euros. Elle n'est pas prononcée par la formation plénière de la CNIL, mais par un sous-ensemble indépendant de celle-ci présidée par un magistrat.

L. V. : N'est-ce pas gênant d'être concomitamment donneur de conseils et distributeur de sanctions ?

I. F.-P. : C'est un vrai sujet auquel, notamment au niveau européen, on réfléchit beaucoup. Nous pensons, fondamentalement, qu'on ne peut pas piloter l'univers digital, avec l'existence de mégadonnées, uniquement par la sanction. On n'attrape pas la réalité de l'univers numérique uniquement par la sanction.
Et nous sommes absolument convaincus que nous devons nous situer en amont de la circulation de la donnée afin de proposer des lignes directrices, des outils opérationnels pour la mise en conformité des acteurs ce qui leur assure une plus grande sécurité juridique
Ce n'est pas une position uniforme au niveau européen. Un certain nombre d'homologues, notamment les Néerlandais, sont farouchement

contre le fait que les autorités puissent émettre des « *guidelines* » au motif qu'il y aurait un risque de conflit d'intérêts.
Je crois que ce risque existe, mais il peut tout à fait être levé à condition, évidemment, que les autorités ne s'engagent pas dans du consulting ad'hoc auprès des entreprises. Il ne s'agit pas de cela. On ne va pas remplacer les avocats ou les fonctions de ce type.
En revanche, lorsqu'il s'agit de donner des lignes directrices sur un secteur, sur un type de pratique, sur les *cookies* par exemple ce qui est très délicat, nous n'hésitons pas à le faire.
Et je crois que là, il n'y a pas conflit d'intérêts.

L. V. : Envisagez-vous de délivrer des labels de qualité ?

I. F.-P. : Nous avons la capacité de délivrer des labels depuis 2012. Concrètement, la Commission établit des référentiels relatifs à des produits ou à des procédures avec les professionnels d'un secteur concernés et ensuite, ceux-ci peuvent faire une demande d'homologation individuelle. Nous avons aujourd'hui élaboré 4 référentiels et nous avons délivré 44 labels, en matière de formations « informatique et libertés », d'audits de traitements, de produit de coffre-fort électronique et de gouvernance. Ce dernier référentiel, le plus récent (2015) est particulièrement intéressant, je pense, pour l'audit interne : il introduit la protection des données comme un enjeu transversal au sein des entreprises et est construit autour du Correspondant Informatique et Libertés.
Cependant, nous estimons que la protection des données personnelles ne doit pas être le monopole du Correspondant Informatique et Liberté, lorsqu'il existe, bien sûr, mais plus généralement de la direction juridique ou de la direction technique.
En fait, c'est un programme transversal qui doit être piloté au plus haut niveau pour inspirer une gouvernance prenant en compte, dans tous les secteurs, la place des données.
C'est bien sûr important dans les directions marketing, parce que la relation client sera de meilleure qualité si on respecte la protection des données personnelles, et les clients sont de plus en plus sensibles à cela. C'est aussi une dimension importante de la DRH, parce qu'en interne, les salariés ont besoin de savoir que l'on respecte leurs données.
Les entreprises qui respectent ce référentiel sur la gouvernance ont donc la possibilité d'avoir un label Protection des données CNIL.

L. V. : Comment les missions de la CNIL s'inscrivent-elles dans le cadre de la réglementation européenne ?

I. F.-P. : La Commission européenne a élaboré un texte qui est en discussion depuis trois ans et qui devrait normalement aboutir en 2015 avec application directe en 2017. Nous sommes entrés dans la phase finale de la négociation avec les trois institutions européennes : Conseil, Commission et Parlement. Ce règlement devrait être un coup de tonnerre : il allège fortement le contrôle amont et renforce considérablement le contrôle aval ce qui devrait mobiliser grandement les auditeurs internes. En revanche, la phase *compliance* – les outils de conformité – reste à bâtir. Ce sera également un coup de tonnerre par rapport aux acteurs internationaux, parce qu'on va les soumettre au droit européen, dès lors qu'ils ciblent un citoyen ou un consommateur européen, et même s'ils n'ont pas d'établissement en Europe. Il y a un dernier élément à noter c'est celui de la nécessaire coopération entre les différentes CNIL nationales, coopération qui doit être souple et participative.

L. V. : Concernant le *big data* et la protection des données personnelles, j'ai le sentiment qu'on reproche à la CNIL, d'être trop protectrice des données et pas assez innovatrice. Qu'en est-il réellement ?

I. F.-P. : C'est un débat qui est maintenant assez classique. Je crois qu'il est complètement faux pour plusieurs raisons. Il est vrai que l'innovation, de plus en plus, passe à travers des données : le *big data*. De multiples exemples montrent que, dans des secteurs extrêmement différents, c'est en traitant différemment les données, en ayant un accès inédit à certaines d'entre elles, en les croisant, etc., que l'on peut faire naître des services et donc une innovation.
Pour autant, je pense que les personnes sont – et toutes les études, dans tous les pays le montrent – de plus en plus conscientes de cette utilisation des données par une multitude d'acteurs et par le fait que finalement, cette utilisation leur est assez opaque et hors contrôle. Ce qu'apporte la protection des données à l'innovation, c'est la capacité d'avoir de la confiance. Et la confiance, c'est fondamental. Il n'y a pas de *business* sans confiance.
Donc, si l'on veut une innovation robuste, pas simplement une innovation de conquête à très court terme de parts de marché, pour ceux qui ont une marque à défendre, qui ont une relation client de qualité à préserver, on voit bien que la protection des données leur apporte un argument, un moyen de fidéliser des clients. Dans l'environnement du numérique qui est un environnement extrêmement volatil, c'est aussi un moyen de fidéliser des clients. En fait, je crois que c'est toujours le débat entre le court terme et le moyen terme. Si on est dans l'immédiat court terme, on peut s'affranchir de la protection des données, en disant : « Après tout, je fais n'importe quoi avec les données. Je vais produire de l'innovation et puis ça va marcher. »
Je pense que c'est un raisonnement qui peut fonctionner à très court terme, mais qui ne marche sûrement pas à moyen terme.
Or, pour construire du *business*, il faut travailler dans le moyen et long terme. Et j'ai tendance à penser que le moyen terme se rappelle toujours à nous. Si l'on s'affranchit de la protection des données personnelles, quelque chose va « revenir » vers le service, vers l'innovateur, pour se rappeler à son souvenir ; et il est beaucoup moins coûteux pour une entreprise d'intégrer assez en amont de son processus de déploiement d'un service, d'une innovation, la protection des données personnelles.

> ***« C'est en traitant différemment les données que l'on peut faire naître des services et donc une innovation »***

Je m'inscris totalement en faux avec l'idée qu'il faut opposer innovation et protection des données personnelles. Je crois que c'est une vue qui est en réalité extrêmement myope de l'économie numérique.
En revanche, il faut que la CNIL soit capable d'élaborer avec les professionnels des outils concrets de conformité permettant à cette innovation de se déployer. C'est ce à quoi nous nous attelons depuis quelques mois à travers les « packs de conformité ».
Je crois beaucoup à ces packs car ils illustrent un nouveau visage de la régulation, plus négociée et plus opérationnelle. Leur utilité est d'ailleurs consacrée dans le projet de loi d'Axelle Lemaire en préparation.

L. V. : En 2006, avec le Sarbanes Oxley Act américain, on a beaucoup parlé de Whistleblowing et

l'on a estimé que la CNIL était d'une très grande timidité pour définir le périmètre de responsabilité des lanceurs d'alerte. Qu'en est-il aujourd'hui ?

I. F.-P. : Il se trouve qu'en 2006, on en a beaucoup parlé parce que c'était nouveau et que la CNIL a souhaité, au nom de la protection des données, que la responsabilité des lanceurs d'alerte, prise en application de cette loi anticorruption soit la plus restreinte possible compte tenu des autres moyens de signalement existant.
Progressivement, les autorisations de la CNIL se sont dilatées et toute une série de thématiques sont rentrées dans leur champ de responsabilité.

Ce n'est pas à la CNIL de légiférer sur les lanceurs d'alerte mais je pense très honnêtement que les lanceurs d'alerte sont extrêmement utiles. Je crois que ce sont des contrepouvoirs démocratiquement utiles permettant de briser les silences. Mais ils doivent rester des solutions de complément de dispositifs de *reporting* interne qui existent à l'intérieur des entreprises, que ce soient les syndicats, les DRH, les directions financières ou l'audit interne.

L. V. : Existe-t-il, et ce sera ma dernière question, des CNIL dans les pays francophones d'Afrique et d'ailleurs ?

I. F.-P. : Oui, effectivement, a été mis en place, en 2006, le réseau francophone des autorités de protection des données qui, aujourd'hui, regroupe 16 pays et dont la CNIL assure le secrétariat (AFAPDP). C'est une communauté extrêmement dynamique, très intéressante, dont l'objectif est évidemment de mutualiser le plus possible les ressources, les transferts de compétences entre le nord et le sud, et de constituer aussi une voie un peu autre dans la communauté internationale de protection des données. Je ne dirai pas une 3e voie mais, entre le « tout marché » ou une vision qui serait trop étatiste des données, il peut y avoir une approche qui soit humaniste, moderne et pragmatique de la protection des données. Nous accordons donc beaucoup d'importance à ce travail au sein du réseau francophone.

Récemment, il a aussi été créé un réseau africain des autorités de protection des données. Les pays africains sont à la confluence de deux questions : la transition démocratique et le développement de l'économie numérique. Dans la construction d'un Etat démocratique, la protection des données personnelles est très importante pour l'exercice de la liberté d'expression, la liberté d'aller et venir, la constitution des états-civils, etc. Et puis il y a un autre aspect, c'est évidemment le développement de l'économie numérique que la protection des données permet d'asseoir sur des bases solides. Donc en fait, ces deux dimensions, à la fois politique et sociétale, et économique font que la protection des données est un objectif de la plus haute importance pour ces pays qui sont de plus en plus actifs au plan international. L'AFAPDP a beaucoup œuvré pour être plus présente au sein de la Conférence mondiale sur la protection des données, afin de faire entendre la voix francophone.

L. V. : Je vous remercie. ■

CNIL
Commission Nationale de l'Informatique et des Libertés

La CNIL est l'autorité en charge de veiller à la protection des données personnelles. Elle dispose d'un pouvoir de conseil, de contrôle sur place et de sanction administrative. Elle anime le réseau des Correspondants « Informatique et Libertés ». Elle analyse les conséquences des nouveautés technologiques sur la vie privée. Enfin, elle travaille en étroite collaboration avec ses homologues européens et internationaux.

Actions de la CNIL :

- **Informer :** la CNIL est investie d'une mission générale d'information des personnes sur leurs droits et leurs obligations.
- **Conseiller et réglementer :** la CNIL régule et recense les fichiers, autorise les traitements les plus sensibles avant leur mise en place.
- **Sanctionner :** la CNIL peut infliger des sanctions financières aux responsables de traitements qui ne respectent pas la loi.
- **Protéger :** la CNIL aide les citoyens dans l'exercice de leurs droits : banque, travail, consommation, administration, internet...
- **Contrôler :** la CNIL contrôle les fichiers et vérifie si les responsables de fichier respectent la loi informatique et libertés.
- **Anticiper :** la capacité à comprendre et anticiper les développements technologiques est désormais indispensable aux autorités de protection des données.

Protéger la vie privée et les libertés dans le monde numérique

CYBERSÉCURITÉ ET PROTECTION DES DONNÉES

Quel rôle pour l'audit interne ?

16 - Cybersécurité : un domaine incontournable et à valeur ajoutée pour l'audit interne

19 - Tendances significatives de l'enquête Global State of Information Security 2014 de PwC

22 - Cybersécurité et protection des données personnelles le point de vue du Cigref

24 - La conformité à la loi informatique et libertés a été un levier d'action

26 - L'audit interne face aux risques de cybersécurité

© gemina - Fotolia.com

Cybersécurité : un domaine incontournable et à valeur ajoutée pour l'audit interne

Jean-Pierre Hottin et **Fabrice Garnier,** Associés, PwC

Lorsque l'on regarde les plans d'audit interne des sociétés et organisations de toutes tailles, une question peut se poser : pourquoi la technologie prend-elle une part aussi faible, alors que tout autour de nous il n'est question que de numérique de ruptures technologiques et d'ERP ? Un Directeur audit interne nous confiait récemment qu'il estimait que plus de la moitié de ses missions devraient désormais porter sur des thématiques autour des systèmes d'information… en particulier les aspects de sécurité des systèmes d'information.

La cybersécurité au cœur de l'approche technologique des départements audit interne

Le schéma 1 illustre la manière dont un département audit interne pourrait prendre en considération la dimension technologique, avec en particulier les quatre grands domaines à considérer.

Les aspects de cybersécurité tiennent une place importante, ce qui est confirmé à l'aune des menaces bien réelles que la presse révèle régulièrement, et ce que confirme également notre dernière enquête internationale sur la profession d'audit interne, avec, comme second sujet de préoccupation pour les répondants, la sécurité des données (confidentialité, intégrité, disponibilité, traçabilité), juste derrière la complexité règlementaire.

Cela étant, force est de constater que peu de Directions audit interne – si l'on met de côté quelques grands groupes et les grands établissements financiers – ont réellement les capacités de s'attaquer à ce domaine, laissant souvent à la Direction informatique cet élément critique de l'univers d'audit.

Un besoin croissant d'assurance pour les parties prenantes

Les administrateurs interrogés dans le cadre de notre dernière publication *« Annual Corporate Director Survey »* ont souligné l'importance croissante qu'ils accordent à ce sujet. Plus de 65 % veulent consacrer plus de temps aux risques informatiques et à la cybersécurité. Pourtant si l'on regarde les résultats de la dernière enquête sécurité présentés dans ce dossier, les administrateurs apparaissent encore insuffisamment impliqués sur des sujets critiques tels que la revue des risques, et cela malgré la recrudescence des cyber menaces ainsi qu'un impact toujours plus important sur les métiers (pertes financières importantes et en hausse notamment).

Les directions informatiques ne sont pas restées inactives et ont pour la plupart mis en

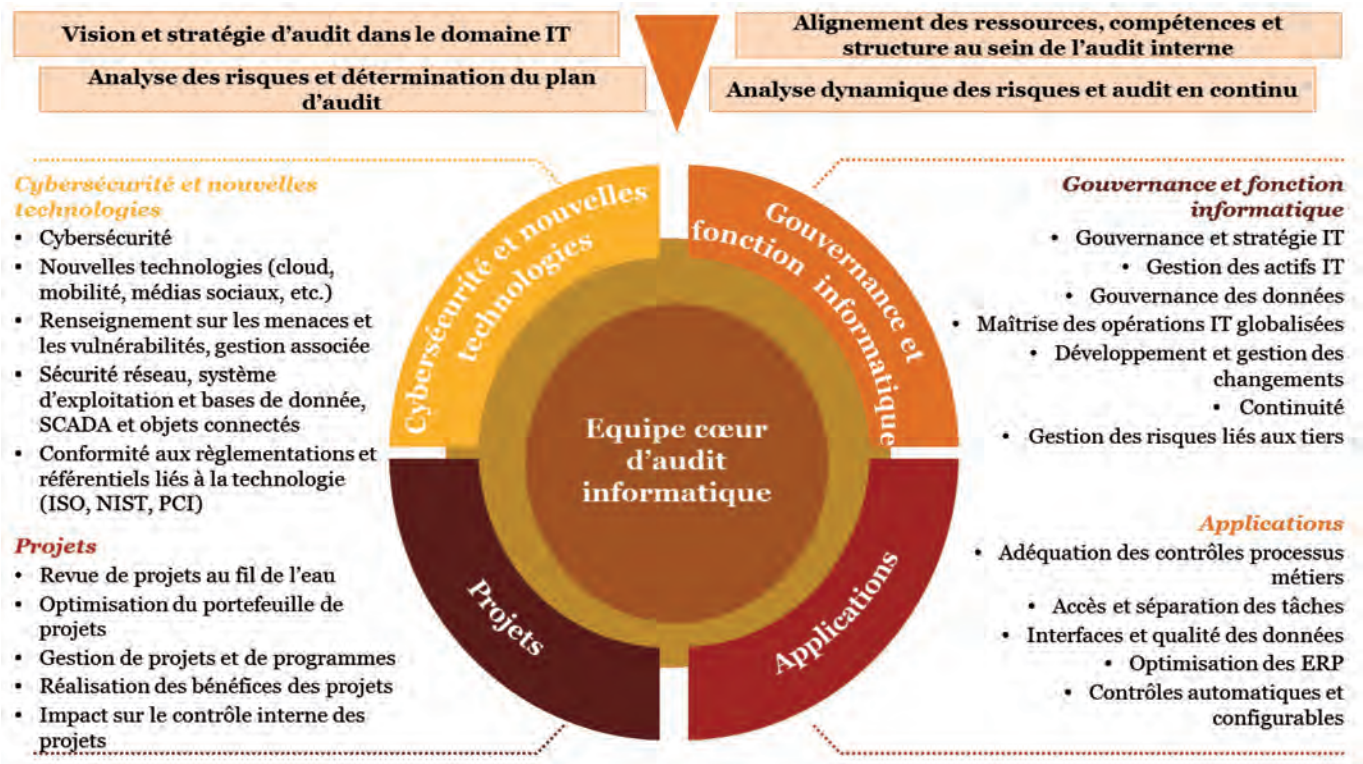


Schéma 1

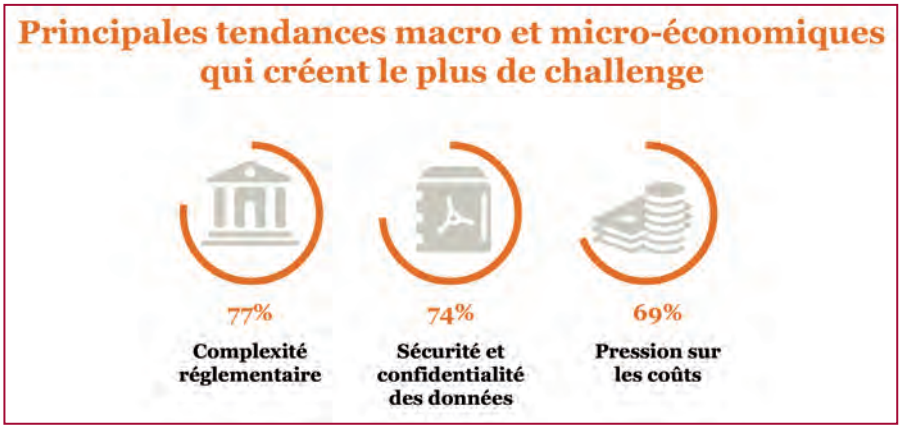
place des fonctions dédiées à la sécurité des systèmes d'information, qui ont en charge d'organiser :

- la prévention, avec par exemple des programmes de sensibilisation des salariés et des prestataires ;
- la protection, avec par exemple des dispositifs de chiffrement des emails, des outils de protection contre les intrusions ;
- la détection, avec par exemple des outils de détection des intrusions de codes malicieux, et la mise en place de SOC *(Security Operations Center)* ;
- et la réponse avec par exemple la mise en place de processus et d'équipes de gestion d'incidents et de crise (CSIRT).

Ces fonctions sont au cœur de la seconde ligne de maîtrise mais, au-delà des contrôles permanents, elles ne peuvent pas toujours réaliser des audits ciblés pour s'assurer que l'ensemble des filiales/unités respectent les mesures préconisées.

Ces fonctions, même si elles sont en capacité de fournir un certain niveau d'assurance, ne peuvent répondre complètement au besoin d'assurance objectif et indépendant que peuvent demander les parties prenantes, à plus fortes raisons dans un domaine nécessitant une très forte expertise technique.

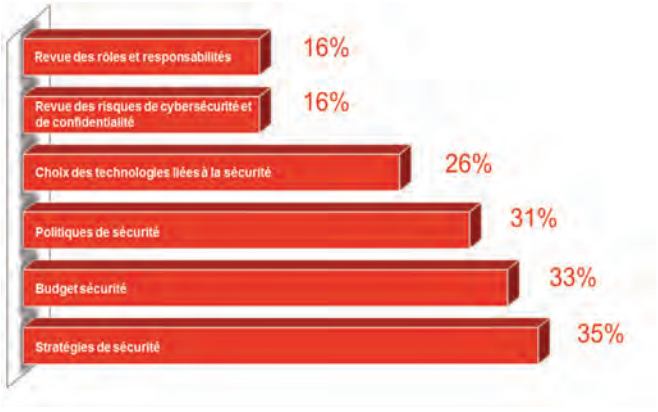
L'audit interne ne peut donc rester en dehors du jeu et doit pouvoir organiser – à la mesure de ses capacités – une réponse appropriée aux attentes et aux enjeux.



Quel espace d'intervention pour l'audit interne ?

La présence d'une seconde ligne de maîtrise structurée va permettre le plus souvent de positionner l'audit interne sur deux types d'intervention :

- l'audit de la gouvernance de la sécurité des systèmes d'information, qui visera en particulier à s'assurer que les fonctions intervenant en seconde ligne ont défini des dispositifs appropriés, répondant aux bonnes pratiques du secteur, mais surtout permettant d'aligner ces dispositifs et de les adapter aux enjeux réels de l'entreprise. La protection absolue n'existe pas et l'entreprise fait des choix pour focaliser les moyens et les investissements sécurité sur les enjeux métiers réels… ;
- des audits ciblés sur des enjeux métiers, liés par exemple à de nouveaux développements stratégiques pour l'entreprise (développement des canaux de vente internet, acquisition de *start-up*, systèmes industriels…), ou en réponse à une actualité brûlante – sur lesquels les dirigeants et administrateurs vont demander des réponses rapides – comme par exemple sur l'état de la compromission des systèmes et son étendue dans le cadre de fuite de données liées à la propriété intellectuelle.



Degré d'implication des conseils d'administration sur les principaux sujets liés à la sécurité

L'audit de la gouvernance devra couvrir plusieurs thèmes, l'une des grilles de lecture pouvant être celle des 17 principes du COSO, avec, par exemple :

- comprendre et vérifier l'adéquation de l'organisation mise en place, et la clarté des rôles et responsabilités en matière de sécurité des SI ;
- s'assurer qu'une politique de gestion des compétences adaptée est mise en place, dans un domaine où ces compétences deviennent vite obsolètes ;
- s'assurer que les risques sont évalués à la lumière des enjeux métiers, avec une capacité à les remettre en perspective lors de changements importants pouvant affecter la qualité des dispositifs de maîtrise déployés (acquisitions, applications en mode Saas...), permettant de focaliser les moyens sur les sujets clef ;
- s'assurer que des politiques et procédures ont été définies et communiquées, au bon niveau de l'organisation, en ligne avec les bonnes pratiques et les référentiels existant, comme la norme ISO27001 ;
- s'assurer que le dispositif prend bien en considération l'entreprise étendue, notamment les prestataires externes ainsi que les acteurs de la chaîne de valeur des processus de l'entreprise ;
- s'assurer que les mécanismes de contrôle permanent et périodique sont adaptés aux risques identifiés.

Les compétences à mobiliser sont à la fois organisationnelles et techniques – il faudra comprendre comment l'organisation mise en œuvre s'articule avec le reste de l'entreprise, tout en étant capable de mener des tests ciblés pour corroborer les résultats des audits et du pilotage mis en place par les fonctions sécurité. La compréhension des enjeux d'affaires sera déterminante pour porter les conclusions auprès des parties prenantes et mobiliser sur les éventuels plans d'action.

L'audit pourra porter sur une dimension en particulier. Il peut s'agir par exemple de tester la solidité des dispositifs de détection et de réponse (maturité du SOC). Ce qui est important, c'est la capacité à réagir suffisamment rapidement pour limiter l'impact de la réalisation de menaces qu'il est impossible d'éviter complètement. Nos expériences récentes dans ce domaine montrent que les délais de réaction peuvent être mal estimés – de l'envoi des autorités dans les deux heures de la détection d'une tentative d'intrusion interne à la découverte de plusieurs jours à plusieurs semaines ou mois après, par l'équipe sécurité des intrusions menées avec succès !

Les audits ciblés seront quant à eux focalisés sur des enjeux métiers. Lorsque l'on cherche à identifier les domaines dans lesquels mener ce type d'audit, il peut être intéressant de s'appuyer sur une analyse des risques que représentent les différentes menaces, en décomposant les motifs, les objectifs visés par les attaques et les impacts qui pourront en résulter, en termes opérationnels.

Les compétences nécessaires dans ce type d'audit seront avant tout techniques – il faudra être en capacité de donner un niveau d'assurance élevé sur les dispositifs techniques mis en œuvre dans le domaine de l'audit. Il pourra s'agir de revues d'architectures techniques, de revues de codes mais aussi de tests d'intrusion ou plus largement de simulation d'APT *(Advanced Persistent Threat)*.

Lorsque la seconde ligne de maîtrise sera peu structurée, l'audit interne aura intérêt à choisir des thèmes d'intervention très ciblés, en lien avec des sujets métiers très pragmatiques, afin de permettre une sensibilisation plus efficace de la Direction générale. L'appui sur des données d'étalonnage (benchmarks)s sera également essentiel pour appuyer les conclusions.

Comment acquérir la compétence nécessaire ?

L'audit interne doit se doter de sa propre capacité d'assurance dans le domaine cybersécurité. Les enjeux sont trop importants pour ne pas être en mesure de challenger la seconde ligne de maîtrise, qui doit le plus souvent naviguer entre menaces et contraintes budgétaires pour ajuster son dispositif.

Cette capacité sera soit interne, pour les fonctions qui en ont la capacité – avec l'enjeu de maintien dans le temps des compétences – soit externe, avec dans ce cas un pilotage étroit de prestataires externes intervenant pour l'audit interne, à même de co-construire une assurance indépendante et objective. ■

Menaces	Motifs	Objectifs	Impacts
État-nation	• Avantage économique, politique et/ou militaire	• Secrets commerciaux • Informations commerciales sensibles • Technologies émergentes • Infrastructures critiques	• Perte d'atout concurrentiel • Perturbation d'infrastructures critiques
Crime organisé	• Gain financier immédiat • Collecte d'informations en vue de gains financiers futurs	• Systèmes financiers/de paiement • Données personnelles identifiables • Informations sur les cartes de paiement • Données médicales protégées	• Enquêtes réglementaires et pénalités coûteuses • Poursuites judiciaires intentées par les consommateurs et les actionnaires • Perte de confiance des consommateurs • Pertes financières
Hacktivistes	• Influence politique et/ou changement social • Pressions sur les entreprises pour qu'elles modifient leurs pratiques	• Secrets d'entreprise • Informations commerciales sensibles • Informations sur les dirigeants, le personnel, les clients et les partenaires commerciaux	• Perturbation des activités • Marque et réputation • Perte de confiance des clients et des consommateurs
Insiders	• Avantage personnel, gain financier • Vengeance professionnelle • Patriotisme	• Ventes, opérations, stratégies de marché • Secrets d'entreprise, propriété intellectuelle, R&D • Activités • Données personnelles	• Divulgation de secrets commerciaux • Perturbations des opérations • Marque et réputation • Impact sur la sécurité nationale

© Sergey Nivens - Fotolia.com

Tendances significatives de l'enquête Global State of Information Security 2014 de PwC

Philippe Trouchaud et **Nuvin Goonmeter,** Associés, PwC

Les tendances significatives de l'enquête 2014 dédiée à la Cybercriminalité, se résument en ce qui suit.

La cybercriminalité augmente et les budgets sécurité diminuent

Le nombre de cyber-attaques recensées en 2014 est en hausse de 48 % dans le monde.
Notre étude réalisée en coordination avec les magazines CIO et CSO, révèle que le nombre d'incidents déclarés a augmenté de 48 % à travers le monde en 2014, pour atteindre un nombre total de **42,8 millions**, soit l'équivalent de 117 339 attaques par jour.
Depuis 2009, les incidents détectés ont progressé de 66 % en moyenne par an.
Globalement, **le coût annuel moyen attribué aux incidents de cybersécurité atteint 2,7 millions de dollars en 2014,** soit une augmentation de 34 % par rapport à 2013. Les grosses pertes financières ont été plus fréquentes cette année puisque les pertes de 20 millions de dollars ou plus ont quasiment doublé pour les entreprises (+ 92 % par rapport à 2013).
Pourtant, c'est la première fois depuis 2010 que le budget moyen alloué à la sécurité de l'information baisse, pour tomber à 4,1 millions de dollars, soit 4 % de moins qu'en 2013.

L'Europe et les grandes entreprises particulièrement menacées

C'est en Europe que les incidents de cybersécurité augmentent le plus fortement, avec une hausse de **41 % des incidents détectés en 2014.** L'augmentation atteint 11 % en Amérique du Nord et 5 % pour la région Asie-Pacifique.

Les grandes entreprises – dont les revenus annuels bruts sont de 1 milliard de dollars ou plus – détectent près de 36 % d'incidents en

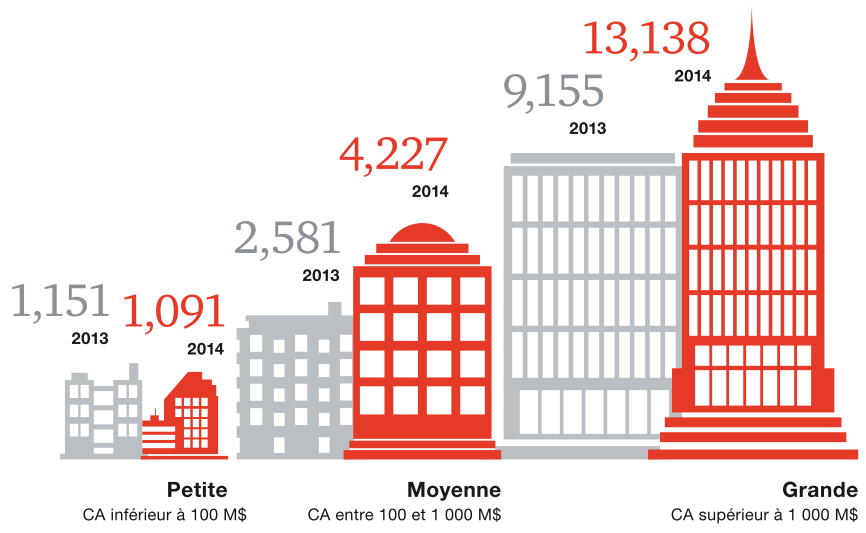


Schéma 1 : Evolution du nombre d'incidents de sécurité détectés par taille d'entreprise

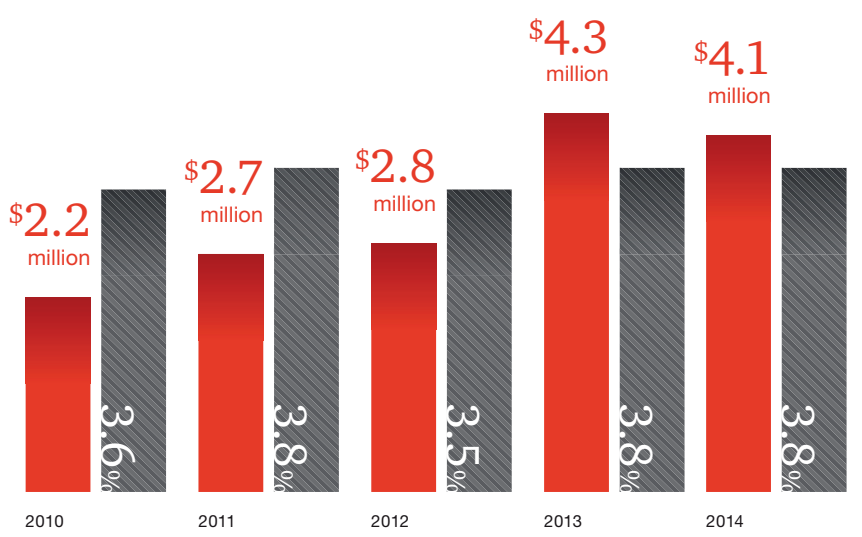


Schéma 2 : Evolution des budgets alloués à la sécurité (évolution du montant moyen et du pourcentage par rapport au budget informatique total)

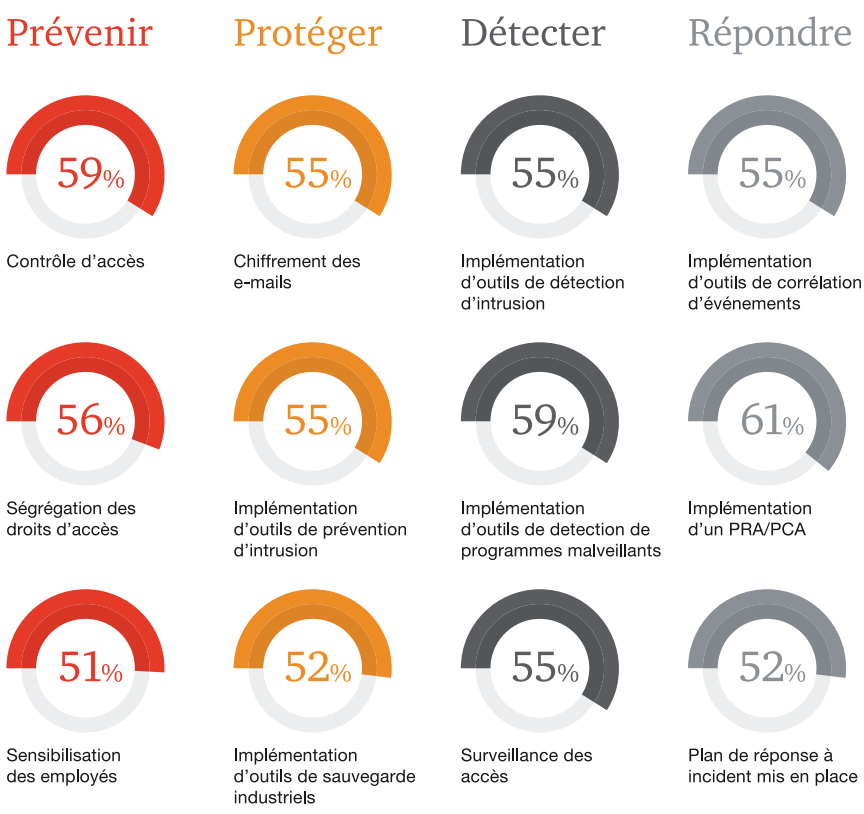


Schéma 3 : Pourcentage de répondants ayant mis en place les différentes mesures

plus par rapport à l'année dernière en France. Les organisations de taille moyenne – avec des revenus entre 100 millions à 1 milliard de dollars – ont vu le nombre d'incidents augmenter de 64 % (Cf. schéma 1).

Les budgets mondiaux dédiés à la sécurité de l'information restent faibles et diminuent en 2014

Les budgets de cybersécurité sont en recul, en particulier dans les secteurs de l'aéronautique et de la défense (-25 %), des technologies (-21 %), de l'automobile (-16 %) et de la distribution et des biens de consommation (-15 %).

La tendance sur les trois dernières années n'est pas constante et le budget de cybersécurité moyen est descendu à 4,1M$, représentant une réduction de 4 % par rapport à 2013 (Cf. schéma 2).

Les fondamentaux ne sont pas toujours en place

Les pratiques en matière de sécurité doivent rester en phase avec l'évolution constante des menaces. L'inter connectivité croissante des systèmes et des entreprises, qui génère une croissance exponentielle des données et de leur partage avec des partenaires et fournisseurs, devrait faire porter une attention particulière sur les tiers et prestataires. Le constat de notre enquête est que le focus sur la sécurité des prestataires a diminué – malgré l'augmentation du nombre d'incidents liés à ces prestataires.

La maîtrise des prestataires devrait, selon l'un des participants interrogé, s'appuyer sur des *due diligence* robustes pour s'assurer qu'ils sont en mesure de répondre aux exigences, être supportées par des clauses contractuelles adéquates, et être confortées par un pilotage continu pour s'assurer que les mesures restent en place.

Lorsque l'on regarde dans le détail le niveau d'application de bonnes pratiques fondamentales, force est de constater que beaucoup de répondants ont encore des marges de progrès, sur des sujets clefs comme l'analyse des risques sur les fournisseurs critiques, l'inventaire des prestataires qui gèrent des données personnelles (50 % seulement déclarent le faire).

Malgré une ouverture des systèmes d'informations des entreprises aux sous-traitants, nous constatons aujourd'hui un manque de contrôle. Certaines bonnes pratiques de sécurité demeurent encore peu mises en œuvre et suivies (Cf. schéma 3).

Les collaborateurs sont les premiers responsables des incidents de sécurité

Les incidents provoqués par les collaborateurs actuels de l'entreprise ont augmenté de 10 % en 2014 par rapport à 2013, et représentent 35 % des incidents de sécurité déclarés. Il faut noter que souvent les salariés compromettent involontairement les données de leur entreprise, en perdant leurs appareils mobiles ou en étant la cible de *phishing*.

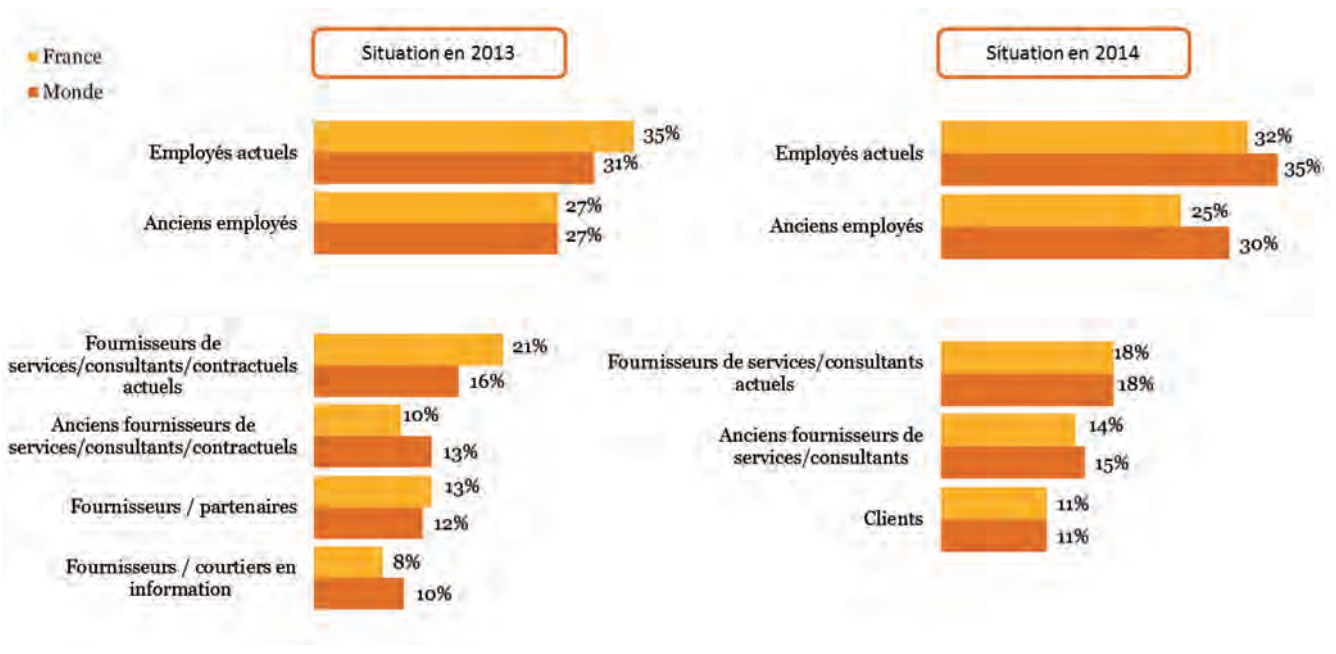


Schéma 4 : Evolution comparée des sources d'incidents de sécurité

Les incidents de cybersécurité attribués aux actuels et anciens fournisseurs et consultants extérieurs ont progressé respectivement de 15 et 17 %.
De même, les cyber-attaques menées par un État ont augmenté de 86 %, en particulier sur les secteurs de l'énergie et de l'aéronautique & défense.
Les cyber-attaques attribuées à des concurrents, dont certains peuvent être soutenus par des Etats, sont en hausse de l'ordre de 64 % (Cf. schéma 4).

Adopter le management du risque : plus d'agilité et de réactivité pour les entreprises face à des menaces en perpétuelle mutation

Les entreprises doivent passer d'une approche de la sécurité de l'information basée sur la prévention et le contrôle à une philosophie fondée sur le risque, pour privilégier leurs actifs les plus précieux face aux menaces les plus dangereuses. Évaluer les risques permet de les rendre assurables et ainsi d'améliorer les pratiques vertueuses.
Une sensibilisation efficace aux enjeux de la cybersécurité exige un engagement de la direction, ce qui d'après l'étude fait souvent défaut. En effet, à peine un répondant sur deux explique disposer, au sein de son entreprise, d'une équipe dédiée à ces questions, qui se réunit régulièrement pour discuter, coordonner et communiquer la stratégie face à ces enjeux.
Les entreprises confiantes dans leur dispositif de cybersécurité n'ont pas toutes mené une analyse de risques sur leurs infrastructures internes et sur leurs prestataires (Cf. schéma 5).

* * *

Il est **crucial que les entreprises établissent des politiques et procédures de prévention et de réaction** qui soient adaptables à toutes les parties prenantes de l'entreprise. ■

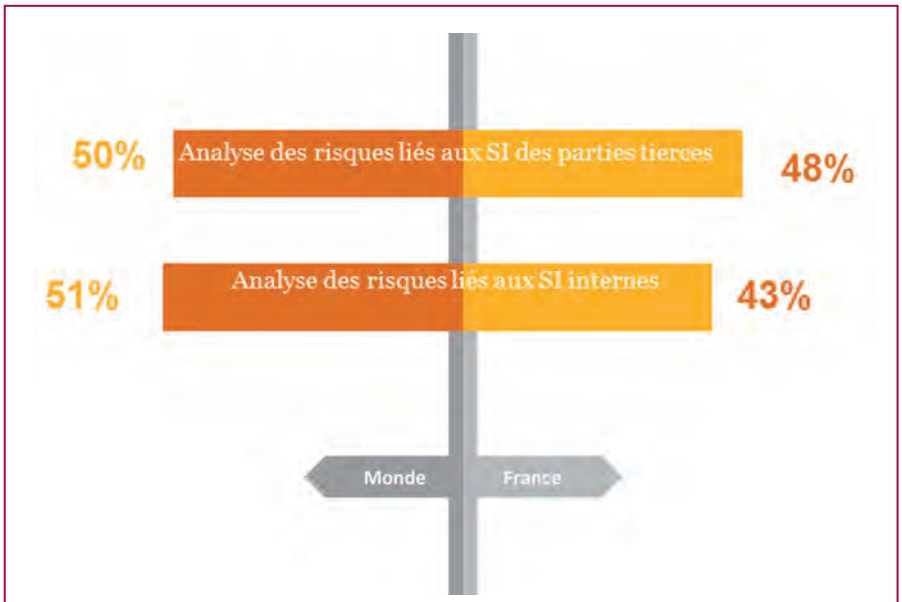


Schéma 5 : Part des répondants ayant mis en place une démarche d'analyse des risques

Cybersécurité et protection des données personnelles

© BilionPhotos.com - Fotolia.com

le point de vue du CIGREF[1]

Avec la révolution numérique, l'information est devenue l'un des principaux actifs de l'entreprise, à condition toutefois qu'elle soit maîtrisée, c'est-à-dire collectée, validée, stockée, sécurisée et traitée pour accompagner la prise de décision. La question de la protection de cette information est au cœur des préoccupations des entreprises et devient un peu plus prégnante chaque jour du fait du développement exponentiel des données (90 % des données mondiales ont été créées au cours des deux dernières années), structurées et non structurées.

Comme tout actif clé de l'entreprise, l'information est soumise à un grand nombre de risques, et son caractère immatériel en fait une cible toute désignée dans le cyber espace. A l'heure où les attaques se font de plus en plus fréquentes et violentes, les entreprises et administrations publiques sont obligées de réagir sur des temps très courts. Cette urgence permanente ne doit cependant pas prendre le pas sur les réflexions concernant les évolutions des risques à moyen terme, et sur les stratégies qui pourraient permettre de les réduire.

Données personnelles et Big Data

Si toutes les données de l'entreprise n'ont pas nécessairement la même valeur, il y a une catégorie qui nécessite une attention toute particulière face aux cyber-menaces : il s'agit des données à caractère personnel. Leur protection nécessite la synergie de plusieurs dimensions, à la fois techniques, organisationnelles et réglementaires.
L'actualité ne cesse hélas de témoigner de la récurrence des cyberattaques sur les données clients ou d'employés. Les risques encourus sont lourds de conséquence : en cas de piratage, les retombées en termes d'image et de réputation peuvent nuire au business, et le non-respect de la règlementation en matière de protection des données à caractère personnel est passible de sanction s'élevant jusqu'à 2 % du chiffre d'affaire de l'entreprise concernée. Tant de menaces qui planent au-dessus des entreprises, et les mettent face à de nombreux challenges en matière de cybersécurité et de protection des données personnelles, notamment dans le contexte du Big Data.
Les données numériques constituent un actif essentiel pour les entreprises. Toute donnée possède une valeur incrémentale ; cela signifie qu'elles n'ont pour la plupart aucune valeur brute, mais qu'elles deviendront par leur croisement et leur interaction, porteuses de sens et de valeur pour l'entreprise.
On comprend qu'avec les technologies de traitement des Big Data, où l'hybridation des données constitue le postulat de base, la protection des données personnelles devienne un sujet de plus en plus complexe et difficile à maîtriser. La notion de donnée personnelle est elle-même en débat : sa définition et son périmètre se sont considérablement étendus avec le numérique. Une

donnée personnelle ne correspond pas forcément aux données d'identité communément partagée dans l'administration (nom, adresse, profession etc.) : à l'ère du numérique, une donnée personnelle est aussi un identifiant, une adresse IP, autrement dit, toutes données qui renvoient indirectement à une personne physique. Autant dire qu'avec les potentiels technologiques actuels de traitement de Big Data, la possibilité d'identifier une personne « indirectement » est presque systématique. Aujourd'hui, les piratages se font sur des SI entiers : cela signifie que des bases de données peuvent être facilement recoupées et permettre la corrélation d'information personnelles voire sensibles, et ce malgré un chiffrage préalable. La cybersécurité autour des données personnelles nécessite une prise de conscience au niveau organisationnel afin d'assurer une évaluation des risques le plus en amont possible, suivre de manière attentive le cycle de vie des données personnelles et surveiller de près leur intégrité pour minimiser les risques.

La garantie de la sécurité des données personnelles engagent donc de nouvelles responsabilités pour l'entreprise qui devront se focaliser à la fois sur les techniques de chiffrage mais également sur la formation et la sensibilisation.

Se protéger du risque Cyber

La protection du capital immatériel a toujours été un sujet majeur pour le CIGREF, non seulement de manière réactive, mais également proactive. Accompagnant la vision des entreprises en pleine transformation numérique, le CIGREF a identifié la maîtrise des risques en matière de cybersécurité comme un enjeu majeur dans son ouvrage « Entreprise 2020, enjeux et défis ». Dans la lignée de ce constat, une étude prospective a été menée avec Futuribles International dans le but de proposer aux entreprises une vision claire des évolutions possibles de leur environnement afin de concevoir leurs stratégies de cybersécurité. Il est ressorti de cette étude « Entreprises et Cybersécurité à l'Horizon 2020 » une série de recommandations transversales liées aussi bien à l'organisation interne des sociétés qu'à leurs relations avec les parties prenantes :

- **Accompagner le changement du métier de RSSI :** le cyberespace occupant une place de plus en plus importante dans les entreprises, les domaines de compétences des RSSI peuvent s'élargir, notamment sur la dimension stratégique.
- **Garder le contrôle de la cybersécurité en interne :** dans un cadre où de nombreuses entreprises font appel à des prestataires externes pour leur cybersécurité, il leur appartient de maîtriser la chaîne de valeur d'autant plus que le marché apparaît dominé par des acteurs non européens dont les liens avec leur Etat sont parfois marqués.
- **Faire de la donnée un élément central de l'entreprise :** Les entreprises devront s'intéresser aux nouveaux métiers liés à la donnée (*chief data officer, data scientist*, etc.), réfléchir à l'insertion de ces nouveaux métiers dans leur organisation actuelle.
- **Mettre en place des plates-formes d'information et des outils de détection d'attaques cyber :** Cela permettrait d'avoir une vision plus globale des cyber-criminels, d'identifier plus facilement les données sensibles, d'élaborer des systèmes de protection communs et d'améliorer la détection des agressions.
- **Développer une veille sociétale :** Les individus peuvent plus facilement comprendre et interagir avec les entreprises, mais ils peuvent également les opposer en portant atteinte à leur image (atteintes à l'e-réputation) ou en mettant en place des systèmes économiques hors des canaux des entreprises (économie de l'échange et du partage, monnaies alternatives, etc.).
- **Renforcer la législation européenne en matière de protection des données :** la place prégnante des acteurs GAFA dans les services aux entreprises relatifs au stockage et à la gestion des données peut entraîner des dérives diverses s'il n'existe pas un cadre législatif strict.
- **Renforcement de la R&D :** la problématique de la dépendance technologique montre la nécessité d'encourager le développement technologique en France et en Europe, notamment au travers de Clusters associant entreprises, Etat et instituts de recherche.
- **Développer la « culture cyber » :** les failles de sécurité viennent très souvent des comportements des utilisateurs, nécessitant donc le développement d'une culture et des réflexes de sécurité dans l'entreprise.

> ***« La cybersécurité autour des données personnelles nécessite une prise de conscience au niveau organisationnel »***

La cybersécurité passe par la sensibilisation de tous les acteurs

Mais au-delà des moyens technologiques et organisationnels mis en œuvre dans les entreprises pour maitriser la sécurité liée à l'IT, le facteur humain, l'utilisateur du SI de l'entreprise, représente l'un des risques majeurs encourus. C'est également l'un des plus difficiles à appréhender et à maitriser.

Parce que chaque employé de l'entreprise a accès au système d'information de l'entreprise, et donc potentiellement à un certain nombre de données sensibles, la sécurité numérique en entreprise doit être portée par l'ensemble des collaborateurs. Tous ont un rôle important à jouer dans la protection de leur entreprise. C'est pourquoi il est nécessaire que la communication sur ce sujet soit portée par les plus hautes instances dirigeantes au sein de l'entreprise, pour que les bonnes pratiques de sécurité soient intégrées dans la culture et les valeurs de l'entreprise.

Les risques de cybercriminalité et de cyberterrorisme ont connu une augmentation de fréquence d'occurrence et de gravité au cours des deux dernières années. Sujet encore mal connu et ne remportant pas l'intérêt de la grande majorité des employés, il est primordial de trouver un moyen de l'aborder afin que tous soient sensibilisés.

C'est dans ce contexte que le CIGREF a fait développer par Daesign un Serious Game de sensibilisation à la sécurité des usages numériques. Ce jeu, intitulé « *Keep an Eye Out* », permet aux collaborateurs d'acquérir les bonnes pratiques de sécurité au travers d'univers représentatifs des situations qu'ils sont susceptibles de rencontrer dans leur vie professionnelle et personnelle.

* *
*

La cybersécurité est devenu un enjeu majeur et stratégique aujourd'hui pour toutes les entreprises et administrations, et le cas particulier des données personnelles nous oblige à réagir vite car ce sont les droits fondamentaux des citoyens qui sont en première ligne. Ce n'est que par une collaboration entre les parties prenantes, la sensibilisation de tous et la maîtrise des processus liés que la résolution de cette problématique pourra être menée à bien. ■

[1] *CIGREF : Club Informatique des Grandes Entreprises Françaises*

La conformité à la loi informatique et libertés a été un levier d'action

© tashatuvango - Fotolia.com

Sophie Tailliez, Chef de la mission audit et management des risques chez Maisons & Cités

AR&C : Comment se pose la problématique relative aux données personnelles chez un bailleur social ?

Sophie Tailliez : En tant que bailleur social, le groupe Maisons & Cités collecte de nombreuses informations qui concernent ses locataires et ses salariés. Nous disposons aussi d'informations relatives aux demandeurs d'un logement social ou à nos partenaires économiques. Nous recevons ou envoyons aussi des données dans le cadre de nos relations avec nos autres parties prenantes : collectivités, Etat, Caisse d'allocations familiales... Ce sont des données qui sont traitées par des applications métiers et des outils de bureautique, avec le plus souvent une automatisation des traitements. Néanmoins, il est évident que le risque porte sur la violation des données personnelles. Nous nous devons donc de les protéger : c'est bien sûr une obligation légale mais c'est surtout un acte de responsabilité vis-à-vis de nos locataires, salariés, demandeurs, fournisseurs et parties prenantes. Il s'agit d'un gage de confiance.

AR&C : Vous parlez d'obligation légale : la loi fixe un cadre strict sur ce sujet et, d'ailleurs, la Commission Nationale Informatique et libertés (CNIL) a porté une attention particulière à votre secteur d'activité ?

S. T. : Effectivement, la loi définit les principes à respecter lors de la collecte, du traitement et de la conservation des données à caractère personnel. Elle prévoit également un certain nombre de droits pour les personnes auprès desquelles sont collectées de telles données. De surcroît, en juillet 2014, la CNIL a publié un pack de conformité dédié spécialement au logement social. Le pack décline les dispositions de la loi informatique et libertés dans le champ opérationnel couvert par les bailleurs sociaux pour leurs actes les plus courants.

AR&C : Comment votre organisation est-elle donc structurée pour répondre à cette problématique ?

S. T. : Dès 2011, Maisons & Cités a nommé un correspondant informatique et libertés (CIL) qui est rattaché à la direction des affaires juridiques. A cette époque, le CIL a réalisé une cartographie des traitements, ainsi qu'une revue de conformité.
La parution du pack de conformité a été l'occasion en 2015 d'une mise à jour de la cartographie avec l'identification des données sensibles et la réalisation d'une nouvelle revue. Pour cela, le CIL s'est fait accompagner par un cabinet externe expert Cette seconde revue de conformité ne s'est cette fois pas limitée aux traitements automatisés, mais a également intégré les traitements papiers créés dans le cadre de la gestion locative et de la gestion des ressources humaines. Suite à cette revue, des actions correctrices ont été identifiées et un plan d'actions a été présenté aux collaborateurs audités.
Il faut souligner que la collaboration entre la direction des affaires juridiques et la direction des systèmes d'information était essentielle et a été particulièrement efficace.

AR&C : Justement, depuis quand votre DSI intervient sur cette problématique ?

S. T. : Notre DSI s'est particulièrement mobilisée sur le sujet dès 2012 en raison des risques liés à la cybersécurité. Elle a initié une démarche de sécurisation de son système d'information. Une liste des principaux risques susceptibles de l'affecter a été dressée, notamment les intrusions internes et externes, l'usurpation d'identité, l'écoute des réseaux privés et publics, le vol, la perte, la

destruction de matériel, la perte des données de la messagerie, les actes de malveillance. Elle a donc forcément été étroitement associée à la revue de conformité.

AR&C : Pouvez-vous nous donner des exemples concrets des résultats de cette collaboration au sein de la 2e ligne de maîtrise ?

S. T. : Elles sont variées. Je pense entre autre à la mise en place d'un dictionnaire des mots interdits dans les zones de commentaires libres de notre progiciel de gestion locative, à la possibilité pour le CIL d'accéder à tous les commentaires et aux zones de commentaires libres et de les modifier afin d'être en conformité avec la loi, à la validation par le CIL des demandes d'autorisation préalables à la mise en œuvre de traitement automatisé de données à caractère personnel ou encore à l'anonymisation des locataires par cryptage automatique dans les délais légaux. Mais cela s'appuie aussi sur une évolution des comportements des utilisateurs qui sont régulièrement sensibilisés par la DSI au rôle du CIL au regard de nos obligations réglementaires.

AR&C : Au-delà de la protection des données personnelles, que fait la DSI sur le sujet de la cybersécurité ?

S. T. : Depuis plusieurs années, elle a engagé un plan d'actions qui vise à nous sécuriser : elle organise régulièrement des tests d'intrusions internes et externes, elle a publié une toute nouvelle charte des utilisateurs, elle a créé une charte des administrateurs, elle a durci la politique de mots de passe, et a revu le dispositif d'habilitations pour préparer la montée de version de notre progiciel de gestion.

AR&C : Quel a été votre rôle en tant que responsable de la fonction audit interne ?

S. T. : La mission d'audit et de management des risques est à chaque fois intervenue comme un « catalyseur » auprès des directions supports. Nous avions identifié comme risques majeurs les risques d'intrusions ainsi que le risque de non-conformité à la réglementation Informatique et libertés. Ils avaient d'ailleurs été inscrits au plan d'audit interne validé en conseil d'administration. J'aimerais vraiment souligner l'implication des directions concernées – la direction des systèmes d'information et la direction des affaires juridiques – qui se sont saisies de ces occasions pour mobiliser leurs collaborateurs autour des recommandations et des plans d'actions. La conformité à la loi Informatique et libertés a été un levier d'action.
En outre, certains audits qualité intègrent les risques liés à la cybersécurité et la protection des données personnelles, tels que les audits du processus « administrer le système d'information » et celui de la direction des ressources humaines. Cela nous permet de consolider, par le biais de la qualité, le cercle vertueux et efficace que doit être l'audit.
Nous n'avons pas la prétention d'être parfait, loin de là, et nos marges de progression restent encore importantes. Mais grâce à la démarche qualité d'amélioration continue et à celle de maîtrise des activités avec le contrôle interne et le management des risques, nous essayons de progresser à chaque fois. La 2e ligne de maîtrise l'a bien compris. Et même si l'audit est un temps de contrainte et de remise en question, c'est à chaque fois l'occasion de s'améliorer. Je rends d'ailleurs hommage à mes collègues audités et auditeurs qui s'investissent et se mobilisent. ■

LE GROUPE MAISONS & CITÉS

Le groupe Maisons & Cités s'est constitué en 2002 avec la création de l'Epinorpa et le rachat de la SAS Soginorpa, société créée en 1985 par Charbonnages de France ayant en charge la gestion des logements des Houillères du Nord-Pas-de-Calais. L'acquisition de la coopérative HLM Maisons & Cités Habitat a ensuite permis d'engager une activité de construction et ainsi d'élargir l'offre de logements.

En 2014, Maisons & Cités Soginorpa est devenue une SA d'HLM. Premier bailleur HLM de la région Nord-Pas-de-Calais, elle est aussi la seconde ESH de France.

Son patrimoine de 63 000 logements est constitué en très grande majorité de logements individuels avec jardin. Il se singularise par une qualité architecturale et urbanistique exceptionnelle : 40 % du parc fait partie du périmètre inscrit au patrimoine de l'Humanité (Bassin minier patrimoine mondial).

La clientèle de Maisons & Cités présente également la particularité d'être constituée à 30 % d'ayants droit du statut du mineur. Ces anciens mineurs ou veuves de mineurs sont logés à titre gratuit. La clientèle de locataires est quant à elle constituée à près de 60 % de ménages avec enfants.

Maisons & Cités emploie 887 collaborateurs.

www.maisonsetcites.fr

©Sam Bellet

L'audit interne face aux risques de cybersécurité

© Natalia Merzlyakova - Fotolia.com

Farid Al Mahsani, Expert en gestion des risques à l'Unité permanente anticorruption (Québec)

Mohamed Nabil Tir, Coordonnateur stratégique à Revenu Québec

Les gouvernements et les organisations (entreprises, institutions financières, hôpitaux et autres) collectent, traitent, stockent des informations confidentielles et transmettent les données à travers les réseaux. Le volume et le degré sophistiqué des cyberattaques nécessitent une attention soutenue pour protéger les organisations considérées comme « sensibles », les renseignements personnels et la sauvegarde de la sécurité nationale. Les cyberattaques et l'espionnage numérique sont considérés comme les principales menaces pour la sécurité nationale des pays. Le budget consacré à la cybersécurité reflète bien cette importance, démesuré dans le cas des États-Unis (14 milliards de dollars prévus dans le budget 2016[1]) et modéré dans celui du Canada (58 millions de dollars prévus en 2015-2016[2]).

Notre article comprend trois parties : la première définit les concepts de cybersécurité, de cyberespace et de cyberattaque ; la deuxième partie est consacrée aux mythes de la cybersécurité ; la troisième partie présente le rôle de l'audit interne face aux risques de cybersécurité à travers le modèle des trois lignes de défense.

Qu'est-ce que la cybersécurité ?

Le terme «cybersécurité», appelé aussi sécurité des technologies de l'information, est largement utilisé et ses définitions sont variables. Nous vous proposons les trois suivantes :

- Pour Merriam webster[3], la cybersécurité est l'ensemble des mesures prises pour protéger un ordinateur ou un système informatique contre un accès non autorisé ou contre des attaques.
- Selon la *National Initiative for Cybersecurity Careers and Studies* (NICCS)[4], la cybersécurité est *l'activité ou le processus, l'habileté ou la capacité, ou le fait par lequel l'information et les systèmes de communication et d'information qui y sont contenus sont protégés ou défendus contre les dommages, l'utilisation, la modification ou l'exploitation non autorisée.*
- Le Comité sur les systèmes de sécurité nationale[5] définit la cybersécurité comme étant *la capacité à protéger ou défendre l'utilisation du cyberespace contre les cyberattaques.* Ce qui nous amène à définir deux autres concepts : le cyberespace et la cyberattaque.

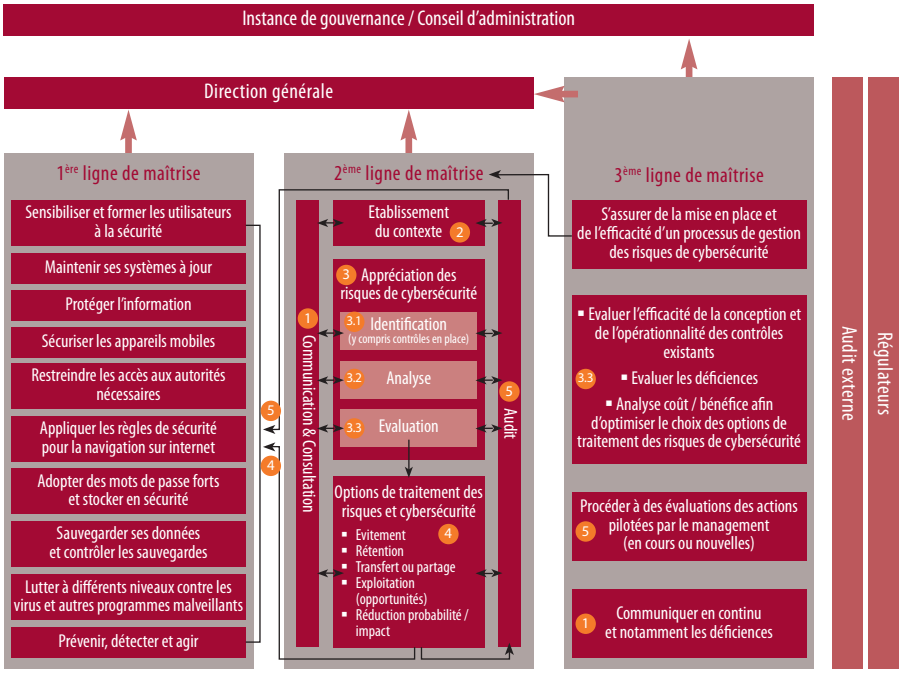
  Le cyberespace est un *domaine global avec un environnement d'information consistant en un réseau indépendant des infrastructures des systèmes d'information, y compris l'Internet, les réseaux de télécommunications, les systèmes informatiques et les processeurs et contrôleurs embarqués*[6]. Alors que la cyberattaque est *une attaque, via le cyberespace, en ciblant l'utilisation d'une entreprise dans le but de perturber, de désactiver, de détruire, ou de malicieusement contrôler un environnement ou une infrastructure informatique ou de détruire l'intégrité des données ou encore de voler des informations contrôlées*[7].

On peut dire que la cybersécurité consiste à protéger ou défendre l'utilisation des ressources du cyberespace contre l'accès non autorisé qu'il soit intentionnel ou non.

Les mythes de la cybersécurité

L'environnement de cybersécurité, qu'on peut qualifier de volatil, exige des efforts permanents de l'auditeur. Parmi ces efforts, l'auditeur devrait prendre en considération les mythes de la cybersécurité[8], notamment les suivants :

- **Le contrôle des systèmes est plus sécurisé si nous ne nous connectons pas à Internet.** Or, il suffit que des clients de l'entreprise soient connectés à Internet pour que cette dernière subisse les conséquences des risques de pertes de biens, des données, etc. de ses clients. Exemples : à la suite d'un vol de numéro de carte de crédit ou du vol d'identité d'un client, ce dernier cesse une partie ou la totalité de ses activités avec l'entreprise le temps qu'il règle ses problèmes.
- **Nous devons nous concentrer sur les terroristes.** Certes, le phénomène du terrorisme est plus présent compte tenu de l'effet de l'incertitude élevée causée notamment par des guerres actuelles (Irak, Syrie, Libye, Yémen, etc.). Néanmoins, les attaques informatiques sont quotidiennes et concernent l'ensemble des acteurs de la société. À la différence d'un terroriste, qui a souvent un calendrier politique initial et a besoin de se déplacer pour exécuter son acte, un pirate informatique peut agir de n'importe quel coin de la planète, assis confortablement dans le sofa de son salon et sans forcément une intention hostile.
- **Les « *hackers* » n'ont pas de connaissances fines comme par exemple celles des Systèmes de contrôle et d'acquisition de données** (SCAD ou SCDA en anglais) **ou des Automates programmables industriels** (API ou PLC en anglais). Or, les pirates informatiques n'ont nul besoin de ces connaissances pour bloquer pendant quelques heures des sites internet[9]. Ils se définissent d'ailleurs comme étant des personnes s'attachant à *comprendre le fonctionnement d'un mécanisme, afin de pouvoir bidouiller pour le détourner de son fonctionnement originel*[10].



Le modèle des trois lignes de défense : rôle de l'audit dans les risques de cybersécurité

Schéma adapté à partie des lignes directrices ECIIA / FERMA sur la 8e directive de l'UE relative au droit des sociétés, article 41 et du schéma de l'IIA

Ces actions ont été identifiées dans le Guide Belge de la cybersécurité

D'autres efforts sont consacrés à la compréhension des types et sources des cyberattaques (voir les exemples ci-après), de la dépendance à l'égard du département de la Sécurité TI et de la vulnérabilité des systèmes DCS *(Distributed Control System)* ou PLC *(Programmable Logic Controllers)*.

Exemples de sources de menace à la cybersécurité [11]

- Bots opérateurs de réseaux utilisant un réseau, un botnet, des compromis, des systèmes télécommandés pour coordonner des attaques utilisant l'hameçonnage, le pourriel et des logiciels malveillants.
- Des États qui s'adonnent à des activités hostiles de collecte de renseignements et d'espionnage.
- Concurrents commerciaux.
- Groupes criminels.
- Pirates informatiques.
- Terroristes.

Exemples de types de cyberattack [12]

- Cross-Site Scripting) : type de faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions hostiles sur les navigateurs web des victimes.
- Attaque par déni de service qui consiste en une tentative de submerger un système ou un réseau informatique via un grand nombre de communications afin d'empêcher les utilisateurs d'y accéder[13].
- Les bombes logiques : code de programmation volontairement inséré dans des logiciels provoquant une fonction malveillante lorsqu'une ou plusieurs conditions précisées sont remplies.
- Cheval de Troie.
- Ver.
- Virus.

Les trois lignes de défense : L'audit interne et les risques de cybersécurité

De par sa définition, *l'audit aide l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, les processus de management des risques et de contrôle*[14].

Autrement dit, dans le cas de la cybersécurité, l'audit s'assure de l'efficacité du système de contrôle interne du cyberespace qui a notamment pour objectifs[15] :

- l'exécution d'opérations ordonnées, éthiques, économiques, efficientes et efficaces ;
- le respect des obligations de rendre compte ;
- la conformité aux lois et réglementations en vigueur ;

- la protection des ressources contre les pertes, les mauvais usages et les dommages.

À ces objectifs s'ajoutent les dimensions proprement liées à la sécurité de l'information[16] à savoir :

- Assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée.
- Assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelconque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues.
- Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance, assurant ainsi une stricte confidentialité.
- Permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.
- Se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, dont un dispositif d'identification avec lequel elle est en lien.

Dans le cadre d'une mission d'audit de sécurité de l'information, la méthodologie d'audit ne diffère pas d'autres domaines et peut être abordée de deux façons : à haut niveau « audit stratégique » exigeant une expertise avancée ou au niveau opérationnel « audit opérationnel » exigeant ainsi les connaissances et les moyens nécessaires au déroulement de la mission d'audit.

Audit de la stratégie de cybersécurité

Au niveau stratégique, l'auditeur s'intéresse à la pertinence de la stratégie de cybersécurité, son évolution et son interaction avec les environnements interne et externe. La faisabilité et les ressources nécessaires peuvent faire aussi l'objet d'un audit. Ce dernier peut être réalisé selon un plan pluriannuel et d'une manière cyclique. A ce stade, et selon le modèle des trois lignes de défense illustré ci-dessus, l'auditeur concentre ses efforts aux première et deuxième lignes de défense. À la première ligne, il procède à l'évaluation des actions pilotées par le management afin de contenir le risque de cybersécurité, tandis qu'à la deuxième ligne, l'auditeur s'assure de la mise en place et de l'efficacité d'un processus de gestion des risques de cybersécurité. En résumé, l'auditeur s'assure que la stratégie de cybersécurité adoptée reflète la mission et les valeurs organisationnelles ainsi que le code de conduite et les règles de gouvernance de l'organisation.

Audit opérationnel de la sécurité de l'information

L'audit apprécie l'efficacité de la conception et de l'opérationnalité des contrôles existants en matière de sécurité de l'information telle que présentée à la deuxième ligne de défense. Aussi, il peut parfois participer au processus d'évaluation des risques et de mise en œuvre des contrôles des systèmes d'information afin de s'assurer du niveau de sécurité en amont. Ainsi, des contrôles préventifs seront prévus en début de processus afin de contrer la survenance des défaillances ou plus tard dans le processus afin de les détecter rapidement (ex : définition des rôles et des responsabilités, activités de sensibilisation, contrôle et mise à jour des accès informatiques, journalisation et routine de détection, duplication des données, etc.). Un autre point important que l'auditeur devrait prendre en considération est l'analyse coût/bénéfice afin d'évaluer si les avantages de l'option de traitement sélectionnée l'emportent sur les coûts associés.

Dans le cadre de ces missions d'audit, l'auditeur doit approfondir ses examens afin de s'assurer du bon fonctionnement au plan opérationnel de la stratégie de cybersécurité des microprocessus de l'organisation. L'efficacité de la mise en œuvre de cette stratégie dépend de sa cohérence avec les enjeux stratégiques et le cadre réglementaire de l'organisation. L'auditeur doit porter une attention particulière aux enjeux stratégiques, réglementaires et opérationnels dans le choix de son référentiel d'audit. À cet effet, il peut être accompagné par un expert en matière de sécurité d'information. Les types de mission d'audit pouvant être réalisés sont :

- audit de conformité aux référentiels règlementaires ;
- audit de vulnérabilité périodique qui comprend l'outil automatisé d'analyse de vulnérabilités, test et évaluation de sécurité, tests d'intrusion, revue de code (ISO27005) ;
- suivi de sécurité (enquête et inspection).

Par ailleurs, l'auditeur doit s'assurer que le management a mis en place des plans de mesure d'urgence et de continuité des opérations. À cet effet, l'existence d'un processus efficace d'escalade des évènements portant atteinte à la sécurité de l'information est requise.

* *
*

De plus en plus de pays ont mis en place une stratégie de cybersecurité . C'est le cas notamment enAllemagne , en Australie, au Canada, aux États-Unis, en France et auLuxembourg où plusieurs moyens ont été mis en place pour contenir les risques de la cybersécurité en s'assurant de la protection de la vie privée. Néanmoins, malgré ces moyens, il arrive encore que des renseignements personnels soient dérobés comme ce fût le cas tout récemment (5 juin 2015) aux États-Unis : le

Audit de la stratégie de cybersécurité Examen de la 1ere ligne de défense		Audit de la sécurité d'information Examen de la 2e ligne de défense	
Éléments ou critères de contrôle	Composantes du cycle de gestion	Éléments ou critères de contrôle	Composantes du cycle de gestion
▪ Vision ▪ Mission ▪ Codes de déontologie ▪ Organes de gouvernance ▪ Contexte politique	Processus de mise en œuvre de la stratégie de cybersécurité	▪ Audit de conformité aux référentiels règlementaires ▪ Audit de vulnérabilité périodique ▪ Suivi de sécurité	▪ Objectifs organisationnels et opérationnels ▪ Moyens, méthodes et ressources nécessaires ▪ Pilotage, suivi et systèmes d'information

Dimensions de la sécurité de l'information				
Disponibilité	Intégrité	Confidentialité	Authentification	Irrévocabilité

New York Times a révélé que l'Administration Obama a annoncé la perte de données d'au moins 4 millions de fonctionnaires, provenant du Bureau de la gestion du personnel *(Office of Personnel Management)*, ce qui semblerait être une des plus graves violations de données des employés fédéraux[17]. C'est pourquoi, à notre avis, l'auditeur doit intégrer la protection des renseignements personnels ainsi que la sécurité de l'information dans toute mission d'audit quelle que soit sa portée.

L'auditeur devrait aussi sortir de sa zone de confort et saisir l'opportunité de faire partie de la solution. Autrement dit, l'auditeur ne devrait pas se contenter de ne faire que des recommandations pour l'entité auditée mais se questionner aussi sur l'impact financier de ces recommandations, en particulier dans des projets TI, surtout dans un contexte de restriction budgétaire. Pour ce faire, l'auditeur peut se servir notamment de l'analyse coût/bénéfice et ce, d'une façon systématique. Cette stratégie peut être payante non seulement pour l'organisation (choix de la solution la plus optimale) mais aussi pour l'image de l'audit interne. ■

---

[1] *Selon Reuter, afin de mieux protéger les réseaux fédéraux et privés contre les menaces de piratage informatiques, l'administration Obama propose pour l'exercice 2016 la somme de 14 milliards de $ pour les efforts de la cybersécurité. http://www.reuters.com/article/2015/02/02/usa-budget-cybersecurity-idUSL1N0VC0XH20150202 (page visitée le 9 juin 2015).*

[2] *Gouvernement du Canada (2015). Budget 2015 - Plan budgétaire - Chapitre 4.3- Protéger les Canadiens. Le Plan d'action économique de 2015 propose d'accorder 58 millions de dollars sur cinq ans, à compter de 2015-2016, pour mieux protéger les cybersystèmes et l'infrastructure virtuelle essentiels du gouvernement du Canada contre les cyberattaques. http://www.budget.gc.ca/2015/docs/plan/ch4-3-fra.html (page visitée le 12 juin 2015).*

[3] *Dictionnaire en ligne : Merriam-Webster (traduction libre; site consulté le 28 mai). http://www.merriam-webster.com/dictionary/cybersecurity*

[4] *DHS, (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies : Department of Homeland Security. October 1, 2014:http://niccs.us-cert.gov/glossary#letter_c (consulté le 28 mai 2015).*

[5-6-7] *CNSS, (2010). National Information Assurance Glossary. Committee on National Security Systems (CNSS). Instruction No. 4009. http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf (consulté le 29 mai 2015).*

[8] *E Byres, J Kay, J Carter, (2010). Myths and Facts Behind CyberSecurity of Industrial Control. http://www.pimaweb.org/conference/april2003/pdfs/MythsAndFactsBehindCyberSecurity.pdf (page consultée le 1er juin 2015).*

[9] *Selon le journal de Québec du 8 juin 2015, le piratage des sites Internet de la région du Saguenay-Lac-Saint-Jean (Québec, canada) , dans la nuit du 5 au 6 juin 2015, est l'œuvre d'une seule personne localisée en Turquie. http://www.journaldequebec.com/2015/06/08/sites-web-attaques-par-des-pirates-informatiques (page consultée le 10 juin 2015).*

[10] *Amaelle Guiton (2013), Hackers. Au cœur de la résistance numérique. Éditions Au diable vauvert, 2013, page 17.*

[11-12] *United States Government Accountability Office (2013). Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. Report to Congressional Addressees. Pages 5 et 6. http://www.gao.gov/assets/660/652170.pdf .*

Voir aussi le site internet du Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, France (CERT-FR), www.cert.ssi.gouv.fr/ .

[13] *Michael W. Elliott (2012). « Évaluation et traitement du risque », ARM, The Institute, Pennsylvania, page 10.29.*

[14] *Définition proposée par l'Institut français de l'audit et du contrôle interne (IFACI).*

[15] *Lignes directrices sur les normes de contrôle interne à promouvoir dans le secteur public, Publiées par l'INTOSAI*

[16] *Secrétariat du Conseil du trésor du Québec (2014). Directive sur la sécurité de l'information gouvernementale, Québec, Canada. http://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/directive_securite_information2014.pdf*

[18] *David E. Sanger and Julie Hirshfeld Davis (2015). Hacking Linked to China Exposes Millions of U.S. Workers. The New York Times, 4 juin 2015. http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html?action=click&contentCollection=U.S.&module=RelatedCoverage&region=Marginalia&pgtype=article (page consultée le 5 juin 2015).*

REJOIGNEZ-NOUS SUR LES RESEAUX SOCIAUX
ACTUALITES - LIVE TWEET - PUBLICATIONS DE LA RECHERCHE - DEBATS - NETWORKING - OFFRES D'EMPLOI
LinkedIn
www.facebook.com/ifaci
www.fr.linkedin.com/company/ifaci
www.twitter.com/ifaci_officiel
ifaci
institut français de l'audit et du contrôle internes
98 Bis Bd Haussmann, 75008 PARIS
institut@ifaci.com - 01 40 08 48 00

© beeboys - Fotolia.com

Pour une nouvelle approche intégrée

Objectifs, processus, risques, contrôles et gouvernance

ir. Tommaso Capurso, MIA, CCSA, CIA, QA, EFARM, CRMA, ISO31000 Risk Management Professional
Chef de la division d'audit « Opérations et Systèmes techniques » et « Sécurité d'exploitation » à l'audit interne de la SNCB (Belgique)

Le thème du présent article a fait l'objet d'un exposé à l'occasion de la Conférence du 30ème anniversaire de l'AMACI (l'IIA Maroc) (7 et 8 mai 2015 à Marrakech).
Ce thème, proposé par le Comité scientifique de l'AMACI, constitue un double défi :

- défi en termes d'attente de « nouveauté » (je resterai prudent sur ce critère, vu les références citées datant parfois de quelques décennies voire plus) ;
- défi dans la recherche de modélisation et d'intégration des divers concepts auxquels les auditeurs internes sont en principe familiers. Ce sont en effet les mots-clefs intervenant dans la « définition » de l'audit interne.

Cet article vise à illustrer quelques modalités d'approche intégrée de la gouvernance organisationnelle (Norme IIA, N 2110). La gouvernance de gestion intégrée de projet, également abordée à Marrakech, est importante. Les normes de l'IIA sont en effet là pour nous rappeler qu'il y a lieu d'évaluer aussi les risques en matière d'efficacité et d'efficience des opérations et des programmes (N 2110, N 2120, N 2130 A1).
Pour limiter la taille de la présente publication, ce volet pourra faire l'objet d'un « papier » ultérieur distinct.

Une petite métaphore mathématique et graphique

Faisons-nous plaisir. La littérature indique souvent que « objectifs », « risques » et « contrôles » sont liés et doivent être « alignés ». Larry Hubbard *(« Control Self-Assessment : a practical guide »,*

Figure 1 : Pour une nouvelle approche intégrée (source : dessin adapté, « Le risque d'entreprendre », Essentiels Milan, série Polynômes, 1999)

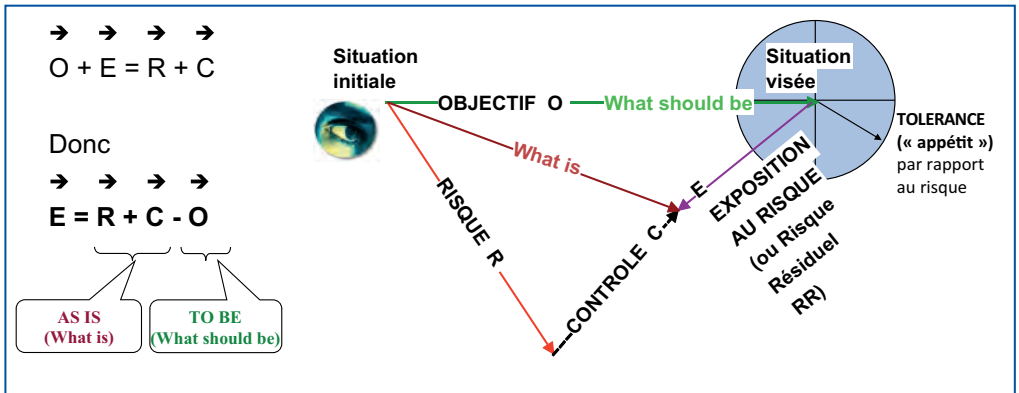


Figure 2 : L'équation objectif-risque-contrôle

The IIA, 2000) évoque, sans l'énoncer, une « formule » d'interaction. Il ajoute que « Evaluer les contrôles pour atteindre les objectifs n'est pas possible sans considérer les risques pouvant empêcher l'atteinte de ces objectifs. Dès lors, que vous vous concentriez d'abord sur le risque ou sur le contrôle dans le processus d'évaluation, vous ne pouvez réellement évaluer l'un sans avoir une pleine compréhension de l'autre ».

Du schéma proposé (figure 2), on peut aisément déduire quelques définitions simples :

- le risque, c'est tout ce qui peut détourner de l'atteinte de l'objectif ;
- le contrôle, c'est tout ce qui peut contribuer à atteindre l'objectif.

La superposition du risque et du contrôle (le *« what is »* ou *« AS IS »)* peut être comparé à l'objectif, soit au *« what should be »* ou *« TO BE »*. L'écart entre les deux est l'exposition au risque ou risque résiduel. Les amateurs de géométrie vectorielle retrouveront dans la proposition d'équation le célèbre « théorème de Chasles ». Il est à noter que l'observateur (« l'œil ») se place à la situation initiale et contemple le déroulement dans le temps vers la situation visée.
Le concept de processus ne complique guère le schéma, car il se superpose au « vecteur » objectif : il s'agit en fait d' « une chaîne d'activités qui, à partir d'un ou de plusieurs inputs, produit, en consommant des ressources, un ou plusieurs outputs qui ont une valeur pour un client » (*« Le reengineering »*, M.Hammer et J.Champy, Dunod, 1993). Le processus (du latin *« pro cedere »* : aller vers l'avant) est donc la série d'opérations produisant la transformation de la « situation initiale » vers la « situation visée ».
Pour les quatre premiers concepts du titre, le tour est donc joué !

Quid d'un modèle de gouvernance intégrée ?

Se référer à quelques définitions : toujours utile !

Les normes IIA définissent, dans leur glossaire, le gouvernement d'entreprise comme : « Le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs ».
La norme N 2110 souligne que **l'audit interne doit en particulier déterminer si ce processus permet la promotion des règles éthiques et des valeurs appropriées au sein de l'organisation. On devine ainsi qu'une organisation ne peut en fait créer de la valeur que… si elle dispose de valeurs.**
Jack Welch, ancien CEO de General Electric (1981-2001), l'avait bien compris et avait l'habitude de consacrer pas mal de son temps à expliquer l'importance des « valeurs » à son personnel (« Jack Welch, 24 leçons de *leadership* », J.Krames, Ed.Maxima, 2008) :

- **« Les valeurs de l'entreprise détiennent le véritable pouvoir » ;**
- « Soutenez et encouragez les employés qui incarnent les valeurs les plus importantes de l'entreprise » ;
- **« Les entreprises passent beaucoup trop de temps sur leurs chiffres et pas assez sur leurs valeurs ».**

La norme ISO26000:2011, relative à la responsabilité sociétale, inclut au §6.2.1.1 une définition intéressante de la gouvernance de l'organisation. Il s'agit :

- d'un système par lequel une organisation prend des décisions et les applique en vue d' atteindre ses objectifs ;
- de mécanismes formels de gouvernance (processus, structures) ;
- de mécanismes informels, en fonction des valeurs et de la culture de l'organisation, souvent sous l'influence des personnes qui la dirigent ;
- d'un cadre des prises de décision au sein de l'organisation.

Elle insiste par ailleurs sur la nécessité d'une démarche holistique et sur l'interdépendance de ses composantes (redevabilité, transparence, comportement éthique,…).

Comme le souligne aussi la norme ISO31000:2009, relative au management du risque, l'important, finalement, c'est la qualité de la prise de décision (choix argumentés, priorités d'actions,...).

Différentes approches sociologiques de la gouvernance

L'évolution des sciences humaines a permis de distinguer deux types d'approches :

- **l'approche « descendante » (prescriptive),** visant à stimuler la conformité : culture de la règle et du contrôle. Dans son essence, elle vise à préserver les « avoirs » de l'entreprise. Elle représente l'organisation du « quoi/comment » et met en place des « garde-fous » (les contrôles) pour atteindre les objectifs ;
- **l'approche « montante » (participative),** visant à stimuler la coopération, la coordination, bref l'implication et l'initiative du personnel : culture de la finalité et du résultat. On pourrait reformuler en suggérant que cette approche vise à développer les « êtres ». Elle reflète l'organisation du « pour quoi », en se basant sur des « garde-intelligents » (les « travailleurs du savoir »), avec une attention particulière à développer la confiance.

La société coopérative Desjardins a magnifiquement synthétisé la dualité de la gouvernance dans un slogan d'entreprise : « Conjuguer avoirs et êtres », actualisé depuis en : « Coopérer pour créer l'avenir ».
Bien entendu, les organisations sont complexes, travaillent dans des contextes sectoriels variés, régulés ou non, et présentent des histoires et des cultures multiples. Le positionnement du curseur entre les deux types d'approches peut donc significativement varier d'une organisation à l'autre.

Une intégration continue et persévérante

Rappelons en effet les efforts constants et convergents d'intégration, comme en témoignent les publications notamment de l'IIA. Citons par exemple (extraits) :

- *« Enhancing integrated reporting. Internal audit value proposition »*, 2015.

- « *An integrated report explains how an organization creates value over time* » ;
- « *Trust & greater transparency* ».
- *Practice guide « Assessing organizational governance in the public sector »*, 10/2014.
- « *Non-Financial Reporting: Building trust with internal audit. Enhancing governance through internal audit* », ECIIA, 2015
  - « *Implementation of integrated management, reporting and assurance* » ;
  - « *The benefits of this reform in terms of greater transparency, trust and long term performance will depend on the quality of the reports issued* ».
- GTAG 3 : « *Continuous auditing: coordinating continuous auditing and monitoring to provide continuous assurance* », 2ème édition, 03/2015.

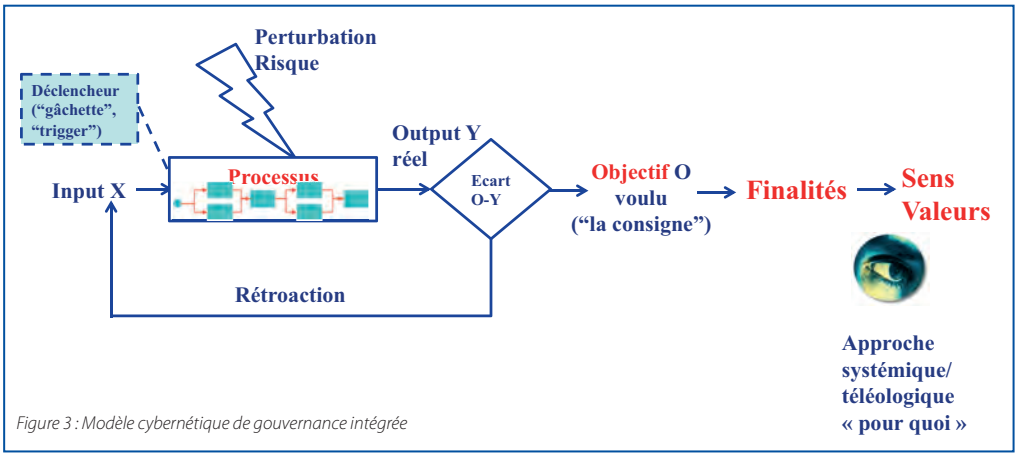


Figure 3 : Modèle cybernétique de gouvernance intégrée

La confiance, clef de voûte de la gouvernance

On constate ces dernières années, en particulier depuis la crise financière de 2008, un nombre significatif de publications, y compris dans les références IIA précitées, évoquant la question de la « confiance ».
Jack Welch (op.cit.) montre sereinement la voie à suivre :

- **« Faites confiance, déléguez et laissez le champ libre : vous ne pouvez pas tout faire vous-même.** La clé pour diriger consiste à favoriser le développement et à renforcer d'autres leaders. Vous ne saurez jamais de quoi les gens sont capables si vous ne leur donnez pas l'opportunité de prendre les choses en main » ;
- « Vous ne pouvez gérer la confiance que chacun a en soi ».

La cybernétique pour aider à modéliser la gouvernance intégrée

Développer un modèle intégré nécessite une vision « systémique ».
Norbert Wiener nous offre un concept pertinent pour notre réflexion : la cybernétique. Il est l'auteur de « *Cybernetics or control and communication in the animal and the machine* » (1948).
Etrange référence bibliographique pour un auditeur interne ? Quelle est donc la relation entre « cybernétique » et « gouvernance » ?
Le mot « cybernétique » provient du grec « κῦβερνήτης » (kubernêtês), qui signifie « pilote, gouverneur », mais aussi « gouvernail, gouvernement ». On y arrive tout doucement : gouvernance.
Dans le modèle intégré proposé, le lecteur doit accrocher son œil d'abord sur le « sens », les « valeurs », puis regarder de la droite vers la gauche : vers les finalités, les objectifs qui en sont les déclinaisons opérationnelles et enfin sur le dispositif asservi représenté, muni d'une boucle de rétroaction.
L'approche « téléologique » mentionnée dans le schéma a déjà fait l'objet d'une publication dans la revue « Audit » de l'IFACI (« S'intéresser aux objectifs et aux signes créateurs de valeur », T.Capurso & D.Coffyn, n°160, juin 2002).
Tout processus de l'organisation nécessite d'être déclenché ; une fois mis en route, il produit, à partir des inputs, des outputs, qui peuvent différer de la « consigne » (l'objectif assigné). Il peut en outre être exposé à des « perturbations » (des « risques »).
L'écart *output*/objectif est ensuite détecté et l'organisation réagit en fournissant un *feedback* (une rétroaction) pour corriger les inputs nécessaires et ainsi tenter d'atteindre l'objectif.

Dans le modèle de la figure 3, le contrôle interne, cher à l'auditeur, est à la fois :

- le *feedback* (information, mesure d'écart) sur la façon dont le système atteint (ou non) son objectif (le détecteur, comme dans le cas d'un thermostat) ;
- tous les moyens, tangibles et intangibles visant à assurer que les objectifs fixés sont atteints (l'actionneur).

Le contrôle interne assure la rétroaction donc la fonction de « régulation ».

Traduction de la gouvernance intégrée en modèle managérial

La norme ISO9001, concernant les systèmes de management de la qualité, définit systématiquement l'organisation comme un « organisme », c'est-à-dire comme « une personne ou groupe de personnes ayant sa propre structure fonctionnelle avec des responsabilités, autorités et relations en vue d'atteindre ses objectifs ».
Le management, conscient des « valeurs », des finalités et des objectifs de l'entreprise, effectue une construction mentale de sa vision managériale et des relations précitées au sein de l'organisme.
Il coordonne trois types (classiques) de processus :

- pilotage (« *corporate leadership* ») ;
- *business* (« métiers ») ;
- support.

Les deux derniers n'appellent pas de commentaires particuliers.
La notion de « *leadership* » nécessite toutefois quelques éclaircissements.

Jack Welch (encore lui !) indique dans une interview accordée à D.Roth, CEO de LinkedIn (04/2015) : **« Le *leadership* se résume en deux mots : vérité et confiance ».**
Victor Hugo en propose une métaphore tranchée : « L'homme fort dit "Je suis" et il a raison : il est ; l'homme faible dit 'Je suis' et il a aussi raison : il suit ».
La norme ISO9000:2005 (Systèmes de management de la qualité - Principes essentiels et vocabulaire) a formulé 8 principes de management de la qualité. L'un d'eux est le « *leadership* », dont le sens est : « Les dirigeants établissent la finalité et les orientations de l'organisme. Il convient qu'ils créent et maintiennent un environnement interne dans lequel les personnes peuvent pleinement s'impliquer dans la réalisation des objectifs de l'organisme ».
La même norme ajoute qu'il en découle notamment les actions suivantes :

- **créer et entretenir des valeurs communes** et des modèles de comportement fondés sur l'équité et l'éthique à tous les niveaux de l'organisme ;
- **établir la confiance et éliminer les craintes.**

La (future) version ISO9001:2015 indique par ailleurs que la finalité du *leadership* est **« aligner les**

stratégies, politiques, processus et ressources afin d'atteindre les objectifs ».

Enfin, pour chacun des 3 processus (pilotage, *business*, support), il y a lieu de considérer que les dispositifs à gérer sont des « systèmes socio-techniques » (et non pas seulement des processus et des structures. Pour simplifier la représentation, ils ont été explicités seulement dans le processus de pilotage). Précisons qu'**un système socio-technique est en interaction avec l'environnement externe et est composé des éléments suivants :**

- **l'organisation :** hiérarchie, organigramme, rôles et responsabilités, système documentaire et informationnel (procédures, normes, bases de données, ...) ;
- **la technologie :** équipements, matériels, infrastructures ;
- **le facteur humain :** le personnel en charge. Il peut s'agir, selon le cas, du maillon « fort » ou... du maillon « faible » du dispositif.

Pour contribuer à maîtriser la conception et le fonctionnement des systèmes et processus de management, on voit éclore une multiplicité de normes de systèmes de management, auxquelles les managers peuvent se référer pour asseoir et développer leur gouvernance.

Les normes ISO applicables aux systèmes de management fournissent un modèle à suivre pour mettre en place et gérer ce type de systèmes.

Citons par exemple les normes de systèmes de management suivantes : (http://www.iso.org/iso/fr/ home/standards/management-standards.htm): ISO9001 (Qualité) ; ISO14001 (Environnement) ; ISO50000 (Energie) ; ISO18001 & 45001 (Santé et sécurité au travail) ; ISO22300/22313 (Sûreté et sécurité/Continuité d'activité) ; ISO21500 (Management de projet) ; ISO27000 (Technologies de l'information) ; ISO20121 et 21101 (Services) ; ISO11000 (Gestion collaborative d'une relation d'affaire) ; ISO/DIS 34001.3 (Prévention et contrôle de la fraude) ; ISO19600 (Conformité) ; etc.

Approche cindynique de la gouvernance intégrée : un autre regard

Une gouvernance efficace doit viser à assurer la transparence, la confiance et éviter, idéalement, toute asymétrie de l'information. A cet effet, **nous préconisons une saine « confrontation » des regards / perceptions des divers acteurs de l'organisation : « De la discussion jaillit la lumière »** (« Le modèle L'Oréal », B.Collin et D.Rouach, Ed. Pearson, 2009).

François Dalle a inventé chez L'Oréal une expression inspirée de…son nom. Le terme « salle de réunion » y a été remplacé par « salle de confrontation ». L'idée essentielle était l'alignement des différentes composantes du management (animation des hommes, de la culture, des structures et de la stratégie) pour assurer la cohérence entre les différentes composantes internes et aussi externes.

Pour soutenir la structuration de cette saine confrontation, nous suggérons l'utilisation de la méthode cindynique, appliquée à plusieurs reprises et présentée en détail dans diverses conférences (T.Capurso, p.ex. « Méthodologie des cindyniques en inci-accidentologie », AMRAE, Deauville 02/2012 ; « *Practical application of « cindynics », the Science of danger, for internal auditors* », Conférence internationale de l'IIA, Orlando, 07/2013).

Les « cindyniques », littéralement du grec ancien « *κίνδυνος* » (« dangers »), ont été conçues à l'origine comme l'ensemble des sciences et des techniques qui étudient les dangers / risques (naturels, technologiques,…) et en particulier les risques majeurs. Ce néologisme a été développé par Georges-Yves Kervern, qui l'a présenté lors du colloque international sur les risques, organisé les 7 et 8 décembre 1987 à l'UNESCO. Le concept a ensuite été publié dans un premier livre, « L'archipel du danger », qu'il a coécrit avec Patrick Rubise (Ed. Economica, 1991).

Les cindyniques font partie du courant de pensée « systémique », qui considère l'organisation comme un un système complexe, composé d'éléments en interaction et interrelation permanente entre eux et avec l'environnement.

Pour mémoire, le biologiste Ludwig Von Bertalanffy, a développé dès 1932 la théorie générale des systèmes dans le but d'identifier les règles qui « organisent les relations et les interactions entre les parties des organismes ».

Dans l'approche cindynique, chaque acteur est caractérisé par cinq « attributs » ou cinq « axes », constituant son « hyperespace du danger » (Cf. figure 5).

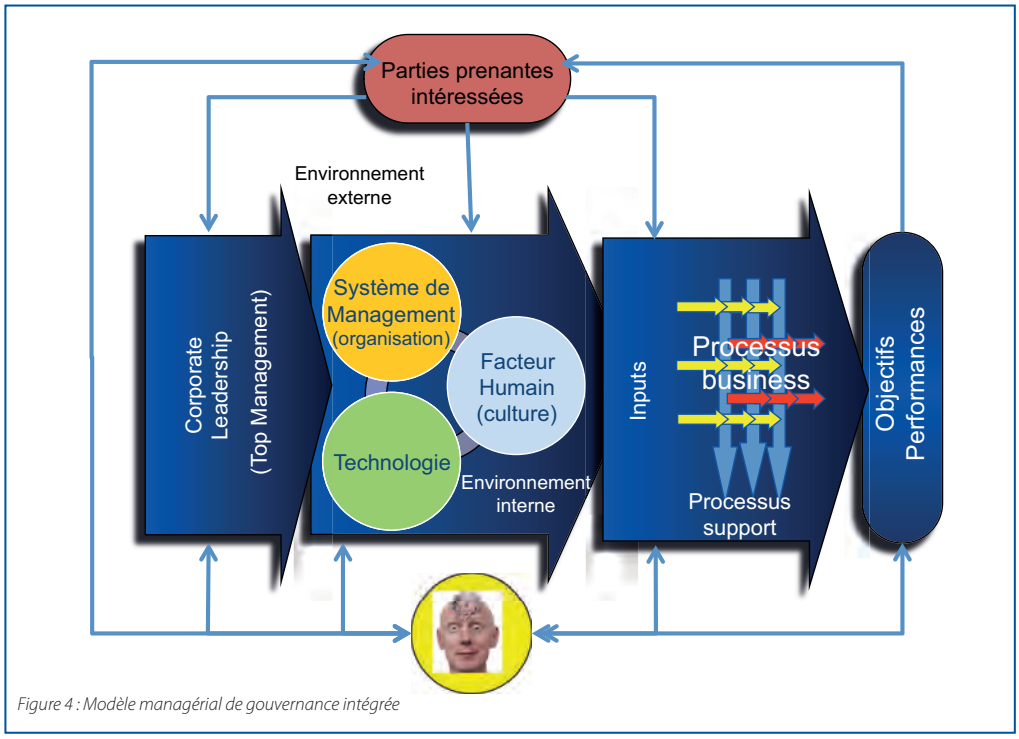


Figure 4 : Modèle managérial de gouvernance intégrée

Prenons un exemple concret de confrontation de perceptions d'acteurs. Sélectionnons en particulier l'axe « Statistique ». La navette Challenger a explosé en vol le 28/01/1986, 73 secondes après le décollage. L'enquête officielle sur la problématique des joints toriques des *boosters* a montré que, avant la décision d'autorisation du lancement :

- pour la NASA, la probabilité d'accident par défaillance des joints était marginale et variait par ailleurs selon que l'on interrogeait les ingénieurs (1%) ou la direction de tir (perception mille fois moindre que chez les ingénieurs !) ;
- pour le fournisseur, Morton Thiokol, les joints n'étaient pas fiables ni validés pour les basses températures régnant

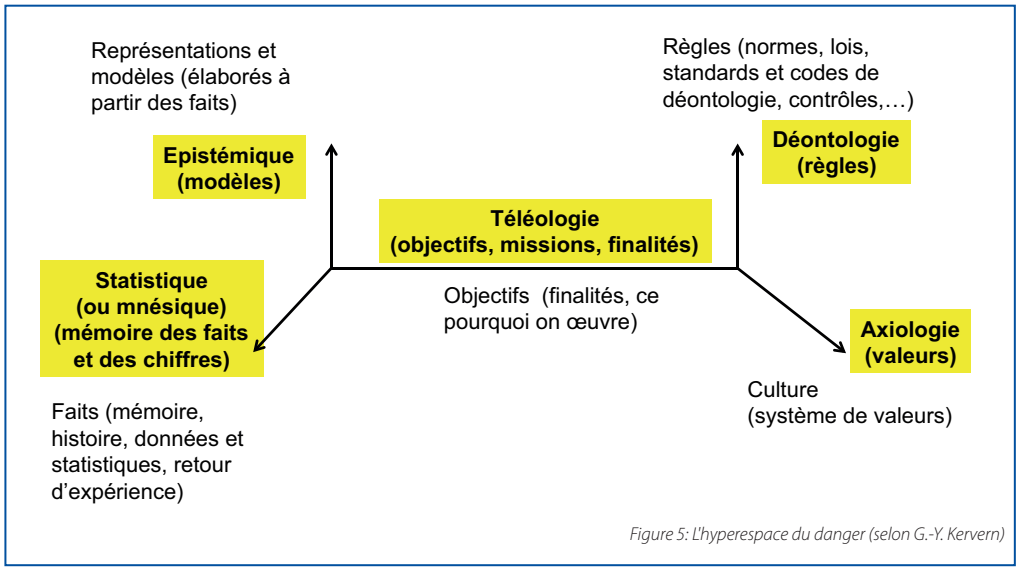


Figure 5: L'hyperespace du danger (selon G.-Y. Kervern)

en Floride ce jour-là. Le responsable des études a cédé sous la pression : « Enlevez votre chapeau d'ingénieur et mettez votre casquette de manager ! ».

Finalement, ce sont des critères d'engagement commercial / de productivité (le programme de lancement de la navette spatiale était déjà fortement en retard) qui ont prévalu sur la sécurité. Dilemme fréquent, à méditer pour les entreprises !

Dans l'approche cindynique, il s'agit d'identifier les incohérences (« déficits », « dissonances », « disjonctions »), à l'aide d'une typologie spécifique prédéfinie, afin d'imaginer ensuite les mesures de traitement nécessaires. G.-Y. Kervern a standardisé, à cet effet, 10 « déficits systémiques cindynogènes » (4 déficits culturels ; 2 déficits organisationnels ; 4 déficits managériaux).

L'organisation peut in fine être modélisée comme l'interaction d'un « réseau » d'acteurs, caractérisés chacun par son « hyperespace du danger ».

Le raisonnement proposé dans le cadre du présent article est donc la modélisation cindynique des confrontations de perceptions. Imaginez les confrontations séquentielles *Top/down* ou *Bottom/up* dans les chaînes d'acteurs internes et externes. La gouvernance intégrée peut finalement se comprendre comme un dispositif global d'harmonisation / de synchronisation des perceptions, de communication fluide et transparente et de prévention de l'asymétrie de l'information, donc d'irrigation de la confiance (Cf. figure 6).

* *
*

La compréhension d'une gouvernance intégrée nécessite d'accepter de « manager dans la complexité » (D.Genelot, Insep Consulting, 2011).

Une démarche collaborative et créative s'avère de plus en plus nécessaire, les savoirs et les capacités d'initiative relevant de chacun au sein de l'entreprise.

La confiance est indispensable; elle se construit et se détruit sur base de facteurs rationnels et irrationnels. A ce titre, une attention particulière doit être accordée aux flux d'information afin de réduire les écarts de perception (« asymétrie de l'information ») et de renforcer les processus de prise de décisions et de création de valeur à tous les niveaux.

Une gouvernance efficace vise, de manière ultime, à une triple unité :

- unité de temps ;
- unité de lieu ;
- unité d'action.

Les esthètes de l'art théâtral classique avaient déjà défini ce « canon » (« règle des trois unités ») au 17ème siècle.
Pour le coup, question nouveauté, caramba, c'est raté ! ■

ir. Tommaso Capurso est le représentant de l'IIA Belgique à l'UFAI, dont il a été Vice-Président pour l'Europe (hors France) de 2008 à 2012. Il est le Chef de la Division d'audit « Opérations et Systèmes techniques » et « Sécurité d'exploitation » à l'Audit Interne de la SNCB (Belgique). Il est membre de plusieurs Comités d'audit dont celui de l'OIF (Organisation Internationale de la Francophonie), qu'il préside.

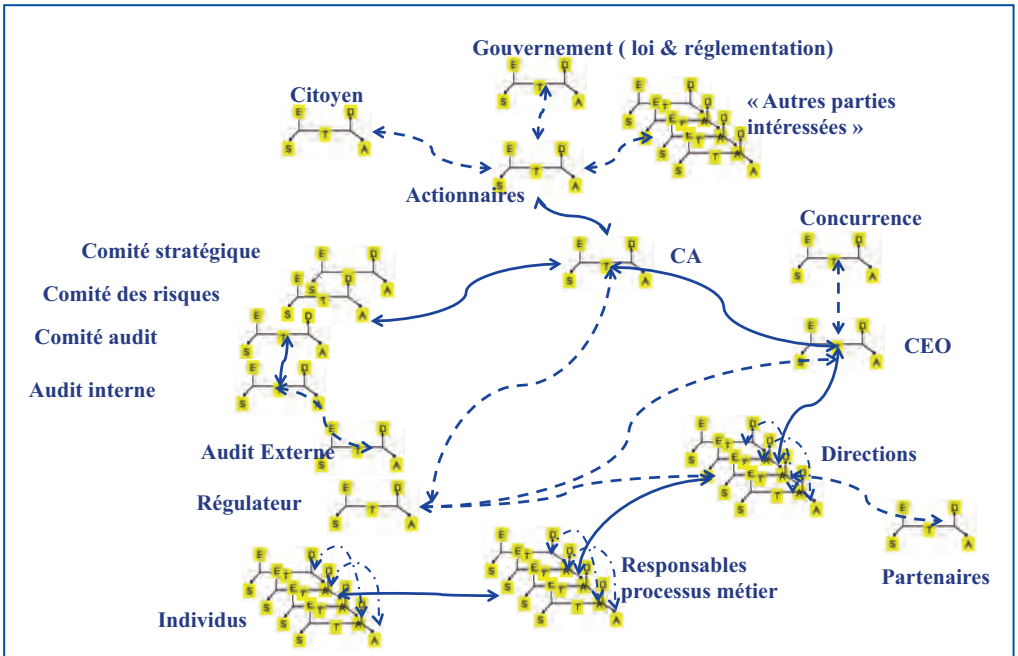


Figure 6: Modélisation cindynique des confrontations de perceptions

La fraude interne dans les collectivité territoriales

Un risque zéro ?

Au cours de ces dernières années, les législations européenne et nationale se sont renforcées pour prévenir les risques de corruption, trafic d'influence, prise illégale d'intérêt… Si ces risques ont été très présents dans les débats, la problématique de la fraude interne dans le secteur public est, en revanche, un sujet rarement abordé.

Le groupe collectivités locales de l'IFACI travaille actuellement à l'édition d'un cahier de la recherche sur la fraude interne dans les collectivités territoriales. Ce cahier devrait être publié au cours du deuxième semestre 2015.
Nous vous proposons aujourd'hui un premier regard sur cette question.

Les collectivités locales sont-elles à l'abri de la fraude interne ?

Le Département de Seine-Saint-Denis a mis en lumière, à l'occasion d'une mission d'audit interne, des fraudes aux prestations sociales. Cet audit avait pointé une fragilité de la sécurité des habilitations informatiques. Les auditeurs ont réalisé des tests qui ont mis en exergue des incohérences et permis la découverte de faux usagers et/ou de fausses prestations. Le coût de ces malversations est de l'ordre de trois millions d'euros, tandis que la période concernée s'étend sur plusieurs années.
Cet évènement rappelle que le risque de fraude interne, s'il reste occasionnel, n'en demeure pas moins une réalité.
Les hommes et les femmes qui incarnent le service public peuvent, ni plus ni moins que leurs collègues du privé, céder à certaines tentations. Et, à l'instar de toute organisation, les collectivités territoriales ont les moyens de lutter contre la fraude lorsqu'elles mettent en place des outils adéquats.
Les entreprises européennes perdent en moyenne 5 % de leurs revenus annuels du fait de la fraude (source : Deloitte 2013). Dans un contexte de raréfaction de l'argent public et d'exigence accrue des citoyens et des contribuables quant à l'utilisation de l'argent public, ce risque ne peut plus être ignoré.
Les collectivités territoriales, comme toutes institutions publiques, sont certes protégées par le cadre institutionnel et, en particulier, la séparation de l'ordonnateur et du comptable et le contrôle des chambres régionales des comptes. Ces gardes fous sont cependant insuffisants pour pallier tous les risques et ne peuvent les exonérer de renforcer leurs dispositifs de contrôle interne.
Elles sont aujourd'hui confrontées à un défi, d'autant plus important qu'elles conjuguent :

- Des types de dépenses qu'il est aisé de détourner. En effet, les aides à la personne sont un terreau particulièrement favorable à la fraude. Elles combinent de gros volumes de dossiers, des process de reconduction mensuelle automatique sur des durées longues et des montants individuels peu importants.
- Un risque d'image important dans une société qui pose un regard souvent critique sur la dépense publique.

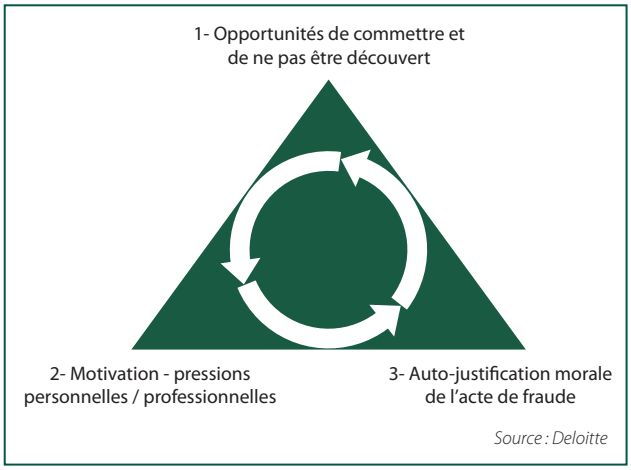
Face à cette nécessité, elles ont certainement à interroger la performance de leurs outils de contrôle interne sur leurs trois lignes de maîtrise, de l'autocontrôle jusqu'à l'évaluation du contrôle interne, l'audit.

Collectivités territoriales et fraude interne : que faire ? Comprendre, prévenir, contrôler

Comprendre : qui fraude, pourquoi, sur quoi ?

Qui fraude ?
Dans une étude publiée en 2013, KPMG tente de dresser **le portrait du fraudeur** à partir d'une population de 596 fraudeurs étudiés entre 2011 et 2013 dans 78 pays :

- 70 % ont entre 36 et 55 ans ;
- 75 % sont des hommes ;
- 61 % fraudent dans leur propre entreprise et 41 % y étaient employés depuis plus de 6 ans ;
- dans 70 % des fraudes, il y a eu collusion, soit en interne, soit en externe ;
- la personnalité des fraudeurs est majoritairement conviviale et extravertie. 39 % bénéficient d'un grand respect de leurs collègues ;
- 54 % ont des diplômes universitaires ;
- 42 % sont des cadres.



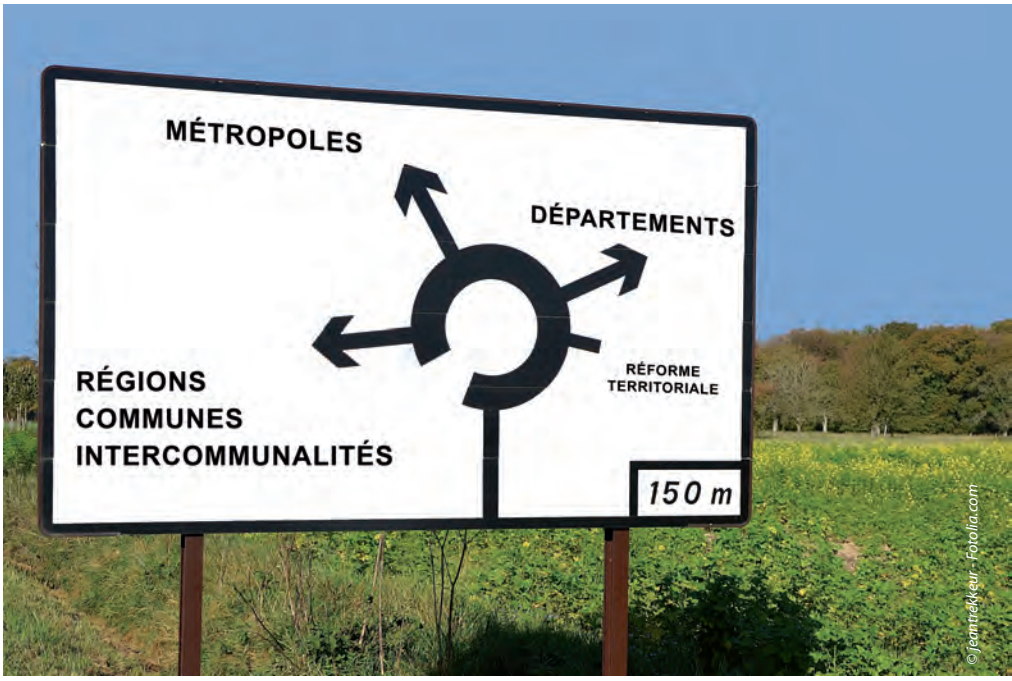
Source : Deloitte

Pourquoi ? L'avènement d'une fraude nécessite un contexte particulier
Selon l'approche largement acceptée, intitulée « triangle de fraude » ou « triangle de Cressey », trois facteurs sont des déclencheurs de fraude :

- les « opportunités » (tentations, failles, exceptions) qu'il faut réduire le plus possible ;
- les « pressions » (objectifs irréalistes, besoin de reconnaissance, changement de « train de vie ») qui sont perceptibles dans des changements de comportements ;
- une rationalisation de l'acte (évènements particuliers engendrant de la rancœur, un isolement, un rejet de l'agent)… Le fraudeur doit pouvoir justifier son acte pour le rendre acceptable à ses yeux. Cette justification

rationnelle lui permet de croire qu'il n'a rien fait de mal (tout le monde fait pareil, je n'ai pas un salaire à la hauteur de mon travail et de mes compétences…).

Sur quoi : dans quels secteurs les risques de fraude sont-ils prédominants ?
La collectivité doit recenser, via une cartographie des risques de fraude, les processus et/ou les directions où les risques de fraude sont le plus probable avec les impacts les plus forts.
Ce travail peut se construire en interne mais également à travers des échanges entre collectivités et la mise en commun d'une base incident.



© Jeantrekeur - Fotolia.com

Prévenir

Puisque l'acte de fraude nécessite opportunité et autojustification, la lutte contre la fraude est d'abord une affaire de prévention.

Cette prévention doit s'entendre dans sa double acception :

- **Une culture de lutte contre la fraude** conjuguant implication, éthique et transparence : charte de déontologie, sensibilisation et formation des agents, communication claire sur une politique de tolérance zéro…
- **Des outils de contrôle interne préventifs performants :** définition claire des responsabilités et des délégations de signature, séparation de fonctions, processus formalisés, sécurité des biens, sécurité informatique, en particulier des droits d'accès, des habilitations et du paramétrage…

Cette politique de prévention peut également se traduire par des actes managériaux forts : mise en place d'un système de protection des lanceurs d'alertes, d'un déontologue positionné sur les risques de conflits d'intérêt…

Contrôler

La lutte contre la fraude nécessite également la mise en place d'une politique de contrôle, d'autant plus nécessaire que les opportunités et modalités de la fraude se renouvellent perpétuellement.
Ces contrôles peuvent être :

- Soit embarqués : contrôles permanents, analyse des évènements anormaux…
- Soit ponctuels : intégration du risque de non prise en compte de la fraude dans le dispositif global de contrôle interne pour chaque audit réalisé…

* * *

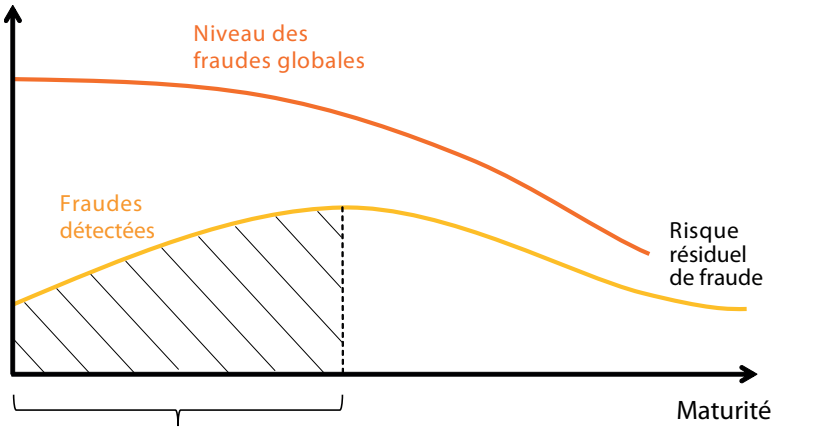
Il semble essentiel aujourd'hui que les collectivités territoriales prennent le chemin emprunté depuis dix ans par les entreprises en termes de prise de conscience de la réalité de ce phénomène et de la nécessité de mettre en place les outils permettant de le contrer.

Deux risques sont à anticiper dans ce chantier.

Le risque de discrédit des agents, réel ou subjectif. Il est donc primordial de présenter les fraudeurs comme une exception, autrement dit d'insister sur les valeurs et la probité de la grande majorité des agents de la fonction publique.

Un second risque existe. Celui de voir, dans les premiers temps, les fraudes se multiplier. Que les collectivités se rassurent, il s'agit d'un phénomène connu dans toute campagne de prévention. L'explication ne réside pas dans une recrudescence des fraudes, mais est liée à une meilleure visibilité de celles-ci. Rapidement la courbe des fraudes découvertes va diminuer, de même que celle des fraudes globales, ce qui constitue l'objectif même de cette politique. ■

La recherche de la fraude augmente la fraude ? Un paradoxe apparent



Durant une première phase, la mise en place des contrôles de fraude va mécaniquement augmenter le nombre de fraudes découvertes.
Il est important de comprendre que ce n'est pas le contrôle qui génère la fraude mais qu'il la rend lisible.

Source : PwC 2007

Groupe collectivités locales de l'IFACI

© Minerva Studio - Fotolia.com

Trois réflexions sur les outils développés sur Excel

Marcel Lukatis, IAE d'Aix-Marseille
Lauréat du prix Olivier Lemant

J'ai choisi de consacrer mon mémoire à **l'audit de la gestion et de l'architecture des UDA développées sur Excel** pour deux raisons. D'abord et surtout parce que je suis passionné par ce logiciel et les innombrables possibilités qu'il offre en termes de traitement de données et de souplesse d'application. La deuxième raison ne m'est venue qu'après mes premières heures de recherches et m'a conforté dans le choix du sujet. Je suis en effet tombé sur un article du Forbes Magazine et j'ai été stupéfait d'y lire qu'Excel était considéré comme le logiciel le plus dangereux de la planète. L'argumentaire de cette assertion était appuyé sur le fait qu'Excel est déployé au niveau de toutes les instances décisionnelles d'une institution alors que les analyses effectuées sur ce logiciel ne sont que très rarement contrôlées. Bien qu'il s'agisse d'un sujet de nature plutôt technique, j'ai voulu mettre l'accent en priorité sur l'aspect gestion et contrôle interne en abordant des sources de conflit qui n'émergent pas uniquement des enjeux techniques. Dans ce bref article seront présentées les trois réflexions qui ont constitué une trame pour mes recherches, mais d'abord je propose une entrée en matière en rappelant au lecteur ce qu'est un outil développé sur Excel.

Les UDA conçues sur Excel : Les EUDA

Une des nombreuses difficultés que j'ai rencontrées lors de mes travaux de recherche était liée à l'emploi d'un lexique adéquat pour l'objet de mon mémoire. De nombreux termes existent pour décrire ce qu'est un outil développé par un utilisateur dans un environnement qui n'est pas soumis aux standards de développement applicatif. Cependant, aucun d'entre eux ne me convenait réellement dans la mesure où ils étaient souvent trop généralistes pour convenir précisément aux outils développés sur Excel. Les termes les plus répandus sont par exemple EUCA *(End User Computer Application)* et UDA *(User Developped Applications)* qui renvoient tous deux aux applications développées par les utilisateurs quelle que soit la plateforme de conception.

Dans l'objectif de faciliter la lecture de mon mémoire et d'éviter tous problèmes d'ambigüité, je me suis permis le néologisme EUDA *(Excel User Developped Applications)* pour simplifier davantage la définition. Ce terme fait référence à tout type de fichiers Excel à usage professionnel dont l'utilisateur et le concepteur sont la même personne et dont la conception n'a pas suivi un cycle classique de développement.

> ***« L'être humain est naturellement disposé à commettre des erreurs quels que soient son niveau d'expertise et le niveau de complexité du projet »***

L'erreur est humaine

J'ai constaté à ma plus grande surprise que les ressources maitrisant les outils Excel du point de vue du contrôle interne sont plutôt limitées, ce qui est d'autant plus étonnant vu le niveau de démocratisation et le périmètre d'application du logiciel dans le monde institutionnel, éducatif et administratif.

L'institution la plus réputée pour ses recherches est EuSpRig *(European Spreadsheet Risks Interest Group)* dont un des représentants est Raymond R. Panko, professeur au Shidler College, que j'ai cité plusieurs fois dans mon mémoire en raison de ses excellents travaux sur l'occurrence des erreurs dans les outils Excel et sur l'erreur humaine de manière générale. Ayant un parcours de physicien, Panko était un des premiers à analyser le phénomène des *spreadsheet tools* qui a émergé au milieu des années quatre-vingt-dix. Il a comparé leur conception aux logiciels classiques en adaptant une approche par les erreurs, et a constaté que les erreurs commises dans les EUDA sont les mêmes que dans la construction logicielle traditionnelle alors que les techniques de développement appliquées diffèrent complètement.

La conclusion qu'il a tirée de ses recherches est que l'être humain est naturellement disposé à commettre des erreurs quels que soient son niveau d'expertise et le niveau de complexité du projet.

Les travaux de Panko deviennent intéressants pour les théoriciens parce qu'ils démontrent un paradoxe qui semble être inhérent aux outils Excel. Certains d'entre eux ont un rôle important dans l'entreprise et une complexité comparable à celle des logiciels traditionnels alors que leur conception ne suit pas le processus de développement classique. Une absence de processus de développement supervisé dans un environnement où l'utilisateur et le concepteur sont la même personne devient d'autant plus critique si on considère le constat de Panko sur l'occurrence de l'erreur.

Panko résume son observation dans un de ses travaux par une brève et simple citation d'Alexandre Pope : l'erreur est humaine.

Quand Excel décrédibilise l'ERP

Bien que l'approche par les erreurs soit une manière efficiente d'aborder le sujet, je ne voulais pas m'arrêter uniquement aux erreurs humaines pour justifier la nécessité de contrôles internes des EUDA. C'est pour cette raison que j'ai décidé d'élargir ma recherche en analysant la relation entre Excel et les progiciels de gestion intégrée.

Les ERP *(Enterprise Resource Planning,* qui est le terme anglais pour PGI) apportent essentiellement l'avantage de la concentration de la donnée. Toutes les données produites par les différentes instances de l'ERP sont rassemblées en une seule et unique base de données. Cette fonctionnalité inhérente aux ERP permet de résoudre les problèmes qui sont liés à la disparité des différentes applications au sein de l'entreprise, à savoir notamment l'évolution divergente de la même donnée.

> ***« Excel occupe aujourd'hui encore, et malgré l'émergence des PGI, un rôle fondamental dans la gestion des entreprises »***

Lorsqu'une EUDA est déployée dans l'objectif de retraiter de la donnée avant l'alimentation dans l'ERP, cet avantage de l'ERP est remis en question.

Bien que de nombreuses entreprises se soient déjà équipées d'une PGI, Excel continue souvent à agir en tant que « sous-marin » et constitue parfois la véritable source des données renseignées dans l'ERP, ce qui va à l'encontre de l'avantage apporté par ce dernier. Le recours à Excel pour alimenter l'ERP, ou même pour le remplacer, peut par ailleurs être retracé de manière générale à un refus de l'ERP par les employés dû à la peur du changement, car l'implémentation d'un ERP apporte probablement les changements les plus conséquents dans le quotidien professionnel des employés, ou à un manque de formation.

L'auditeur a selon moi tout intérêt à vérifier les interconnections entre Excel et l'ERP dans les entités auditées parce qu'elles sont souvent révélatrices d'anomalies cachées.

La fraude sur Excel

Nul ne peut nier qu'Excel occupe aujourd'hui encore, et malgré l'émergence des PGI, un rôle fondamental dans la gestion des entreprises, tous services confondus. Cette prédominance devient particulièrement évidente dans le monde bancaire où la réglementation change perpétuellement (i.e. le calcul de l'*Exposure At Default* ou EAD qui va encore évoluer dans le cadre de Bâle III).

Il est généralement trop coûteux et chronophage pour une banque de petite taille ou de taille moyenne d'adapter l'ERP ou le logiciel aux nouvelles réglementations. C'est pour cette raison que beaucoup d'entre elles ont recours à des outils développés sur Excel qui sont plus simples à maintenir et à adapter aux évolutions de la réglementation.

Ce qui est étonnant dans ce constat est qu'il y a suffisamment d'exemples d'entreprises ayant réalisé des pertes à cause d'une erreur dans un fichier Excel (par exemple la perte de JP Morgan en 2012).

Cependant, bien qu'Excel continue d'être massivement déployé dans toutes les instances opérationnelles et décisionnelles d'une entreprise, quasiment aucun cas de fraude réalisée grâce à Excel, à l'exception d'Allfirst Bank en 2002, n'a été recensé.

N'ayant pu trouver d'explications valables, exploitables ou quantitativement justifiées à ce constat, ce dernier s'est imposé comme l'ouverture de fin idéale pour mon mémoire. Bien que la fraude sur Excel ne semble tenir qu'à la manipulation d'une cellule ou d'un code VBA, il s'avère que des conditions et des circonstances très précises sont nécessaires pour réaliser un tel acte.

Compte tenu du faible intérêt des auditeurs pour ce sujet, je pense que chacun d'entre eux devrait y méditer et prendre une telle situation en considération. ■

De nationalité allemande, Marcel Lukatis a passé une majeure partie de ses études supérieures en France où il a obtenu une Licence en Langues étrangères appliquées de l'université d'Angers et un Master en Audit interne et gouvernance des entreprises de l'IAE Aix-Marseille *Graduate School of Management*.

En 2015, le prix Olivier Lemant lui a été décerné par l'IFACI pour le meilleur mémoire de fin d'études avec pour sujet l'*Audit de la gestion et de l'architecture des UDA développées sur Excel*.

© yurchello108 - Fotolia.com

Le business de l'anti-corruption

The Economist a publié dans son édition du 9 mai un article sur ce que l'hebdomadaire britannique nomme « le business de l'anti-corruption » *(the anti-bribery business)*. Pour illustrer son propos, The Economist donne l'exemple de Walmart. Le numéro un mondial de la grande distribution essaie actuellement de solder une affaire de corruption de quelques centaines de fonctionnaires mexicains (cf. revue Audit n°209)[1].

Des frais d'avocats et d'expertise colossaux

Depuis la révélation des faits en 2012, Walmart aurait déjà dépensé 800 millions de dollars en frais d'avocats et d'audits spécialisés. Le montant final sera supérieur au milliard de dollars, et pourrait avoisiner les 2 milliards. Cette estimation ne comprend ni les probables amendes et transactions à l'amiable, ni les coûts internes (le temps passé par les collaborateurs sur le sujet).

The Economist avance un montant similaire dans le cas de Siemens. Siemens a été mis en cause en 2008 par les autorités américaines dans une affaire de corruption active sur plusieurs marchés émergents (cf. revue Audit n°200). Depuis lors, la société aurait dépensé 1,5 milliard de dollars en frais d'avocats et de conseil en lien avec cette affaire.

Un recours systématique au FCPA par les Etats-Unis depuis 2007

Cette évolution s'explique par le recours par l'administration américaine au FCPA *(Foreign Corrupt Practices Act)* depuis 2007 (cf. revue Audit n°200[2]). Cette loi, en vigueur depuis 1977, n'avait été que peu utilisée jusqu'au milieu des années 2000, la sanction maximale infligée étant inférieure à 50 M$. Depuis 2007, le nombre de mises en cause dans le cadre du FCPA et le montant des amendes ont considérablement augmenté. Les amendes se chiffrent désormais souvent en centaines de millions de dollars, Alstom détenant l'amende record de 770 M$ (négociée en 2014).

The Economist recense environ 200 affaires de poursuites pour des problèmes de corruption actives à l'export dans le monde en 2014 : 130 se situent aux Etats-Unis, 30 en Allemagne, les autres dans les grands pays de l'OCDE.

Le nombre de cas hors des Etats-Unis est également en augmentation, plusieurs pays ayant récemment renforcé leur arsenal législatif. Hors d'Europe, la Chine et le Brésil ont fait de même, et sont engagées dans de vastes campagnes de lutte contre la corruption ; le Brésil s'apprêterait d'ailleurs à mettre en cause plusieurs des fournisseurs impliqués dans l'affaire Petrobras.

Cette tendance ne concerne encore qu'un petit nombre de pays à l'échelle mondiale. Ainsi, la convention OCDE interdisant la corruption d'agents publics étrangers a été ratifiée par 41 pays, mais la moitié d'entre eux n'ont encore jamais prononcé de sanctions dans ce cadre.

Néanmoins, se félicite The Economist, la tendance est irréversible, et les affaires de corrup-

tion à l'export ont désormais bien plus de chances de terminer devant les tribunaux qu'il y a une dizaine d'années.

Une inflation des frais de défense

The Economist dénonce la dérive que peuvent induire ces procédures, notamment pour satisfaire aux exigences des autorités américaines. Ainsi, le département « Conformité » de Siemens est passé, à la suite de l'affaire sus-citée, de quelques personnes à plus de 400 collaborateurs. De même, la société américaine de cosmétiques Avon, mise en cause dans une affaire de corruption en Chine, a payé deux fois plus en frais d'avocats et d'audit (350 M $) qu'en amende.

L'une des raisons pour ces coûts d'expertise exorbitants est que les sociétés mises en cause essaient de prouver que les faits incriminés ne se produisent pas ailleurs, dans d'autres filiales ou avec d'autres clients.

D'après The Economist, les cabinets d'avocat ou d'audit poussent souvent à des solutions extrêmes, en sur-estimant les obligations des sociétés mises en cause, et donc les honoraires à payer. A tel point que la directrice de la division criminelle du *Department of Justice* américain a dû recommander à certaines sociétés de modérer leurs efforts, jugeant qu'ils portaient sur un périmètre inutilement vaste, pour un coût disproportionné, et avec comme effet de retarder la résolution des affaires.

Une absence de jurisprudence problématique

Outre le montant des frais d'avocat et d'expertise, deux autres critiques sont faites au système américain. La première porte sur la durée des procédures, ce qui ne concerne d'ailleurs pas que la justice américaine. Certaines affaires, comme celles impliquant Alstom ou Walmart, sont en effet parties pour durer 10 ans, augmentant ainsi les coûts administratifs et rallongeant la période pendant laquelle la réputation de la société est exposée.

La seconde critique porte sur le système de règlement à l'amiable qui pousse la quasi-totalité des sociétés incriminées à négocier un accord avec les autorités plutôt que d'aller au contentieux devant un juge. Ainsi, il n'y a eu jusqu'ici qu'une seule société cotée qui ait été jusqu'au procès dans le cadre du FCPA. Or, les accords à l'amiable sont confidentiels, très peu de détails filtrant sur le contenu des faits de corruption et sur l'argumentaire suivi pour calculer les transactions.

D'après The Economist, même les sociétés relativement sûres de leur fait préfèrent négocier un accord à l'amiable avec les autorités américaines, permettant de clore l'affaire, plutôt que de courir le risque d'un procès avec toutes les conséquences négatives potentielles sur leur réputation, et l'incertitude quant à l'issue du procès. Cela fait qu'il n'y a pas de jurisprudence sur laquelle s'appuyer pour interpréter la loi FCPA et analyser les risques juridiques. Certains avocats de sociétés poursuivies dans le cadre du FCPA dénoncent la situation de toute puissance dans laquelle cela place les procureurs du *Department of Justice*.

D'autres voix commencent à s'élever pour dénoncer ces excès. Ainsi, plusieurs banques américaines ont récemment contesté l'interprétation qui était faite de leur habitude de recruter des « fils ou filles de » en Chine. Les banques estiment qu'on ne peut considérer comme illégal le fait d'embaucher un collaborateur dans l'espoir de remporter des contrats.

L'affaire ALCOA : le faux départ de l'anti-bribery Act

Ailleurs dans le monde, le Royaume-Uni a voté de façon médiatique l'anti-bribery Act. Force est de constater que le recours à cette loi reste encore exceptionnel : la Suisse et l'Italie ont ainsi ouvert plus d'affaires que la Grande-Bretagne en 2014, d'après The Economist.

De plus, la mise en oeuvre de l'anti-bribery Act a souffert de quelques revers spectaculaires, comme l'affaire Alcoa. Dans cette affaire, portée devant les tribunaux, un intermédiaire (M. Dahdaleh) avait versé quelques dizaines de millions de dollars de pots de vin à des officiels bahreinis pour un projet de construction d'usine métallurgique, pour le compte d'Alcoa. Le procès devant la justice britannique s'est terminé par une absolution générale, les témoins se rétractant ou ne se présentant pas.

Le risque des poursuites multiples

Pour The Economist, l'affaire Alcoa ne remet pas en cause la tendance générale, qui est bien à l'augmentation du nombre de poursuites pour des affaires de corruption. L'hebdomadaire souligne également le risque que plusieurs pays intentent des actions pour les mêmes faits. Comme l'a illustré récemment l'affaire BNP Paribas, les Etats-Unis ont une vision très large du concept de territorialité, et ont donc tendance à se saisir d'affaires n'ayant qu'un rapport ténu avec leur pays. Des poursuites concomitantes dans deux pays de l'OCDE ne sont ainsi pas à exclure, comme l'illustre le cas d'Alstom, qui doit répondre, pour les mêmes faits, à la fois devant la justice britannique et devant la justice américaine.

The Economist cite en conclusion Klaus Moosmayer, le responsable de la conformité de Siemens, qui estime que le manque de coordination entre les autorités judiciaires nationales (et donc le risque de multiplier les enquêtes) est un véritable défi pour les sociétés internationales. « Les grandes multinationales seront toujours mises en cause, de façon plus ou moins occasionnelle, pour des affaires de corruption suspectée. Elles doivent pouvoir être sûres que si elles choisissent de rendre publics ce type d'agissements lorsqu'elles les découvrent, elles ne vont pas être poursuivies et condamnées plusieurs fois ». ■

Antoine de Boissieu

« Les Etats-Unis ont une vision très large du concept de territorialité, et ont donc tendance à se saisir d'affaires n'ayant qu'un rapport ténu avec leur pays »

[1] *La justice américaine a depuis lors élargi l'enquête aux activités de Walmart dans d'autres pays émergents, notamment la Chine, l'Inde et le Brésil.*

[2] *Le FCPA est une loi américaine votée en 1977 punissant les actes de corruption de fonctionnaires étrangers.*

Guide d'audit des achats et des ventes

Pierre Schick, ESCP (MBA et DMSE), HEC (Cesa Achats), licencié ès sciences économiques
Auteur de plusieurs ouvrages, enseignant

L'auteur propose d'aider le dirigeant et les managers opérationnels afin qu'ils puissent effectuer de façon concrète un auto-diagnostic de l'organisation et du fonctionnement des activités achats et ventes et ainsi mieux se concentrer sur leurs métiers.

Promouvoir et organiser la qualité du contrôle intégré

Il est maintenant assez bien compris que l'audit interne est une activité qui doit être confiée à une équipe, intervenant au troisième degré de la ligne de maîtrise des risques, en vue notamment de vérifier la fiabilité de certains processus, tandis que le contrôle interne (qu'il serait judicieux d'appeler « contrôle intégré ») est un dispositif impliquant tous les acteurs à chaque niveau d'une organisation.
Reste que la mise en œuvre du contrôle interne peut nécessiter une impulsion pour le faire vivre au quotidien.
Il s'agit de promouvoir au sein d'une entité une culture de contrôle assurée ensuite d'une certaine permanence. Et il est donc bien naturel que quelqu'un s'en occupe, au moins temporairement, avant que le relais soit pris par tous. Cette personne appelée contrôleur interne intervient au second degré de la ligne de maîtrise.
Cette démarche est d'autant plus nécessaire que si les grandes entreprises, et à plus forte raison les groupes, peuvent disposer d'équipes en mesure de se prononcer sur l'existence et la fiabilité d'un dispositif de contrôle intégré, il faut aussi considérer le cas des PME, voire des petites collectivités territoriales et associations où la fonction d'audit interne existe rarement, bien qu'elle soit, là comme ailleurs, nécessaire.
Promouvoir et organiser la qualité du contrôle intégré est donc une obligation. C'était vrai hier ; il l'est sans doute plus encore aujourd'hui avec l'évolution des activités de contrôle et de gestion des risques dont la nouvelle définition met davantage l'accent sur la prévention que sur la détection. Cette ambition forte met indirectement en relief la nécessité d'un dispositif de contrôle pertinent et de qualité et aussi bien maîtrisé que possible par ceux qui en ont la responsabilité.
C'est à cette nécessité que répondent les notions de plus en plus affirmées depuis quelques années d'autocontrôle, d'autoévaluation, d'autodiagnostic ou de self-audit. Chacune d'elles a une définition correspondant à sa spécificité. Mais toutes renvoient à la responsabilité directe des acteurs du contrôle. Encore faut-il que ceux-ci disposent des outils adaptés à leur action. L'autodiagnostic ou self-audit est l'un de ces outils.
Son but est d'apporter un appui méthodologique – par exemple, mais pas exclusivement, à des dirigeants d'un groupe – afin de réaliser des diagnostics visant à renforcer le management des équipes, maîtriser les risques de l'organisation, améliorer l'efficacité administrative, fiabiliser les opérations et les circuits d'informations, localiser les sources de dysfonctionnement, réduire les zones d'incertitude, préciser les indicateurs de gestion et les procédures à suivre.
Il s'agit de responsabiliser les acteurs et notamment les dirigeants, afin qu'ils effectuent leur propre évaluation de la qualité et de la maîtrise de leur système de contrôle interne.

La démarche d'amélioration du contrôle interne est participative

Prévenir les dysfonctionnements d'une organisation et/ou repérer ceux qui sont en germe, identifier leurs causes, connaître les pratiques d'organisation communément adoptées par chaque fonction pour maîtriser ses risques, réclame énergie, méthode et outils.
La démarche d'autodiagnostics (ou de self-audit) est une démarche participative lancée par la direction générale d'une société.
Elle consiste à faire élaborer par les directeurs et les chefs de service un autodiagnostic sur le système de contrôle interne de l'entreprise, généralement avec l'animation du contrôleur de gestion ou contrôleur interne de la société et l'assistance éventuelle d'un conseil ou auditeur interne s'ils existent.
Elle contribue au renforcement de l'efficacité et de la cohésion de toutes les équipes de l'entreprise.
Le travail accompli par chaque équipe est important et permet, à l'issue de plusieurs réunions de travail, d'identifier à la fois les forces et les points à améliorer dans les fonctions et l'organisation de l'entreprise.
Contrairement à la situation d'audit ou de conseil en organisation, où les responsables doivent s'approprier le diagnostic de l'auditeur ou du consultant, la direction, dans le cas d'un autodiagnostic, est amenée à manifester sa capacité d'écoute vis-à-vis des problèmes relevés et à faciliter la mise en œuvre des solutions proposées. ■

Dans le sillage de l'esprit pionnier développé dans son Guide de self-audit (Editions Eyrolles) – publié en collaboration avec Olivier Lemant – Pierre Schick focalise son analyse sur les deux fonctions clés de l'entreprise que représentent les achats et les ventes, entre questionnements d'autodiagnostics, modes d'emploi en forme de tableaux des risques et « usage » de l'audit interne.

EN BREF

Comment renforcer la crédibilité du reporting intégré ?

L'IIRC *(International Integrated Reporting Council)* publie un document qui résume le point de vue des diverses parties prenantes de la consultation publique lancée en 2014 sur l'assurance relative au reporting intégré. Il s'agit d'apporter plus de crédibilité et de confiance au reporting intégré en s'interrogeant sur :

- la priorité à accorder aux activités d'assurance, notamment celles qui sont réalisées par l'audit interne ;
- les caractéristiques de mécanismes efficaces d'assurance ;
- les coûts et les bénéfices de ces évaluations ;
- les compétences et la qualité requises ;
- la robustesse des systèmes internes, notamment l'implication des organes de gouvernance ;
- les défis techniques à relever.

Pour plus d'information :

- *http://integratedreporting.org/wp-content/uploads/2015/07/IIRC-Assurance-Overview-July-2015.pdf*
- *http://www.ifaci.com/recherche/les-productions-de-la-recherche/reporting-integre-388.html*

Renforcer les 3 lignes de maîtrise avec le référentiel COSO

L'utilisation du Référentiel intégré de contrôle interne du COSO peut contribuer à l'amélioration des structures de gouvernance qui soutiendront l'efficacité des systèmes de contrôle interne et de gestion des risques des organisations. Ainsi, ce livre vert décrit les responsabilités de chacune des 3 lignes de maîtrise et de leurs parties prenantes au regard des 17 principes du COSO.

Pour plus d'information :

- *http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf*
- *http://www.ifaci.com/61/109/1/COSO-Referentiel-Integre-de-Controle-Interne.html*
- *Prise de position - Trois lignes de maîtrise pour une meilleure performance (IFACI - AMRAE)*
- *http://194.177.36.87/IFACI/New-CRIPP.pdf*

Conformité aux lois sur la concurrence : quel rôle pour l'audit interne ?

Les conséquences financières et juridiques du non-respect des lois relatives à la protection de la concurrence et à la lutte contre les ententes illicites sont régulièrement à la une de l'actualité. L'audit interne a-t-il un rôle à jouer en la matière ?
L'autorité britannique de la concurrence répond par l'affirmative dans un guide qui rappelle les questions clés que chaque conseil d'administration devrait se poser.
Ce document indique aux responsables de l'audit interne comment aider leurs instances de gouvernance en leur apportant assurance et conseil sur ces problématiques. Par exemple, l'environnement de contrôle favorise-t-il les comportements anti-concurrence ? L'entreprise est-elle en mesure d'anticiper les sanctions, y compris en initiant des négociations avec les autorités compétentes ?
Cet axe de travail est la preuve que le rôle stratégique de l'audit interne n'est pas un mythe.

Pour plus d'information :

- *https://www.gov.uk/government/publications/competition-law-risk-a-short-guide*
- *http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=71#*

Bâtir une relation de confiance pour des recommandations efficaces

La création de valeur par l'audit interne passe par la capacité à proposer des recommandations comprises et acceptées par les clients d'audit puisque ces derniers seront en charge de leur mise en place. Pour ce faire, le client d'audit doit être impliqué tout au long de la mission et dès la phase de préparation. Cette relation de confiance repose notamment sur :

- la compréhension de l'activité auditée,
- une écoute active,
- la capacité à mettre en perspective les informations recueillies,
- une attitude orientée résolution de problème.

Pour plus d'information :

- *Normes et MPA série 2200 : planification de la mission*
- *Normes et MPA série 2400 : communication des résultats*
- *Décryptage : Audit interne et décision (www.ifaci.com)*

ifaci
institut français de l'audit et du contrôle internes

Formation 2015

- 20% pour un participant inscrit simultanément à 4 formations

SESSIONS	Durée	Tarifs adhérents	Tarifs non adhérents	janv.	févr.	mars	avril	mai	juin	juillet	sept.	oct.	nov.	déc.
SE FORMER À LA MAÎTRISE DES ACTIVITÉS ET AU CONTRÔLE INTERNE														
S'initier à la maîtrise des activités et au contrôle interne	2 j	950 €	1 125 €	15-16	4-5	9-10	1-2	6-7	8-9	2-3	10-11	1-2	5-6	3-4
Réaliser une cartographie des risques	3 j	1 675 €	1 875 €	19-21	9-11	11-13	8-10	11-13	10-12	6-8	14-16	5-7	16-18	7-9
Elaborer le référentiel de maîtrise des activités	2 j	1 200 €	1 350 €	22-23	12-13	16-17	14-15	19-20	16-17	9-10	17-18	8-9	19-20	10-11
Piloter un dispositif de maîtrise des activités et de contrôle interne	2 j	1 200 €	1 350 €	26-27	19-20	18-19	16-17	27-28	18-19		23-24	14-15	24-25	16-17
Le contrôle interne des systèmes d'information	2 j	1 200 €	1 350 €	29-30		24-25			23-24			12-13		
Maîtrise des activités, contrôle interne et communication	2 j	1 200 €	1 350 €		17-18			21-22		1-2	21-22	19-20		14-15
SE FORMER À L'AUDIT INTERNE														
Les fondamentaux de l'audit interne														
S'initier à l'audit interne	2 j	950 €	1 125 €	12-13	5-6	2-3	2-3	5-6	4-5/29-30		7-8	5-6	4-5	3-4
Conduire une mission d'audit interne : la méthodologie	3+1 j	1 675 €	1775 €	14-16	10-12	4-6	8-10	11-13	9-11	1-3	9-11	7-9	16-18	7-9
Maîtriser les outils et les techniques de l'audit	3 j	1 625 €	1 775 €	19-21	16-18	9-11	13-15	18-20	15-17	6-8	14-16	12-14	23-25	14-16
Maîtriser les situations de communication orale de l'auditeur	2 j	1 050 €	1 150 €	22-23	19-20	12-13	16-17	21-22	18-19	9-10	17-18	15-16	26-27	17-18
Réussir les écrits de la mission d'audit	2 j	1 050 €	1 150 €	29-30	23-24	19-20	20-21	26-27	23-24	7-8	21-22	21-22	19-20	10-11
Exploiter les états financiers pour préparer une mission d'audit	3 j	1 525 €	1 675 €	26-28		23-25		27-29			28-30		23-25	
Désacraliser les systèmes d'information	3 j	1 525 €	1 675 €			16-18			1-3		23-25			2-4
Détecter et prévenir les fraudes	2 j	1 050 €	1 150 €		26-27		22-23		4-5		21-22	19-20		8-9
Le management														
Piloter un service d'audit interne	2 j	1 300 €	1 450 €		12-13				11-12			8-9		
Manager une équipe d'auditeurs au cours d'une mission	1 j	685 €	770 €			16				6			17	
L'audit interne dans les petites structures	1 j	685 €	770 €					4					27	
Balanced Scorecard du service d'audit interne	1 j	685 €	770 €			27					25			
Le suivi des recommandations	1 j	685 €	770 €	28			16		15		30		18	
Préparer l'évaluation externe du service d'audit interne	2 j	1 300 €	1 450 €		10-11			12-13					19-20	
L'audit interne, acteur de la gouvernance	1 j	685 €	770 €				17					1		
Audit interne, contrôle interne et qualité : les synergies	1 j	685 €	770 €		23		15					2		
Les audits spécifiques														
Audit du Management de la Continuité d'Activités	2 j	1 300 €	1 450 €		24-25				25-26			21-22		
Audit de la fonction Comptable	2 j	1 300 €	1 450 €				13-14					12-13		
Audit de performance de la gestion des Ressources Humaines	3 j	1 525 €	1 675 €				28-30						23-25	
Audit de la fonction Achats	2 j	1 300 €	1 450 €		26-27			26-27				14-15		
Audit des Contrats	1 j	685 €	770 €					18					4	
Audit de la fonction Contrôle de Gestion	2 j	1 300 €	1 450 €			30-31						7-8		
Audit de la Sécurité des Systèmes d'Information	2 j	1 300 €	1 450 €			19-20					28-29			
Audit des Processus Informatisés	2 j	1 300 €	1 450 €				9-10						25-26	
Audit de la Conformité à la Législation Sociale	2 j	1 300 €	1 450 €		16-17							5-6		
Audit du Développement Durable	2 j	1 300 €	1 450 €					19-20				13-14		
Audit des Projets et Investissements	2 j	1 300 €	1 450 €				2-3						23-24	
SE FORMER DANS LE SECTEUR PUBLIC														
Le contrôle interne dans le secteur public	2 j	1 300 €	1 450 €			5-6				7-8			16-17	
Pratiquer l'audit interne dans le secteur public	4 j	1 950 €	2 150 €				14-17				14-17			1-4
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 €						17-19		16-18			2-4
Pratiquer l'audit interne dans une banque ou un établissement financier	4 j	1 950 €	2 150 €						22-25		22-25			7-10
SE FORMER DANS LE SECTEUR DES ASSURANCES														
Le contrôle interne dans le secteur des assurances	2 j	1 300 €	1 450 €		5-6			5-6			7-8		5-6	
Pratiquer l'audit interne dans le secteur des assurances	4 j	1 950 €	2 150 €			10-13			16-19			13-16		14-17
SE FORMER DANS LES SECTEURS INDUSTRIE ET COMMERCE														
Audit de la gestion des stocks et de la logistique	2 j	1 300 €	1 450 €		3-4					9-10				
Audit du processus de ventes	2 j	1 300 €	1 450 €				7-8					15-16		
ACQUÉRIR UNE CERTIFICATION														
Préparation au CIA - Partie 1	2 j	950 €	1 125 €			11-12			2-3		8-9			2-3
Préparation au CIA - Partie 2	2 j	950 €	1 125 €			18-19			8-9		14-15			9-10
Préparation au CIA - Partie 3	3 j	1 525 €	1 675 €			24-26			17-19		23-25			15-17
CRMA Training	2 j	995 €	1 170 €	*Dates sur notre site internet : www.ifaci.com*										

CRMA™
CERTIFICATION IN RISK MANAGEMENT ASSURANCE

Gestion des Risques :

Auditeurs internes, le comité d'audit et la direction générale comptent sur vous !

Norme 2120 – Management des risques : L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration.

Afin de renforcer la capacité des auditeurs internes à exercer efficacement leurs responsabilités en matière d'évaluation des processus de management des risques, l'IIA a développé la certification CRMA (Certification in Risk Management Assurance).

Le CRMA est un examen de 2 heures, composé de 100 Questions à Choix Multiples. Il est conçu pour les auditeurs internes et les professionnels de la gestion des risques qui interviennent sur les périmètres de l'évaluation des risques, sur les processus de gouvernance, sur l'évaluation de la qualité et l'auto-évaluation des contrôles.

Marquez des points !

Détenir le CRMA 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.

POUR EN SAVOIR PLUS ...

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

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

ifaci
institut français de l'audit et du contrôle internes

The Institute of Internal Auditors