GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Management de l'audit des systèmes d'information

2ème édition

The Institute of Internal Auditors

Janvier 2013

Copyright © 2013 par l'Institute of Internal Auditors, 247 Maitland Ave., Altamonte Springs, Floride, 32701-4201, États-Unis. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de consultation ou transmise sous quelque forme que ce soit, ni par aucun moyen (électronique, mécanique, reprographie, enregistrement ou autre) sans autorisation écrite préalable de l'éditeur.

L'IIA publie ce document à titre informatif et pédagogique. Cette publication entend donner des informations, mais ne se substitue en aucun cas à un conseil juridique ou comptable. L'IIA ne fournit pas ce type de service 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.

Contenu

Résumé 4

1. Introduction 5

2. Stratégie « métier », processus et projets 7

3. Infrastructure et processus SI 8

4. Approche fondée sur les risques 12

5. Univers d'audit 13

6. Savoir-faire et compétences 14

7. Réaliser des missions d'audit des SI 15

8. Rapports 17

9. Outils d'audit 18

10. Conclusion 20

Annexe A : Normes de référence 21

Annexe B : Modèles d'architecture des SI 22

Auteurs et relecteurs 23

Résumé

Les systèmes d'information (SI) ont une influence omniprésente sur l'audit interne. L'émergence de nouveaux risques implique de repenser les procédures pour gérer ces risques de façon adéquate. Le processus d'audit des SI n'est globalement pas différent de celui d'autres travaux d'audit : l'auditeur planifie la mission, identifie et documente les contrôles pertinents, vérifie l'efficacité de la conception et du fonctionnement de ces contrôles, en tire les conclusions et rédige son rapport. Les responsables de l'audit interne (RAI) rendent régulièrement compte des conclusions des missions d'audit des SI aux principales parties prenantes telles que le Conseil, la direction générale, le directeur des systèmes d'information, les régulateurs et les auditeurs externes. Ce guide a pour objectif d'aider les RAI à planifier et à gérer les travaux d'audit avec une efficacité et une efficience accrues en analysant comment :

- **Déterminer les domaines nécessitant des ressources en audit des SI.** Quelles sont les missions qui nécessiteront l'intervention de spécialistes en audit des SI ? A la lumière des lignes directrices exposées dans ce document, le RAI devrait être à même de planifier le recours à des auditeurs des SI pour une couverture adéquate de périmètre à auditer. Les ressources en audit des SI sont généralement rares, alors que la demande est forte. Définir les besoins en audit des SI permet au RAI d'assurer la réalisation des missions planifiées dans ce domaine. Quelle que soit la taille des équipes d'audit interne, il reste primordial de disposer des compétences adéquates pour les travaux d'audit spécifiques. Celles-ci peuvent exister en interne ou être recherchées en externe, selon les capacités de l'organisation.

- **Évaluer les risques liés aux SI.** Les risques liés aux SI évoluent continuellement de concert avec la technologie. Certains sont liés à la technologie elle-même et d'autres à la manière dont elle est utilisée. Ce guide aide le RAI à comprendre comment identifier et évaluer au mieux les risques relatifs aux SI. Ainsi, les ressources de l'audit des SI pourront se recentrer sur les domaines qui présentent le plus de valeur ajoutée pour l'organisation.

- **Réaliser des travaux d'audit des SI.** Du fait de la prolifération et de la complexité des SI, il devient indispensable de disposer de procédures d'audit des SI appropriées, qui peuvent être intégrées aux audits de routine des opérations et des processus afin de gérer les risques spécifiques identifiés durant la phase de planification. L'audit effectué d'après des listes de vérification ou sur la base d'une enquête est insuffisant.

En outre, le guide donne au RAI des indications sur l'éventail de compétences que les auditeurs des SI devraient posséder pour apporter des connaissances et une expertise suffisantes à la fonction d'audit, ainsi que des outils pour aider l'auditeur à effectuer les tests liés aux SI et pour répondre à des attentes spécifiques concernant les rapports. Ce guide a pour objectif de donner des informations pragmatiques et claires, ainsi que des recommandations spécifiques qu'un RAI peut mettre en œuvre immédiatement. Ce guide veille à fournir des critères qu'un RAI peut utiliser pour évaluer la maturité des capacités en audit des SI et s'assurer que les travaux de l'équipe d'audit interne correspondent à un haut niveau d'exigence.

1. Introduction

Les risques auxquels est confrontée l'organisation, les types d'audits à effectuer, les modalités de priorisation dans l'univers d'audit et la manière de formuler des constats pertinents sont autant de préoccupations des RAI. Ce guide pratique d'audit des technologies de l'information (GTAG) est destiné aux RAI et aux personnes chargées de la supervision des missions d'audit des SI et des tests des SI intégrés dans d'autres missions.

Il a pour vocation de les aider à répondre aux questions stratégiques concernant la planification, l'exécution et les rapports sur les travaux d'audit des SI. Il étudie les aspects fondamentaux ainsi que les nouveaux enjeux. Une évaluation annuelle des risques réalisée dans le cadre de l'élaboration du plan d'audit qui ne couvre pas les risques informatiques serait considérée comme déficiente (voir les Normes 1210.A3, 1220.A2 et 2110.A2). L'audit interne devrait tenir compte de trois aspects :

- Un taux important de dispositifs de contrôle interne clé pour l'organisation sont susceptibles de reposer sur un système informatisé. Par exemple : la politique d'une organisation précise qu'avant de régler la facture d'un fournisseur, il convient de procéder à une triple vérification de cohérence *(three way watch)*, entre un bon de commande, un bon de livraison et une facture. Dans le passé, un employé rapprochait physiquement les documents, les agrafait et les classait. Aujourd'hui, le progiciel de gestion intégré (ERP) procède automatiquement à ces rapprochements sur la base de règles préconfigurées, et de niveaux de tolérance. Les écarts sont automatiquement enregistrés dans des comptes prévus à cet effet. Pour auditer efficacement ce contrôle, l'auditeur peut avoir besoin d'accéder aux paramètres de configuration des systèmes ERP, ce qui fait appel à des compétences techniques que ne possèdent pas tous les auditeurs.

- Les organisations doivent comprendre les risques stratégiques induits par les environnements complexes des SI. L'adoption des SI comme facilitateur pour les métiers modifiera les risques stratégiques d'une organisation. Celle-ci doit comprendre ce changement et prendre les mesures appropriées pour gérer ces risques.

- Le développement des contrôles généraux des SI et des contrôles applicatifs devrait gérer convenablement les risques relatifs aux SI. Les contrôles des SI doivent protéger efficacement les activités d'une organisation et garantir que sa compétitivité n'est pas affectée ; les systèmes défectueux risquent de nuire fortement à la réputation. Par exemple : considérons le processus automatisé décrit ci-dessus, dans lequel le bon de commande arriverait via un site Internet et serait transmis directement à l'entrepôt par le progiciel ERP. Si un client commande par erreur 100 palettes au lieu de 100 unités et que l'organisation a entièrement intégré ses processus dans l'ERP ; il est possible que le système vérifie le stock, constate qu'il n'y a pas 100 palettes disponibles, révise le plan de production afin de produire 100 palettes et envoie automatiquement des bons de commande pour des matières premières via l'échange de données informatisées *(Electronic Data Interchange, EDI)*. Sans les contrôles préventifs ad hoc, cette erreur risquerait de ne pas être détectée avant la réception des biens par le client.

Une des difficultés les plus fréquentes est de comprendre les liens entre contrôles des SI, *reporting* financier, fraudes, activités, conformité et autres domaines clés. C'est relativement facile lorsque vous évaluez des contrôles dans le cadre d'un système applicatif (par exemple, les paramètres de la triple vérification de cohérence évoquée ci-dessus). Ça l'est nettement moins lorsque vous évaluez des technologies connexes qui peuvent avoir un impact bien plus important sur l'organisation que les contrôles propres à une seule application ou un seul processus.

Supposons par exemple qu'une organisation émette des paiements électroniques qu'elle envoie à ses fournisseurs. Ces paiements sont acheminés

par voie électronique vers des comptes bancaires sur la base des numéros de routage SWIFT *(Society for Worldwide Interbank Financial Telecommunication)* pour chaque compte fournisseur. Tous les numéros de l'*Automated Clearing House* (ACH) sont stockés quelque part dans une table du système de base de données de l'organisation. Un administrateur de base de données, quiconque ayant un droit d'accès à la base de données, ou des individus sans droit d'accès mais possédant les compétences techniques leur permettant d'accéder à la base de données peuvent modifier chaque entrée de cette table pour y faire figurer le numéro ACH de leur propre compte bancaire. Dès qu'un paiement électronique est traité, les fonds sont crédités sur le compte bancaire du contrevenant. Une telle manipulation contournerait tous les mécanismes de sécurité, de contrôle et de piste d'audit en place au sein du processus et de l'application.

Dans le scénario ci-dessus, il est facile de comprendre comment la défaillance d'un contrôle au niveau de la base de données peut produire davantage de dégâts qu'une défaillance au niveau des paramètres de la triple vérification de cohérence. La probabilité et l'impact potentiel des risques inhérents à l'environnement des SI devraient donc être soigneusement pris en compte dans le cadre de l'évaluation annuelle des risques.

2. Stratégie « métier », processus et projets

La stratégie « métier », facteur déterminant pour identifier l'univers d'audit, est à prendre en compte impérativement lors de l'évaluation des risques. La stratégie « métier » articule les objectifs de l'organisation et les moyens à mettre en œuvre pour les atteindre. Il est important que le RAI et le management de l'audit interne comprennent cette stratégie et le rôle de la technologie dans l'organisation, ainsi que les interactions entre les deux. L'un des outils pouvant être utilisé par le RAI pour évaluer la stratégie « métier » d'une organisation et son influence sur les travaux d'audit des SI est le *GTAG 11 : Élaboration d'un plan d'audit des SI.* Ce guide donne aux RAI des informations sur la compréhension de l'environnement des SI de l'organisation dans un contexte opérationnel.

Les composantes des SI figurant à la section 3 facilitent l'explication des relations entre les activités opérationnelles et l'infrastructure des SI, et l'identification du volet informatique d'autres domaines identifiés dans l'univers d'audit lors de l'évaluation des risques.

Une cartographie étendue peut permettre d'identifier les domaines critiques tels que l'infrastructure, les applications, les processus et les liens (tant internes qu'externes) pouvant être soumis à des risques qui n'avaient pas encore été identifiés. Ce processus de cartographie aidera le RAI à évaluer les risques relatifs aux SI et les seuils de tolérance au sein de l'organisation, et donne une perspective pertinente sur les risques non identifiés, qui devrait être communiquée à la direction générale et au management des SI.

Généralement, les ressources spécialisées de l'audit interne peuvent être sollicitées pour donner une assurance quant à la réalisation d'étapes de projets informatiques. Le RAI devrait évaluer le niveau de compétences et de connaissances requis pour réaliser ces travaux et affecter les ressources appropriées. Dans certains cas, une expertise externe est nécessaire. Pour plus de détails, se référer au *GTAG 12 : Audit des projets SI.*

3. Infrastructure et processus SI

1. Définition des SI

L'une des difficultés auxquelles un RAI est confronté lorsqu'il détermine l'implication des ressources d'audit informatiques est d'appréhender les usages du SI dans l'organisation. Le téléphone et les messageries vocales en font-ils partie ? Les systèmes d'accès et d'identification, ainsi que les systèmes de sécurité physique devraient-ils être inclus ? Et que faire si ces derniers sont externalisés ? Voici quelques-unes des questions auxquelles il faut répondre lorsqu'il s'agit de déterminer comment allouer ses ressources d'audit des SI.

Les SI sont spécifiques à chaque organisation. Deux organisations opérant dans le même secteur peuvent avoir des environnements de SI très différents. Même au sein d'une même organisation, les contrôles peuvent être centralisés, décentralisés ou les deux à la fois. Les ordinateurs portables, les réseaux sociaux et le cloud repoussent les frontières d'un contrôle centralisé et introduisent des risques et des facteurs spécifiques.

Cette section aidera les RAI à envisager les SI au sein d'une organisation. Certaines composantes sont intégrées à des procédures et des processus manuels et certaines peuvent être envisagées isolément. Il existe des risques informatiques dans chaque domaine de l'organisation, et ils varient considérablement. Pirater le site Internet d'une organisation et détourner un paiement électronique sont, par exemple, des risques très différents pour l'organisation.

2. Tenir compte de chaque niveau du SI

Pour un audit des SI efficace, il est nécessaire d'étudier et de classer par ordre de priorité les risques inhérents à chaque niveau du SI et d'y allouer les ressources d'audit en fonction de ces risques. Si le volet SI du plan d'audit ne prévoit pas une évaluation de chacun des niveaux, il est probable que le plan d'audit dans son ensemble ne traite pas correctement les risques liés aux SI.

Dans certains cas, il peut se révéler utile de traiter tous les niveaux sur plusieurs années, en faisant un focus particulier chaque année, au lieu de couvrir tous les niveaux sur une seule année. Les plans par roulement allant au-delà de trois ans peuvent être inadéquats en raison de la rapidité des changements qui s'opèrent dans l'environnement des SI.

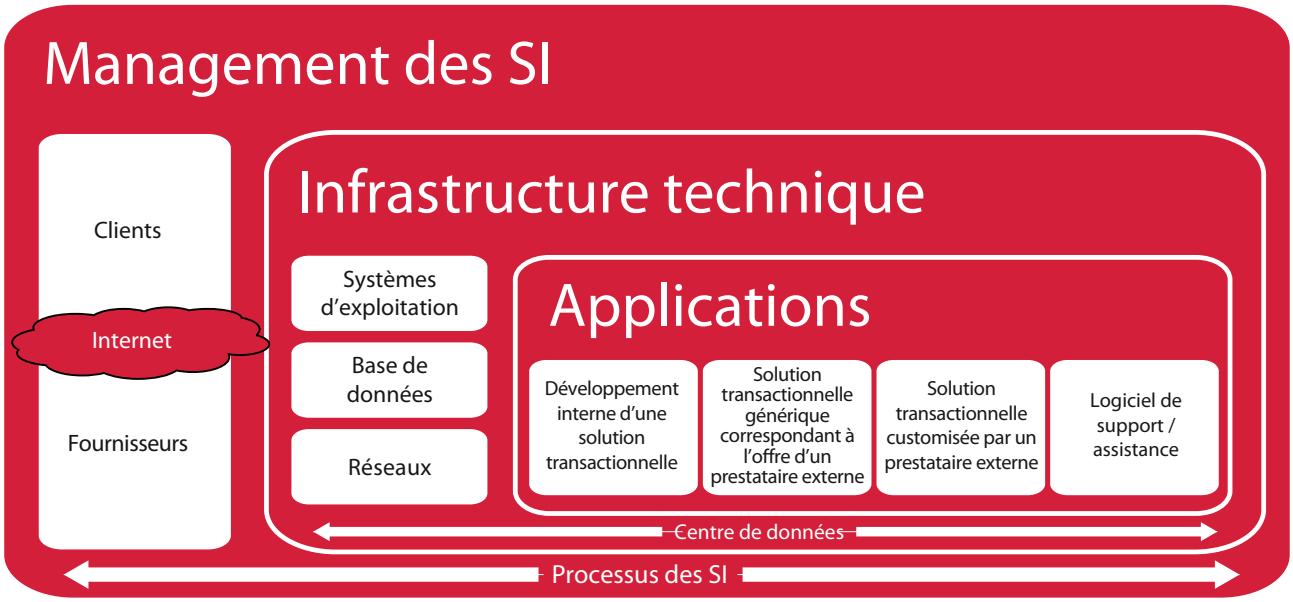

Figure 1

Quelles ressources allouer à chaque niveau? A quelles fins ? La réponse à ces questions délicates devrait naturellement découler des processus d'évaluation des risques, du jugement professionnel et d'une analyse stratégique. Au-delà de l'allocation précise des ressources, il s'agit de s'assurer que tous les niveaux du SI sont pris en compte.

3. Quels sont les niveaux à considérer ?

Le SI d'une organisation peut-être illustré selon la figure 1.

Chaque organisation est différente, mais cette représentation aidera à identifier les processus clés des SI dans la plupart des organisations. D'autres modèles d'architecture des SI peuvent être envisagés et sont référencés à l'Annexe A.

Les Technologies de l'information et de la communication (TIC) peuvent être appréhendées à travers les principaux niveaux suivants :

- le management des systèmes d'information,
- l'infrastructure technique,
- les applications,
- les connexions externes.

(Cf. figure 2)

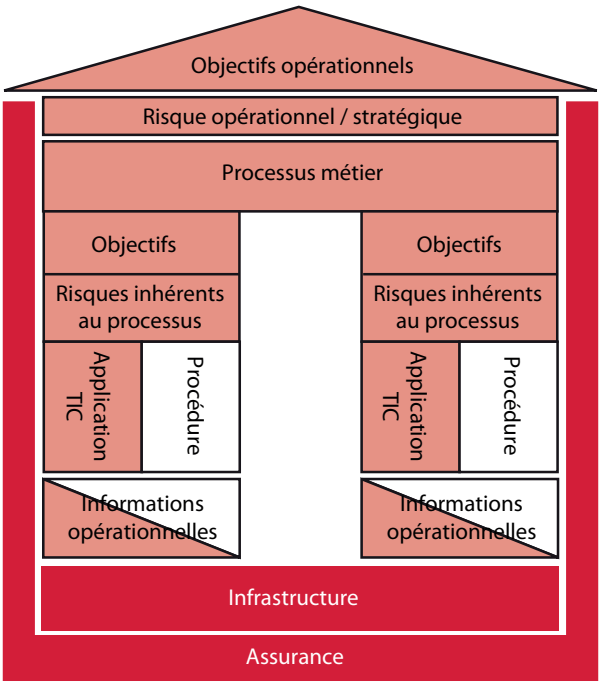

Figure 2

Attention : ce graphique ne définit pas des catégories du plan d'audit des SI. La planification des missions d'audit des SI peut être organisée en fonction des processus de l'organisation, ou conformément à un cadre standard. Ce graphique a pour objectif d'aider à expliciter les liens entre les SI et l'organisation et à s'assurer que des ressources d'audit sont allouées à chaque niveau. L'organisation d'audits spécifiques est laissée à l'appréciation du responsable de l'audit interne.

4. Management des systèmes d'information

Le management des SI concerne les personnes, les règles, les procédures et les processus qui gèrent les services et les installations des SI. L'intégrité du traitement et des données repose sur les tâches spécifiques régulièrement réalisées par le personnel administratif. En conséquence, cette composante englobe la surveillance, la programmation, la planification, la gestion des fournisseurs, la gestion des problèmes et des incidents, la gestion des changements, la gestion des projets informatiques, le plan de continuité d'activité, la gestion de la sécurité, la gouvernance des SI, etc.

Ces fonctions relèvent de processus métier. L'approche d'audit sera donc similaire à une mission classique. L'auditeur considèrera les acteurs et leurs tâches, plutôt que la configuration d'un système technique. Néanmoins, dans certains cas, la gestion des processus porte sur les installations techniques que l'audit devra prendre en considération. De même, certains contrôles peuvent nécessiter des compétences spécialisées. En principe, les compétences d'un auditeur interne expérimenté seront suffisantes.

5. Infrastructure technique

L'infrastructure technique sous-tend, soutient les principales applications métier et facilite leur mise en œuvre. En règle générale, ce niveau comprend :

- **Les systèmes d'exploitation –** L'ensemble des programmes qui assurent le fonctionnement des ordinateurs. Citons par exemple Z/OS, UNIX, Windows, et OS/400. Tous les programmes et les fichiers sont gérés par le système d'exploitation. Les actions engagées au niveau du système d'exploitation parviennent en général à contourner la plupart des dispositifs de sécurité et des contrôles existant au niveau du processus.
- **Les fichiers et les bases de données –** Toutes les données électroniques de l'organisation, critiques ou autres, sont contenues dans des fichiers qui peuvent faire partie d'une base de données. Les bases de données (qui peuvent être un seul fichier ou un groupe de fichiers) comprennent des tables contenant des données, des relations entre des données élémentaires et des index de données élémentaires. La flexibilité des structures d'une base de données explique qu'elles soient utilisées pour la plupart des traitements opérationnels et des applications de remontée d'informations. Ces bases sont par exemple Oracle, MS SQL Server et DB2. Les actions engagées au niveau des bases de données tendent également à contourner la plupart des contrôles qui existent au niveau du processus.
- **Réseaux –** Pour que les données circulent dans une organisation, il faut qu'elles disposent d'un vecteur, qui peut être un câble, une fibre optique ou un système sans fil. Le réseau se compose d'éléments physiques tels que des câbles, des appareils qui gèrent le trafic sur le réseau, comme les commutateurs, les routeurs ou les pare-feux, et des programmes qui commandent la circulation des données. L'intégrité du réseau joue un rôle important dans l'exhaustivité et l'exactitude des données d'une organisation. Par exemple, lorsque l'agent d'un entrepôt prépare l'expédition d'un produit en scannant un code-barres, la transaction est enregistrée dans le Grand Livre en passant par le réseau où elle est traitée. Mais que se produit-il si elle ne passe pas par le réseau ? Que se passe-t-il si elle est modifiée en cours de route, ou disparaît complètement ? Comment l'organisation le saurait-elle ?
- **Centres de données –** L'équipement informatique est situé dans des centres de données et des salles des serveurs, qui constituent l'infrastructure physique et assurent, la sécurité physique et environnementale permettant de protéger l'infrastructure technique et les applications.

Les audits de l'infrastructure technique sont axés sur la revue des paramètres de configuration technique en association avec les processus de gestion y afférents.

6. Applications

Les applications métier sont des programmes qui exécutent des tâches spécifiques liées aux activités de l'organisation. Elles font partie intégrante du processus métier et ne peuvent être considérées séparément des processus qu'elles soutiennent. Les applications appartiennent généralement à deux catégories :

- Les solutions transactionnelles sont principalement des logiciels qui traitent et enregistrent les transactions, par exemple des logiciels de traitement des bons de commande, de saisie dans le Grand Livre et de gestion des entrepôts.
- Les logiciels support sont des logiciels spécialisés qui facilitent les activités métier mais ne traitent généralement pas les transactions. Ils servent par exemple au stockage des données, à la messagerie électronique, à la télécopie, à la veille stratégique *(business intelligence)*, à la gestion électronique des documents (GED) et à la conception.

Alors que les solutions transactionnelles constituent généralement l'essentiel de l'effort d'audit, certains logiciels support tels que ceux qui viennent en appui du reporting externe ou les appli-

cations qui contrôlent des machines peuvent également être soumis à des risques importants.

L'audit interne doit évaluer continuellement les risques émergents pour l'organisation et identifier la réponse d'audit requise. Les connaissances spécialisées requises pour certains aspects des SI peuvent rendre ce processus complexe.

7. Connexions externes

Le réseau de l'organisation ne fonctionne pas isolément. Il est quasiment toujours connecté à de nombreux autres réseaux externes. Internet est celui qui vient le premier à l'esprit, mais trop souvent, les auditeurs commettent l'erreur de ne pas aller au-delà.

En réalité, il est fort probable que le réseau de l'entreprise soit connecté à de nombreux autres réseaux (dont le *cloud* et les logiciels des prestataires de services). Par exemple : l'organisation opère-t-elle via un échange de données informatisées (EDI) ? Si tel est le cas, son réseau est certainement connecté à celui d'un prestataire d'EDI, ou peut-être directement au réseau d'un partenaire commercial. L'organisation externalise-t-elle sa fonction de stockage ? Si oui, les deux réseaux sont aussi probablement reliés. Les risques associés aux réseaux d'autres organisations et les contrôles y afférents sont différents de ceux applicables aux connexions Internet.

Dans la mesure où les organisations continuent d'automatiser leurs processus clés, les tiers ont de plus en plus accès à leur réseau, souvent via Internet. Prenons par exemple la possibilité de vérifier le solde d'un compte bancaire ou l'état d'avancement d'une expédition. Les clients qui utilisent ces fonctions entrent probablement dans le réseau interne de ces entreprises via Internet.

Du fait que l'organisation ne maîtrise pas les réseaux extérieurs, les communications provenant (ou transmises vers) des réseaux externes devraient être rigoureusement contrôlées et surveillées en fonction du risque qu'elles représentent pour l'organisation. Il peut être difficile de définir des procédures d'audit des SI pour gérer ce risque car l'organisation ne peut auditer que ce qu'elle contrôle. Il est donc primordial d'auditer au minimum les points d'entrée et de sortie.

4. Approche fondée sur les risques

Toutes les dimensions de la gestion d'un service d'audit interne reposent sur une approche fondée sur les risques, notamment l'élaboration et le maintien des programmes d'audit, la gestion des ressources humaines et la conduite des missions. Cette section se concentre sur la partie de l'évaluation des risques inhérents aux SI.

L'évaluation des risques relatifs aux SI réalisée par l'audit interne permet d'identifier des missions d'audit spécifiques à plus forte valeur ajoutée potentielle pour la période considérée. Les risques relatifs aux SI ne nécessitent pas de méthodologie distincte. Il est important d'utiliser la même méthodologie pour tous les types de risques afin de veiller à l'homogénéité du processus d'évaluation pour l'ensemble de la fonction d'audit interne.

Les risques sont généralement exprimés en termes de combinaison d'impact et de probabilité d'occurrence d'un évènement. Il est souvent difficile d'évaluer exactement les risques, notamment pour les séries d'événements peu probables. Les journaux d'erreurs et les statistiques donnent des éléments utiles pour ces évaluations. Dans certains cas, l'examen des impacts est suffisant (par exemple la perte d'un centre de données) – et il n'est pas nécessaire de connaître le cheminement des événements qui en seraient à l'origine, ni la probabilité d'occurrence – pour savoir qu'il faut être attentif au risque.

Il est souvent possible de définir des critères qui s'appliquent à tous les types de risques liés aux SI, mais se manifestent différemment. Par exemple, l'exposition potentielle peut être appréhendée par des indicateurs d'envergure ou de criticité opérationnelle. Par exemple, le nombre d'applications sous-tendues par un centre de données pourrait être indicatif de son niveau de criticité (éventuellement pondéré en fonction de son importance), et le nombre de serveurs qu'il héberge peut éventuellement caractériser sa taille. La taille d'un projet, en revanche, se mesure à son budget, et sa criticité opérationnelle au nombre d'entités fonctionnant à l'aide de l'application. Le nombre d'incidents recensés ou les projets menés à bien par l'organisation peuvent mesurer la probabilité d'occurrence.

Outre la collecte de données, la conduite d'entretiens avec les principales parties prenantes telles que le management des SI, le management opérationnel et les experts constitue également une source importante pour l'évaluation des risques relatifs aux SI. Les interviews peuvent aider à quantifier les risques difficiles à mesurer directement.

Il est primordial de tenir compte de l'évolution rapide de la technologie et de son utilisation par l'organisation. Aussi l'évaluation des risques doit-elle être fréquemment mise à jour. Ceci est parfaitement illustré par l'importance croissante des problématiques de protection de la vie privée découlant de l'existence et de l'utilisation des réseaux sociaux. Pour une description plus détaillée de cette problématique, vous pouvez consulter le Guide pratique de l'IIA, *L'audit des risques d'atteinte à la vie privée.*

Enfin, pour une description plus détaillée de l'évaluation des risques relatifs aux SI, vous pouvez consulter le *GTAG 11 : Élaboration d'un plan d'audit des SI.*

5. Univers d'audit

Pour constituer les bases de l'allocation et de la prévision des ressources en audit des SI et pour assurer la couverture nécessaire à la fourniture d'une assurance raisonnable concernant les risques relatifs aux SI, les domaines impliquant des SI et nécessitant des compétences spécialisées en audit des SI devraient être identifiés dans l'univers d'audit.

Il ne devrait pas y avoir d'univers d'audit des SI distinct. Les travaux d'audit des SI devraient être intégrés à l'univers d'audit global car les SI et les processus métier qu'ils sous-tendent sont fortement interdépendants. Par exemple, les applications informatiques métier feront généralement partie de l'univers d'audit global à l'intérieur d'un processus métier. La structuration de l'univers d'audit devrait permettre un regroupement par type d'audit et donc une identification des missions nécessitant des compétences spécialisées (par exemple, l'audit des applications et des processus des SI).

Pour les processus de regroupement/structuration, on s'appuie généralement sur la structure utilisée par le management des SI, qui figure habituellement dans la stratégie des SI. Idéalement, cette structure est basée sur des référentiels tels que COBIT, ITIL, COSO (pour de plus amples détails, voir la section 7), etc.

Dans une organisation complexe, un univers d'audit très détaillé peut facilement comporter des milliers d'éléments relatifs aux SI. Cet univers d'audit sera alors difficile à gérer car sa production, sa mise à jour, et l'évaluation des risques pour tous les éléments nécessiteront des efforts importants. En revanche, si les éléments relatifs aux SI sont trop généraux, ils ne pourront sans doute pas servir de base à l'élaboration du plan d'audit.

Voici quelques principes importants qui devraient être suivis lors du développement des composants SI de l'univers d'audit :

- Veiller à l'exhaustivité en intégrant les éléments pertinents, notamment ceux qui peuvent ne pas être évidents (par exemple les activités externalisées telles que les prestataires de services à l'étranger, des éléments opérationnels très importants sur le plan des SI et les processus métier automatisés).
- Lors du processus de mise à jour, mettre l'accent sur les thèmes nouveaux et émergents. Citons par exemple le *cloud computing*, les médias sociaux ou l'utilisation d'appareils mobiles.
- L'univers d'audit ne devrait pas être tenu secret, mais doit être partagé avec les parties prenantes concernées (par exemple le management des SI et d'autres fonctions) afin de favoriser la communication de données et de suggestions d'amélioration.

Pour de plus amples informations, voir le *GTAG 11 : Élaboration d'un plan d'audit des SI.*

6. Savoir-faire et compétences

Une thématique récurrente dans de nombreuses organisations, concerne l'écart entre d'une part l'utilisation des systèmes informatiques et la dépendance des organisations à leur égard, et d'autre part, les ressources utilisées pour identifier et gérer les risques découlant de ces technologies. Il est donc primordial que la fonction d'audit interne tienne compte des systèmes d'information lorsqu'elle évalue les processus de gouvernance, de management des risques et de contrôle.

Pour gérer ces risques, un RAI doit veiller à ce que son équipe possède les compétences requises. Ceci est préconisé par le *Code de déontologie du Cadre de Référence International des Pratiques Professionnelles de l'audit interne* (CRIPP) de l'IIA, qui exige que les auditeurs internes effectuent uniquement des services pour lesquels ils possèdent les connaissances, les compétences et l'expérience requises, ainsi que par la Norme 1210 : *Les auditeurs internes doivent posséder les connaissances, le savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles.* La fonction d'audit interne devrait posséder ou obtenir, collectivement, les connaissances, le savoir-faire et autres compétences nécessaires. L'IIA propose un référentiel des compétences qui aide à identifier les compétences nécessaires à l'exécution des activités d'audit interne.

Le RAI devrait obtenir l'avis et l'assistance de personnes qualifiées si le service d'audit interne ne possède pas les connaissances, le savoir-faire et les autres compétences nécessaires pour s'acquitter de tout ou partie d'un audit des SI. Les ressources affectées à la réalisation des missions planifiées ont un rôle critique. Par exemple, les compétences requises pour auditer la configuration d'un pare-feu sont très différentes de celles nécessaires pour auditer les tables dans une base de données. Pour une mission donnée requérant telles ou telles compétences, il est donc essentiel de trouver l'auditeur adéquat. Le RAI doit savoir qu'aucun auditeur ne peut effectuer tous les travaux d'audit des SI et que souvent, certaines missions nécessitent plutôt des compétences concernant des applications et d'autres missions nécessiteront des auditeurs plus compétents en matière d'infrastructure.

Par conséquent, un RAI qui a une bonne appréhension de l'univers d'audit, des risques générés par l'utilisation des SI, ainsi que des compétences en audit des SI dont il dispose, devrait être à même de cibler les efforts de recrutement et de formation en conséquence. En l'absence du savoir-faire et des compétences informatiques nécessaires, ou s'il est décidé de ne pas former ou embaucher de collaborateurs possédant ces compétences, le RAI peut faire appel à un prestataire de services externe pour étoffer ou compléter l'équipe d'audit interne (sous-traitance ou *co-sourcing*)[1].

Pour s'acquitter des responsabilités relatives à l'audit des SI, le RAI devrait se poser des questions clés concernant la gestion des compétences et du savoir-faire des auditeurs :

- Toutes les composantes des SI de l'organisation sont-ils inclus dans le processus de planification et tous les domaines à haut risque ont-ils été identifiés ?
- Existe-t-il une vue d'ensemble de l'éventail des compétences nécessaires pour auditer l'usage des SI de l'organisation et les compétences déjà disponibles ?
- Le service d'audit dispose-t-il d'une politique sur la gestion des connaissances manquantes (par exemple recrutement, sous-traitance ou *co-sourcing*) ?
- Les auditeurs des SI possèdent-ils la formation, les certifications et l'expérience requises ? Si ce n'est pas le cas, le service d'audit interne a-t-il mis en place un plan pour pallier ce manque ?
- Le service d'audit interne dispense-t-il la formation adéquate aux auditeurs pour appréhender l'usage du SI, les risques y afférents et les modalités d'audit appropriés ?

[1] *Pour de plus amples détails, voir la MPA 1210.A1-1 : Recours à des prestataires externes.*

7. Réaliser des missions d'audit des SI

Le déroulement de missions d'audit des SI n'est généralement pas différent de celui d'autres missions. L'auditeur planifie, identifie et documente les contrôles pertinents, vérifie l'efficacité de la conception et du fonctionnement de ces contrôles, en tire des conclusions et rédige son rapport. Puisque la plupart des responsables de l'audit interne connaissent bien ce processus général, il n'est pas rappelé ici. Toutefois, le RAI doit connaître et gérer certaines problématiques relatives aux missions d'audit des SI.

1. Collaboration entre auditeurs des SI et autres auditeurs

Lorsqu'il effectue une mission, l'audit interne devrait s'efforcer d'avoir une perspective globale. Certains domaines des SI seront probablement audités exclusivement par des spécialistes des SI (principalement ceux qui sont axés sur l'infrastructure tels que les centres de données, les réseaux, ou les processus des SI comme les services d'assistance) ; en revanche, pour les revues des applications, l'audit de l'ensemble de la chaîne de valeur, incluant les métiers et les SI, apportera le plus grand bénéfice. Ces types de missions devraient se concentrer sur les objectifs opérationnels et tous les risques (dont ceux relatifs aux SI) doivent être évalués selon cette perspective. Cet exercice peut être difficile, mais également très positif car il permet de cerner les liens de dépendance du métier vis-à-vis des SI. Par exemple, si les missions d'audit des SI révèlent qu'il n'existe pas de plan de continuité d'activité, les auditeurs des SI et les auditeurs opérationnels peuvent collaborer pour décrire l'impact de la durée de l'interruption anticipé dans le scénario de crise pour le métier (par exemple, en termes de baisse de la production, retards dans le paiement des salaires, impossibilité de vendre des produits). Peu importe qui est responsable des audits spécifiques, l'attention de l'audit interne devrait être centrée sur la collaboration pour obtenir des résultats optimaux.

2. Cadres de référence et normes

L'une des difficultés que rencontrent les auditeurs lorsqu'ils effectuent un audit des SI est la détermination d'un référentiel. La plupart des organisations n'ont pas élaboré de références de contrôle des SI pour toutes les applications et technologies. L'évolution rapide de la technologie pourrait rendre ces références rapidement obsolètes et donc inutiles.

Un RAI devrait avoir une série d'objectifs de contrôle des SI, et devrait pouvoir trouver un cadre de référence approprié même s'il n'est pas à 100% adapté à son environnement.

3. COSO et COBIT

Où un RAI peut-il trouver une série cohérente d'objectifs de contrôle des SI ? Les cadres de référence *Contrôle interne et management des risques de l'entreprise* du *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) constituent des sources d'information fréquemment consultées, mais ils ne sont pas spécifiquement axés sur les SI. L'environnement de contrôle reposant sur le COSO devrait être complété par des objectifs de contrôle des SI plus détaillés, qui permettront d'évaluer plus efficacement l'environnement de contrôle des SI. Il existe un certain nombre de possibilités à cet égard.

Le CobiT *(Control Objectives for Information and related Technology)*, initialement publié en 1994 par l'ISACA *(Information Systems Audit and Control Association)*, est l'un des référentiels de contrôle et de gouvernance des SI couramment utilisé. La version 5.0 du CobiT a été publiée en 2012. Le CobiT n'a pas pour vocation de concurrencer le COSO ou d'autres référentiels, mais peut être utilisé pour les compléter en les enrichissant avec des objectifs de contrôle des SI plus ciblés.

4. Règles, normes et procédures

Un référentiel comme le CobiT propose une série d'objectifs de contrôle des SI communément admis, qui aide le management à concevoir une politique d'évaluation et de gestion des risques liés aux SI. Le management se sert généralement d'un tel référentiel pour le développement d'un système cohérent de règles, normes et procédures relatives aux SI. L'Annexe A donne une vue d'ensemble des sources pertinentes pour les règles, les normes et les procédures.

8. Rapports

Comme pour tous les autres travaux d'audit interne, les RAI rendent compte régulièrement des résultats des missions d'audit des SI aux principales parties prenantes telles que le Conseil[1], la direction générale, le directeur des systèmes d'information, les régulateurs et les auditeurs externes. Pour des lignes directrices plus détaillées sur la façon de communiquer avec les principales parties prenantes, voir le guide pratique de l'IIA, *Interaction with the board*.

Les destinataires des rapports d'audit peuvent appartenir à des niveaux hiérarchiques plus élevés que ceux qui sont interviewés ou qui exécutent les contrôles. Il est donc nécessaire de communiquer précisément et clairement les informations les plus importantes, de façon à ce que les constats ou les enjeux soient compris et que le management puisse réagir. Il est inutile d'effectuer un audit de qualité si le management ne met pas en œuvre des plans d'action efficaces pour gérer les problématiques et les risques identifiés. Le management ne s'intéresse généralement pas aux détails du processus d'audit. Il souhaite connaître les défaillances, leurs conséquences potentielles et les mesures à prendre pour y remédier.

Lorsqu'il effectue une mission, l'auditeur interne devrait s'efforcer d'avoir une perspective globale. La plupart des organisations étant dépendantes des SI, les rapports sur les risques et les contrôles relatifs aux SI devraient faire partie des activités d'assurance du RAI. Si des processus SI et l'infrastructure SI peuvent (et peut-être devraient pour des raisons d'efficacité) être audités séparément, en règle générale, l'audit de l'ensemble de la chaîne de valeur (dont les métiers et les SI) apportera le plus grand bénéfice. Ces types d'audit peuvent être nettement plus axés sur les risques opérationnels, qui sont plus facilement communiqués au management que les risques relatifs aux SI. Les risques relatifs aux SI débouchent *in fine* sur des risques opérationnels, mais le lien entre les deux n'est pas toujours clair.

Un certain nombre de questions concernant la communication se posent : Convient-il de procéder à un audit des réseaux sans fil, à un audit de l'architecture et de la conception des réseaux ou bien à une revue de la conception d'une application électronique ? Si les missions sont ainsi dissociées, il y a fort à parier que les constats porteront sur des détails pour chaque technologie. Pour certains publics, cette approche pourrait être appropriée, mais le Conseil ou la direction générale pourraient ne pas s'intéresser ou comprendre les détails des questions techniques. Ils veulent généralement que les constats d'audit soient reliés aux problématiques opérationnelles. En conséquence, les travaux d'audit des SI doivent s'intégrer aux travaux des auditeurs de processus / opérationnels / financiers et aux procédures qu'ils mettent en œuvre. Ceci est particulièrement vrai dans les environnements comportant des applications ERP importantes, dont les systèmes comportent un grand nombre de contrôles clés de processus. N'oublions pas que dans certains cas, l'audit de composants centraux de l'infrastructure tels que les centres de données ou les réseaux sans fil sera difficile ; il sera donc pertinent d'auditer individuellement ces domaines. Toutefois, les risques identifiés durant la mission doivent être traduits en langage opérationnel et en risques métier.

Les rapports devraient être rédigés pour des lecteurs avertis, mais qui ne possèdent peut-être pas d'expérience spécifique dans le domaine audité, et le message ne doit être ni délayé ni noyé dans un langage technique. L'objectif du RAI est de présenter un message clair, compréhensible et équilibré.

[1] *Le terme* Conseil *est utilisé au sens donné dans le glossaire des* Normes, *à savoir : « Le niveau le plus élevé des organes de gouvernance, responsable du pilotage, et/ou de la surveillance des activités et de la gestion de l'organisation. Habituellement, le Conseil (par exemple, un conseil d'administration, un conseil de surveillance ou un organe délibérant) comprend des administrateurs indépendants. Si une telle instance n'existe pas, le terme « Conseil », utilisé dans les Normes, peut désigner le dirigeant de l'organisation. Le terme « Conseil » peut renvoyer au comité d'audit auquel l'organe de gouvernance a délégué certaines fonctions. »*

9. Outils d'audit

Les RAI devraient chercher à utiliser des outils et/ou des techniques pour accroître l'efficience et l'efficacité de l'audit. En règle générale, les outils d'audit requièrent un investissement, si bien que le RAI devrait soigneusement évaluer le rapport coût/avantages de toute solution avant de s'y engager. Les outils d'audit peuvent être répartis en deux catégories : les facilitateurs d'audit (qui ne sont pas abordés ici), qui viennent en support du processus global d'audit (par exemple un outil de gestion des documents de travail électroniques), et les outils de tests : outils qui automatisent la réalisation des tests d'audit (comme les outils d'analyse des données et les techniques d'audit assisté par ordinateur).

1. Outils de tests des SI

Les outils de tests permettent d'automatiser des tâches d'audit chronophages, comme l'examen de vastes bases de données. En outre, le recours à un outil pour exécuter des procédures d'audit confère une certaine cohérence. Par exemple, si un outil est utilisé pour évaluer la configuration de la sécurité d'un serveur, tous les serveurs testés au moyen de cet outil seront évalués par rapport aux mêmes critères. Exécuter ces procédures manuellement laisse du champ à une interprétation de la part de l'auditeur. Enfin, l'utilisation de ces outils permet aux auditeurs de tester la totalité d'une base de données, et non un simple échantillon de transactions, d'où un niveau d'assurance bien supérieur.

Les RAI devraient savoir que les mêmes considérations s'appliquent tant à l'acquisition d'outils d'audit des SI qu'au choix de n'importe quel autre outil opérationnel (par exemple fonctionnalité, support).

Outils d'analyse de la sécurité

Un vaste ensemble d'outils permettent d'examiner différentes catégories de dispositifs et/ou d'utilisateurs, et de déceler les expositions à des risques liés à la sécurité. Il existe de nombreux types d'analyse de la sécurité, les principaux étant les outils d'analyse de réseau :

Outils d'analyse de réseau – Ces outils sont des programmes logiciels qui peuvent être lancés sur un réseau pour y recueillir des informations. Classiquement, les pirates informatiques utilisent ce type d'outils au début d'une attaque afin de déterminer la structure du réseau. Les auditeurs des SI peuvent y recourir pour diverses procédures d'audit, notamment :

- La vérification de l'exactitude des diagrammes de réseau par une cartographie du réseau,
- L'identification des dispositifs clés du réseau qui appellent une attention supplémentaire de la part des auditeurs,
- La collecte des informations concernant le trafic autorisé sur un réseau (étayant directement le processus d'évaluation des risques liés aux SI).

Outils d'évaluation de la vulnérabilité

La plupart des technologies, lorsqu'elles ne sont pas personnalisées, souffrent d'un certain nombre de vulnérabilités standard, comme l'existence d'identifiants, de mots de passe ou de paramètres par défaut. Ces outils d'évaluation offrent une solution automatisée pour vérifier ces vulnérabilités.

Ces outils peuvent être utilisés pour les pare-feux, les serveurs, les réseaux et les systèmes d'exploitation. Nombre de ces outils sont « prêts à utiliser » *(« plug and go »)* : l'auditeur les branche sur tout ce qu'il souhaite analyser, et l'outil produit un rapport des vulnérabilités identifiées.

Il est important que l'auditeur exploite ce type d'outils pour plusieurs raisons, notamment parce que ce sont les outils qu'un pirate informatique utiliserait pour monter une attaque contre l'organisation. Néanmoins, il convient de les utiliser avec vigilance car certains de ces outils sont potentiellement dangereux et peuvent compromettre l'intégrité des systèmes qu'ils scannent. L'auditeur devrait examiner avec le responsable de la sécurité l'utilisation qu'il prévoit de faire de ces outils et

coordonner les tests avec le management des SI afin de veiller à ce que le calendrier des tests n'affecte pas la production. Dans certains cas, le responsable de la sécurité ou les administrateurs systèmes emploient déjà régulièrement certains de ces outils dans le cadre des processus de gestion des systèmes. Si tel est le cas, il peut être envisagé d'exploiter ces résultats dans les travaux d'audit des SI, s'ils sont correctement conçus et exécutés.

Outils d'analyse des applicatifs de sécurité

Bon nombre d'applications intégrées comportent des outils d'analyse de la sécurité en fonction de règles préconfigurées. Ces outils peuvent également évaluer la séparation des fonctions au sein d'une application. Le RAI devrait être conscient du fait que la plupart de ces outils sont assortis d'un ensemble de règles préconfigurées ou proposées par le fournisseur comme relevant des « meilleures pratiques ».

10. Conclusion

L'apparition de nouveaux risques liés à la technologie impose de repenser les procédures pour bien gérer ces risques. Il ne fait aucun doute qu'au cours des 15 dernières années, la technologie a modifié la nature de la fonction d'audit interne. Aujourd'hui, les RAI devraient s'interroger sur les risques auxquels est confrontée l'organisation, les types d'audits à effectuer, les modalités de priorisation dans l'univers d'audit et sur la manière de communiquer des constats pertinents au Conseil et à la direction générale.

La stratégie métier guide la définition de l'univers d'audit et l'évaluation des risques. Elle détermine les éléments importants pour le Conseil et le management, et les domaines dans lesquels les activités sont susceptibles de changer. Il est donc important que le RAI comprenne tant la stratégie métier que le rôle des SI dans l'organisation et l'impact qu'ils ont l'un sur l'autre.

Lorsque le RAI cartographie les activités de l'organisation et son infrastructure, il peut observer de façon privilégiée l'impact des différentes relations entre les SI et les métiers. Les projets SI sont souvent des éléments clés du changement, dans les organisations, et le mécanisme utilisé par le management pour mettre en œuvre la stratégie opérationnelle.

Les difficultés auxquelles un RAI est initialement confronté lorsqu'il développe les composantes SI du plan d'audit concernent l'identification des activités SI au sein de l'organisation. Sachant que les environnements des SI sont très diversifiés, un RAI peut chercher à définir les SI en termes de composantes. Chaque composante est différente et importante à la fois. L'utilisation d'une approche fondée sur les risques est un concept général qui s'applique à quasiment toutes les activités d'audit interne. L'univers d'audit devrait tenir compte des SI car il existe des interdépendances importantes entre les SI et les métiers.

Pour gérer ces risques, un RAI doit veiller à ce que son équipe possède les compétences requises. En outre, les RAI devraient chercher à utiliser des outils et/ou des techniques pour accroître l'efficience et l'efficacité de l'audit. Comme pour n'importe quel outil, les outils d'audit requièrent un investissement en temps et en ressources, si bien que le RAI devrait soigneusement évaluer le rapport coût/avantages de toute solution avant de s'y engager.

Enfin, le processus pour réaliser une mission relative aux risques SI n'est généralement pas différent de celui d'autres travaux d'audit : l'auditeur planifie la mission, identifie et documente les contrôles pertinents, vérifie l'efficacité de la conception et du fonctionnement de ces contrôles, en tire des conclusions et rédige son rapport. De même, les RAI rendent compte régulièrement des résultats des travaux d'audit des SI aux principales parties prenantes telles que le Conseil, la direction générale, le directeur des systèmes d'information, les régulateurs et les auditeurs externes.

Annexe A : Normes de référence

Les normes citées ci-après peuvent être prises en considération :

ISO 27001 – ISO 27001/ISO 17799 – L'Organisation internationale de normalisation (ISO) a édité une norme générique sur la sécurité des SI reconnue à l'échelle internationale. Il s'agissait au départ d'une norme britannique (BS 7799), qui a été transformée en norme ISO et qui est désormais connue sous l'appellation ISO 27001. Elle présente les bonnes pratiques communément admises concernant la gestion de la sécurité des SI et constitue un document de référence utile à partir duquel les auditeurs des SI peuvent mener à bien leurs missions.

http://www.iso.org

Capability Maturity Model Integration (CMMI) – Le Software Engineering Institute (SEI) de l'université Carnegie Mellon a élaboré le concept de Capability Maturity Models (CMM, modèles de maturité des capacités) relatifs à différents processus au sein d'une organisation, notamment en ce qui concerne le déploiement de logiciels. L'approche la plus récente est CMMI.

http://www.sei.cmu.edu

United States Computer Security Resource Center – Le United States Computer Security Resource Center est une division du National Institute of Standards and Technology (NIST) qui propose une série complète de publications offrant des informations détaillées sur le contrôle de la sécurité des SI. Parmi ses publications, citons « Guidelines for Securing Wireless Local Area Networks (WLAN) » et « Guidelines on Security and Privacy in Public Cloud Computing. » Ces normes énoncent des bonnes pratiques qui peuvent être utilisées dans tous les secteurs.

http://csrc.nist.gov

SysAdmin, Audit, Network, Security (SANS) Institute – Source d'information parmi les plus fiables pour ce qui est de la formation et de la sensibilisation à la sécurité des SI, le SANS Institute publie de nombreux documents traitant des différents aspects de la sécurité pour diverses technologies. Les publications du SANS exposent un certain nombre de critères incontournables au regard desquels l'auditeur des SI peut effectuer son audit.

http://www.sans.org

IT Infrastructure Library (ITIL) – L'ITIL est l'approche la plus généralement admise de la gestion des services des SI dans le monde. L'ITIL donne un ensemble homogène de meilleures pratiques tirées des secteurs public et privé à l'échelle internationale.

http://www.itil-officialsite.com

Normes propres aux fournisseurs – De nombreux fournisseurs de solutions technologiques publient des recommandations sur la sécurité et le contrôle applicables à la technologie qu'ils produisent. SAP, par exemple, édite un guide sur la sécurité qui énonce des recommandations détaillées pour la sécurité et les contrôles de l'application SAP ERP. Souvent, ces normes fournisseurs ne prennent pas en compte la sécurité et le contrôle au même niveau que, par exemple, une publication NIST, mais elles donnent une bonne base de départ. Les RAI devraient donc vérifier auprès des fournisseurs de systèmes critiques pour les missions si des normes spécifiques sont disponibles. Dans bien des cas, les fournisseurs n'ont rien publié, mais le groupe d'utilisateurs associé à cette technologie a édité une ou des publication(s) (par exemple les différents groupes d'utilisateurs de SAP aux États-Unis).

Annexe B : Modèles d'architecture des SI

Les modèles d'architecture des SI et les références pouvant être pris en compte sont :

The Abu Dhabi IT Architecture & Standards Framework – Basé sur un référentiel comportant huit niveaux, il couvre tous les aspects d'un environnement des SI notamment : Métiers, Accès et présentation, Application, Données, Intégration, Infrastructure, Sécurité et Exploitation.

http://adsic.abudhabi.ae

AndroMDA – Des applications modernes sont construites à l'aide de plusieurs composants connectés les uns aux autres, chacun d'entre eux ayant une fonctionnalité spécifique. Les composants qui effectuent des fonctions similaires sont généralement regroupés en niveaux. Ces niveaux sont organisés en pile dans laquelle les composants d'un niveau utilisent les services de composants d'un niveau inférieur. Un composant dans un niveau donné utilisera généralement la fonctionnalité d'autres composants de son propre niveau ou de niveaux inférieurs.

http://www.andromda.org

TOGAF® – The Open Group Architecture Forum a développé et maintient le TOGAF, une norme reconnue au niveau mondial en matière d'architecture d'entreprise.

http://www.opengroup.org

Auteurs et relecteurs

Auteurs
Stephen Coates, CIA, CGAP, CISA
Max Haege
Rune Johannessen, CIA , CCSA, CRMA , CISA
Jacques Lourens, CIA , CISA, CGEIT , CRISC
Cesar L. Martinez, CIA , CGAP

Relecteurs
Steve Hunt, CIA , CRMA , CISA, CGEIT
Steve Jameson, CIA , CCSA, CFSA, CRMA

Réviseurs
Marie-Elisabeth Albert, CIA
Béatrice Ki-Zerbo, CIA
Gilles Trolez

GTAG®

A PROPOS DE L'INSTITUTE OF INTERNAL AUDITORS

Fondé en 1941, The Institute of Internal Auditors (IIA) est une organisation professionnelle internationale dont le siège mondial se situe à Altamonte Springs, en Floride, aux États-Unis. L'Institute of Internal Auditors est la voix mondiale, une autorité reconnue, un leader incontesté et le principal défenseur de la profession d'auditeur interne. C'est également un acteur de premier plan pour la formation des auditeurs internes. Il est représenté en France par l'IFACI.

A PROPOS DES GUIDES PRATIQUES

Les guides pratiques détaillent la réalisation des activités d'audit interne. Ils contiennent des processus et des procédures, tels que les outils et techniques, les programmes et les approches pas-à-pas, et donnent des exemples de livrables. Les guides pratiques s'inscrivent dans le Cadre de référence international des pratiques professionnelles de l'audit interne de l'Institute of Internal Auditors. Ces guides pratiques relèvent de la catégorie des dispositions fortement recommandées. La conformité à ces guides pratiques n'est donc pas obligatoire, mais fortement recommandée. Ces guides ont été officiellement révisés et approuvés par l'IIA.
Le Global Technologies Audit Guide (GTAG) est un type de guide pratique qui aborde, dans un langage courant, une question d'actualité liée à la gestion, au contrôle ou à la sécurité des technologies de l'information.
Pour de plus amples informations sur les documents de référence proposés par l'Institute, vous pouvez consulter notre site Web, www.theiia.org.guidance ou www.ifaci.com.

AVERTISSEMENT

L'Institute of Internal Auditors publie ce document à titre informatif et pédagogique. Cette ligne directrice n'a pas vocation à apporter de réponses définitives à des cas précis, et doit uniquement servir de guide. L'Institute of Internal Auditors vous recommande de toujours solliciter un expert indépendant pour avoir un avis dans chaque situation. L'Institute dégage sa responsabilité pour les cas où des lecteurs se fieraient exclusivement à ce guide.

COPYRIGHT

Le copyright de ce guide pratique est détenu par l'Institute of Internal Auditors et par l'IFACI pour sa version française. Pour l'autorisation de reproduction, prière de contacter l'Institute of Internal Auditors à l'adresse guidance@theiia.org ou l'IFACI à l'adresse recherche@ifaci.com.

The Institute of Internal Auditors
247 Maitland Avenue, Altamonte Springs
Florida 32701, États-Unis
Téléphone : +1 407 937 1100
Télécopie : 1 407 937 1101
Site Web : www.theiia.org
Courrier électronique : guidance@theiia.org

IFACI
98bis, Boulevard Haussmann
75008 PARIS, France
Téléphone : 01 40 08 48 00
Fax : 01 40 08 48 20
Site Web : www.ifaci.com
Courrier électronique : recherche@ifaci.com

The Institute of Internal Auditors

ifaci
institut français de l'audit et du contrôle internes