Surfer sur les SI
Le Top 10 des risques SI

LES TECHNOLOGIES

Rapport Principal

Le rôle de l'audit interne

Philip E. Flora
CIA, CISA, CFE, CCSA

Sajay Rai
CPA, CISSP, CISM

The IIA Research Foundation

CBOK
The Global Internal Audit Common Body of Knowledge

À propos du CBOK

CHIFFRES CLÉS

14 518* répondants

166 pays

23 langues

NIVEAUX HIÉRARCHIQUES

Responsables de l'audit interne 26%

Directeurs de mission ou senior managers 13%

Superviseurs ou managers 17%

Auditeurs internes 44%

*Le taux de réponse varie selon les questions.

Le CBOK *(Common Body of Knowledge)* est la plus grande étude actuellement menée sur l'audit interne à l'échelle mondiale. Elle comprend notamment des enquêtes auprès des professionnels de l'audit interne et de leurs parties prenantes. L'enquête mondiale sur la pratique de l'audit interne, qui apporte une vision complète des activités et des caractéristiques de la profession partout dans le monde, fait partie des éléments fondamentaux du CBOK 2015. Ce projet s'appuie sur deux enquêtes internationales réalisées précédemment sur le même sujet par la Fondation de la recherche de l'IIA, en 2006 (9 366 réponses) et en 2010 (13 582 réponses).

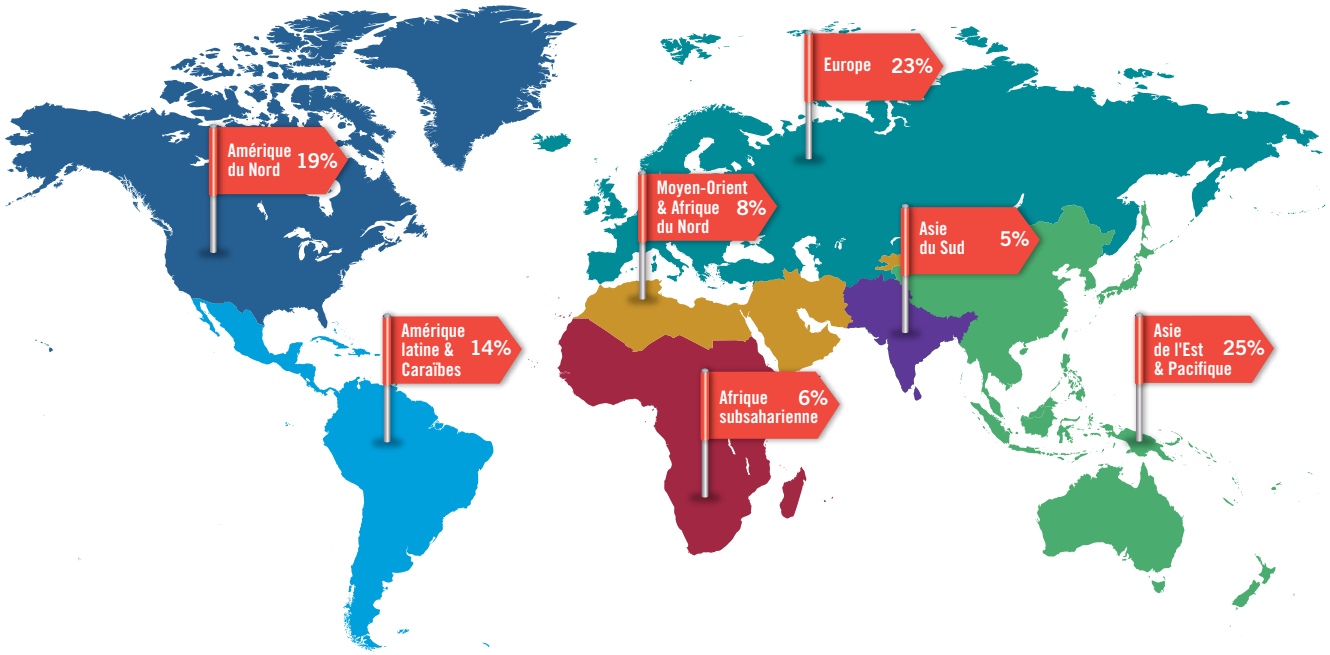
Les rapports de l'enquête seront publiés une fois par mois jusqu'en juillet 2016 et pourront être téléchargés gratuitement grâce à la généreuse contribution d'individus et d'organisations professionnelles, mais également de chapitres et d'instituts de l'IIA. Plus de 25 rapports devraient voir le jour, sous forme :

- de rapports portant sur des thématiques générales ;
- de gros plans approfondissant des problématiques clés ;
- de faits marquants concernant un thème ou une région spécifique.

Ces rapports s'intéresseront à différentes problématiques réparties selon huit catégories, parmi lesquelles les technologies liées aux systèmes d'information (SI), les risques, et la gestion des talents.

Rendez-vous sur le site du CBOK Resource Exchange à l'adresse www.theiia.org/goto/CBOK pour télécharger les derniers rapports, au fur et à mesure de leur publication.

Enquête 2015 du CBOK sur les pratiques de l'audit interne : répartition géographique des participants



Note : Les zones géographiques correspondent aux catégories définies par la Banque mondiale. Concernant l'Europe, moins de 1 % des répondants étaient originaires d'Asie centrale. Les réponses à l'enquête ont été recueillies entre le 2 février et le 1er avril 2015. Le lien hypertexte vers l'enquête avait été diffusé via une liste d'adresses électroniques, les sites Internet de l'IIA, des lettres d'information et les réseaux sociaux. Les questionnaires partiellement remplis ont été inclus dans l'analyse dès lors que les informations sur la population interrogée étaient complètes. Dans les rapports du CBOK 2015, les questions spécifiques sont intitulées Q1, Q2, etc. La liste complète des questions est disponible sur le site du CBOK Resource Exchange.

Les thèmes du CBOK

Le futur

Les perspectives internationales

La gouvernance

La gestion du service

Les risques

Normes et certifications

La gestion des talents

Les technologies

Table des matières

Synthèse

Les principaux risques émergents liés aux systèmes d'informations (SI) sont-ils correctement identifiés et gérés au sein de notre organisation ? Voici l'une des principales questions que se posent les administrateurs, membres de comités d'audit et de Conseils partout dans le monde. Ce rapport fournit des informations clés aux auditeurs internes et à leurs parties prenantes, afin de les aider à appréhender et surveiller les principaux risques SI du moment.

Vous y trouverez :

- Le Top 10 des risques SI ;
- Les questions que l'auditeur interne doit impérativement se poser concernant ces risques ; et
- Les principales actions à entreprendre par les services d'audit interne pour y faire face.

Les dix principaux risques SI visés dans ce rapport ont été identifiés grâce à des entretiens avec des responsables de l'audit interne et des experts en SI du monde entier. En outre, les tendances relatives aux risques SI s'appuient sur les résultats de l'édition 2015 du CBOK sur la pratique de l'audit interne, la plus importante enquête du monde consacrée à la profession. L'ordre de priorité de ces risques peut varier selon le secteur d'activité.

Ce rapport guide le lecteur dans la nébuleuse des problématiques actuelles et émergentes liées aux SI. Il propose également une analyse des risques découlant d'un déficit de compétences SI au sein du service d'audit interne et d'un manque de sensibilisation des administrateurs.

1 Cybersécurité

"S'agissant de la cybersécurité, la plupart des dirigeants n'ont pas conscience du niveau de risque qu'ils assument."

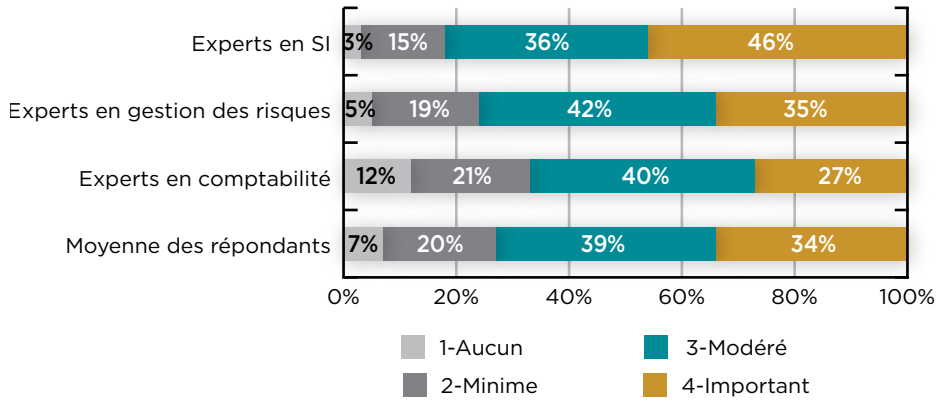
—Scott Klososky, Associé chez Future Point of View, LLC, États-Unis

En matière de système d'information, la cybersécurité est sans doute l'un des thèmes les plus discutés entre les dirigeants, les auditeurs internes et les administrateurs. C'est donc sans surprise le risque n°1 de notre Top 10. L'une des menaces majeures auxquelles les organisations sont confrontées réside dans le vol, par intrusion, d'informations sensibles ou confidentielles. La plupart des organisations sont conscientes des conséquences qu'une telle fuite de données pourrait avoir sur leur image de marque et leur réputation, comme en témoigne la **figure 1.** En effet, plus de 70 % des répondants considèrent le risque de fuite de données comme important ou modéré. Il convient également de souligner que les experts en SI jugent ce risque bien plus significatif (82 %), et ce, probablement parce qu'ils comprennent mieux les SI et savent quelles brèches peuvent être exploitées.

Rôle de l'audit interne

Les auditeurs internes peuvent jouer un rôle crucial au sein de l'organisation et s'assurer que les risques de cybersécurité sont correctement gérés. Selon la taille de l'organisation, les mesures qu'ils prennent et les questions qu'ils posent peuvent varier. Dans les petites organisations (moins de 1 500 salariés), cinq répondants sur dix réalisent peu d'activités d'audit liées à la cybersécurité, voire aucune. Dans les grandes organisations, *a contrario*, quatre répondants sur dix exercent une activité importante dans le domaine. (Q92, n = 9 929).

Figure 1 Niveaux du risque relatif à la fuite de données susceptibles de porter atteinte à l'image de marque



Note : Q93 : À votre avis, quel est le niveau de risque inhérent de votre organisation pour les domaines émergents des systèmes d'information suivants ? Les réponses « Sans objet / Je ne sais pas » n'ont pas été prises en compte. Pour des raisons d'arrondi, le total peut parfois différer de 100 %. n = 1 038 pour les experts en SI ; n = 1 139 pour les experts en gestion des risques ; n = 1 678 pour les experts en comptabilité ; n = 9 426 pour l'ensemble des répondants.

“Les auditeurs devraient s'assurer que leur organisation a mis en place un processus permettant de tirer des leçons de ses propres expériences et de celles des autres. Cela passe par des espaces de collaboration. Par exemple, Financial Services Information Sharing and Analysis Center est une organisation mondiale fortement sollicitée par les établissements financiers pour le partage d'idées dans la lutte contre les cybermenaces.”

—James Alexander, CIA, CFE, CISA, Directeur de la gestion des risques, Unitus Community Credit Union, Portland, Oregon

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

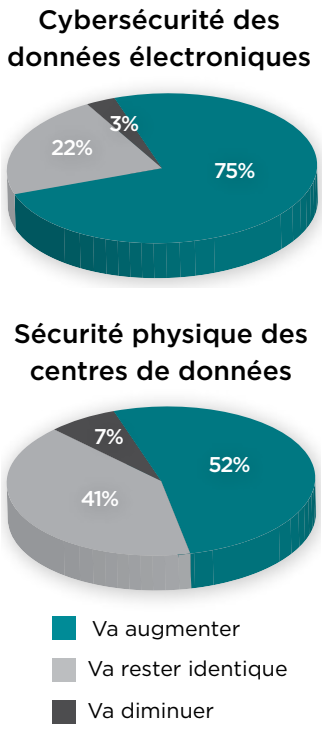
1. L'organisation est-elle en mesure de surveiller les intrusions dans son réseau ?
2. L'organisation est-elle en mesure d'identifier une attaque lorsqu'elle se produit ?
3. L'organisation est-elle en mesure d'isoler l'attaque et de limiter les dommages éventuels ?
4. L'organisation est-elle en mesure de savoir si des données confidentielles font l'objet de fuites ?
5. En cas d'incident, existe-t-il un plan de gestion de crise formalisé, éprouvé et en adéquation avec les niveaux d'exposition de l'organisation ?
6. En cas d'incident, l'organisation dispose-t-elle des capacités d'investigation nécessaires pour y faire face ?
7. Une équipe d'intervention est-elle en place pour gérer les incidents éventuels et, si oui, ses membres connaissent-ils leur rôle et leurs responsabilités ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Réaliser chaque année une analyse indépendante de vulnérabilité et des tests de pénétration du réseau.
2. Vérifier que des exercices de simulation sont effectués dans le cadre du plan de gestion de crise de l'organisation, afin de s'assurer que l'équipe d'intervention est prête à agir en cas d'incident.
3. Réaliser une mission d'audit de l'architecture réseau afin de déterminer si celle-ci est conforme aux règles et procédures définies.
4. Réaliser une mission d'audit sur un incident récent afin de déterminer si les règles, les procédures et les outils ont été appliqués comme prévu, et si des experts en investigation ont été mobilisés au cours de l'incident.

2 Protection des données

Figure 2 Evolution des activités d'audit interne



Note : Q94 : Au cours des deux ou trois prochaines années, estimez-vous que l'activité de l'audit interne dans les domaines suivants liés aux systèmes d'information va augmenter, diminuer ou rester stable ? n = 11 163.

Bien que la cybersécurité fasse l'objet d'une forte couverture médiatique, la protection des données, en matière de confidentialité, d'intégrité et d'accès, est tout aussi essentielle et arrive en 2e position du Top 10.

Par le passé, la plupart des organisations s'attachaient essentiellement à se protéger sur le périmètre de leur réseau. Elles dépensaient une part non négligeable de leur budget sécurité pour l'établissement d'un périmètre de défense, en investissant dans des dispositifs tels que des pare-feux, des systèmes de prévention et de détection des intrusions, des outils de filtrage des contenus ou encore des mécanismes de surveillance du réseau. Néanmoins, au vu des récents cas de fuite de données à grande échelle, il est clair que cette stratégie est caduque. Les intrus désireux d'attaquer le réseau d'une organisation y parviendront d'une manière ou d'une autre. Il s'agit donc désormais d'opter pour un système multi-niveaux de défense des données critiques, plutôt que pour une protection à un seul niveau du réseau.

En règle générale, un programme efficace de protection des données est piloté à un niveau hiérarchique élevé, par exemple par le responsable de la sécurité des systèmes d'information, et comprend systématiquement les éléments suivants :

- Un solide processus d'évaluation des risques ;
- Des politiques efficaces de gouvernance et de conformité ;
- Des règles et des normes formalisées et diffusées ;
- Un plan de sensibilisation et de formation efficace ;
- Des procédures efficientes de contrôle des accès ;
- Des plans éprouvés de reprise après sinistre, de continuité d'activité et de résolution des incidents ;
- Des processus de gestion des actifs, du réseau, des patchs et du changement qui fonctionnent ;
- Des mesures strictes en matière de sécurité physique.

Rôle de l'audit interne

L'audit interne peut jouer un rôle crucial en s'assurant de l'efficacité et de l'efficience du programme de protection des données de l'organisation. Le plan d'audit interne devrait toujours inclure des missions liées à la sécurité physique et à la cybersécurité, bien que ce second volet soit voué à se développer plus rapidement. En effet, comme l'illustre la **figure 2**, plus de 75 % des répondants prévoient d'accroître leurs activités liées à la cybersécurité, contre 52 % pour la sécurité physique.

“Les activités liées à la sécurité de l'information et à la gestion des risques ne permettront pas de maîtriser les principales menaces si les collaborateurs ne savent pas comment s'y prendre et qu'ils ne détiennent pas les pouvoirs nécessaires pour agir.”

—Grace Lwanga,
Directeur technique,
Audit des SI, World Vision International

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Quelle est la date de dernière révision et mise à jour de la politique de protection des données ?
2. Quel est le taux de participation au plan de formation en matière de sécurité des données ? Cette formation est-elle obligatoire ? Quelles sont les conséquences pour les collaborateurs qui n'ont pas suivi la formation ?
3. Quelle est la date de la dernière évaluation des risques ? Les nouveaux prestataires externes ont-ils été soumis à une évaluation des risques ?
4. Des simulations pour déterminer si l'organisation est prête à faire face aux éventuels incidents sont-elles réalisées ?
5. Quelle est la date du dernier test de reprise après sinistre ? A-t-il été probant ? Quels ont été les problèmes rencontrés ?
6. Quelles sont les exigences de conformité de l'organisation ? La loi américaine *Health Insurance Portability and Accountability Act* (HIPAA) de 1996 ? La loi Sarbanes-Oxley (SOX) de 2002 ? Les normes de sécurité PCI ?
7. Les intrus peuvent-ils pénétrer dans les locaux de l'organisation grâce à l'ingénierie sociale ? (par exemple lorsqu'un individu mal intentionné engage une conversation anodine avec un collaborateur en dehors du bâtiment, puis y pénètre en même temps que le collaborateur au moment où celui-ci scanne son badge.)
8. Les activités des utilisateurs privilégiés (c'est à-dire ceux qui sont autorisés à gérer l'environnement des SI) sont-elles enregistrées et surveillées ?

PRINCIPALES ACTIVITES DE L'AUDIT INTERNE

1. Réaliser une analyse de vulnérabilité du réseau interne.
2. Vérifier le processus d'examen du contrôle des accès. Les propriétaires des données ou des processus examinent-ils réellement la liste des accès ou est-ce une simple formalité, l'approbation de la liste étant effectuée sans en prendre vraiment connaissance.
3. Faire appel à des tiers pour simuler une attaque et auditer les résultats. Par exemple, dans les grandes et moyennes organisations, mener des opérations de *phishing* (« hameçonnage ») par courrier électronique afin de déterminer l'efficacité du plan de sensibilisation et de formation.
4. Réaliser une mission d'audit du processus de sauvegarde des données critiques et vérifier que des sauvegardes sont régulièrement effectuées.
5. Réaliser une mission d'audit des activités des utilisateurs privilégiés et vérifier que seuls les utilisateurs concernés disposent de ces privilèges. Vérifier que les utilisateurs privilégiés sont enregistrés et surveillés.
6. Réaliser une mission d'audit des tiers ayant accès aux actifs critiques de l'organisation, ou pour les grandes organisations, examiner leurs rapports SSAE 16 *(Statement on Standards for Attestation Engagements)*.

3 Projets SI

"Les organisations doivent apprendre rapidement de leurs erreurs dans le développement de systèmes. Elles seront ainsi mieux à même de développer et d'utiliser plus efficacement des applications essentielles pour leur activité."

—Edward Carr,
Responsable de l'audit des SI,
Bureau d'audit interne,
État de l'Ohio

Une large part du budget SI est consacrée aux projets, si bien que ces derniers arrivent en 3ème position de notre Top 10. Pour rester viables, toutes les organisations ont besoin de développer ou de mettre à jour leurs systèmes d'information. Malheureusement, les chances de réussite sont faibles. D'après le rapport CHAOS publié par le cabinet d'analyste Standish Group, les projets SI sont répartis en trois catégories :

- Projets globalement réussis : 16,2 %
- Projets contestés : 52,7 %
- Projets compromis (annulés) : 31,1 %

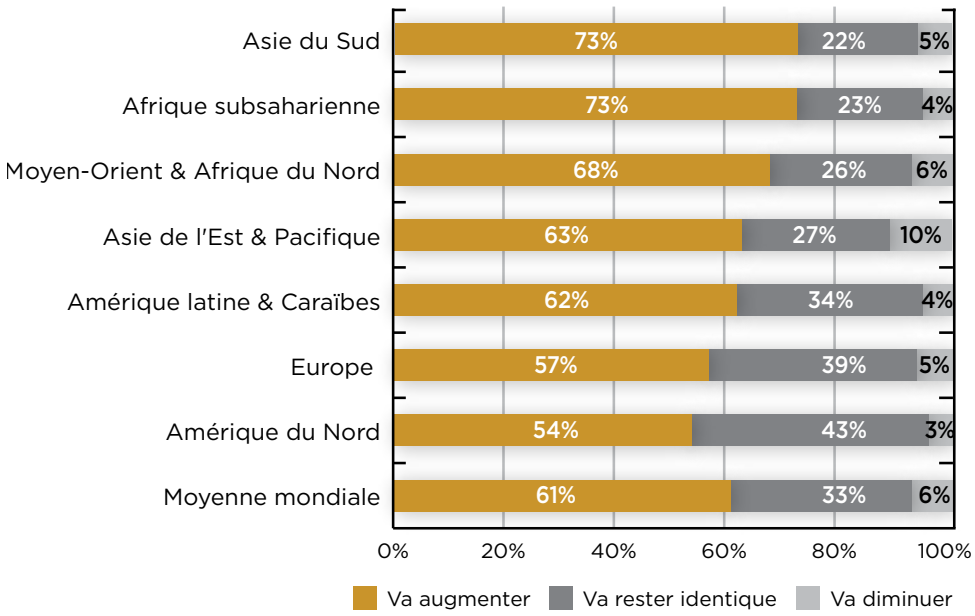
Selon une autre étude, les défaillances logicielles coûteraient 50 à 80 milliards de dollars par an aux organisations.*

La majorité des répondants du CBOK reconnaît qu'il est important de continuer, voire d'augmenter, les activités d'audit liées aux projets SI (voir figure 3). Environ six répondants sur dix envisagent un accroissement du nombre de mission dans ce domaine.

Les objectifs des principaux projets SI doivent être surveillés tout au long de la

* CIO Journal, janvier 2014, extrait du Wall Street Journal.

Figure 3 Evolution des activités d'audit liées aux grands projets SI



Note : Q94 *: Au cours des deux ou trois prochaines années, estimez-vous que l'activité de l'audit interne dans les domaines suivants liés aux systèmes d'information va augmenter, diminuer ou rester stable ? Thème : Audit/assurance pour la gestion des grands projets. n = 11 019.*

NON-RESPECT DES ATTENTES

Voici une liste non exhaustive des raisons les plus fréquentes pour lesquelles les projets SI ne répondent pas aux attentes du management :

- Date de fin de projet imposée (cette date est fixée avant que l'équipe projet établisse un calendrier approprié et/ou ne réalise une évaluation technique du projet)
- Besoins non réalistes
- Inadéquation entre les attentes et les ressources
- Absence d'exploitation des retours d'expériences concernant les projets peu performants
- Rapports d'étape rares ou inexacts (absence d'analyse de la valeur ajoutée)

phase de développement et après leur mise en œuvre.

Les défaillances généralement observées sont les suivantes : non-respect des échéances, dépassement du budget, moindre efficience par rapport aux prévisions, logiciels défaillants car non testés avant leur déploiement, moindre intégration par rapport au plan initial, fonctionnalités moindres par rapport au *business case* indiqué dans le projet approuvé.

Le manque de leadership constitue un autre problème majeur car il peut nuire au projet à plusieurs niveaux. En voici quelques exemples classiques :

- Le sponsor du projet au niveau de la direction apporte un soutien limité ou ne s'implique pas.
- Les assistants à la maîtrise d'ouvrage (business analyst) sont peu efficaces ou n'ont pas suivi les formations appropriées.
- La gestion des risques est insuffisante ou médiocre.
- Le chef de projet ou son management sont peu efficaces ou expérimentés.
- Le comité de pilotage du projet est inefficace.

Rôle de l'audit interne

L'audit interne devrait envisager de réaliser des missions à chacune des étapes du cycle de développement des systèmes. Traditionnellement, ce cycle comprend les étapes suivantes : étude de faisabilité, étude des besoins, définition des besoins, conception détaillée, programmation, tests, installation et revue post-déploiement.*

* Voir le glossaire de l'ISACA à l'adresse suivante : www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Comment les projets sont-ils approuvés au sein de l'organisation ?
2. Comment les projets sont-ils lancés ou initiés au sein de l'organisation ?
3. Comment les projets sont-ils gérés au sein de l'organisation ?
4. Les grands projets sont-ils sponsorisés par un manager au niveau hiérarchique suffisant ?
5. Existe-t-il un comité de pilotage du projet et, si oui, se réunit-il régulièrement ?
6. Si des prestataires interviennent dans le développement du projet, quel est le processus de gestion du contrat et de la relation ?
7. Des rapports d'étape mensuels sont-ils fournis ?
8. Quelle est la procédure à suivre en cas de dépassement de budget ou d'échéances ?
9. Un processus d'annulation des projets dont les objectifs ne sont pas atteints est-il en place ?
10. La direction des systèmes d'information (DSI) réalise-t-elle des études de satisfaction auprès des utilisateurs concernant les résultats et le coût des projets SI ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Réaliser des missions tout au long du cycle de vie des principaux projets SI. Ce cycle de vie comprend les éléments suivants : respect des contrats, gestion de projet, coûts (dotation en personnel et frais du prestataire), avancement du projet, demandes de modification, programme d'encouragement/de primes, etc.
2. Prendre part aux audits du projet avec les équipes qualité ou d'audit du prestataire, afin de limiter le nombre d'interventions et/ou d'acquérir de nouvelles connaissances, tout en minimisant les risques de perturbation du projet.
3. Réaliser une mission d'audit de la méthodologie de gestion de projet de l'organisation.
4. Examiner le portefeuille projets et vérifier que la méthodologie est appliquée, notamment pour les projets qui dépassent le budget ou les échéances.
5. S'assurer que les utilisateurs sont impliqués dans les modifications apportées au périmètre et aux livrables du projet.
6. Une fois le projet terminé, examiner les résultats de l'étude de satisfaction réalisée auprès des utilisateurs par la DSI, ou mener une telle étude afin de vérifier les résultats fournis par la DSI.
7. Déterminer si des analyses postmortem des échecs ou des retours d'expérience sont effectuées et exploitées pour améliorer les processus des futurs projets.

Pour de plus amples informations, consultez le GTAG 12 de l'IIA, *Audit des projets SI*, 2009, disponible à l'adresse suivante : www.theiia.org, rubrique « Standards & Guidance » ou sur le site de l'IFACI : www.ifaci.com.

4 Gouvernance des SI

DÉFINITION DE LA GOUVERNANCE DES SI

La gouvernance des SI comprend la direction, les structures organisationnelles et les processus qui garantissent que les technologies de l'information soutiennent la stratégie et les objectifs de l'organisation.

— Source : Cadre de Référence International des Pratiques Professionnelles de l'audit interne (IIA / IFACI, 2013).

COMPOSANTES D'UNE GOUVERNANCE DES SI EFFICACE

- Structures de l'organisation et de la gouvernance
- Encadrement et soutien
- Planification stratégique et opérationnelle
- Prestations de services et évaluation
- Organisation et gestion des risques SI

— Source : GTAG 17 : Auditing IT Governance (Altamonte Springs, Floride : The Institute of Internal Auditors, juillet 2012).

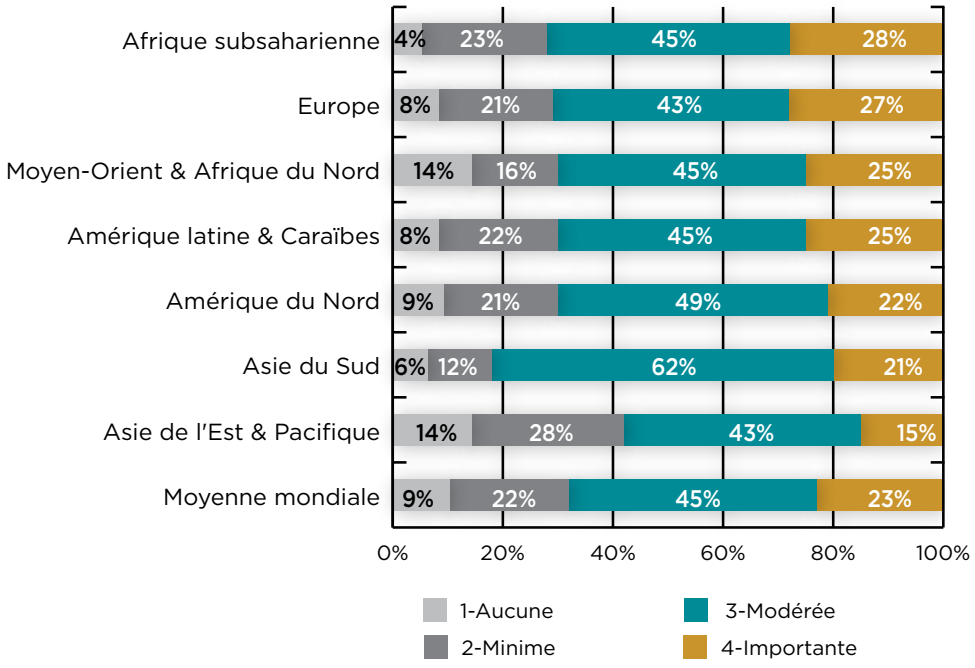
Les récents scandales qui ont éclaté dans le monde des affaires ont mis en cause le gourvernement d'entreprise mais également la gouvernance des SI. Cette thématique constitue donc le 4ème risque du Top 10.

Dans de nombreuses organisations, le management s'interroge sur les sommes dépensées pour les SI, si bien que l'accent est davantage mis sur le contrôle des coûts dans ce domaine. Cette attention particulière résulte également de l'écart grandissant entre les besoins métiers, tels que perçus par les DSI, et les capacités des SI, telles que perçues par les opérationnels. Pour être efficace, tout programme de gouvernance des SI doit, au minimum :

- Être explicitement aligné sur les besoins métiers ;
- Créer une valeur mesurable pour les métiers ;
- Prévoir des dispositifs de contrôle et de devoir de rendre compte des ressources, des risques, des performances et des coûts.

Environ trois répondants sur dix déclarent avoir une activité d'audit interne nulle ou

Figure 4 Niveau d'activité relatif à la gouvernance des SI



Note : Q72 : Quelle est l'étendue des revues du gouvernement d'entreprise de votre département d'audit interne ? Thème : Revues des politiques et procédures de gouvernement d'entreprise relatives à l'utilisation des systèmes d'information. Responsables de l'audit interne uniquement. Les réponses « Sans objet/Je ne sais pas » n'ont pas été prises en compte. n = 2 545.

PLANIFIER UNE MISSION D'AUDIT DE LA GOUVERNANCE DES SI

Pour définir le périmètre d'une mission d'audit de la gouvernance des SI et la mener à bien, l'équipe en charge de la mission devrait :

- Déterminer si la DSI est en phase avec les objectifs et les stratégies de l'organisation et les comprend.
- Mesurer l'efficacité de la gestion des performances et des ressources SI.
- Évaluer les risques susceptibles de nuire à l'environnement SI.

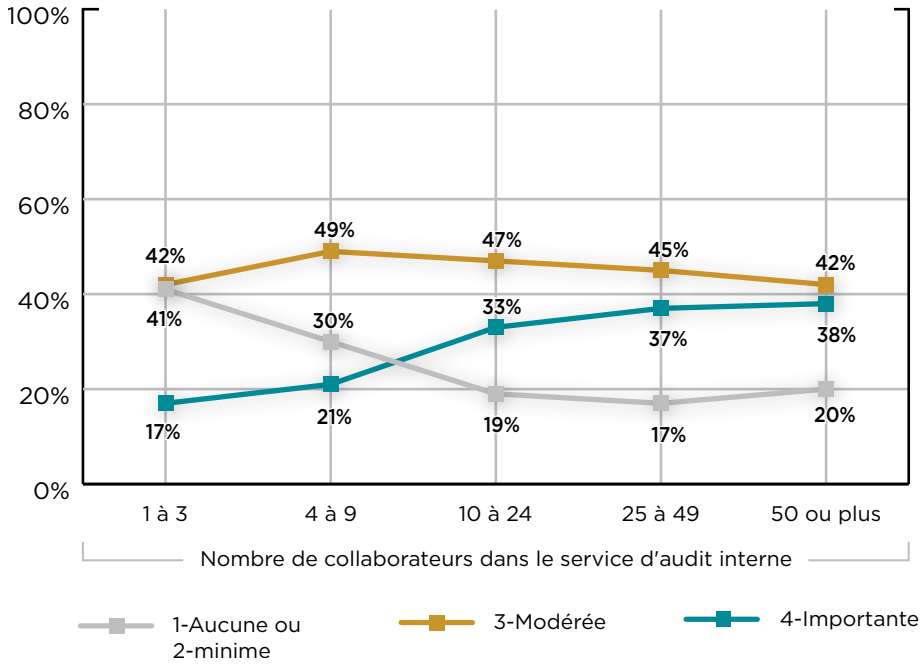
— Source : GTAG 17 : Auditing IT Governance (Altamonte Springs, Floride : The Institute of Internal Auditors, 2012), p. 15.

minime dans le domaine de la gouvernance des SI, ce qui est plutôt préoccupant (voir **figure 4**). Compte tenu des sommes dépensées pour les SI et de leurs impacts sur les clients et les opérations, presque tous les services d'audit interne devraient au moins exercer une activité modérée dans le domaine de la gouvernance des SI. Les plus nombreux à déclarer avoir une activité modérée ou importante dans ce domaine sont les répondants originaires d'Asie du Sud (huit sur dix).

Rôle de l'audit interne

L'audit interne peut aider l'organisation en lui donnant l'assurance que les SI sont performants et que des dispositifs de contrôle appropriés sont mis en place pour maîtriser les risques en fonction de la tolérance au risque de l'organisation. Un autre objectif opérationnel tout aussi important consiste à s'assurer que l'infrastructure des SI permet effectivement de saisir les opportunités qui feront progresser l'organisation. Il s'avère que les services d'audit interne de petite taille ont des difficultés à consacrer du temps à la revue de la gouvernance des SI. Dans les services de moins de trois collaborateurs, quatre répondants sur dix déclarent avoir une activité nulle ou minime dans le domaine de la gouvernance des SI (voir **figure 5**).

Figure 5 Niveau d'activité relatif à la gouvernance des SI selon la taille du service d'audit interne



Note : Q72 : Quelle est l'étendue des revues du gouvernement d'entreprise de votre département d'audit interne ? Thème : Revues des politiques et procédures de gouvernement d'entreprise relatives à l'utilisation des systèmes d'information. Responsables de l'audit interne uniquement. Les réponses « Sans objet/Je ne sais pas » n'ont pas été prises en compte. n = 2 497.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Quelles activités la DSI exerce-t-elle pour s'aligner sur les besoins de l'organisation ? À quelle fréquence la DSI rencontre-t-elle les opérationnels pour comprendre leurs besoins ?
2. Comment les métiers perçoivent-ils les capacités et les performances de la DSI ?
3. Comment la DSI mesure-t-elle sa valeur ajoutée pour les métiers ?
4. Comment les responsables de la DSI dimensionnent-ils l'effectif de leur service ?
5. La DSI évalue-t-elle régulièrement les risques SI ?
6. La DSI a-t-elle définit des indicateurs clés de performance ? Les suit-elle ?
7. Comment la DSI gère-t-elle ses coûts ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Évaluer l'exemplarité au plus haut niveau *(tone at the top)* de la DSI en ce qui concerne la culture de l'organisation, la satisfaction des besoins, l'atteinte des indicateurs de performance, la réalisation des contrats de services, le service client, etc.
2. Réaliser régulièrement une mission d'audit de la DSI afin de déterminer si elle est en phase avec les priorités stratégiques de l'organisation et les comprend.
3. Examiner l'efficacité de la gestion des performances et des ressources SI.
4. Évaluer les risques susceptibles de nuire à l'environnement SI.
5. Vérifier et analyser les indicateurs de coûts liés à l'environnement SI.
6. Réaliser une enquête auprès des métiers afin de savoir comment les responsables opérationnels perçoivent les capacités et les performances de la DSI.
7. Le cas échéant (au moins pour les grandes organisations), comparer le programme de conformité de l'organisation aux référentiels reconnus tels que le COBIT *(Control Objectives for Information and Related Technology)*, le COSO *(Committee of Sponsoring Organizations of the Treadway Commission)*, le NIST *(National Institute of Standards and Technology)*, et les normes ISO 27001 et 27002 de l'Organisation internationale de normalisation.

5 Prestations informatiques externalisées

"Externaliser mes prestations informatiques, c'est comme confier les clés de mon royaume en toute confiance au prestataire et attendre de lui qu'il traite les informations comme je le ferais."

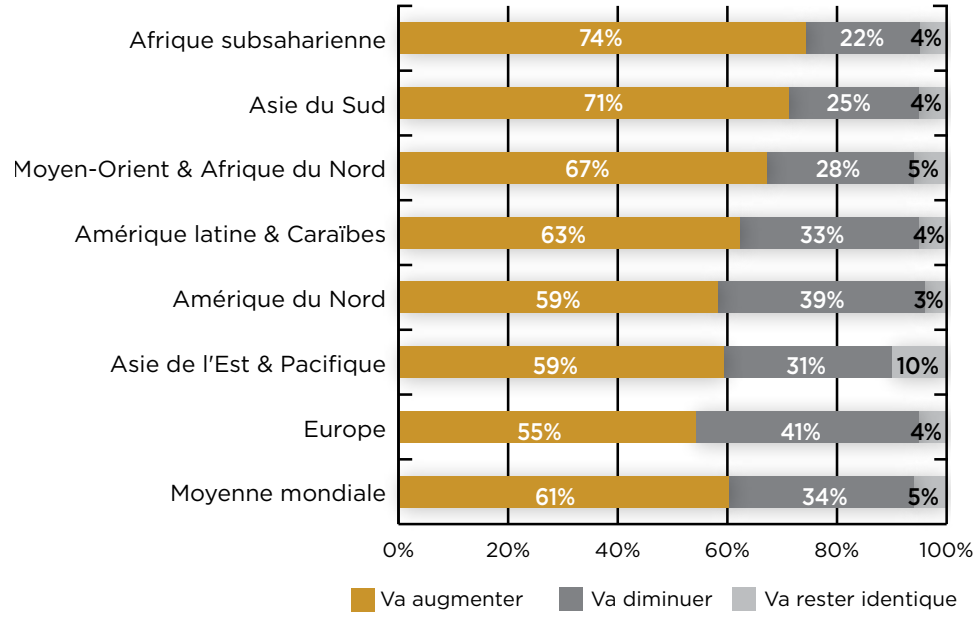
—Drew Perry, CISSP, CISA , Responsable de la conformité des SI, Ashland, Inc.

L'accent accru mis sur les coûts des SI a entraîné l'externalisation de certaines prestations informatiques clés. La gouvernance des SI est donc devenue une priorité encore plus importante, et les prestations informatiques externalisées se placent en 5e position de notre Top 10. L'externalisation peut exposer l'organisation à des risques susceptibles de rester inconnus jusqu'à ce qu'une défaillance survienne. Dans certains cas, des processus de SI essentiels peuvent échapper au contrôle direct du management. En moyenne, six auditeurs internes sur dix déclarent s'attendre à une hausse du nombre de mission d'audit des prestations informatiques externalisées au cours de l'année prochaine (voir **figure 6**). La plus forte augmentation est attendue en Afrique subsaharienne, et la plus faible en Europe.

Rôle de l'audit interne

Les auditeurs internes peuvent éviter l'apparition de certains problèmes liés à l'externalisation en s'impliquant le plus possible en amont. Par exemple, l'audit interne devrait s'assurer que le contrat initial couvre les aspects suivants : supervision, surveillance, audit, sécurité physique et logique, dotation en personnel approprié, interlocuteur clé, accès à l'information, plans de continuité d'activité / reprise après sinistre, contrats de niveau de service, et reporting.

Figure 6 Évolution du nombre de mission d'audit des prestations informatiques externalisées



Note : Q94 *: Au cours des deux ou trois prochaines années, estimez-vous que l'activité de l'audit interne dans les domaines suivants liés aux systèmes d'information va augmenter, diminuer ou rester stable ? Thème : Audit des achats informatiques, y compris pour des tiers ou des services externalisés. n = 11 020.*

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Les services externalisés sont-ils importants pour l'organisation ?
2. L'organisation dispose-t-elle d'une stratégie d'externalisation bien définie ?
3. Quelle structure de gouvernance régit les opérations externalisées ? Les rôles et responsabilités sont-ils clairement définis ?
4. A-t-on procédé à une analyse de risque détaillée au moment de la mise en place de l'externalisation, et régulièrement durant la durée du contrat ?
5. Existe-t-il des contrats formels ou des conventions de services pour les activités externalisées ?
6. Le contrat de services définit-il les indicateurs clés de performance qui permettent d'observer les performances du sous-traitant ?
7. Comment vérifie-t-on que les contrats ou les contrats de services sont bien respectés ?
8. Quels mécanismes utilise-t-on pour remédier au non-respect du contrat de services ?
9. Les responsabilités sont-elles clairement définies et ont-elles été convenues avec le prestataire de services concernant la propriété des données, du système de communication, du système d'exploitation, des logiciels utilitaires et des applications ?
10. Quel processus permet de s'assurer du fonctionnement efficace du dispositif de contrôle interne du côté du prestataire de services ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. S'impliquer dès les premières étapes du processus d'externalisation.
2. Effectuer des missions chez les sous-traitants et examiner leurs contrats de services et leurs indicateurs clés de performance.
3. En cas de non-conformité, contrôler les services fournis par des tiers et déterminer si les mesures appropriées ont été prises.
4. S'assurer que tous les codes sources fournis par le sous-traitant ont été analysés et ont fait l'objet d'une recherche de programmes malveillants.
5. Evaluer le processus de prise de décision appliqué pour déterminer quels domaines SI devraient être externalisés.
6. Sélectionner l'un des principaux sous-traitants et examiner l'évaluation des risques réalisée avant sa sélection.

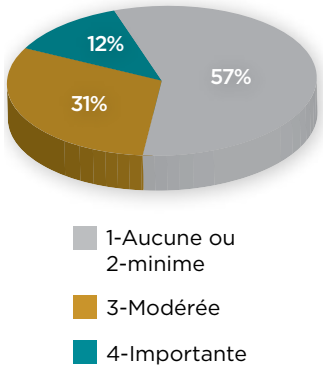
POUR EN SAVOIR PLUS

Auditing Outsourced Functions, 2e édition, par Mark Salamasick (Altamonte Springs, Floride : Fondation de la recherche de l'IIA, 2012).

GTAG 7 : *L'infogérance,* 2e édition (IIA / IFACI, 2012).

6 Utilisation des réseaux sociaux

Exhibit 7 Activité relative à l'utilisation des réseaux sociaux par les collaborateurs



Note : Q92 : Concernant la sécurité des systèmes d'information, quelle est l'étendue des activités de votre département d'audit interne dans les domaines suivants ? Les réponses « Sans objet/ Je ne sais pas » n'ont pas été prises en compte. n = 9 747.

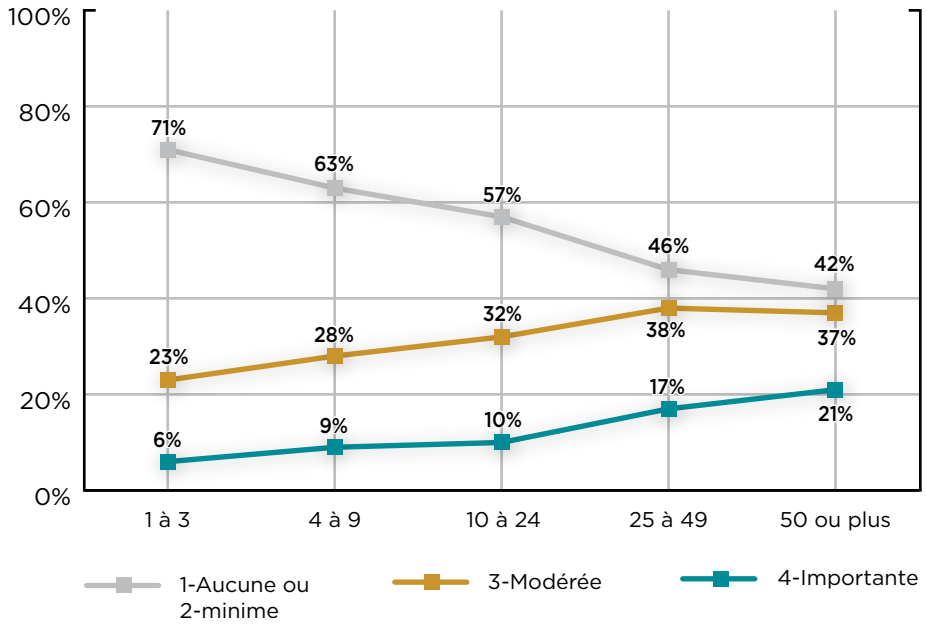
RESOURCES

Auditing Social Media: A Governance and Risk Guide, par Peter Scott et Mike Jacka (John Wiley & Sons, en partenariat avec l'IIA, 2011).

La rapidité de diffusion des communications via les réseaux sociaux a contraint les organisations à définir des règles et procédures en la matière. Cette thématique arrive donc en 6e position de notre Top 10. Les règles établies mettent essentiellement l'accent sur les différentes modalités d'utilisation des réseaux sociaux par les collaborateurs, et sur les restrictions auxquelles ces derniers sont soumis quant aux contenus qu'ils peuvent partager via ces outils. Si un collaborateur enfreint ces règles et publie un message compromettant, l'organisation peut être exposée aux risques suivants :

- Poursuites judiciaires pour diffamation, harcèlement, atteinte à la vie privée, etc. ;
- Fuites d'informations exclusives ou de secrets commerciaux, susceptibles d'avoir une incidence sur la compétitivité ;
- Atteintes à la réputation de l'organisation du fait de communications calomnieuses, désobligeantes ou imprudentes.

Figure 8 Activité relative aux réseaux sociaux selon la taille du service d'audit interne



Note : Q92 : Concernant la sécurité des systèmes d'information, quelle est l'étendue des activités de votre département d'audit interne dans les domaines suivants ? Thème : Procédures de votre organisation relatives à l'utilisation des médias sociaux par les collaborateurs. Les réponses « Sans objet/Je ne sais pas » n'ont pas été prises en compte. n = 8 980.

Comme l'illustre la **figure 7**, l'activité de l'audit interne concernant l'utilisation des réseaux sociaux par les collaborateurs est actuellement très faible. Près de six répondants sur dix font le constat d'une activité nulle ou minime, et seul un répondant sur dix déclare exercer une activité importante en la matière. Les services d'audit interne de plus grande taille sont davantage susceptibles d'être actifs dans ce domaine (voir **figure 8**). Parmi ces derniers néanmoins, quatre sur dix indiquent encore avoir une activité nulle ou minime.

Pour faire face aux risques liés aux réseaux sociaux, les organisations doivent intégrer les étapes suivantes dans leurs procédures :

1. Définir une politique d'utilisation des réseaux sociaux appropriée pour l'organisation ;
2. Diffuser cette politique dans le cadre d'un plan de sensibilisation et de formation sur les questions de sécurité ;
3. Mettre en œuvre cette politique grâce au déploiement d'un logiciel de filtrage des contenus dédié aux systèmes d'information, comme le Web 2.0 ;
4. Surveiller les résultats afin de s'assurer que cette politique est bien appliquée ;
5. Sanctionner les infractions à cette politique.

Rôle de l'audit interne

Les auditeurs internes peuvent jouer un rôle crucial dans la gestion des risques liés aux réseaux sociaux. Ils peuvent donner des conseils pendant la mise en œuvre des différentes étapes citées ci-dessus. Par ailleurs, l'audit interne devrait envisager d'inclure une mission d'audit de l'utilisation des réseaux sociaux dans son plan annuel.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Comment les réseaux sociaux sont-ils utilisés pour toucher les clients ?
2. Quel contenu est autorisé à être publié sur les réseaux sociaux ?
3. Existe-t-il un groupe ou une personne responsable de la surveillance des contenus publiés sur les réseaux sociaux (et qui les analyse systématiquement) ?
4. Quel contenu le logiciel de filtrage surveille-t-il ? Qui surveille les alertes lancées par le logiciel ?
5. Qu'encourt un collaborateur qui enfreint la politique relative aux réseaux sociaux ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Evaluer les règles et procédures applicables en matière de réseaux sociaux.
2. Examiner l'adéquation du plan de sensibilisation et de formation afin de s'assurer qu'il couvre le thème des réseaux sociaux.
3. Comprendre l'utilisation du logiciel de filtrage des contenus et son efficacité dans le contrôle des entrées et des sorties de contenus.
4. Réaliser une analyse indépendante des réseaux sociaux afin d'identifier les contenus concernant l'organisation.

7 Informatique mobile

« L'information se déplace avec l'utilisateur. Les données des appareils mobiles doivent donc faire l'objet de mesures de sécurité aussi robustes que celles des Sièges de ces organisations. Tablettes, ordinateurs personnels, téléphones portables, montres intelligentes, etc. Tous ces appareils constituent de petits centres de données dans lesquels la plupart des informations stratégiques de l'organisation sont stockées (ou qui contiennent suffisamment de renseignements pour faciliter les attaques sur les serveurs centraux). Le nombre d'équipements volés et/ou perdus ne fait qu'aggraver la situation. »

— Alejandro Rembado
Responsable de l'audit interne,
Telefónica de Argentina

La multiplication des appareils mobiles, ainsi que les améliorations apportées aux systèmes d'information, aux fonctionnalités et aux applications, ont bousculé les habitudes et donné un nouveau sens aux expressions « informatique mobile » et « travailleur mobile ». Il s'agit du 7e risque de notre Top 10. Auparavant, le travailleur mobile utilisait un ordinateur portable et se connectait à distance au réseau de l'organisation. Aujourd'hui, il peut bénéficier d'une plus grande puissance informatique en utilisant des appareils mobiles, comme un téléphone ou une tablette, qui contiennent des applications spécialement conçues pour ces activités.

Grâce aux appareils mobiles, les utilisateurs jouissent d'une puissance informatique portable et d'une connectivité Internet partout où il existe une connexion Wi-Fi ou cellulaire. Ils peuvent également disposer d'un appareil 2 en 1 : à usage personnel et professionnel. Parallèlement, les appareils mobiles, qu'ils appartiennent à l'organisation ou au collaborateur, ont entraîné l'apparition d'une multitude de risques liés aux différents dispositifs et configurations réseau. Cette situation remet en cause les approches de gestion des risques traditionnellement adoptées par les DSI.

Risques liés à la sécurité

Les informations stockées sur les appareils mobiles peuvent inclure des données personnelles ou propres à l'organisation. Celles-ci peuvent être compromises en cas de perte ou de vol de l'appareil, si l'utilisateur quitte l'organisation sans supprimer les données de son appareil, ou si des dispositifs de contrôle de sécurité appropriés ne sont pas mis en place et ne fonctionnent pas comme prévu.

Risques liés à la conformité

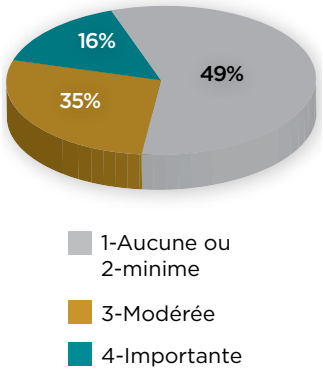
Avec l'introduction de la politique « Apportez vos outils personnels » (*Bring Your Own Device*, ou BYOD), les organisations comptent beaucoup sur les utilisateurs pour respecter les règles et procédures applicables, telles que les directives relatives à la mise à jour des logiciels et à l'exploitation des systèmes. Les utilisateurs qui estiment que les mises à jour sont trop fréquentes ou nuisent à la performance de leur appareil peuvent choisir de ne pas les installer ou de contourner les mesures de contrôle.

Risques liés à la protection de la vie privée

La politique BYOD peut soulever des préoccupations en matière de protection de la vie privée du point de vue de l'organisation et des collaborateurs. Par exemple, il peut devenir de plus en plus de difficile de protéger la vie privée des parties prenantes l'organisation dont les informations personnelles identifiables sont accessibles ou stockées sur un appareil intelligent. A contrario, les collaborateurs peuvent craindre une surveillance intrusive via leur appareil intelligent, ou la suppression accidentelle de leurs données personnelles (photos et contacts) en même temps que les données de l'organisation sont effacées.

> *En Afrique et dans certaines régions du Moyen-Orient, le risque est plus important qu'ailleurs en raison de l'utilisation intensive des téléphones portables pour accéder aux services de banque en ligne.*
>
> —Grace Lwanga, Directeur technique, Audit des SI, World Vision International

Figure 9 Activité concernant l'utilisation des appareils mobiles



Note: Q92*: Concernant la sécurité des systèmes d'information, quelle est l'étendue des activités de votre département d'audit interne dans les domaines suivants ?*

Risques liés à la gestion de la flotte d'appareils

Dans le cadre de la politique BYOD, il est nécessaire d'instaurer une gestion des services de support SI, en nombre croissant. Compte-tenu de la diversification accrue des appareils, les réseaux peuvent présenter de plus en plus de vulnérabilités. En outre, en cas de mise à niveau, l'obligation de se débarrasser de l'ancien appareil peut accroître les risques liés à la gestion. Lorsque la politique BYOD s'applique aux prestataires de services externes, la gestion des données de l'organisation stockées sur les appareils de ces derniers peut également aggraver ces risques.

Risques juridiques

Les conséquences juridiques liées au stockage des données de l'organisation sur des appareils intelligents doivent être pris en considération. Par exemple, quelles sont les obligations en matière de rétention de données dans l'éventualité d'un litige ou de l'utilisation d'une preuve numérique (e-discovery) ?

Rôle de l'audit interne

Comme le montre la **figure 9**, seuls 51 % des services d'audit interne affichent une activité modérée ou importante dans le domaine des appareils mobiles. Autrement dit, près de la moitié des organisations exercent une activité nulle ou minime en la matière.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Existe-t-il un processus permettant le recensement de tous les appareils mobiles ?
2. Comment le vol ou la perte d'appareils mobiles sont-ils gérés ?
3. Comment la politique BYOD est-elle gérée ?
4. Comment les contenus stockés sur les appareils mobiles d'un collaborateur qui s'en va sont-ils gérés ?
5. Les appareils mobiles sont-ils cryptés ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

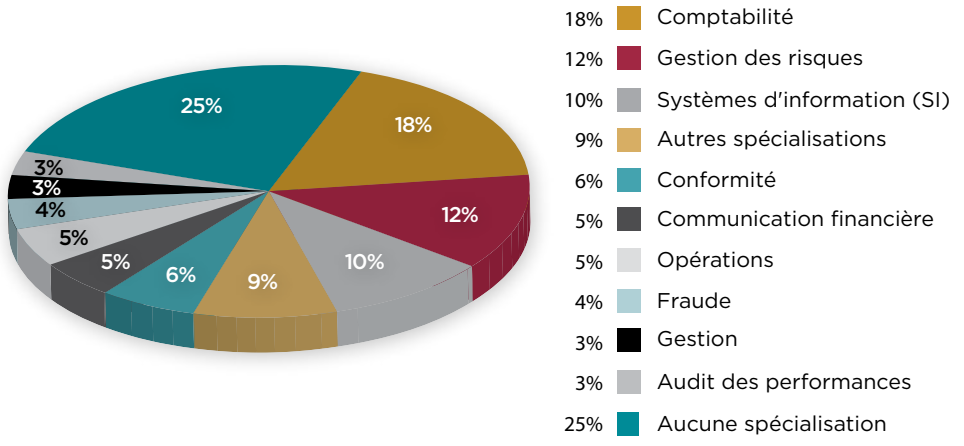
1. Réaliser une mission d'audit du processus d'inventaire des appareils mobiles.
2. Evaluer les modalités de gestion des appareils perdus ou volés.
3. Comprendre comment l'organisation décide si telle ou telle information peut être stockée sur des appareils mobiles.
4. S'assurer qu'aucune information sensible n'est stockée sur des appareils mobiles ou, si tel est le cas, vérifier que les informations sont cryptées.

8 Compétences des auditeurs internes en matière de SI

Le nombre réduit d'auditeurs SI compétents est un problème persistant pour l'audit interne. C'est le 8ème point de notre Top 10. Seuls 10 % des répondants se déclarent experts en SI (voir **figure 10**). D'après Mark Salamasick, directeur du département Audit de l'Université du Texas, plusieurs raisons justifient ce constat, la plus courante étant que les professionnels des SI ont la possibilité d'être exposés à des technologies plus novatrices et d'exiger une rémunération plus élevée que celle des auditeurs SI. « En règle générale, les auditeurs dotés d'une expérience et d'une expertise SI ne sont pas au même niveau de rémunération que les autres professionnels des SI. C'est pourquoi la plupart des organisations doivent composer avec des auditeurs SI moins qualifiés. »

Pour accroître le nombre d'auditeurs SI, l'une des méthodes consisterait à former les auditeurs financiers et opérationnels présentant une certaine affinité pour les SI. Ces professionnels formés en interne pourraient cependant avoir du mal à asseoir leur crédibilité auprès de la DSI et du management. Selon Sudarsan Jayaraman, directeur général du service de conseil en SI de Protiviti au Moyen-Orient : « Les auditeurs SI doivent se spécialiser davantage pour être en mesure de mener à bien les multiples activités et missions d'audit à hauts enjeux qui leur sont confiées. Sans des compétences de haut niveau et une expérience en tant que professionnels des SI, le management est souvent peu satisfait de leurs performances et des résultats de leurs missions ».

Figure 10 Spécialisations techniques des répondants



Note: Q11 : Outre les séminaires sur les fondamentaux de l'audit interne, avez-vous suivi des formations dans d'autres domaines auxquelles vous consacrez la majorité de votre temps ? n = 13 144.

Rôle de l'audit interne

L'audit interne peut prendre un certain nombre de mesures pour faire face au déficit de compétences SI auquel le service est confronté. Il s'agit, dans un premier temps, de dresser l'inventaire des lacunes de compétences au sein de l'équipe en :

1. prenant connaissance des différents types de technologies utilisées dans l'organisation ;
2. rapprochant les compétences SI de l'équipe des technologies utilisées dans l'organisation ;
3. identifiant les besoins de compétences nécessaires pour traiter les technologies non-encore couvertes par l'équipe d'audit interne.

Une fois les compétences manquantes identifiées, l'audit interne peut choisir entre plusieurs options.

Option 1 : Développer ces compétences en interne en y consacrant le budget approprié et en formant l'équipe.

Option 2 : Mettre en œuvre un processus de rotation d'experts SI en collaboration avec le directeur des systèmes d'information (DSI).

Option 3 : Faire appel à un prestataire de services tiers à des fins de sous-traitance ou de co-traitance.

PRINCIPALES ACTIVITES D'AUDIT INTERNE

Les initiatives suivantes peuvent favoriser le développement des relations entre l'audit interne et la DSI, et accroître la sensibilisation aux processus SI en général.

1. Établir des relations avec les collaborateurs SI clés et démontrer la valeur ajoutée que l'audit des SI apporte à l'organisation.
2. Participer aux réunions clés concernant les SI (par ex. comité de pilotage de projets SI, mises à jour concernant la sécurité des SI, nouveaux SI, etc.) afin de mieux comprendre les risques et les enjeux significatifs dans le domaine des SI.
3. Rencontrer régulièrement les principaux membres de la DSI, y compris le directeur des systèmes d'information et le responsable de la sécurité des systèmes d'information.
4. Engager des auditeurs possédant une expérience dans le domaine des SI afin d'accroître les compétences du service d'audit interne et de renforcer sa crédibilité auprès du management.
5. Réaliser des missions d'audit de la gouvernance des SI.
6. Travailler en collaboration avec d'autres services de gestion des risques, de gouvernance, de contrôle et de conformité, et partager des informations avec eux sur les principaux risques de l'organisation, afin de limiter les doublons et les interruptions dans le travail des collaborateurs SI, déjà surchargés.

Il convient enfin de communiquer au Conseil les progrès réalisés dans le cadre de ces six initiatives. Ainsi, le Conseil et le comité d'audit seront en mesure de mieux comprendre les SI, et l'audit interne rendre compte du renforcement de son efficacité dans ce domaine.

9 Technologies émergentes

Les SI évoluent et se transforment à une vitesse incroyable, ce qui peut rapidement générer de nouveaux risques pour l'organisation. Cette thématique vient en 9ème de notre Top 10. Les technologies émergentes peuvent avoir diverses conséquences selon les organisations. Pour certaines, l'utilisation d'appareils intelligents peut constituer une forme de technologie émergente, tandis que d'autres en font déjà un usage bien établi. Dans ce chapitre, les technologies émergentes sont définies comme celles qui ne sont pas encore utilisées au sein de l'organisation mais qui pourraient être déployées dans un futur proche. En voici quelques exemples :

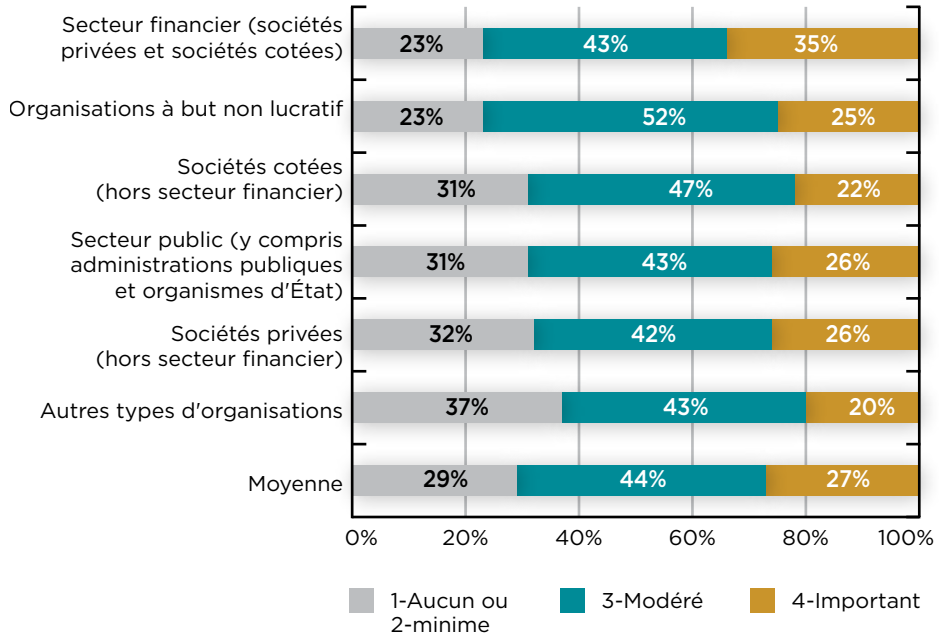
- Analyse prévisionnelle de données
- *Big Data*
- *Fog computing* (« informatique en nuage », extension du cloud computing à la périphérie du réseau de l'organisation)
- Impression 3D (imprimantes programmées pour façonner des objets en trois dimensions)
- Internet des objets (les objets de la vie courante, comme le réfrigérateur ou le micro-ondes, sont équipés de la connectivité réseau et peuvent envoyer et recevoir des données)
- Robotique

Il est également possible que certaines technologies soient déjà déployées dans un secteur (comme le *Big Data* dans le secteur financier) et pas encore dans d'autres. Toutes ces différences semblent également influer sur le niveau de risque perçu. Comme le montre la **figure 11**, c'est dans le secteur financier que le niveau de risque inhérent concernant la fiabilité du *Big Data* est perçu comme le plus élevé.

Rôle de l'audit interne

L'audit interne peut jouer un rôle crucial dans l'adoption de technologies émergentes. Il peut intervenir aux tous premiers stades du processus d'évaluation d'une nouvelle technologie et fournir des recommandations en termes de risques et d'activités de contrôle requises. Par exemple, si l'organisation envisage d'intégrer des services de *cloud computing* pour la première fois, l'audit interne peut rejoindre le groupe de travail dédié afin d'identifier les risques nouveaux que cela implique (ou, dans certains cas, les risques qui ont été réduits).

Figure 11 **Niveau de risque concernant la fiabilité du *Big Data* selon le type d'organisation**



Note : Q93 : À votre avis, quel est le niveau de risque inhérent de votre organisation pour les domaines émergents des systèmes d'information suivants ? Les réponses « Sans objet/Je ne sais pas » n'ont pas été prises en compte. Pour des raisons d'arrondi, le total peut parfois différer de 100 %. n = 9 373.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Existe-t-il une équipe chargée de l'évaluation des technologies émergentes ?
2. Existe-t-il un processus formel d'évaluation des technologies émergentes ?
3. Comment les risques associés aux technologies émergentes sont-ils identifiés ?
4. Quels sont les projets en cours qui incluent le déploiement de nouvelles technologies dans l'environnement de production ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Obtenir un inventaire des technologies actuellement utilisées.
2. Prendre connaissance des nouveaux projets qui incluent le déploiement de technologies émergentes.
3. Evaluer le processus de gestion des risques relatifs aux technologies émergentes (comment les risques sont-ils identifiés lors de l'évaluation des technologies émergentes ?).
4. Échanger avec l'équipe de la DSI pour comprendre leur stratégie pour l'adoption de technologies émergentes.

10 Sensibilisation du Conseil et du comité d'audit aux enjeux SI

"Les problèmes rencontrés résultent le plus souvent d'une mauvaise compréhension de l'organisation (de son fonctionnement et de tous les scénarios possibles auxquels elle peut être confrontée). Pour surmonter cette difficulté et donner aux collaborateurs la possibilité d'agir avant qu'il ne soit trop tard, il est essentiel de faire en sorte que chacun comprenne parfaitement la situation et les solutions envisageables."

—Brian Barnier, Principal, ValueBridge Advisors & Fellow, OCEG

Dans un grand nombre d'organisations, le Conseil possède une expertise limitée en matière de SI. C'est le 10e et dernier risque SI de notre liste. Le Conseil doit démontrer un niveau de connaissances approprié pour être en mesure de demander des précisions sur la performance des SI au DSI. Selon Gunther Meggeneder, Senior Vice President Audit interne et conformité chez ista International : « Dans les années à venir, le Conseil et le comité d'audit devront acquérir une plus grande expertise en matière de SI, tout comme ils s'étaient progressivement dotés de solides compétences financières. » Les SI constituent un atout majeur pour l'organisation et requièrent un fort investissement. Il est donc risqué pour le Conseil de ne pas disposer des connaissances nécessaires en la matière. D'après Scott Klososky, associé chez Future Point of View, LLC : « D'ici quatre ou cinq ans, chaque Conseil devrait intégrer un expert en SI, ou tout au moins un tel expert siègeant dans un de leurs comités consultatifs. »

Rôle de l'audit interne

L'audit interne joue un rôle crucial car il représente le principal vecteur de sensibilisation aux SI pour le Conseil et le comité d'audit. Il doit mesurer le niveau de connaissance du comité d'audit en matière de SI et jouer le rôle de formateur et/ou de conseiller.

QUESTIONS QUE L'AUDITEUR INTERNE DOIT IMPÉRATIVEMENT SE POSER

1. Quelle est la stratégie de l'organisation lorsque des changements sont prévus dans le domaine des SI ?
2. Le comité d'audit comprend-il les risques SI et peut-il faire le lien avec les risques de l'organisation ?
3. Le comité d'audit comprend-il son rôle et ses responsabilités quant aux mesures de sensibilisation aux enjeux et risques SI pour l'organisation ?

PRINCIPALES ACTIVITES D'AUDIT INTERNE

1. Obtenir un inventaire des technologies actuellement utilisées.
2. Prendre connaissance des nouveaux projets qui incluent le déploiement de technologies émergentes.

Conclusion

Les auditeurs internes s'attachent à nourrir une réflexion stratégique, à comprendre l'organisation, et à lui apporter une valeur ajoutée. Ils doivent désormais se montrer proactifs pour identifier les technologies émergentes susceptibles d'influer sur leur organisation. Les experts formulent les recommandations suivantes :

1. Établir un processus pour avoir une bonne connaissance du contexte.
2. Guetter les signaux d'alerte au sein du secteur ou de l'environnement de l'organisation.
3. Envisager tous les scénarios possibles auxquels l'organisation peut être confrontée.
4. Recenser les opportunités et les risques associés aux technologies émergentes et les examiner afin d'en déterminer l'impact potentiel.
5. Lorsqu'une opportunité ou un risque est identifié, prendre les mesures nécessaires pour le suivi des plans d'action.

Si l'avenir reste imprévisible, une chose est sûre : l'environnement des SI va évoluer, et les auditeurs internes devront être prêts à s'adapter.

Équipe du projet

Équipe de développement du CBOK

Co-présidents du CBOK :
Dick Anderson (États-Unis)
Jean Coroller (France)
Président du sous-comité chargé de l'enquête sur les pratiques de l'audit interne :
Michael Parkinson (Australie)
Vice-présidente de l'IIARF : Bonnie Ulmer
Analyste principal des données : Dr. Po-ju Chen
Développeur de contenu : Deborah Poulalion
Gestionnaires du projet : Selma Kuurstra and Kayla Manning
Rédactrice en chef : Lee Ann Campbell

Comité de revue du rapport

Ulrich Hahn (Allemagne)
Steve Hunt (États-Unis)
Richard Martin (États-Unis)
Michael Parkinson (Australie)
Kurt Reding (États-Unis)
Dave Williams (États-Unis)

Parrainage

Ce rapport a été réalisé sous le parrainage du chapitre de l'IIA d'Austin. Nous tenons à le remercier pour sa généreuse contribution.

À propos des auteurs

Note : Ce rapport est le fruit d'une collaboration entre Phil Flora, qui a établi la liste des dix principaux risques SI, réalisé des entretiens avec des experts du monde entier et rédigé le contenu initial, et Sajay Rai, qui a préparé le texte définitif et élaboré, pour chaque chapitre, les questions fondamentales à se poser et les principales activités de l'audit interne.

Philip E. Flora (CIA, CISA, CFE, CCSA) est directeur chez FloBiz & Associates, LLC, membre du groupe YCN, et conseiller en formation de l'IIA. Il a plus de 30 ans d'expérience en audit et a été responsable de l'audit interne au sein d'une organisation à but non lucratif pendant plus de 16 ans. Il a participé à l'élaboration d'un programme de développement du leadership en audit interne, qui a contribué à former plus de 50 futurs responsables. Phil est actuellement membre du Conseil d'administration de l'IIARF. Il a également présidé le Comité international de l'IIA et le *Committee of Research and Education Advisors* de l'IIARF. Depuis 2000, il siège à différents comités internationaux de l'IIA. Depuis ces dix dernières années, il intervient régulièrement lors de conférences et de séminaires de formation à l'échelle locale, régionale, nationale et internationale. Phil est diplômé en comptabilité de la Virginia Commonwealth University.

Sajay Rai (CPA, CISSP, CISM) est le co-fondateur et le propriétaire de la société Securely Yours, LLC. Avec plus de 30 ans d'expérience dans les SI, il dispose d'une grande connaissance dans les domaines suivants : sécurité de l'information et risques associés, audit des SI, continuité d'activité, reprise après sinistre, et protection de la vie privée. Avant de lancer sa société, Sajay était associé chez Ernst & Young LLP, en charge de l'activité Advisory dans le domaine des SI pour la ville de Détroit. Il était également responsable des activités Sécurité et Risque d'Ernst & Young à l'échelle nationale. Avant d'intégrer Ernst & Young, il travaillait chez IBM en tant que responsable des activités Sécurité de l'information et Continuité d'activité. Sajay est membre du *Professional Issues Committee* de l'IIA et membre du Conseil du chapitre de l'IIA de Détroit. Il est titulaire d'un master en gestion des systèmes d'information de l'Université Washington de Saint-Louis. Il est également diplomé en informatique de l'Université Fontbonne de Saint-Louis.

Vos dons ont un impact

Les rapports du CBOK sont disponibles gratuitement en libre accès grâce à la généreuse contribution d'individus et d'organisations, mais également de chapitres et d'instituts de l'IIA du monde entier.

Faire un don

www.theiia.org/goto/CBOK

À propos de la Fondation de la recherche de l'IIA

Le CBOK est géré par la Fondation de la recherche de l'IIA (IIARF), qui réalise depuis 40 ans des études novatrices sur la profession d'audit interne À travers différents projets d'exploration des problématiques actuelles, des nouvelles tendances et des besoins futurs, l'IIARF n'a cessé de jouer un rôle moteur pour l'évolution et le développement de la profession.

Limite de responsabilité

L'IIARF publie ce document à titre informatif et pédagogique uniquement. La Fondation ne fournit aucun service juridique ou de conseil, et ne garantit, par la publication de ce document, aucun résultat juridique ou comptable. En cas de problèmes juridiques ou comptables, il convient de recourir à l'assistance de professionnels.

Contacts

The Institute of Internal Auditors (siège mondial)
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201, États-Unis

Copyright © 2015 par la Fondation de la recherche de l'*Institute of Internal Auditors (Institute of Internal Auditors Research Foundation, IIARF).* Tous droits réservés. Pour toute autorisation de reproduction ou de citation, prière de contacter l'Institute of Internal Auditors (research@theiia.org) ou l'IFACI (recherche@ifaci.com). ID # 2015-1402